Региональная научно-техническая конференция студентов, аспирантов и молодых ученых

СТУДЕНЧЕСКАЯ ВЕСНА – 2016

СБОРНИК НАУЧНЫХ СТАТЕЙ

УДК 061.3(082)
ББК 74.58

70-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2016» : сб. науч. ст., под ред. К. В. Дукельского; сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков – СПб. : СПбГУТ, 2016. – 665 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предназначено студентам, аспирантам и специалистам отрасли связи.

Издание изготовлено оргкомитетом конференции при участии редакции электронного научного журнала «Информационные технологии и телекоммуникации»
www.itt.sut.ru
Подписано в печать 30.06.2016. Вышло в свет 30.06.2016. Формат 60x90 1/8. Уст. печ. л. 41,25. Заказ № 021-ИТТ-2016.
Россия, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Председатель
Машков Г. М. – первый проректор–проректор по учебной работе
Заместитель председателя
Антипин Б. М. – директор НИИ «Технологии связи»
Ответственный секретарь
Елагин В. С. – начальник отдела организации научной работы студентов
Члены организационного комитета
Ивасишин С. И. – начальник учебно-методического управления
Казаков Д. Б. – начальник управления информатизации
Григорян Г. Т. – начальник управления маркетинга и рекламы
Ландер Т. С. – начальник управления информационно-образовательных ресурсов
Аникевич Е. А. – начальник отдела организации научно-исследовательской работы и интеллектуальной собственности
Минаков Л. М. – главный специалист отдела аспирантуры и докторантуры
Мышьянов С. В. – главный специалист отдела организации научной работы студентов

ПРОГРАММНЫЙ КОМИТЕТ

Председатель
Бачевский С. В. – доктор технических наук, профессор, ректор
Заместители председателя
Дукельский К. В. – кандидат технических наук, доцент, проректор по научной работе
Алексенко И. А. – кандидат педагогических наук, проректор по воспитательной работе и связям с общественностью
Ответственный секретарь
Владыко А. Г. – кандидат технических наук, начальник управления организации научной работы и подготовки научных кадров
Члены программного комитета
Воробьев О. В. – кандидат технических наук, профессор, декан факультета радиотехнологий связи
Бузюков Л. Б. – кандидат технических наук, профессор, декан факультета инфокоммуникационных сетей и систем
Коротин В. Е. – кандидат технических наук, доцент, декан факультета информационных систем и технологий
Колгатин С. Н. – доктор технических наук, профессор, декан факультета фундаментальной подготовки
Арзуманян Ю. В. – кандидат технических наук, доцент, декан факультета экономики и управления
Лосев С. А. – кандидат исторических наук, профессор, декан гуманитарного факультета
Лубянников А. А. – кандидат педагогических наук, доцент, директор Института военного образования

Неисключительные права на все материалы, опубликованные в данном издании, принадлежат СПбГУТ. Все материалы, авторские права на которые принадлежат СПбГУТ, могут быть воспроизведены при наличии письменного разрешения от СПбГУТ. Ссылка на первоисточник обязательна. По вопросам приобретения неисключительных прав и использования сборника обращайтесь по тел. (812) 312-83-79, e-mail: telecomsut@gmail.com Тип компьютера, процессор, сопроцессор, частота: Pentium IV и выше / аналогичное; оперативная память (RAM): 256 Мб и выше; необходимо на винчестере: не менее 64 Мб; ОС MacOS, Windows (XP, Vista, 7) / аналогичное; видеосистема встроенная; дополнительное ПО: Adobe Reader версия от 7.X или аналогичное. Защита от незаконного распространения: реализуется встроенными средствами Adobe Acrobat.

Радиотехнологии связи

Алексеев М. А. Программное обеспечение для анализа массива данных, измеренных контрольно-измерительным приёмником системы DRM+ 6

Андропов А. В. Выбор и обоснование схемы устройства для создания антенн с круговой поляризацией 10

Артюшкина Д. П., Макаров В. В. Маркетинговые аспекты выбора и реализации SWAP-проектов 14

Болотов А. О., Холюков Р. Г. Исследование влияния динамических головок на технические характеристики усилителя на лампах и усилителя на ПТ в MICRO-CAP 19

Голиков В. А. Моделирование и реализация на цифровом сигнальном процессоре системы аудиоэффектов для электрогитары 24

Девяткин Д. В., Митлаш А. Н. Разработка приложения на основе среды MATLAB для лабораторных работ по изучению свойств тел неопределенности радиосигналов 29

Дедовец Н. С. Разработка спутниковой антенной системы с автослежением 32

Денисов С. Е., Шишкин А. В. Современные способы записи аудиоинформации 36

Иванов А. Д., Ковалева Т. Ю. Результаты моделирования композитного материала для антенных укрытий 41

Ковалева Т. Ю., Пустарнакова Ю. И. Поглощающие материалы для систем связи 45

Коваленко В. Н. Моделирование Солнечной системы в MATLAB 49

Покровский Н. А. Разработка портативного ротационного вискозиметра 54

Стеценко А. И. Акустическая обработка помещения эфирной студии радиовещания радиостанции «Эхо Москвы» в Санкт-Петербурге 58

Сунгатуллин Э. Н., Устименко В. М. Формирование широкополосных помех 63

Тумашов А. В. Разработка математической модели экранированной рамочной антенны для *N* – количества витков 68

Устинова А. И. Наноматериалы в современной аудиотехнике 72

Инфокоммуникационные сети и системы

Абраменкова Д. Ю. Протокол Интернета Вещей *CoAP* 76

Авраменко М. В. Анализ суточных изменений атмосферных явлений при помощи разработанного M2M решения для экологического мониторинга окружающей среды 80

Акишин В. А. Подходы к внедрению концепции Customer Experience Management 85

Викулов А. С. Современные тенденции в планировании сетей Wi-Fi высокой плотности 89

Виткова Л. А., Дудникова М. Н. Исследование проблем информационной безопасности электронного банкинга для физических лиц 94

Высоцкий С. А., Елагин В. С., Пряжников В. С., Сорокин В. А. Исследование возможности реализации и дальнейшего применения DPI на SDN сетях 100

Гойхман В. Ю., Савельева А. А. Классификация и анализ протоколов Интернета Вещей 104

Голубев В. С. Разработка принципов управления адаптивным программным обеспечением 111

Григорьев И. Д. Классификация сервисов прикладного уровня в системе *CNS/ATM* 116

Гричиненко Н. Ю., Громов В. В. Разработка программного обеспечения для обработки данных с датчиков газа и температуры при помощи микрокомпьютера Raspberry PI 2B 120

Гричиненко Н. Ю. Трансляция видеопотока в режиме реального времени 125

Гричиненко Н. Ю. Разработка по для обработки данных с датчиков на языке SWI-PROLOG 129

Громов В. В. Обзор и анализ компонентов для интернет-магазина на базе CMS Joomla 132

Громов В. В. Разработка программы для микроконтроллера ATmega128 для снятия данных с цифрового компаса по ШИМ сигналу 137

Дремина А. Д. Анализ трафика таргетированной рекламы социальных сетей 142

Елагин В. С., Онуфриенко А. В. Технология глубокой инспекции пакетов в программно-конфигурируемой сети 147

Журкин Д. В., Рябова О. Н., Сахаров Д. В. Открытые данные в современном обществе: анализ моделей развития 152

Захарова П. Ю., Штеренберг С. И. Расследование инцидентов информационной безопасности при помощи DLP-систем 157

Золотарева Е. Н., Золотарева К. Н. Уменьшение информационных рисков организации с помощью механизмов контроля привилегированных пользователей 161

Исаков А. С. Развертывание удостоверяющего центра на ОС Unix (Linux) для обеспечения поддержки PKI 165

Кропивко И. В. Исследование аудиостегосистемы, построенной на основе использования эхо-сигналов с передачей их через акустическую среду с внешними шумами 169

Кудрявцева К. А., Ральникова Н. С. Управление рисками на предприятии, использующем волоконно-оптические линии связи 174

Кудрявцева К. А., Ральникова Н. С. Анализ биометрических систем контроля и управления доступом 178

Кулаков М. С. Разработка протокола маршрутизации самоорганизующейся AD HOC сети для систем АЗН-В 182

Левин М. В., Фостач Е. С. Исследование механизмов обеспечения безопасности управления ИТ-инфраструктурой 187

Марданов Д. М. Реализация раздельного сжатия поля особых точек и остаточного поля на основе представления изображения в виде скалярных полей 192

Масюкайте А. В. Исследование принципов организации виртуальных сетевых функций на базе Openstack Networking 196

Метелев Д. А. Организация динамической загрузки параметров при работе с изображениями в виде скалярных полей 200

Мещеряков Я. Д. Поведенческая модель конечного автомата в Modelsim с дальнейшим программированием устройства в ПЛИС Cyclone V 203

Мишин А. С., Перепелица И. И., Пиховкин Н. Л. Исследование распространенности пиратства в РФ среди молодых людей 207

Мишин А. С. Построение экранирующего маршрутизатора, соответствующего требованиям руководящего документа ФСТЭК России 209

Николаев В. Е. Моделирование двухуровневого мультиплексора под программирование в ПЛИС 214

Пиховкин Н. Л., Сахаров Д. В. Обеспечение безопасности распределенной информационно-вычислительной сети с учетом управления рисками 218

Плетнева Н. С. Анализ особенностей жизненного цикла ЗИП в системах класса RMS 222

Поздняков В. А. Разработка системы взаимодействия показателей качества услуг и показателей эффективности сетей электросвязи 227

Помогалова А. В. Разработка мобильного приложения для операционной системы ANDROID 231

Попова С. С. Методика расчета длины регенерационного участка ВОЛС с компенсаторами дисперсии 234

Похлупнёв Д. И., Халилов М. Н. Синтез умножителя на базе ПЛИС Cyclone V Altera 240

Самсонов Э. О. Разработка учебно-лабораторного модуля для исследования спектров полупроводниковых источников излучения 245

Смаль С. Д. Анализ и обнаружение уязвимости выполнения произвольного кода Shellshock 250

Фадеев А. Н. Организация ретрансляции данных в ОВЧ ЛПД режима 4 255

Фицов В. В. Поведение имитационной модели системы DPI при различных законах распределения входного потока заявок 260

Шариков П. И. Методика эффективной защиты байт-кода java-приложения 266

Информационные системы и технологии

Аверкова А. С. Моделирование температурного поля платы компьютера с тремя микросхемами 271

Аль-Мехди С. Т. Сравнительный анализ методов идентификации шаблона на изображении 276

Берин Д. А., Белоус К. В., Давыдова Е. В. Автоматизированная система управления контролем доступа на базе Arduino 279

Березин В. В., Менисов А. Б. Система автоматизированной идентификации информационных действий на Yandex Market, влияющих на рейтинг товара 284

Бовыкин Е. А., Фёдоров Н. С. Оптимизация перемещения лазерной головки с использованием генетических алгоритмов 287

Быжко И. М., Менисов А. Б. Выявления взаимосвязей источников пропаганды ИГИЛ (запрещенной в РФ) 291

Вахрушев Д. О. Исследование средств информационной удаленной поддержки ресурсов инфраструктуры компании 294

Гаврилова А. В. Выбор телеметрируемых параметров с учетом их ценности для распознавания технического состояния космических средств 298

Давыдова Д. С. Оперативный алгоритм спектрально-корреляционной обработки телеметрической информации ракет космического назначения 303

Долгун В. О. Разработка информационной управляющей системы типа «Умный дом» 308

Дудаков Л. С., Тарлыков А. В. Решение задачи визуализации процедурно генерируемого ландшафта при помощи алгоритма на основе структуры «дерево квадрантов» 311

Заварина О. А. Разработка автоматизированной системы создания и обработки данных учебно-методического комплекса 316

Звонарев В. В., Парамонов И. Ю., Петрова И. С. Проблемные вопросы информационного обеспечения систем противодействия беспилотным воздушным судам 320

Иофик А. Л. Разработка мультимедийного агрегатора научно-технической информации 325

Казачкова В. С., Котлова М. В. Электронный каталог как единый информационный портал музейного фонда Российской Федерации 331

Казначеева Е. С. Разработка информационной модели навигации в пространстве зданий со сложной архитектурой 336

Кондратьев Д. А., Эльсабаяр Шевченко Н. Интеллектуальные профили сервис-ориентированных архитектур 340

Лазев С. В. Разработка программного обеспечения удаленного тестирования для автошкол **344**

Лебедева А. А., Хроменков С. В. Планирование действий интеллектуальных информационных агентов с гарантиями качества их функционирования **349**

Майоров А. А., Тутов А. В., Тутова Н. В. Динамическое размещение виртуальных машин в облачных центрах обработки данных **354**

Медведев И. В. Интеллектуализация геоинформационных систем транспортировки грузов повышенного контроля **358**

Менисов А. Б. Система сбора графических данных социальных сетей **363**

Михайлова Е. А. Построение учебно-тренировочных комплексов с использованием штатного программного обеспечения обработки телеметрической информации **365**

Прохоров Д. О., Трофлянина Н. В., Фомин С. А. Разработка программного анализатора сетевого трафика на основе количественных характеристик потока транспортного уровня **371**

Романова Ю. Н., Янюшкин К. А. Особенности выбора Content Management System **377**

Рудик С. О. Автоматизация производственной деятельности предприятия связи с использованием технологии CSRP **381**

Савлиш В., Смирнова П. В. Интеграция сервис-ориентированных средств для систем ситуационного управления **385**

Семенов А. В., Киреева Н. В. Выбор системы защиты информации на основе анализа имеющихся информационных систем персональных данных **388**

Фатхулин Т. Д. Технологические решения по увеличению пропускной способности оптических волокон **392**

Фролов К. А. Разработка программно-аппаратного модуля автоматизированного учета посещения занятий студентами в течение семестра **397**

Хайбрахманова Е. С. Разработка Web-приложения «Телефонный справочник СПбГУТ» **401**

Шукюрова Л. П. Внедрение цифрового водяного знака в частотную область изображения методом Бенгама-Мемона-Эо-Юнг **405**

Теоретические основы радиоэлектроники

Абраменкова Д. Ю., Шербашов Е. А. Годографы глубины обратной связи Online **410**

Ахметов Р. Р. Спиральные планарные излучатели **415**

Ганбаев А. А. Анализ методов модуляции ВЧ колебаний в ключевых генераторах **419**

Домрачев Н. В., Сазоненко Н. Ю., Сединин А. Д., Тхоржевский И. Л. Анализ результатов расчёта дисперсионного давления в слоистых структурах на основе кремния **424**

Прялухин Д. С. Применение ключевого режима E_m в СВЧ усилителях мощности **430**

Сазоненко Н. Ю., Сединин А. Д., Тхоржевский И. Л. Френелевская дифракция на круглом отверстии. Лабораторная работа нового типа **433**

Хачин Р. С. Реализация заданий самостоятельной работы по физике с помощью математического редактора Mathcad **438**

Черненко В. В. Работа ключевого генератора режима E на нелинейную нагрузку **442**

Экономика и управление в связи

Авраменко М. В., Диптан В. А. Исследование спроса на M2M решение для экологического мониторинга окружающей среды **447**

Баулина А. П., Шарафитдинова Ю. Р. Универсальный мессенджер **452**

Белянчикова М. П. Моделирование финансовой устойчивости компаний подвижной связи **456**

Гудков Д. А., Дмитриев С. Е., Юхневич В. С. Анализ использования многофакторной аутентификации пользователями сети Internet **459**

Остроущенко Н. А., Рогалев М. В., Тураев С. Э. Исследование подхода к использованию паролей у молодежи **464**

Плетнева Н. С. Разработка мобильного приложения «Bonch.Личный кабинет» **468**

Проничев И. Н. Актуальность внедрения системы ГЛОНАСС на предприятии **471**

Хамхоева Х. М. Использование математического аппарата при формировании портфеля ценных бумаг **477**

Шишмарева О. С. К вопросу построения модели организации рекламной деятельности **480**

Югова У. В. Возможности совершенствования системы мотивации труда **484**

Гуманитарные проблемы информационного пространства

Баранова Т. А., Жаранова А. О., Капитоненко В. В. Метафизика нравственности троллинга и автономная воля **490**

Басова Т. Д. Миф как средство формирования новых смыслов в рекламе **495**

Бычкова А. А. Виртуальное пространство как новый канал продвижения **497**

Голубкова М. Д. Специальные мероприятия как инструмент для продвижения автоспортивных компаний **501**

Дорохова Е. А. Способы продвижения компьютерных игр в интернете 505

Елисеев С. М., Кобзев К. О. Ленд-лиз в годы Великой Отечественной Войны 509

Ильменев А. А. Возможности продвижения бизнеса средствами PR 515

Королёв С. А., Котлова М. В. Опыт разработки информационной системы для учреждений здравоохранения 518

Халилов М. Н. Советско-китайский пограничный конфликт 1969 г. из-за о. Даманский: предпосылки и урегулирование 522

Яскина А. Е. Незаконная реклама в интернете и способы её контроля 528

Сети связи специального назначения

Адамович Г. В., Гречихин Л. А., Мелихов Е. М., Чагин П. А. Совершенствование лабораторной установки «Моделирование инфокоммуникационных технологий» для обучения студентов института военного образования 532

Александрова А. В., Марунич С. А., Пономарев Д. М. Защита информации от несанкционированных действий пользователей в сетях связи специального назначения 537

Безбородова А. С., Стахеев К. И. Варианты применение атмосферно-оптических линий связи на объектах специального назначения 541

Березин А. Ю. Подготовка к ведению войн в киберпространстве 545

Березянская В. М., Мартынов А. А., Савинский С. И. История развития отечественной спутниковой связи 549

Бодров И. В., Гаврилов Ю. Г., Чубарев К. С. Эффективность функционирования систем управления связью 554

Воробьев Ю. Г., Гаврилов Ю. Г., Падишин С. А. Методика оценки систем мониторинга системы и сетей связи специального назначения 557

Голованов К. С., Миловидов А. А., Широков С. О. Особенности работы и способы повышения эффективности подземных антенн 562

Гулидов А. А. Предложения по оценке эффективности радиоподавления каналов спутниковой связи 567

Дворников С. С. Предложения по формированию сигналов методом последовательной конкатенации вейвлет-функций 572

Дворников С. С. Вейвлет-сигналы для систем радиосвязи 577

Долгомер А. А. Организация связи при выполнении боевых задач советских разведчиков в тылу противника в годы Великой Отечественной войны 591

Звонарев В. В., Парамонов И. Ю., Петрова И. С., Попов А. С. Алгоритм управления режимами работы беспилотного летательного аппарата в системе передачи информации 599

Иванов Г. Н. Развитие беспроводной связи 604

Иванов Р. В. Предложения по оценке защищенности радиоканалов от структурных помех 608

Корчагин М. С., Фролова Ю. А. Моделирование процессов реализации внедрения ложного DNS-сервера 612

Кривошей О. И., Кривцов С. П., Микина Н. С., Чеботарёв В. И. Построение имитационной модели линий дистанционного управления передатчиками радиоцентра стационарного узла связи с помощью симулятора локальной сети 617

Кузнецов Д. А., Митрошина П. О., Сёмин А. А. Особенности построения радиоканала с беспилотным летательным аппаратом 622

Кузнецов Д. А., Широков А. О., Широков С. О. Анализ помехозащищенности радиоканала 629

Кылосов Д. В. История развития института военной кафедры в России 634

Лимарева Е. Д. Российские изобретатели телеграфа П. Л. Шиллинг и Б. С. Якоби 639

Матвиенко Н. А. Военный интернет в армиях России и США 644

Першин И. С. Особенности использования космических аппаратов в построении системах связи 648

Суранова М. А. Способы построения приемного устройства, как метод защиты от преднамеренных помех противника 651

Чубарев К. С., Щербаченко В. Н. Повышение мобильности полевых подвижных узлов связи 657

Ялунина Т. Р. Компьютерное моделирование нелинейных эффектов в оптических волокнах 661

РАДИОТЕХНОЛОГИИ СВЯЗИ

УДК 654.195

М. А. Алексеев (студент группы РА-21, СПбГУТ)

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АНАЛИЗА МАССИВА ДАННЫХ, ИЗМЕРЕННЫХ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫМ ПРИЁМНИКОМ СИСТЕМЫ DRM+

DRM (Digital Radio Mondiale) – это система цифрового радиовещания. В 2009 году произошло дополнение стандарта системы (появилась возможность вещания в ОВЧ диапазоне). В связи с этим важно иметь набор инструментов для анализа и обработки данных, полученных при тестировании новой, усовершенствованной системы.

DRM, MATLAB, графический интерфейс пользователя, RSCI, цифровое радиовещание.

Первые варианты стандарта DRM работали на частотах до 30 МГц, сейчас же область частот расширилась и включает полосу частот от 174 до 230 МГц. Это расширение и обозначается как DRM+. Таким образом, появление нового стандарта, предусматривающего вещание в формате DRM+, делает необходимым анализ ситуации с вещанием в ОВЧ диапазоне, частотный ресурс которого вместе с возможностями цифровых технологий открывают новые перспективы по развитию высококачественного радиовещания в стране [1].

Контрольно-измерительный приёмник системы цифрового радиовещания DRM+ используется для измерений параметров приемопередающего оборудования, как системы в целом, так и отдельных ее трактов. Он записывает измеренные данные в один файл по протоколу RSCI в шестнадцатеричном коде, что не совсем удобно для обработки и последующего анализа полученных результатов измерений (рис. 1).

Поэтому было бы достаточно актуально создание программы, которая:

- выделяет из общего массива измеренных данных нужные параметры и отображает их в виде графиков и текста;

- производит запись каждого из измеренных параметров данных в отдельные файлы в десятичном виде для дальнейшего анализа;
- удобна в использовании за счёт наличия графического интерфейса пользователя.

```
20 64 72 6d  2b 72 73 65  72 00 00 00  00 72 67 70   drm+rser....rgp
73 00 00 00  d0 01 09 00  3b 2f ff ff  00 1e 15 00   s...Р...;/яя....
00 00 0e 00  12 39 07 07  df 08 0d 01  2f 01 12 72   .....9..Я.../..r
6d 65 72 00  00 00 00 72  77 6d 66 00  00 00 10 06   mer....rwmf.....
df 72 77 6d  6d 00 00 00  00 72 64 62  76 00 00 00   Яrwmm....rdbv...
10 04 15 72  66 72 65 00  00 00 20 04  05 5b 9f 64   ...rfre... ..[цd
6c 66 63 00  00 00 20 00  00 00 0e 72  70 73 64 00   lfc... ....rpsd.
```

Рис. 1. Фрагмент файла, записанного приёмником по протоколу RSCI

Несмотря на то, что для реализации подобного рода задач, как правило задействуется IDE Qt Qreator и язык программирования C++, программу было решено создавать с использованием пакета прикладных программ MATLAB и его специализированной среды GUIDE.

Задача создания программы сводится к обработке протокола *RSCI* (так же некоторая информация выделяется из системных каналов FAC и SDC системы DRM). Каждый из измеренных приёмником параметров записывается в свой TAG элемент (рис. 2) [2]. Для каждого TAG элемента, представленного в таблице 1, в MATLAB был написан свой *m*-файл.

Рис. 2. Структура TAG элемента отношение сигнал/шум протокола RSCI

ТАБЛИЦА 1. Список обрабатываемых программой параметров

TAG *name*	**Параметр**
**ptr*	Тип протокола и версия
rinf	Тип приёмника
rfre	Оценка частоты приёма
rsnr	Отношение сигнал/шум
rdbv	Напряжение на входе приёмника
rmer	Коэффициент ошибок модуляции
rpro	Профиль приёмника

TAG *name*	Параметр
rgps	Время и дата
	Скорость движения приёмника
	Траектория движения приёмника
	GPS координаты
rsta	Статус синхронизации приёма
	Статус декодирования аудио
	Статус декодирования цифровых данных канала FAC
	Статус декодирования цифровых данных канала FAC
*fac_*	Режим модуляции несущих частот в канале SDC
	Скорость кодирования в канале SDC
	Режим модуляции несущих частот в канале MSC
*sdc_*	Режим аудио
	Статус использования SBR

Завершающим этапом создания программы является объединение всех созданных скриптов для обработки данных в одну программу с графическим интерфейсом. Внешний вид интерфейса изображён на рисунке 3.

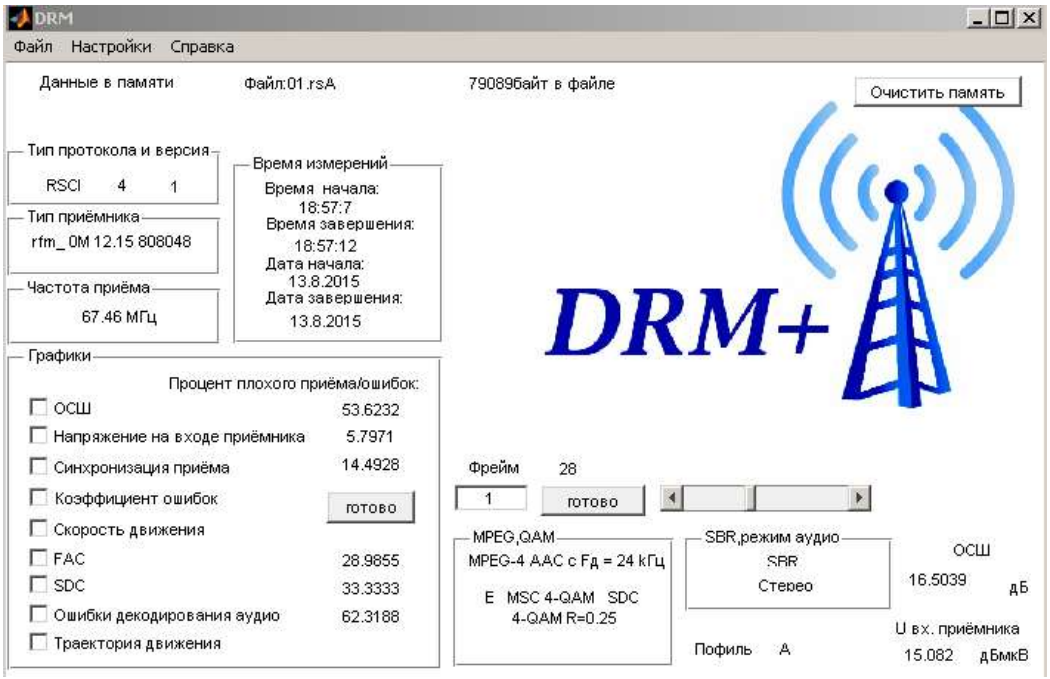


Рис. 3. Интерфейс главного рабочего окна программы

В конце июля 2015 г. в Санкт-Петербурге на частоте 67,46 МГц началось экспериментальное вещание «Радио Маяк» в цифровом формате DRM+ [3]. С помощью обработанных программой данных удалось произвести оценку зон уверенного приёма, совместив траекторию движения

приёмника с картой местности и отметив отношение сигнал/шум в каждой точке приёма (рис. 4).

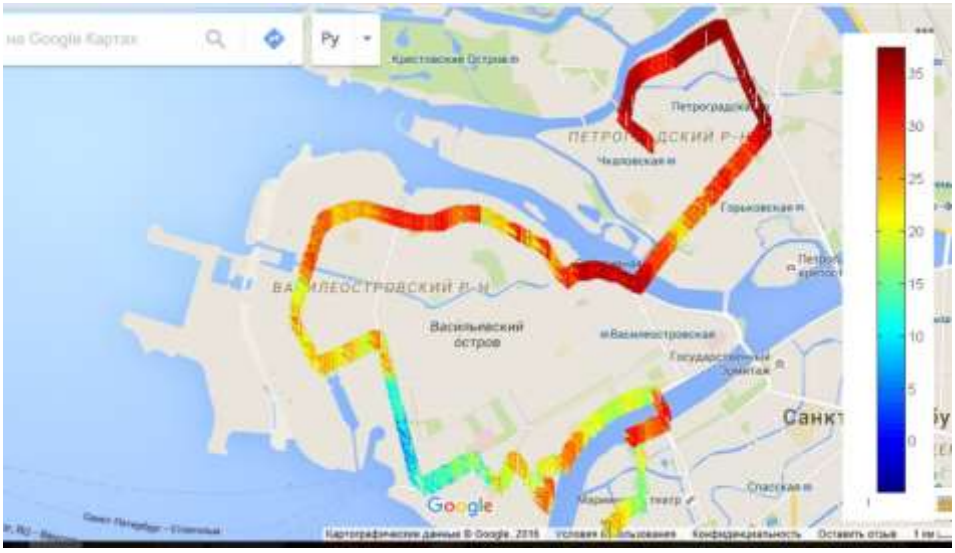


Рис. 4. Оценка зон уверенного приёма. Цветом отображается ОСШ

В дальнейшем можно произвести:

- работу по оптимизации кода, так как на данном этапе программа требует достаточно много оперативной памяти;
- тестирование программы на наличие неучтённых комбинаций действий пользователя, приводящих к её некорректной работе.

После выполнения этих доработок программу можно считать полностью готовой к практическому использованию.

Список используемых источников

1. Рихтер С. Г., Смирнов Д. С. О преимуществах радиовещания в формате DRM+ [Электронный ресурс] // INTERMATIC – 2010 // Материалы VII Международной науч.-техн. конф. «Фундаментальные проблемы радиоэлектронного приборостроения», 23–27 нояб. 2010 г., Москва / под ред. чл.-корр. РАН А. С. Сигова. – М. : Энергоатомиздат, 2010, часть 3. С. 222–225. URL: http://www.conf.mirea.ru/CD2010/ pdf/p3/54.pdf

2. European Telecommunication Standard ETSI TS 102 349 V4.2.1 (2016-03). Technical Specification. Digital Radio Mondiale (DRM) Receiver Status and Control Interface (RSCI); System Specification.

3. Новости и события СПбГУТ 13 августа 2015 года. Экспериментальное вещание в цифровом формате [Электронный ресурс]. URL: http://www.sut.ru/news/public/ns/main/id/2036

Статья представлена научным руководителем,
доктором технических наук, профессором Ковалгиным Ю. А.

УДК 621.372.62

А. В. Андропов (студент группы РК-51М, СПбГУТ)

ВЫБОР И ОБОСНОВАНИЕ СХЕМЫ УСТРОЙСТВА ДЛЯ СОЗДАНИЯ АНТЕНН С КРУГОВОЙ ПОЛЯРИЗАЦИЕЙ

Антенны с круговой поляризацией обладают серьезными преимуществами перед линейно поляризованными в целом ряде случаев. Целесообразность применения эллиптически и кругополяризованных антенн в каждом из частотных диапазонов имеет индивидуальные причины. Однако схемные решения и требования к фазосдвигающим цепям имеют много общего. Статья посвящена выбору схем антенных устройств и фазосдвигающих цепей для диапазонов ОВЧ и УВЧ.

фазовращатель, антенна, эллиптичность, АЧХ, фазовый контур.

Диапазоны ОВЧ и УВЧ загружены различными средствами мобильной радиосвязи, работающие в выделенных участках. При распространении радиоволн метрового и дециметрового диапазонов, поле в точке приема имеет многолучевую структуру в результате приема прямой волны от передатчика и N отраженных волн, приходящих от переизлучателей произвольно расположенных вокруг трассы движения объекта. Каждая отраженная волна, в общем случае, в точке приема имеет эллиптическую поляризацию [1]. Любую волну с эллиптической поляризацией можно представить в виде двух волн с круговой поляризацией взаимно противоположного вращения. Применяя это правило ко всем отраженным волнам, необходимо сделать следующие выводы об эффективности использования приемных антенн круговой поляризации.

Дисперсия поля отраженных волн, принимаемых антенной круговой поляризации, значительно меньше дисперсии суммарного поля волн, принимаемых антенной линейной поляризации. Это объясняется особенностями механизма переотражения волн и свойством антенн круговой поляризации осуществлять волновую поляризационную селекцию. Если приемная антенна, согласованная с прямой волной от передатчика, имеет, к примеру, левостороннюю круговую поляризацию, то деполяризованные компоненты отраженных волн не наведут в ней ЭДС, следовательно, мощность многолучевой помехи на входе приемника уменьшится [1].

С точки зрения рядового потребителя (владельца абонентской станции системы мобильной связи) это не имеет существенного значении в силу больших трудностей создания на абонентской станции антенны с круговой поляризацией. А вот для привилегированных абонентов и станций радиоконтроля эти наблюдения позволяют сделать однозначный вывод. При приеме (обнаружении) абонентов подвижной связи применение ан-

тенн круговой поляризации позволит увеличить дальность и надежность связи (обнаружения).

Для реализации приема кругополяризованных волн в диапазонах ВЧ, ОВЧ, УВЧ и начальной части диапазона СВЧ наиболее широкое распространение получил турникетный вибратор. Эта антенна состоит из двух вибраторов одинаковой длины, расположенных в пространственной и временной квадратурах и питаемых равноамплитудно со сдвигом фаз 90°. Элементом, обеспечивающий сдвиг фазы, является фазовращатель.

В качестве общего названия этим схемам подходит квадратурный делитель мощности на два со сдвигом фаз на выходах 90°, который представляет собой пассивный шестиполюсник, с парой входных и двумя парами выходных зажимов [2]. Такая цепь является разностной, так как в предполагаемой полосе частот поддерживаются определенные амплитудные и фазовые соотношения. В процессе исследования возможных вариантов создания и подготовки опытных образцов, были выявлены требования к электрическим характеристикам (таблица 1), и конструктивному исполнению этих устройств. В значительной степени требования формировались, ориентируясь на запросы служб контроля за использованием радиочастотного спектра.

ТАБЛИЦА 1. Требования к электрическим характеристикам

Рабочий диапазон частот	30–1000 МГц
Сдвиг фаз на выходах	90°±15°
Максимальные амплитудные потери на канал	3,5–4,5 дБ
Разность амплитуд между каналами	< 1 дБ

Требования к элементам конструкции:

1) Ферритовые изделия фазовращателей должны быть рассчитаны на мощность, исключающую возникновение искажений из-за наводок полями близлежащих источников излучения (общие требования по ЭМС к станциям радиоконтроля).

2) Рекомендуется использование SMD ЭРЭ, используемых для поверхностного монтажа, подходящих для массового производства.

3) По возможности, отсутствие элементов, требующих настройки и изготовления моточных изделий, негативно влияющих на коэффициент повторяемости.

4) Применение схемных решений, позволяющих вести монтаж на печатных платах, переходя к несимметричным полосковым линиям, с минимумом элементов симметрирования.

5) Схемное исполнение должно позволять использование инжектированного питания, не влияющего на частотные характеристики фазовращателей.

6) Конструкция должна удовлетворять требованиям к изделиям, используемым на соответствующей транспортной базе.

Разработанная конструкция устройства для ОВЧ УВЧ диапазонов.

На рисунке 1 представлена электрическая принципиальная схема реализованного фазовращателя. Схема состоит из устройства объединения ветвей, исполненного микросборкой ADP-2-10+ и двух ветвей, каждая из которых представляет собой фазовые контура первого порядка. Расчет фазоразностной цепи производился по методике [2], где рассчитывались элементы канонических фазовых контуров.

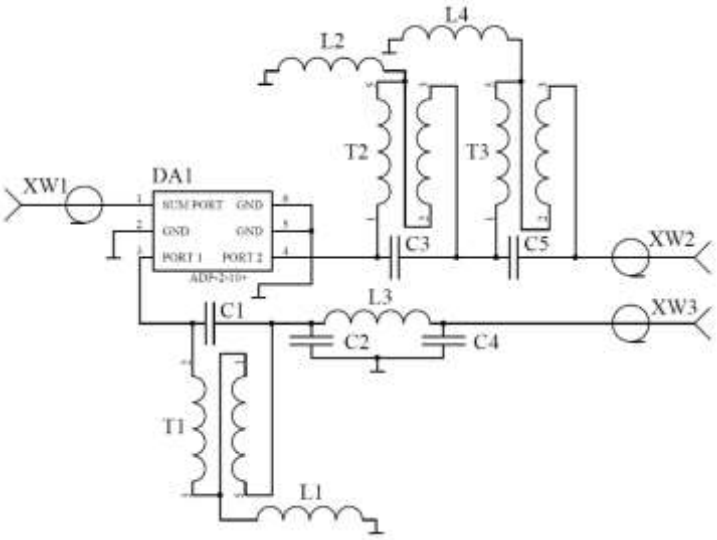


Рис. 1. Схема электрическая принципиальная реализованного фазовращателя

В качестве фазовых контуров было принято использовать неуравновешенные структуры, эквивалентные мостовым, и линии задержки на звеньях типа *К*, изображенных на рисунках 2 и 3 соответственно. Далее, в Microwave Studio производилась оптимизация схемы для достижения наилучшей АЧХ и фазоразностной характеристики.

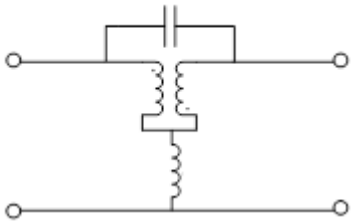


Рис. 2. Фазовый контур, эквивалентный мостовому

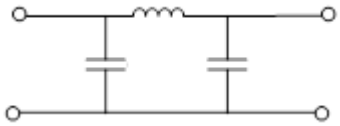


Рис. 3. Линия задержки на звеньях типа *К*

На рисунке 4 представлена АЧХ и ФЧХ устройства, выполненного после оптимизации в Microwave Studio. Необходимо отметить, что удалось

реализовать устройство с минимальными потерями по каналам в широкой полосе частот и необходимым сдвигом фазы, удовлетворяющим выдвигаемым требованиям, что влияет на качество устройства и позволяет экстраполировать расчеты фазовращателей в других диапазонах частот.

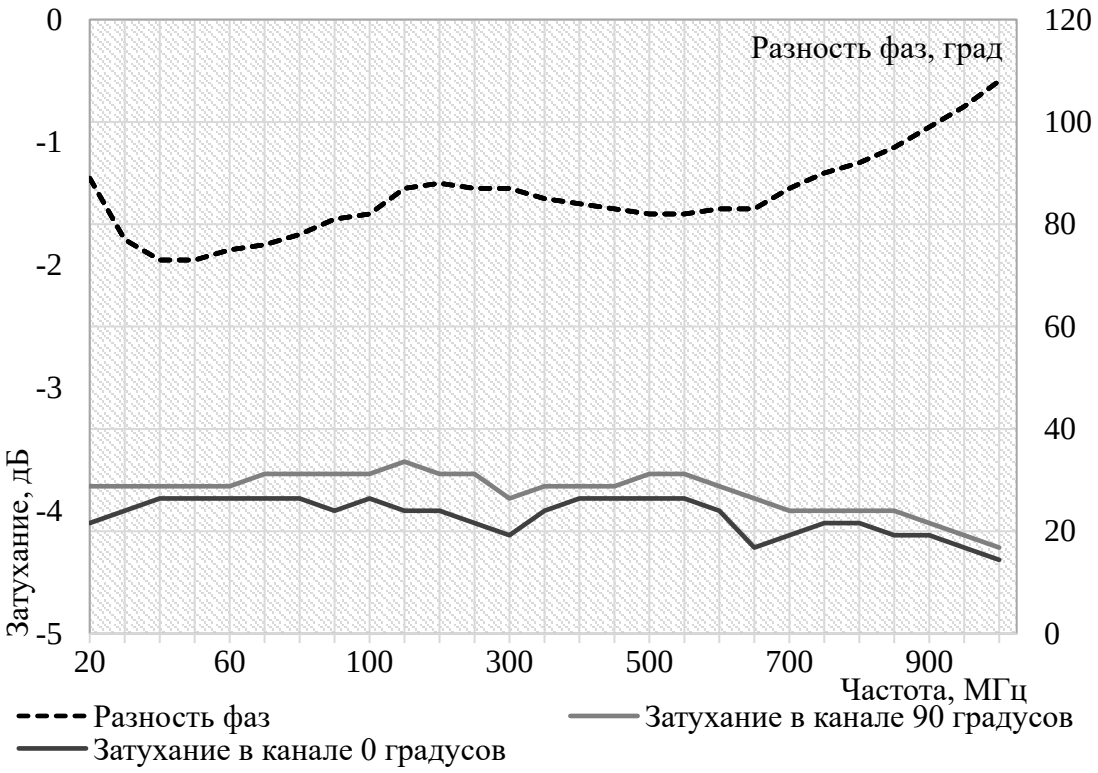


Рис. 4. АЧХ и ФЧХ

Для оценки опытного образца согласно [3] по формуле (1), рассчитан коэффициент R эллиптичности турникетной антенны в предположении, что вибраторы одинаковы.

$$R = \sqrt{\frac{m^2\cos^2\theta - m\sin 2\theta\cos\tau + \sin^2\theta}{m^2\sin^2\theta + m\sin 2\theta\cos\tau + \cos^2\theta}}, \qquad (1)$$

где m – отношение амплитуд по каналам, τ – разность фаз, θ – угол наклона большей оси эллипса.

Результаты расчета приведены на рисунке 5. Значения коэффициента эллиптичности не ниже 0,74 (при общепринятой норме 0,707) во всем диапазоне частот, что позволяет сделать вывод о высоком качестве разработанного устройства.

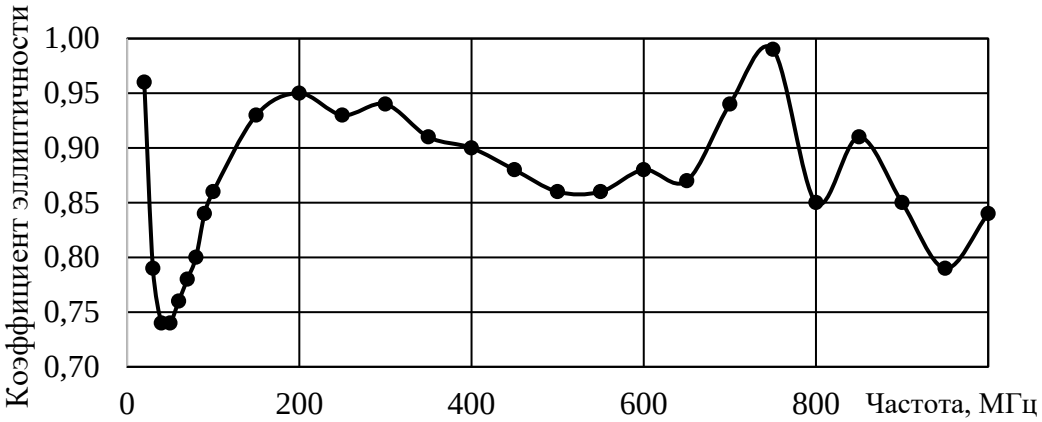


Рис. 5. Результаты расчета коэффициента эллиптичности турникетной антенны

Список используемых источников

1. Головин Э. С. Об эффективности антенн круговой поляризации в системах радиосвязи с подвижными объектами // Радиотехника. 1979. № 7. С. 72–75.
2. Авраменко В. Л., Галямичев Ю. П., Ланне А. А. Электрические линии задержки и фазовращатели. М. : Связь, 1973. 110 с.
3. Юрцев О. А., Рунов А. В., Казарин А. Н. Спиральные антенны. М. : Советское радио, 1974. 224 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Кириком Д. И.

УДК 339.138

Д. П. Артюшкина (студентка группы РМ-21, СПбГУТ)
В. В. Макаров (доктор экономических наук, профессор, СПбГУТ)

МАРКЕТИНГОВЫЕ АСПЕКТЫ ВЫБОРА И РЕАЛИЗАЦИИ SWAP-ПРОЕКТОВ

Жизненный цикл современных инфокоммуникационных технологий составляет примерно пять-десять лет, что делает актуальным рассмотрение проблем, связанных с выбором производителя оборудования для сети сотовой связи. Операторам необходимо найти компромиссный вариант в соотношении цены и качества, увеличив объем и количество реализуемых услуг. Реализация SWAP-проектов является неотъемлемой частью модернизации сотовой сети связи в современном мире. В статье рассмотрены маркетинговые и организационные аспекты SWAP-проектов.

вендоры, операторы, моно- и мультивендорные сети, SWAP.

Сегмент предоставления услуг сотовой связи является наиболее быстро развивающейся частью телекоммуникационного рынка, в силу высокой востребованности услуг сотовой связи в современном мире. Построение сети сотовой связи требует высокого объема инвестиций, и длительных сроков строительства. Модернизация технологий и разработка новых стандартов сотовой связи происходит регулярно, и это вынуждает операторов периодически обновлять оборудование сети [1]. Процесс замены компонентов сети на более современные, и переход к новым стандартам с использованием оборудования одного вендора носит название «SWAP». При проведении капитальных изменений в оборудовании инфраструктуры сети требуется последовательное переключение и отключение базовых станций без утраты соединения и передачи данных. Такие проекты преследуют разные цели, но основной является поддержка рентабельности сотовой сети оператора.

SWAP-проект позволяет перейти на оборудование одного вендора, что является экономически более выгодным, с точки зрения сокращения операционных затрат. Основными маркетинговыми аспектами SWAP-проектов вендоров являются разработка индивидуальных пакетов для оператора, включающих в себя набор оборудования для всей сети, и услуг, по интересной для операторов цене. При этом, вендор выделяет конкурентные преимущества своего оборудования, которые позволят оператору быть более конкурентоспособным.

Выгода от реализации SWAP-проектов для вендора заключается в реализации больших объемов продукции. Проанализируем выгоду и проблемы операторов сотовой связи при реализации SWAP-проектов.

Для операторов сотовой связи использование продукции одного производителя имеет ряд преимуществ. Требуются небольшие затраты на обучение персонала, меньшие трудозатраты, легче и удобнее планировать обновление линеек оборудования. Упрощается интеграция различных компонентов в единую и бесперебойно работающую сотовую сеть за счет уменьшения числа согласующих элементов. Не возникает проблем и с технической поддержкой, так как она является общей для всей инфраструктуры сотовой сети, и за все продукты ответственность возлагается на единого представителя. Наконец, серьезным преимуществом в пользу выбора моновендорной сети можно назвать гибкую ценовую политику. Велика вероятность предоставления поставщиком хорошей скидки, при приобретении целого стека решений, а не какого-то одного.

Ведущими вендорами продвигается идея унификации сети в качестве способа повышения надежности, упрощения эксплуатации, и снижения общей стоимости поддержания сотовой структуры. Предложение пакетных решений, индивидуальных для каждого случая, несомненно, выгодно не только заказчику, но и самим поставщикам, так как позволяет предоставить оператору решения на стыке технологий, которые имеют заведомо

понятные варианты для различных ситуаций. Тщательное тестирование новых технологий минимизирует вероятность возникновения проблем с функциональной совместимостью, помогает выработать заранее продуманный порядок выявления неисправностей и устранения проблем. Использование продукции одного вендора дает возможность добиться гармоничного взаимодействия компонентов инфраструктуры, повысить её эффективность, путем сокращения энергопотребления и эксплуатационных расходов, при этом упростить антенно-фидерную часть и повысить надёжность, что актуально для крупномасштабных интеграционных проектов, где особое внимание уделяется производительности и отказоустойчивости. Вендоры готовы оказать помощь при внедрении их оборудования, предполагая дальнейшее сотрудничество, а, следовательно, взять на себя всю ответственность за его эксплуатацию, что выгодно обеим сторонам.

С этой точки зрения, поставщики стремятся сделать операторов зависимыми от предоставляемых ими товаров, что гарантирует им будущее развитие, поддержание бюджета компании и обеспечение прибыли. Вендор монобрендовой сети развивает программу лояльности для привлечения заказчиков. Каждый поставщик располагает базой клиентов, с которыми может сотрудничать, предоставляя скидки и бонусы, анализируя статистику работы и делая прогнозы на будущее.

При выборе определённого вендора, в случае крупномасштабной монобрендовой сети, заказчик предъявляют к нему высокие требования. Оператора в данном случае будут волновать вопросы, касающиеся стабильности развития потенциального партнера-поставщика, его доли рынка и величины компании, опыта в разработке заказных решений, их полнота и компетентность, спектр продукции вендора и прочее [2]. Безусловно, выбор вендора происходит из нескольких альтернативных вариантов, что обуславливает конкуренцию между ними. Анализ рынка поставщиков позволяет получить функциональное сетевое решение за разумную цену и снизить совокупную стоимость владения.

Примером масштабного SWAP-проекта, который привел к переходу на монобрендовую сеть, может служить недавно закончившаяся модернизация сотовой сети в нескольких регионах Северо-Западного филиала крупнейшим телекоммуникационным оператором «Мегафон». Проект SWAP в 2015 г. был полностью завершен в пяти регионах СЗФО: Твери, Костроме, Ярославле, Смоленске и Иваново. В Петербурге и Ленинградской области он еще продолжается и будет завершен к 2017 г. В результате в Ярославской области связь стала доступна 99,9 % населения, в Ивановской – 99,5 % жителей, а в Костромской – 98,7 %. При этом прирост покрытия территории областей составил в среднем 7–10 % [3]. Ссылаясь на слова представителей «Мегафона», благодаря модернизации сеть 3G в этих регионах стала доступна везде, где живут люди.

Усовершенствование инфраструктуры сети предполагало полную замену оборудования, установленного пять и более лет назад, на более современное и функциональное, поддерживающее ряд проприетарных функций, реализовать которые, используя продукцию разных вендоров, не представлялось возможным. В результате, число обрывов при голосовой связи и передаче пакетов данных, уменьшилось вдвое. Улучшилось покрытие не только в удаленных пунктах, но и внутри помещений. Скорость интернет-доступа стала выше – в Ивановской области средние скорости мобильного широкополосного доступа в Интернет выросли на 35 %. За счет этого увеличилась выручка от услуг мобильной передачи данных и снизились затраты. Часть компонентов сети от разных вендоров содержит взаимодублирующие функции, поэтому высвобождение старого оборудования позволило использовать его для расширения зоны покрытия в других регионах. В одной только Ивановской области зона уверенного обслуживания 2G увеличилась на 15 %. При этом, разумеется, совсем непригодное оборудование было списано. Мегафону успешно удалось создать монобрендовую сеть, полностью готовую к быстрому обновлению до следующего поколения.

Своп-проекты помогают развивать сотовые сети, повышая их рентабельность путем плавной интеграции более современных стандартов и компонентов сотовой сети. К сожалению, для поддержания актуальности инфраструктуры и удовлетворения потребностей абонентов, операторы вынуждены работать с иностранными вендорами, не имея достойных отечественных аналогов. Держать оборудование монобрендовой сети в таком случае становится небезопасно, с точки зрения влияния политической ситуации. Сильная зависимость сети связи от зарубежных стран делает её уязвимой и дает возможность для контроля её эксплуатации странами-поставщиками.

Усиливающийся процесс глобализации рынка телекоммуникационных услуг на мировой арене, может послужить решением вопроса безопасности использования продукции одного вендора. Динамика и масштабы этого рынка значительно прогрессируют в последнее время: по данным статистики ВТО, среднегодовые темпы роста экспорта телекоммуникационных услуг за последнее время составляли 15–20 %. Такое объединение предоставит больше возможностей для оптимального сотрудничества с зарубежными странами, послужит развитием отечественных сетей и укрепит их роль на мировом рынке.

В то же время, при всех вышеперечисленных преимуществах использования оборудования одного вендора, стоит рассмотреть и альтернативный вариант – мультибрендовую сеть. Зарубежные исследования (Gartner, «Debunking the Myth of the Single-Vendor Network») показывают, что операторам следует задуматься и об использовании оборудования нескольких вендоров, так как в ряде случаев это имеет свои преимущества.

Во-первых, заказчик может влиять на ценовую политику разных поставщиков, выбирая оптимальный для себя вариант, тем самым вынуждая конкурентов снижать свои цены на продукцию, например, посредством проведения аукционов. Во-вторых, у оператора появляется возможность выбирать оптимальные технологические решения для конкретных участков сети, и, как следствие, повышать эффективность работы сети в целом путем составления общего решения из частных от разных вендоров, так как каждый из них узко специализирован на определённом типе продукта и повышает качественные характеристики конкретного сетевого оборудования, что способствует обеспечению конкурентоспособности оператора связи [2, 4].

Практика показывает, что получить лучшее сетевое решение за оптимальную цену позволяют мультибрендовые сети. В этом случае, Министерство связи и массовых коммуникаций должно предложить программы регулирования по использованию оборудования различных вендоров. Возможным путем решения этой проблемы станет введение квот на количество оборудования от одного поставщика. Следовательно, операторам придется сотрудничать с разными поставщиками. Заботясь о поддержке российского производства, регулятор может регламентировать обязательное сотрудничество с отечественным вендором сетевого оборудования. Это будет способствовать развитию мультибрендовых сетей, уменьшению «ценовых аппетитов» различных поставщиков в условиях естественной конкуренции и поддержанию политики импортозамещения.

Использование продукции отечественного производителя обезопасит работу сотовой сети в целом, позволяя сохранить суверенитет государства на рынке телекоммуникаций. Стоит также отметить, что вендор, продавая в пакетном решении с аппаратной частью и программное обеспечение, исключает возможность перехода на другой контент, тем самым ограничивая полномочия оператора и делая его зависимым от себя. При возникновении проблем на сети, шансов переключиться или изменить предоставленное обеспечение нет, что ухудшает надёжность работы сети связи. В этом случае, заказчикам полезно было бы найти поставщиков оборудования с открытыми прошивками, но вероятность встретить такое пакетное решение крайне мала.

В заключение, хочется отметить, что при выборе сетевого оборудования нужно учитывать много нюансов, обращая внимание на экономические аспекты построения сети, её безопасность и эффективность. Анализ рынка телекоммуникаций позволяет в первую очередь выбрать подходящего вендора, который ставит во главу угла поддержку открытых промышленных стандартов, что упростит архитектуру и управление разнородной сетью, а также позволит использовать гибкую ценовую политику. На основании изложенного, можно сделать вывод, что долговременное сотрудничество с различными вендорами, и как следствие, мультибрендовые

сотовые сети, являются оптимальным решением как для операторов сотовой связи, так и для поставщиков оборудования.

Список используемых источников

1. Макаров В. В., Горбатько А. В. Инновации, инвестиционная политика и управление качеством услуг компании мобильной связи: монография / под ред В. В. Макарова. СПб. : СПбГУТ, 2014. 288 с.
2. Макаров В. В. Обеспечение конкурентоспособности оператора связи путем инновационного развития // Электросвязь. 2011. № 9. С. 30–33.
3. Шатилин И. «Мегафон» сделал первый «своп» в СЗФО [Электронный ресурс] / "TelecomDaily": [сайт]. URL: http://www.tdaily.ru/news/top-novosti/38399/
4. Макаров В. В., Горбатько А. В. Задача ранжирования сотовой сети при формировании инвестиционной политики // Информатизация и связь. 2011. № 7. С. 85–88.

УДК 621.375

А. О. Болотов (студент группы БРА 1301, МТУСИ)
Р. Г. Холюков (студент группы БРА 1301, МТУСИ)

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ДИНАМИЧЕСКИХ ГОЛОВОК НА ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ УСИЛИТЕЛЯ НА ЛАМПАХ И УСИЛИТЕЛЯ НА ПТ В ПРОГРАММЕ MICRO-CAP

В работе проводится исследование характеристик усилителей мощности на электронных лампах и полевых транзисторах при работе на разную нагрузку. Показано, что характер нагрузки оказывает существенное влияние на технические параметры УМЗЧ. Введение общей отрицательной обратной связи приводит к существенному уменьшению этого влияния.

УМЗЧ, эквивалент динамической головки, Micro-cap, ООС, коэффициент гармоник.

В силу объективной необходимости усилитель мощности звуковой частоты (УМЗЧ) обычно испытывают и настраивают на эквивалент нагрузки в виде активного сопротивления 8 или 4 Ома [1]. Однако реально усилитель мощности звуковой частоты работает на различные динамические головки, имеющие значительные электромеханические резонансы, создающие комплексные сопротивления нагрузки, фазовые сдвиги в выходной цепи усилителя мощности звуковой частоты и деформацию эквивалентной амплитудно-частотной характеристики [2]. В литературе нет всесторонних сведений о технических характеристиках усилителей на лампах и усилителей на полевых транзисторах при работе на эквивалент динамической головки.

Для того, чтобы провести исследование усилителя мощности на электронных лампах были подобраны математические модели электронных ламп для программы Microcap [3]. Характеристики математических моделей ламп были протестированы. Результаты показали, что характеристики математических моделей ламп совпадают с характеристиками ламп из справочника. Принципиальная схема исследуемого УМЗЧ приведена на рисунке 1.

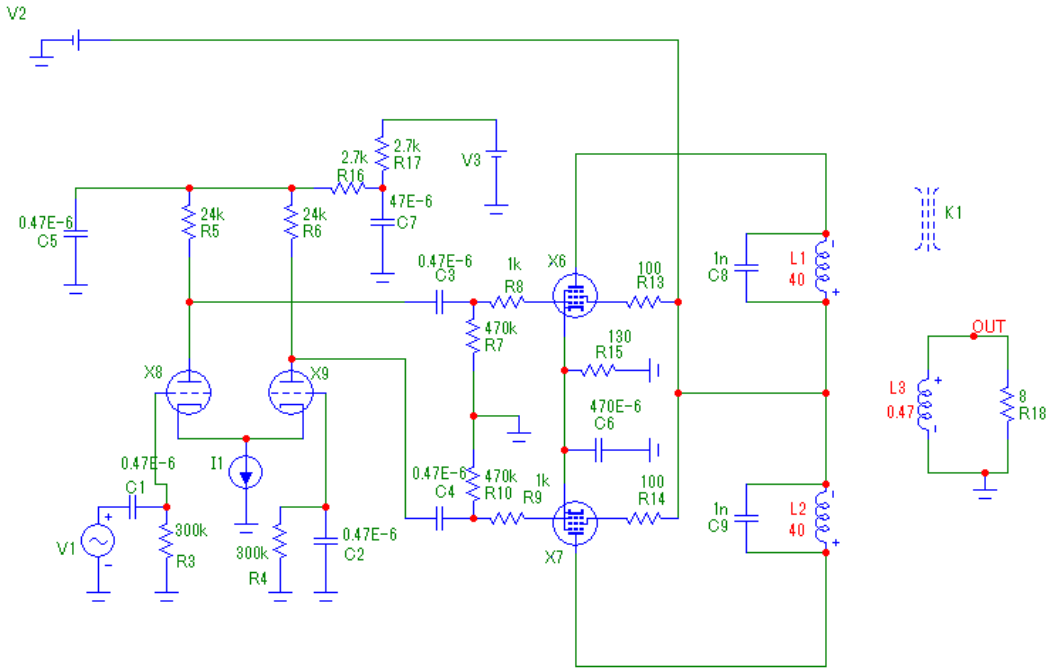


Рис. 1. Принципиальная схема УМЗЧ на электронных лампах

Первый каскад УМЗЧ собран по дифференциальной схеме на триодах 6Н23П (он усиливает напряжение и одновременно выполняет функцию фазоинвертора). В цепи катода используется источник тока, который обеспечивает высокую симметричность каскада. Оконечный каскад собран по двухтактной трансформаторной схеме в режиме близком к АВ на пентодах 6П18П. Трансформатор смоделирован как идеализированный без учета нелинейностей сердечника. По характеристикам лампы было определено необходимое сопротивление нагрузки для получения заданной мощности. Исходя из этого выбран необходимый коэффициент трансформации.

Исследования проводились с нагрузкой в виде резистора 8 Ом, эквивалента одиночной динамической головки и в виде эквивалента двух динамических головок, комплексное сопротивление которых в звуковом диапазоне частот близко к 8 Ом. Параметры УМЗЧ были получены при амплитуде напряжения на входе равной 1 В и частоте 1 КГц. В ходе работы были получены: АЧХ; КПД, средняя мощность в нагрузке, спектр выходного сигнала и коэффициент гармоник [4].

Результаты исследования приведены в таблице 1, в которой сравниваются характеристики УМЗЧ на электронных лампах с разными нагрузками.

ТАБЛИЦА 1. Сравнение характеристики УМЗЧ на электронных лампах с разными нагрузками

	УМЗЧ с нагрузкой в виде резистора	**УМЗЧ с нагрузкой в виде экв. дин. гол.**	**УМЗЧ с экв. 2-х дин. гол.**
Р, Ватт	8,7	6, 9	9,3
КПД, %	42,2	28,7	41,4
Кг, %	2	18,3	12,3

Полученные результаты говорят, что технические показатели УМЗЧ с сопротивлением 8 Ом, отличаются от показателей УМЗЧ с нагрузкой в виде эквивалента одной или двух динамических головок. Это обусловлено в первую очередь высоким выходным сопротивлением УМЗЧ и отсутствием отрицательной обратной связи. Уменьшение выходного сопротивления можно добиться введением общей петли отрицательной обратной связи. Однако в случае лампового усилителя с трансформаторным выходным каскадом плохая фазовая характеристика трансформатора обычно не позволяет ввести обратную связь достаточной глубины.

Далее проводились те же исследования с усилителем мощности звуковой частоты на полевых транзисторах, принципиальная электрическая схема приведена на рисунке 2. Поскольку проходная ВАХ ПТ близка к параболической, это позволяет ожидать меньших нелинейных искажений в случае использования симметричного двухтактного безтрансформаторного выходного каскада.

Первый каскад УМЗЧ на полевом транзисторе (MPF9200) выполнен как схема с общим истоком, с местной обратной связью.

Второй каскад(драйвер), который является предвыходным, также выполнен по схеме с общим истоком на полевом транзисторе (MFE9200)

Оконечный каскад собран по схеме двухтактного истокового повторителя в режиме близкому к АВ на транзисторах (2SK308, 2SJ127). Применяется общая петля отрицательной обратной связи, последовательная по напряжению, охватывающая весь усилитель. Для повышения КПД используется вольт-добавочная емкость С8 [4].

Так же, как и для УМЗЧ на электронных лампах, исследования проводились с нагрузкой в виде резистора 8 Ом, электрическим эквивалентом одиночной динамической головки и электрическим эквивалентом двух динамических головок, комплексное сопротивление которых в звуковом диапазоне частот близко к 8 Ом. Компьютерный эксперимент проводился при амплитуде напряжения на входе равной 1 В и частоте 1 КГц. В ходе работы были получены: АЧХ; зависимости тока, напряжения и мгновенной

мощности, рассеиваемой на стоке; КПД, средняя мощность в нагрузке, спектр выходного сигнала и коэффициент гармоник.

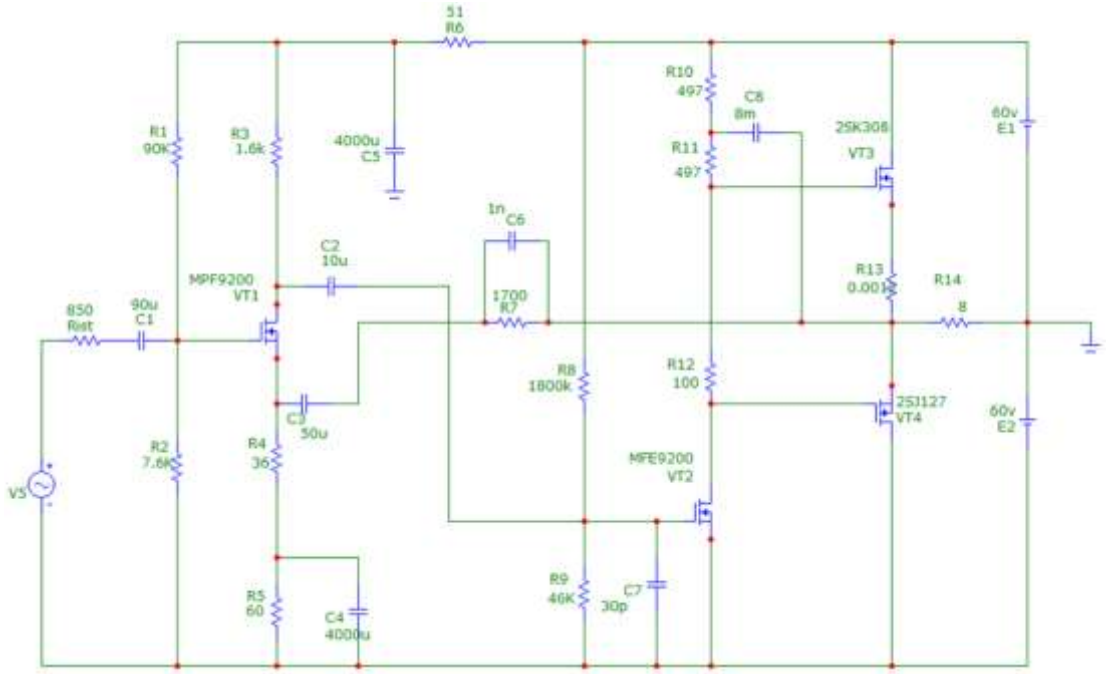


Рис. 2. Принципиальная схема УМЗЧ на полевых транзисторах

В усилителе с дополнительной петлей параллельной отрицательной обратной связи по напряжению (большая глубина ООС) была снята АЧХ и оценен коэффициент гармоник при нагрузке в виде эквивалента двух динамических головок. Основные результаты исследование приведены в таблице 2.

ТАБЛИЦА 2. Основные результаты исследования

	УМЗЧ с нагрузкой в виде резистора	**УМЗЧ с нагрузкой в виде экв. дин. гол.**	**УМЗЧ с экв. 2-х дин. гол.**
Р, Ватт	115,3	55,4	60,3
КПД, %	51,6	32,8	43,3
Кг, %	0, 03	0,04	0,4
Р, Ватт	114,5	169,9	99,7

У усилителя с дополнительной петлей обратной связи АЧХ является равномерной в диапазоне частот от 10 Гц до 20 КГц, не зависимо от вида нагрузки. Коэффициент гармоник равен 0,01 %.

Результаты исследований показывают, что при нагрузке в виде динамических головок могут иметь место значительные перегрузки оконечных транзисторов, по току и пиковой мощности. Поскольку транзисторы, в отличии от электронных ламп, быстрее выходят из строя при перегрузках,

то для предотвращения выхода их из строя необходимо принимать специальные меры по их защите. Увеличение глубины отрицательной обратной связи делает усилитель менее чувствительным к виду динамических головок и уменьшает коэффициент нелинейных искажений.

Вывод по проделанной работе

Трудности введения глубокой отрицательной обратной связи в усилителе мощности звуковой частоты на электронных лампах не позволяют устранить деформацию АЧХ, в основном вызванную высоким выходным сопротивлением УМЗЧ и различными комплексными сопротивлениями разных динамических головок. Согласно таблице 1, работа УМЗЧ на комплексную нагрузку приводит к изменениям практически всех основных технических показателей УМЗЧ. Поэтому желательно вводить глубокую отрицательную обратную связь для того, чтобы ламповый усилитель работал с неизменными техническими параметрами при разных динамических головках, либо необходимо принимать другие схемотехнические решения, снижающие выходное сопротивление без введения общей отрицательной обратной связи, для того чтобы сделать УМЗЧ универсальным. А в УМЗЧ на полевых транзисторах можно вводить глубокую ООС, что позволяет значительно снизить влияния комплексного сопротивления нагрузки в виде различных динамических головок на технические параметры УМЗЧ. Однако глубины отрицательной обратной связи, обеспечивающей Кг = 0,03 %, оказалось недостаточно для устранения изменений технических параметров УМЗЧ. Как при одиночной динамической головке, так и при двух динамических головках имеет место значительное возрастание пиковых (мгновенных) мощностей рассеиваемых на стоке транзисторов. Показано, что причиной этого являются фазовые сдвиги из-за комплексной нагрузки. Проведенные исследования показали, что УМЗЧ на полевых транзисторах при двухпетлевой отрицательной обратной связи сохраняет свои технические параметры при работе на разные динамические головки в отличие от лампового усилителя.

Список используемых источников

1. Дуглас Селф. Схемотехника современных усилителей. М. : ДМК Пресс, 2011. 529 с.

2. Мусатов К. В. Моделирование работы АС с помощью компьютера // Радио. 2013. № 9. С. 12–14; № 10. С. 10–14.

3. Амелина М. А., Амелин С. А. Программа схемотехнического моделирования Micro-Cap, Версии 9, 10. Смоленск : Смоленский филиал НИУ МЭИ, 2013. 618 с.

4. Кубицкий А. А. Методические указания по курсовому проектированию “Электрический расчет и компьютерное моделирование УМЗЧ”. М. : МТУСИ., 2009. 36 с.

Статья предоставлена научными руководителями,
доктором технических наук, доцентом Кубицким А. А., инженером Бажином А. А.

УДК 681.3.06

В. А. Голиков (студент группы РА-21, СПбГУТ)

МОДЕЛИРОВАНИЕ И РЕАЛИЗАЦИЯ НА ЦИФРОВОМ СИГНАЛЬНОМ ПРОЦЕССОРЕ СИСТЕМЫ АУДИОЭФФЕКТОВ ДЛЯ ЭЛЕКТРОГИТАРЫ

Реализация алгоритмов цифровой обработки сигналов (ЦОС) на цифровых сигнальных процессорах (ЦСП) является активно развивающейся областью науки и техники. Для этих целей создается новая элементная база, позволяющая реализовывать все более сложные алгоритмы обработки сигналов и работать с ними в реальном времени. Эта динамика развития предъявляет новые требования и к разработке самих алгоритмов, в частности происходит их усложнение и разработка алгоритмов ЦОС становится отдельной сложной задачей.

цифровая обработка сигналов, аудио, цифровой сигнальный процессор.

Фейзер – это аудиоэффект, имитирующий вращение динамика. Создается эффект за счет фильтрации исходного звукового сигнала, при котором в АЧХ канала связи образуется серия максимумов и минимумов. Максимумы и минимумы осциллируют по оси частот с течением времени (частота осцилляции задается произвольно в зависимости от художественных целей, но, как правило, варьируется в пределах от десятых долей герц до единиц герц). Этот эффект так же называют фазовым вибрато.

Аудиосигнал на входе разделяется на две одинаковые части. Одна из этих частей пропускается через каскадное соединение фазовых звеньев второго порядка и подается на вход сумматора. Вторая часть поступает на сумматор без изменений. При этом в АЧХ фильтра образуется последовательность максимумов и минимумов, по количеству фазовых звеньев второго порядка [1]. Оценка АЧХ фильтра была произведена при помощи тестового сигнала белого шума с распределением Гаусса (см. рисунки 1 и 2)

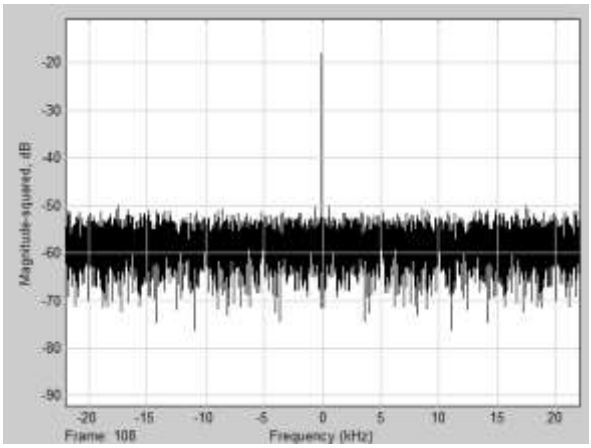


Рис. 1. АЧХ канала связи без фейзера

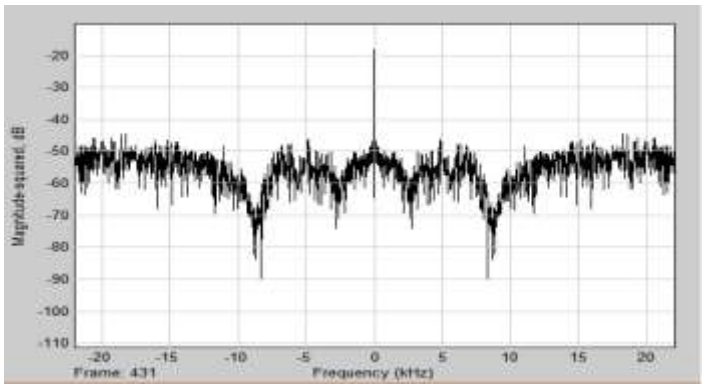


Рис. 2. АЧХ канала связи с фейзером

Для расширения возможностей эффекта фазовые фильтры часто охватываются регулируемой петлей обратной связи. При этом звучание эффекта становится более форсированным, переходные процессы по оси частот расширяются. На рисунке 3показано воздействие линии обратной связи на АЧХ канала.

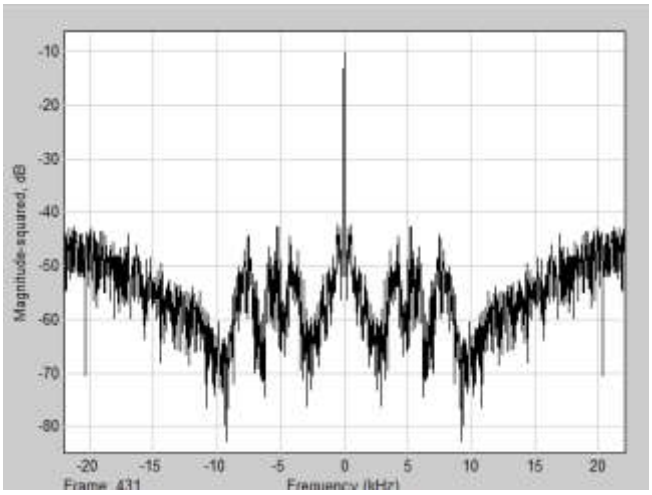


Рис. 3. АЧХ канала с фейзером, охваченным обратной связью

Частоты настройки фазовых звеньев выбираются, как правило, в соответствии с логарифмической (или октавной) шкалой. Например, для четырехзвенного фейзера они могут составлять 500 Гц, 1, 2 и 4 кГц [1]. Сигналы с выходов фазовых звеньев регулируются по величине и суммируются с исходным сигналом. Минимумы характеристики соответствуют тем частотам, на которых происходит сдвиг фазы в 180°.

Значение центральной частоты полосы задерживания модулируется сигналом генератора низкой частоты, частота генерации которого – порядка единиц герц. Эта частота устанавливается сразу для всех звеньев фейзера. При этом максимумы и минимумы АЧХ фильтра будут осциллировать по оси частот. При изменении глубины обратной связи, изменяется форма переходных процессов.

Передаточная функция фазового звена порядка N:

$$H_N(z) = \frac{\sum_{n=0}^{N} k_{N-n} z^{-n}}{\sum_{n=0}^{N} k_n z^{-n}}.$$

Для удобства реализации модели фейзера запишем передаточную функцию фазового звена в следующем виде [3]:

$$H_N(z) = \frac{k_n + z^{-1} H_{N-1}(z)}{1 + k_n z^{-1} H_{N-1}(z)}.$$

Так как требуется реализовать соединение звеньев второго порядка, то передаточная функция примет следующий вид:

$$H_2(z) = \frac{k_2 + z^{-1} H_1(z)}{1 + k_2 z^{-1} H_1(z)},$$

при этом

$$H_1(z) = \frac{k_1 + z^{-1}}{1 + k_1 z^{-1}},$$

где $k_1 = -\cos(\hat{\omega}_0)$, т. е. отвечает за выбор частоты режекции, а коэффициент k_2 задает полосу режекторного фильтра по уровню $\frac{1}{\sqrt{2}}$ (−3 дБ) [4].

Была построена Simulink-модель фейзера (рис. 4). Как можно увидеть на схеме, имеется четыре фазовых звена, построенных на основе описанной выше передаточной функции, соответственно, АЧХ канала должна иметь четыре минимума, осциллирующих по оси частот с течением времени.

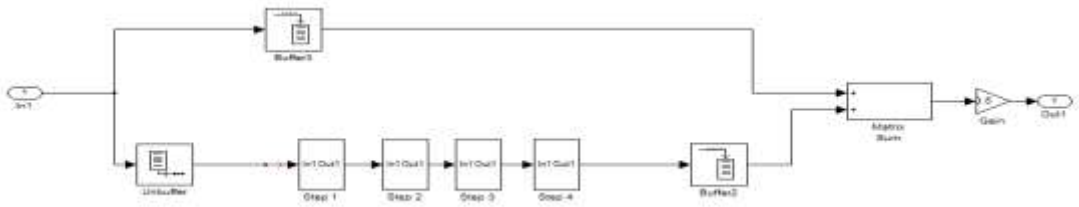


Рис. 4. Simulink-модель фейзера

В качестве элементной базы была выбрана отладочная плата TMS320C5515 EVM.

Процессор TMS329C5515 позиционируется фирмой Texas Instruments, как ЦСП, одной из основных задач которого является запись, обработка и воспроизведение звуковых сигналов [5].

Процессор оснащен аппаратным модулем для вычисления БПФ, что является значительным достоинством для реализации на нем алгоритмов преобразований в частотной области.

Основные параметры процессора [5]:

- тактовая частота 120 МГц,
- TLV320AIC3204 32-битный программируемый стереокодер,
- OLED цветной LCD дисплей (128×128 пикселей),
- большой набор периферии, включая USB 2.0,
- 10 программируемых кнопок,
- 320 килобайт встроенной памяти,
- кроме встроенной флэш памяти возможно расширение SD-картой.

Изображение отладочной платы представлено на рисунке 5.

Рис. 5. Отладочная плата TMS320C5515 EVM

Для получения кода для процессора и дальнейшей установки разработанных алгоритмов на отладочную плату, воспользуемся средствами Simulink Coder (рис. 6).

При помощи этих средств алгоритм, реализованный в виде Simulink-модели, представляется в виде файлов с кодом на языке C, при помощи которого будет получен выходной файл для процессора [6].

Полученный код проходит отладку в интегрированной среде разработки Code Composer Studio и происходит загрузка выходного файла на отладочную плату.

Далее был написан код для взаимодействия процессора с периферией, имеющейся на плате, т. к. соответствующие кодеки не были учтены при генерации кода и алгоритм представлен сгенерированным кодом исключительно в виде вычислительного алгоритма.

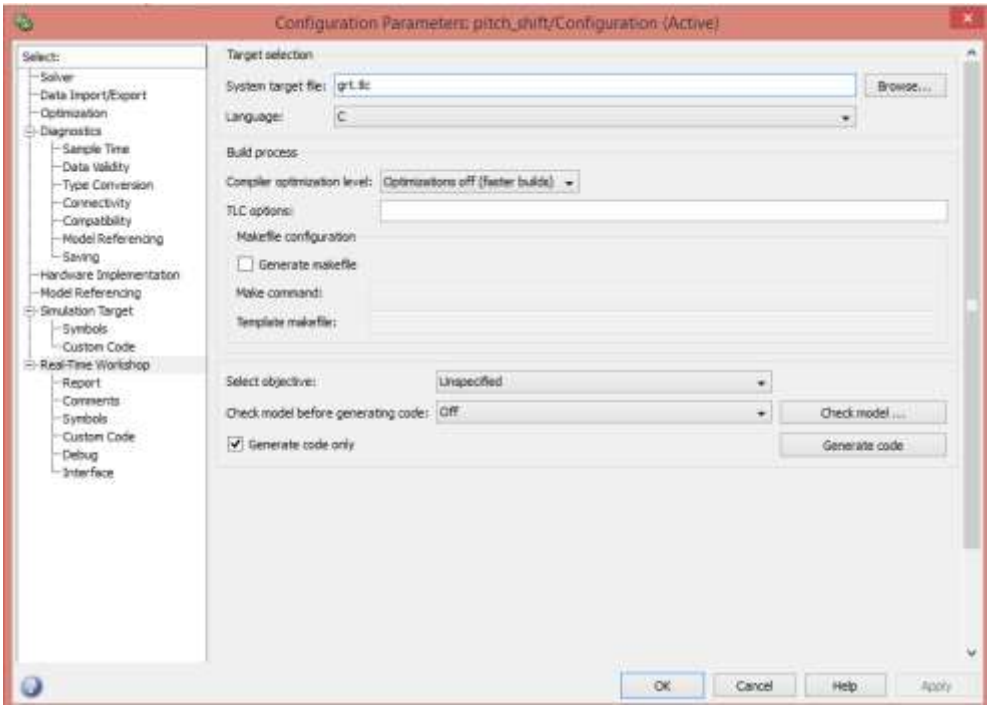


Рис. 6. Окно настроек Simulink Coder

На рисунке 7 изображена схема подключения реализованной системы.

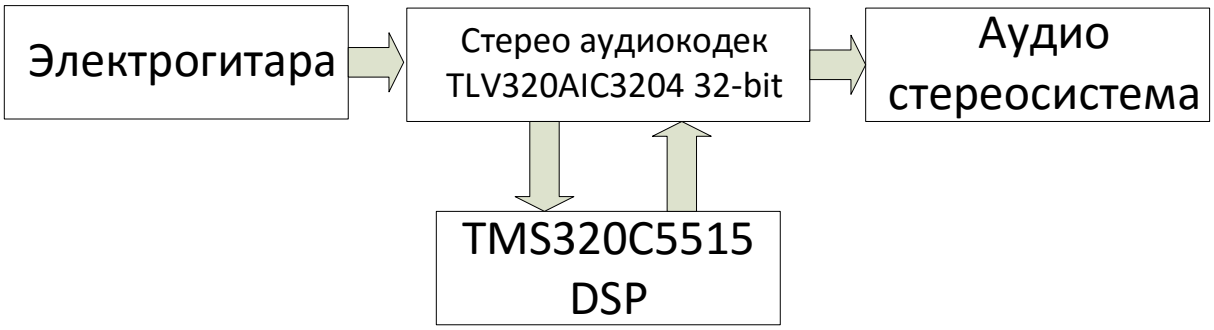


Рис. 7. Схема коммутации системы

Электрогитара подключается в аудиовход и сигнал поступает на стереоаудиокодек, через который происходит обмен информацией с ЦСП. Обработанный сигнал подается аудиокодеком на стереовыход, к которому подключается аудио стереосистема.

Список используемых источников

1. Никамин В. А. Микшерные пульты: учебное пособие. СПб. : изд-во СПбГУТ, 2009. 80 с.

2. Основы цифровой обработки сигналов : учебное пособие / А. И. Солонина, Д. А. Улахович, С. М. Арбузов [и др.]. 2-е изд. СПб. : БХВ-Петербург, 2005. 768 с. ISBN 5-94157-604-8.

3. Phillip A. Regalia, Sanjit K. Mitra, P. P. Vaidyanathan The Digital All-Pass Filter: A Versatile Signal Processing Building Block: PROCEEDINGS OF THE IEEE, VOL. 76, NO. 1, JANUARY 1988, P. 19–37.

4. Vaidyanathan P. P. Multirate systems and filters banks: New Jersey: Prentice hall, 1993.

5. Texas Instruments: [сайт]. URL: http://www.ti.com/

6. Степанов А. Б. Технология реализации алгоритмов цифровой обработки сигналов на цифровом сигнальном процессоре с применением системы MATLAB // Цифровая обработка сигналов и ее применение – DSPA-2016: сб. докл. 18-й Международной конференции. Москва, 2016. Том 2. С. 801–806.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Степановым А. Б.

УДК 519.688

Д. В. Девяткин (студент группы РТ-51М, СПбГУТ)
А. Н. Митлаш (студент группы РТ-51М, СПбГУТ)

РАЗРАБОТКА ПРИЛОЖЕНИЯ НА ОСНОВЕ СРЕДЫ MATLAB ДЛЯ ЛАБОРАТОРНЫХ РАБОТ ПО ИЗУЧЕНИЮ СВОЙСТВ ТЕЛ НЕОПРЕДЕЛЕННОСТИ РАДИОСИГНАЛОВ

Известно, что форма тела неопределенности влияет на разрешающую способность системы по дальности и по скорости. Для получения представления о телах неопределенности, их свойствах в зависимости от типа применяемого сигнала разработано данное приложение.

тело неопределенности, доплеровский сдвиг, спектр, сигнал, радиолокация, радионавигация, MATLAB.

При оптимальном обнаружении сигнала на выходе оптимального приемного устройства формируется сигнал, который полностью совпадает по форме с корреляционной функцией (КФ) зондирующего сигнала [1]. По этой причине особенности разрешения сигнала, оценки его параметров, распознавания целей и множеством других операций взаимосвязаны с такими параметрами как: форма двумерной корреляционной функции (ДКФ) зондирующего сигнала и ее деформация при расстройке системы "фильтр – сигнал" по частоте Ω или рассогласования по времени τ системы "опорный сигнал – принятый сигнал" при корреляционной обработке [2].

На выходе согласованного фильтра (СФ) или коррелятора оптимального обнаруживающего устройства формируются сигналы, которые описываются модулем корреляционного интеграла. Таким образом, можно

сказать, что ДКФ – обобщение корреляционного интеграла в случае рассогласования опорного и принимаемого сигналов по времени на интервал τ и по частоте на значение расстройки Ω. В то же время τ может физически интерпретироваться в качестве несовпадения времени задержки, принимаемого t_R с опорным t_3 при расстройке СФ относительно несущей частоты сигнала. Физически такая ситуация происходит из-за эффекта Доплера при условии движущихся объектов. Следовательно, сечения тела ДКФ при помощи вертикальных плоскостей, параллельных оси Ω и проходящих через различные точки оси τ, позволяют наблюдать зависимость искажений спектра выходного сигнала от задержки принимаемого сигнала относительно опорного. В то же время сечения ДКФ при помощи плоскостей, параллельных оси τ и проходящих через различные точки оси Ω, дают зависимость искажений огибающей выходного сигнала от расстройки по частоте системы "согласованный сигнал – выходной сигнал" [2].

Несмотря на то, что тела неопределенности наглядны, использование их изображения при синтезе и анализе зондирующих сигналов приводит к некоторым неудобствам, поэтому осуществляется переход к различным сечениям плоскостями.

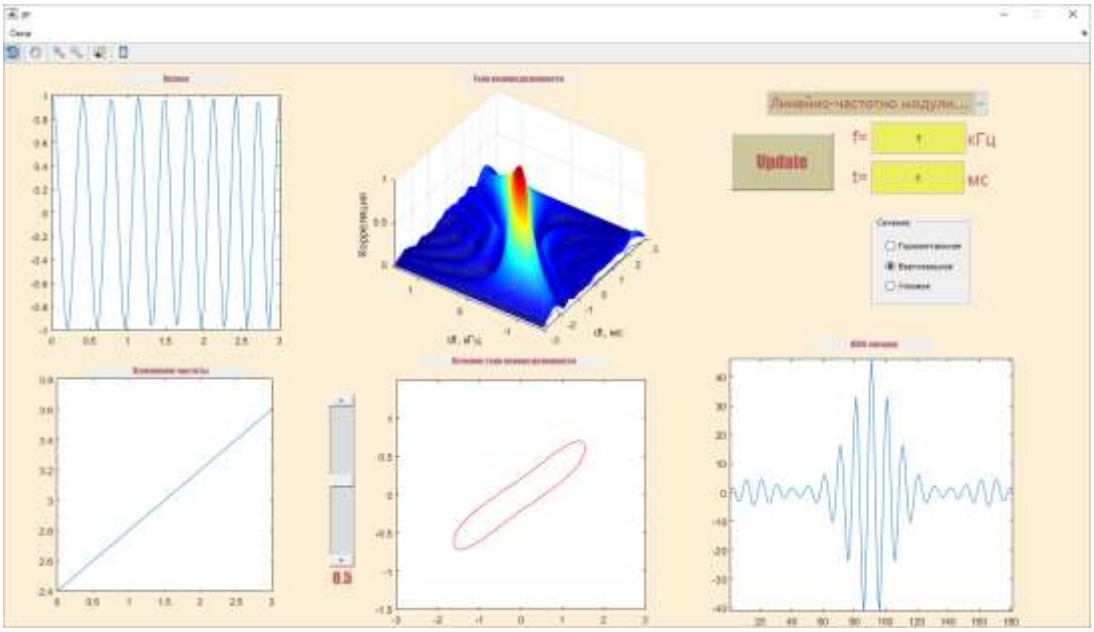


Рис. 1. Интерфейс программы

Разработанная программа обладает следующими возможностями:
- построение различных сигналов,
- построение АКФ сигналов,
- построение тел неопределенности для различных сигналов,
- получение сечений тел неопределенности в различных точках.

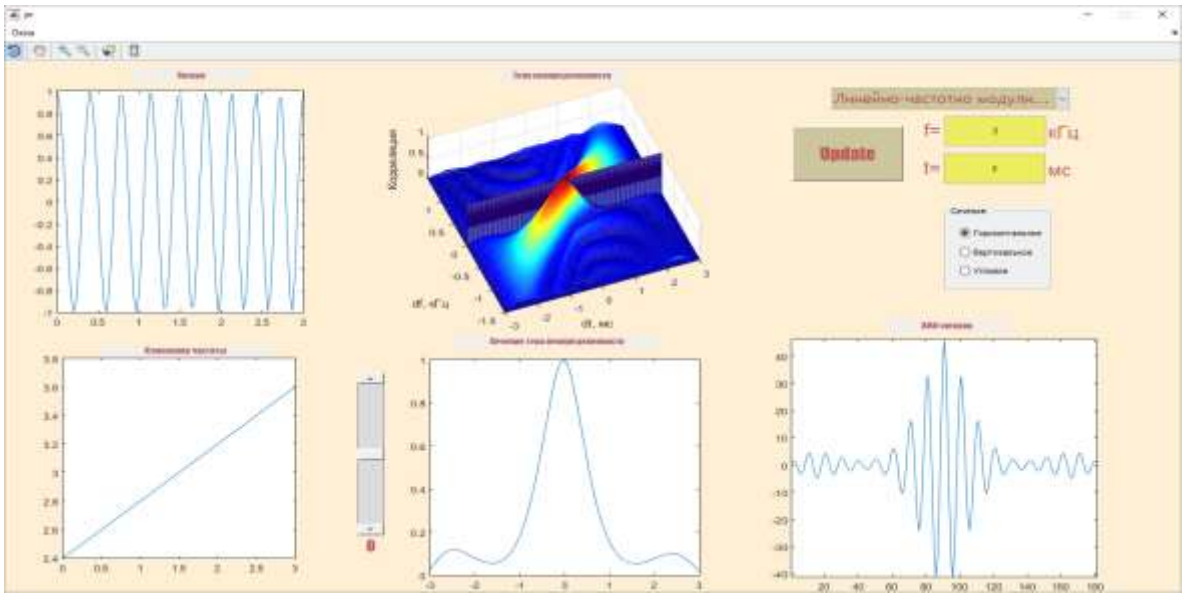


Рис. 2. Сечение тела вертикальной плоскостью

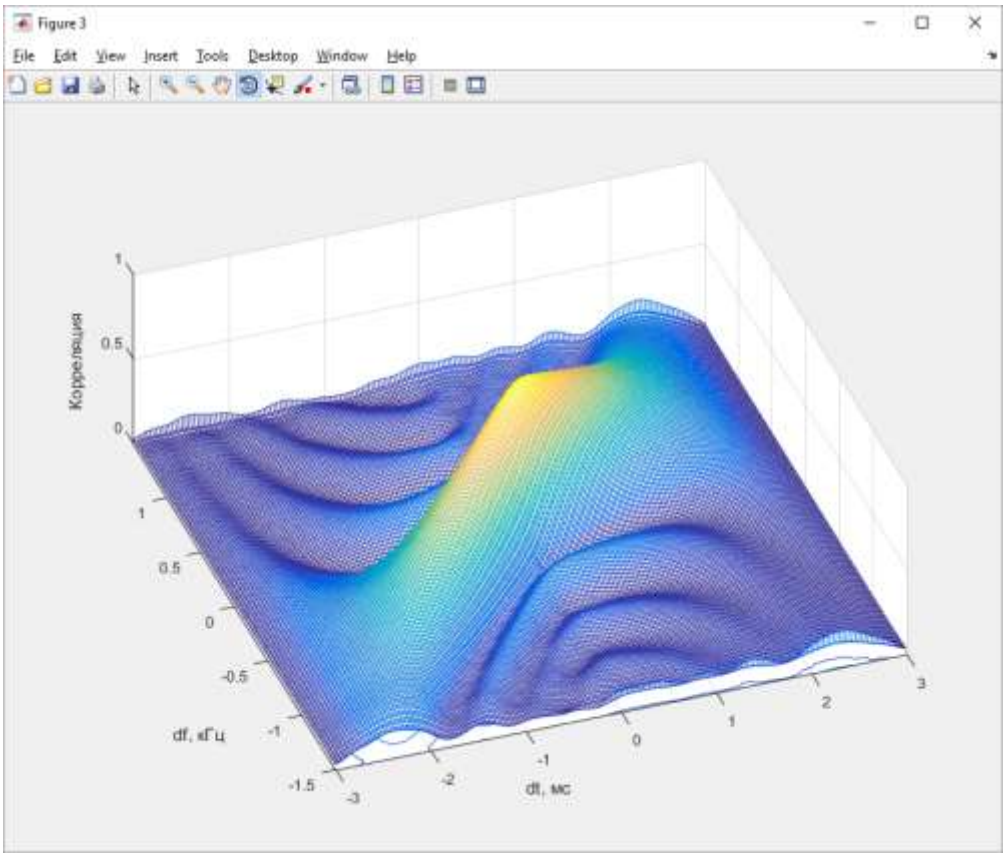


Рис. 3. Окно тела неопределенности ЛЧМ сигнала

Предложенный функционал позволяет организовать лабораторные работы по предметам радиолокации и радионавигации с целью получения представления о телах неопределенности и свойствах сигналов.

Список использованных источников

1. Маковецкий П. В., Охонский А. Г., Поддубный С. С. Сложные сигналы: учебно-методическое пособие. СПб. : ГУАП, 2010. 69 с.
2. Бакулев П. А. Радиолокационные системы: учебник для вузов. М. : Радиотехника, 2004. 320 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Поддубным С. С.

УДК 654.16

Н. С. Дедовец (студент группы РМ-21, СПбГУТ)

РАЗРАБОТКА СПУТНИКОВОЙ АНТЕННОЙ СИСТЕМЫ С АВТОСЛЕЖЕНИЕМ

В данной статье рассмотрены спутниковые антенные системы с автонаведением и автослежением за спутником. Рассмотрены требования, выдвигаемые к подобным системам, а так же алгоритм работы подобных систем.

автонаведение, автослежение, угол места, азимут, антенная система, наведение, позиционирование.

Спутниковые антенные системы с автослежением используются в комплексах связи, устанавливаемых на морских судах, поездах дальнего следования и в прочих местах, где обеспечение связи другим способом не представляется возможным. Подобные системы позволяют оставаться на связи даже в дальних поездках и во время движения, что в двадцать первом веке является принципиально важным для большинства людей. Стоимость таких комплексов довольно высока, кроме этого, в России их не производят, поэтому было решено заняться разработкой алгоритма позиционирования для подобных систем.

На первом этапе были рассмотрены два самые популярных аналога и исходя из этого сформированы требования к разрабатываемой системе. Это системы RaySat E-7000 фирмы Gilat и Телеком – 60 фирмы Viscom. Требовалось создать систему, которая принципиально не будет уступать уже существующим и обеспечит необходимое качество связи, но будет на порядок дешевле.

Большинство подобных антенных систем, а также провайдеров, предоставляющих услуги доступа к сети интернет, работают в Ku диапазоне (10,7–18 ГГц), поэтому было решено его и придерживаться. Для возможности работы со всеми спутниками этого диапазона, используется

и круговая и линейная поляризация. Требования по усилению были выдвинуты, опираясь на характеристики уже существующих систем, не менее 34 дБ на прием и 36 дБ на передачу. Для того, чтобы система могла настроиться на любой спутник в зоне видимости, требуется чтобы была возможность устанавливать угол азимута в диапазоне от 0 до 360 градусов, угол места от 0 до 90.

Далее требовалось рассчитать максимально допустимую погрешность наведения. Для совершения этих расчетов, было принято допущение, что в системе используется параболическая антенна. Необходимо учитывать, что максимально допустимая погрешность зависит от ширины главного лепестка диаграммы направленности, которая в свою очередь зависит от диаметра зеркала антенны. Усиление, требование по которому были выдвинуты выше, тоже определяет диаметр [1]. Требования к системе были сведены в общую таблицу.

ТАБЛИЦА 1. Требования к разрабатываемой системе

Рабочий диапазон частот	10,7–18 ГГц
Поляризация	Линейная и круговая
Усиление на прием не менее	34 дБи
Усиление на передачу не менее	36 дБи
Диапазон перемещения по углу места	от 0° до 90°
Диапазон перемещения по азимуту	от 0° до 360°
Ошибка наведения не более	0,975°

Разработанный алгоритм работы системы позиционирования представлен на рисунке 1. После включения системы начинается этап первоначальной настройки по координатам. Система считывает свои координаты по GPS датчику и координаты спутника из памяти контроллера, затем рассчитывает направление на спутник. Этот этап позволяет ускорить вхождение системы в рабочее состояние при включении так как система не сканирует все пространство, а сразу настраивается в нужное место. Параметры наведения: угол места (1) и азимут (2) рассчитываются по следующим формулам [2]:

$$El = \operatorname{arctg}\left(\frac{\cos\left(Lo_{ES} - Lo_{SAT}\right)\cos\left(La_{ES}\right) - 0{,}15126}{\sqrt{1-\cos^2\left(Lo_{ES} - Lo_{SAT}\right)\cos^2\left(La_{ES}\right)}}\right); \quad (1)$$

$$Az = 180 + \mathbf{arctg}\left(\frac{\mathbf{tg}\left(\mathbf{Lo_{ES}} - \mathbf{Lo_{SAT}}\right)}{\sin\left(\mathbf{La_{ES}}\right)}\right), \quad (2)$$

где El – угол места в градусах; Az – азимут в градусах; La_{ES} – географическая широта (для северного полушария – знак "+", для южного полушария – знак "−"); Lo_{ES} – географическая долгота (для восточного полушария – знак "+", для западного полушария – знак "−"); Lo_{SAT} – географическая долгота точки стояния спутника (для восточного полушария – знак "+", для западного полушария – знак "−").

Так же необходимо учитывать, что во время движения платформа системы наклоняется, поворачивает и т. д., поэтому на следующем этапе происходит подстройка по положению в пространстве. Сначала происходит настройка угла поворота конвертора, учитывая скорость движения, осуществлять эту подстройку каждый цикл не требуется, поэтому присутствует таймер. Затем считываются и обрабатываются показания датчиков, и происходит наклон и поворот платформы антенной системы в нужном направлении. Так же для корректной работы системы необходимо в конце этого этапа производить измерение уровня сигнала.

Затем происходит этап подстройки по уровню сигнала [3], так как есть два параметра: угол места и азимут, которые необходимо настроить, то сначала переменной настройки приравнивается угол места и происходит настройка по нему. Так же для выполнения этого этапа требуется запоминать, увеличивался или уменьшался уровень сигнала в прошлый шаг. Далее происходит смещение переменной на заданный шаг и происходит этап подстройки по положению в пространстве, описанный выше, если уровень сигнала увеличился, значит система движется в правильном направлении и продолжает делать шаги в том же направлении, когда уровень сигнала уменьшился в зависимости от предыдущего изменения и принимается решение, направление движение либо было выбрано правильно и прошло через максимум, тогда положение возвращается на предыдущий шаг и начинается настройка по азимуту, либо направление было выбрано неправильно изначально, в таком случае направление меняется и происходит сканирование таким же образом до поиска максимума. Таким образом находится максимум по обоим переменным и уровень сигнала принимается за максимальный. Система делает в поправки только на положение в пространстве до тех пор, пока уровень сигнала не упадет ниже 0,9 от максимального. В этом случае система заново запускает поиск максимума по уровню сигнала.

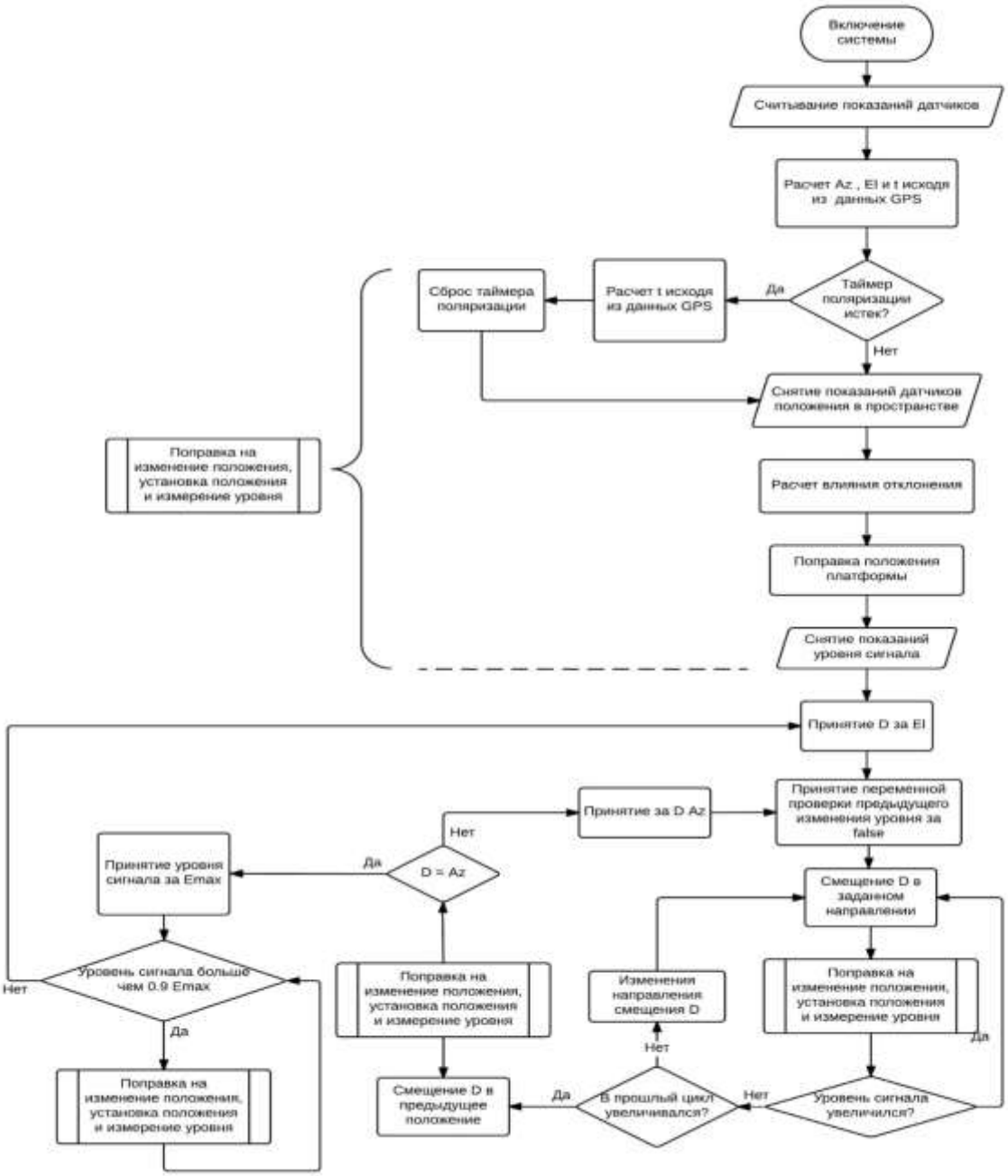


Рис. 1. Алгоритм работы системы позиционирования

По итогу работы в системе присутствуют следующие недостатки:

- не учтен эффект Доплера,
- используемый метод компенсации отклонения в пространстве нерационален.

Список используемых источников

1. Дардари Д., Луизе М. Фаллетти Э. (ред.) Методы спутникового и наземного позиционирования. Перспективы развития технологий обработки сигналов / пер. с англ. М.: Техносфера, 2012. 528 с. ISBN 978-5-94836-338-7.
2. Сомов А. М., Корнев С. Ф. Спутниковые системы связи: учебное пособие для вузов / под ред. А. М. Сомова. М. : Горячая линия – Телеком, 2012. 244 с. ISBN 978-5-9912-0225-1.
3. Индикатор наведения спутниковой антенны [Электронный ресурс] / И. Нечаев. URL: http://www.radioradar.net/radiofan/antenns/ indicator_ prompting_ satellite_ aerial.html

Статья представлена научным руководителем,
старшим преподавателем Прасоловым А. А.

УДК 534.85

С. Е. Денисов (студент группы 311, СПбГИКиТ)
А. В. Шишкин (студент группы 311, СПбГИКиТ)

СОВРЕМЕННЫЕ СПОСОБЫ ЗАПИСИ АУДИОИНФОРМАЦИИ

В данной статье рассмотрены современные методы записи аудиовизуальной информации. Особое внимание обращается на лазерную и магнитооптическую запись. В статье раскрываются принципы и форматы записи, а также основные технические характеристики носителей информации.

звук, аудиоинформация, звукозапись.

Звук – физическое явление, представляющее собой распространение в виде упругих волн механических колебаний в твёрдой, жидкой или газообразной среде. Как и любая волна, звук характеризуется амплитудой и спектром частот [7]. В свою очередь, амплитуда колебаний зависит от мощности источника звука. Человек способен слышать звуковые колебания в диапазоне частот от 20 Гц до 20 кГц [7].

Обратимся к истории звукозаписи. Первыми устройствами для записи и воспроизведения звука были механические музыкальные инструменты. Они могли воспроизводить мелодии, записанные на бумагу, дерево, металлические валики и т. д. Однако эти инструменты не способны были записывать произвольные звуки [9].

Однако в дальнейшем способы записи звука развивались и в настоящее время их возможности поражают воображение.

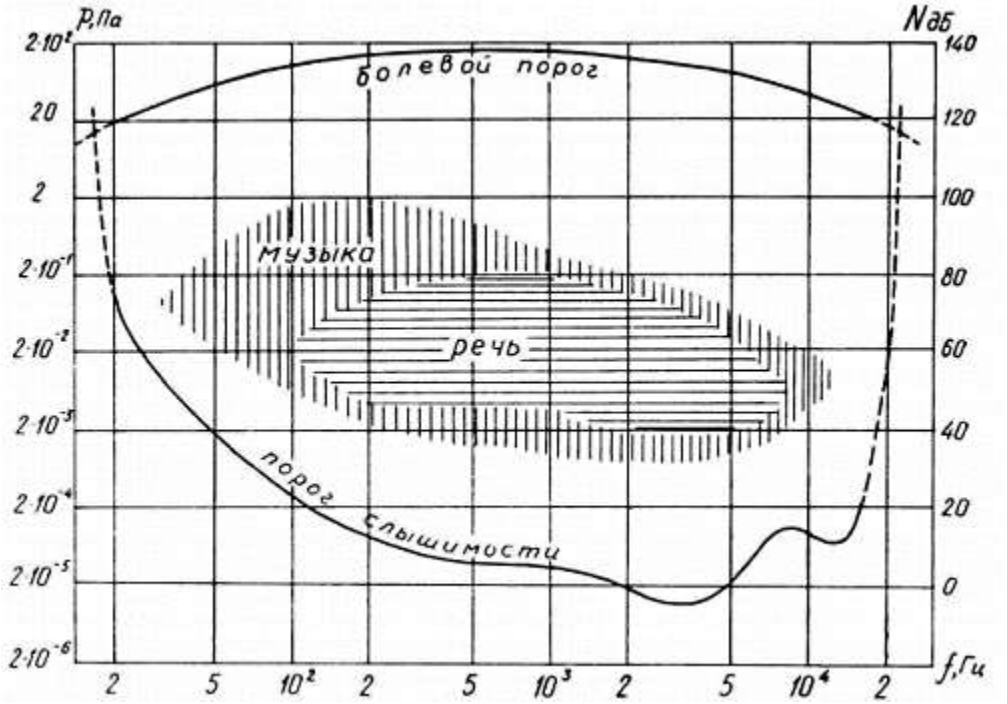


Рис. 1. Область слышимости [6]

Различают основные способы записи аудиоинформации:

- механическая запись,
- электромеханическая запись,
- магнитная запись,
- оптическая запись,
- цифровая звукозапись,
- лазерная запись,
- магнитооптическая запись.

Рассмотрим такие популярные в настоящее время способы записи – лазерную и магнитооптическую.

Лазерная запись

Лазер (от англ. Light Amplification by Stimulated Emission of Radiation – усиление света в результате вынужденного излучения) – прибор, обычно используемый как генератор излучения, который содержит активное вещество и систему возбуждения и управления излучением. При возбуждении активного вещества путём облучения или воздействия электрического поля происходит рекомбинация носителей электрических зарядов и выделяется энергия в виде квантов света [10].

При лазерном способе записи на вращающийся оптический диск с помощью лазерного пучка записываются цифровые сигналы. В результате на диске образуется спиралевидная дорожка, состоящая из впадин (питов) и гладких участков. В режиме воспроизведения лазерный луч, сфокусированный на дорожку, перемещается по поверхности вращающегося диска

и считывает с него данные, при этом питы считываются как нули, а гладкие участки – как единицы. Такой способ записи обеспечивает практически полное отсутствие помех, высокое качество звучания, высокую плотность записи и полное отсутствие механического контакта между носителем и считывающим устройством [9, 10].

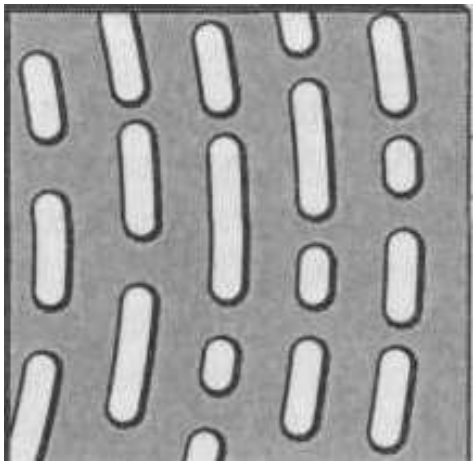


Рис. 2. Фрагмент оптического диска после записи информации

Лазерная запись подразумевает под собой три стандарта аудиоформатов: компакт-диск, DVD-Audio и Super Audio CD.

Рис. 3. Логотипы форматов лазерной записи

Проект формата «компакт-диск» был представлен в 1979 году на пресс-конференции компании Philips. Создание формата проводилось совместно с японской фирмой Sony. В 1980 г. был выпущен стандарт Red Book, который затем стал стандартом компакт-дисков. Максимальное время записей составляет 79,8 мин, минимальное время звуковой дорожки – 4 с, максимальное количество дорожек – 99 [8].

DVD-Audio – цифровой формат DVD, созданный специально для высококачественного воспроизведения звуковой информации [1].

Проект стандарта был представлен в январе 1998 г. (версия 0.9), а окончательная спецификация DVD-Audio 1.0 была утверждена в 1999 г. Запись на диске DVD-Audio может иметь от 1 до 6 звуковых каналов [1].

Формат DVD-Audio отличается от CD высоким качеством записи, многоканальностью, а также универсальностью. Однако для воспроизве-

дения данного формата необходимо обязательное наличие подключенного монитора или телевизора [2].

Формат Super Audio CD (SACD) появился в сентябре 1999 г. Данный формат обеспечивает высочайшее качество записи, полную защиту авторских прав, многоканальное воспроизведение записи, сохранность архивных записей от старения магнитных материалов и т. д.

Емкость SACD стала в 6 раз больше обычного CD (объем – 4,7 ГБ), а кроме звука на них можно записывать текст и изображения [4].

Магнитооптическая запись

Запись ведется при помощи лазерного луча и магнитной головки. Лазер разогревает участок диска на высокой мощности. Затем электромагнитный импульс изменяет намагниченность, создавая отпечатки (питы) на диске. Считывание происходит тем же лазером, но уже на меньшей мощности [9].

В настоящее время существует два формата магнитооптической записи: минидиск (MiniDisc) и Hi-MD.

Рис. 4. Логотипы форматов магнитооптической записи

Минидиск – магнитооптический носитель, используемый для хранения любой информации в виде цифровых данных. Наиболее широко данный формат используется для хранения аудиоинформации [3].

Одним из важнейших достоинств минидиска стала его компактность. Его размеры были меньше, чем обычный CD, однако один минидиск вмещает в себя до 80 мин записи.

Также минидиск имеет важные преимущества: высокую надёжность хранения записи (повышенная устойчивость к магнитным полям), быстрый доступ к любому фрагменту записи, а также возможность многократной записи и стирания информации [11].

Однако поддержка данного формата была свёрнута в 2008 г., т. к. минидиски не стали пользоваться популярностью.

Рис. 5. Минидиск фирмы Olympus

В 2004 г. компания Sony представила новую технологию записи – Hi-MD. Данная технология позволяет записать до 1 Гб данных, причем кроме звуковой информации записаны могут быть любые файлы: документы, изображения и т. д. Данный формат является продолжением технологии «MiniDisc» [5]. Музыкальные треки записываются на Hi-MD по технологии, которая обеспечивает защиту авторских прав.

Рис. 6. Минидиск формата Hi-MD фирмы Sony

В заключение отметим, что технологии и устройства на их основе быстро устаревают, и рассмотренные нами способы записи информации уже сменяются новыми.

Список используемых источников

1. DVD-Audio [Электронный ресурс] / Википедия – свободная энциклопедия: [сайт]. URL: https://ru.wikipedia.org/wiki/DVD-Audio (дата обращения 04.04.2016 г.)

2. DVD-Audio формат [Электронный ресурс] / Flacme.ru: [сайт]. URL: http://flacme.ru/index/0-5 (дата обращения 04.04.2016 г.)

3. MiniDisc [Электронный ресурс] / Википедия – свободная энциклопедия: [сайт]. URL: https://ru.wikipedia.org/wiki/MiniDisc (дата обращения 05.04.2016 г.)

4. SACD – идеальный формат звука [Электронный ресурс]. URL: http://www.videoton.ru/Articles/sacd.html (дата обращения 04.04.2016 г.)

5. Sony HI-MD: новый формат минидиска [Электронный ресурс] / Tom's Hardware: [сайт]. URL: http://www.thg.ru/business/20040622/index.html (дата обращения 07.04.2016 г.)

6. Вахитов Я. Ш. Слух и речь. Конспект лекций по курсу «Электроакустика» (раздел 2) / под ред. М. А. Неупокоевой. Л. : Типография № 12 им. М. И. Лоханкова «Союзполиграфпрома», 1973. 122 с.

7. Звук [Электронный ресурс] / Википедия – свободная энциклопедия: [сайт]. URL: https://ru.wikipedia.org/wiki/Звук (дата обращения 04.04.2016 г.)

8. Звуковой компакт-диск [Электронный ресурс] / Википедия – свободная энциклопедия: [сайт]. URL: https://ru.wikipedia.org/wiki/%D0%97%D0%B2% D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BA%D1%82-%D0%B4%D0%B8%D1%81%D0%BA (дата обращения 04.04.2016 г.)

9. История звукозаписи [Электронный ресурс] / Википедия – свободная энциклопедия: [сайт]. URL: https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1% 82%D0%BE%D1%80%D0%B8%D1%8F_%D0%B7%D0%B2%D1%83%D0%BA%D0%BE%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B8 (дата обращения 04.04.2016 г.)

10. Лазер [Электронный ресурс] / Энциклопедия по МАГНИТНОЙ ЗАПИСИ (от А до Я) : [сайт]. URL: http://www.tps-katyusha.ru/all/enc_09.html (дата обращения 04.04.2016 г.)

11. Рождение и смерть минидиска [Электронный ресурс] / Компьютерра: [сайт]. URL: http://www.computerra.ru/64950/rozhdenie-i-smert-minidiska/ (дата обращения 06.04.2016 г.)

12. Способы записи информации [Электронный ресурс] / Библиофонд, электронная библиотека студента: [сайт]. URL: http://bibliofond.ru/view.aspx?id=446463 (дата обращения 04.04.2016 г.)

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Тихоновой Л. С.

УДК 623.624

А. Д. Иванов (студент группы РК-41м, СПбГУТ)
Т. Ю. Ковалева (кандидат технических наук, доцент, СПбГУТ)

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ КОМПОЗИТНОГО МАТЕРИАЛА ДЛЯ АНТЕННЫХ УКРЫТИЙ

В работе рассмотрены результаты моделирования композитных материалов, предназначенных для элементов антенных обтекателей и укрытий, обеспечивающих пропускание и поглощение в определенных зонах конструкций антенных укрытий.

композитный радиопрозрачный материал, композитный радиопоглощающий материал, защитное покрытие, коэффициент прохождения, коэффициент отражения.

Антенные обтекатели или укрытия (АО, АУ), предназначенные для защиты РЛС от комплекса климатических и поражающих факторов, имеют обычно форму сферы или части сферы. Композитный радиопрозрачный материал (КРМ) АО или укрытия должен обладать свойством радиопрозрачности, обеспечивающим прохождение электромагнитной волны через материал обтекателя без потери электромагнитной энергии.

На дальность действия РЛС оказывают влияние и уровень боковых лепестков диаграммы направленности антенны, которые влияют на форму диаграммы направленности, возникновение ложного обнаружения и, соответственно, на дальность распространения зондирующего сигнала. По уровню боковых лепестков идет обнаружения радиолокационных систем. Снижение уровня боковых лепестков целесообразно осуществлять в комплексе мер защиты, включающих использование фильтров подавления боковых лепестков (ФПБЛ) и использованием поглощающих элементов в конструкциях антенных укрытий [1, 2].

Использование композитного радиопоглощающего материала в АУ или обтекателях вне зоны излучения антенных устройств является эффективным пассивным методом снижения уровня боковых лепестков.

Примерный (схематичный) вариант антенного обтекателя (АО) для базовых станций, представлен на рисунке 1, имеет форму сферы, при чем на часть сферы, вне зоны излучения (1) антенных устройств (3), может быть нанесено защитное покрытие или она может быть выполнена из КРМ (2).

Считается, что уровни ЭМП создаваемые базовыми станциями значительно ниже ПДУ и безопасны для населения. Однако, по мнению ряда ученых, ЭМП базовых станций могут вызвать неблагоприятные последствия для здоровья населения. В связи с вышесказанным, вне зоны излучения целесообразно использовать в конструкциях АО или антенных укрытий защитные радиопоглощающие покрытия или КРПМ, позволяющие снизить уровни электромагнитных полей (за счет боковых лепестков ДН) и, соответственно, снизить уровень воздействия на население.

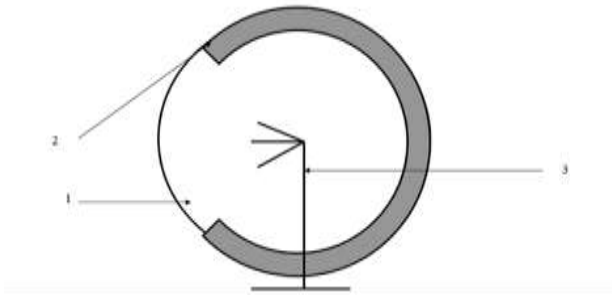


Рис. 1 Обтекатель антенн с защитным покрытием:
1 – стенка антенного обтекателя, *2* – защитное покрытие из КРПМ,
3 – антенное устройство

Радиопрозрачные материалы и изделия из них (РПИ) широко используются в антенных обтекателях самолетов и ракет в условиях аэродинамических и тепловых ударов, дождевой, пылевой, газовой эрозии, ионизирующих излучений, в качестве перегородки-окна в ускорителях и электронных приборах, для обеспечения передачи электромагнитной энергии [2].

Прозрачность этих материалов обеспечивается малыми диэлектрическими. потерями в заданном интервале рабочих температур (tgδ 10^{-2}–10^{-5}, $\varepsilon \leq 10$) и низким уровнем отражения радиоволн ($|\Gamma| \leq 1$ %). Основу таких материалов составляют органические и неорганические. диэлектрики-пластмассы, керамопласты, керамика, плавленый кварц.

Для передающих (приемо-передающих) антенн со слабонаправленной с круговой диаграммой направленности (ДН) в горизонтальной плоскости (рис. 2) целесообразно использовать тип антенного укрытия (АУ) схематично представленный на рисунке 3.

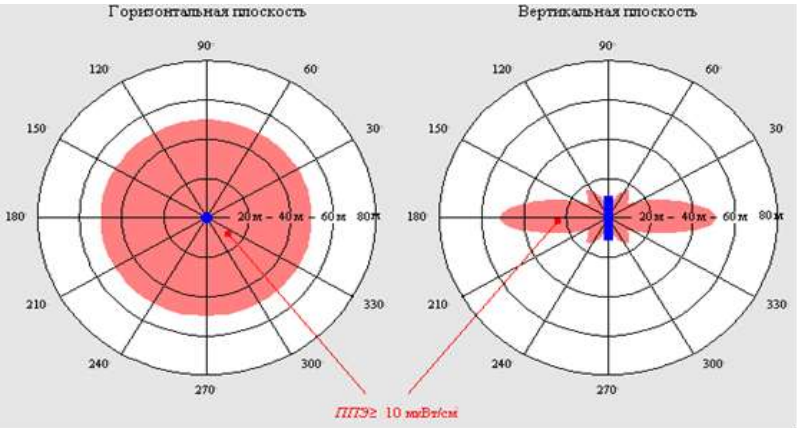


Рис. 2. Диаграмма направленности антенны типа

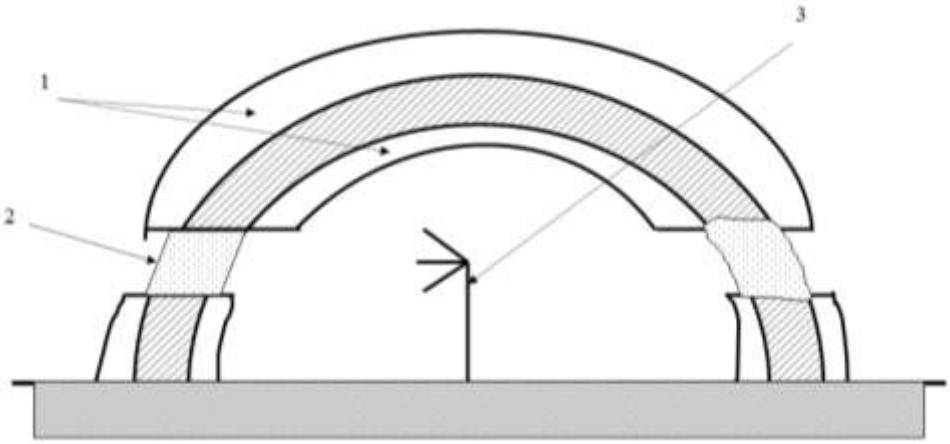


Рис. 3. Антенное укрытие с элементом КРПМ для наземных РЛС:
1 – КРПМ, *2* – окно прозрачности, *3* – антенное устройство

В результате моделирования структур КРМ и КРПМ был произведен расчета элементов антенных укрытий КРМ и КРПМ. Моделирование проводилось по электромагнитным параметрам материалов и по заданным пределам величин коэффициентов прохождения и коэффициентов отражения для рассматриваемых АУ [1, 3].

Эти коэффициенты связаны соотношением:

$$\left|T^2\right| + \left|\Gamma^2\right| = 1. \quad (1)$$

Анализ проводится через коэффициент отражения.

В общем случае коэффициент отражения является величиной комплексной и определяется как:

$$\Gamma = \left|\Gamma\right| e^{j\psi} = E_{\text{отр.}} / E_{\text{пад.}} = Z_0 - Z_{\text{вх.}} / Z_0 + Z_{\text{вх.}}, \quad (2)$$

где $|\Gamma|$ – модуль коэффициента отражения, ψ – фаза коэффициента отражения, E – амплитуда отраженной ЭМВ, Z_0 – волновое сопротивление (импеданс) свободного пространства, $Z_{\text{вх.}}$ – входной импеданс слоя материала.

Коэффициент прохождения слоя КРМ определяется через коэффициент ослабления:

$$T_1 = F_1(1 - r_1)(1 - r_{12})\,(1 + F_1^2 r_{11} r_{12}), \quad (3)$$

где r_1, r_{12} – коэффициенты Френеля.

Результаты расчеты коэффициентов отражения для КРМ и КРПМ представлены в таблицах 1, 2.

ТАБЛИЦА 1. Результаты расчета коэффициента отражения КРМ

№ образца	Коэффициент отражения Г, %			
	Длина волны λ, см			
	0,8	**2**	**3**	**10**
5	1,27	7	1,56	8,4
6	1,56	7	1,56	6,7
7	1,56	9,25	1,56	6,2
8	1,97	6,9	1,97	6,7
9	1,7	6,2	3,1	6,2
10	2,2	6,7	1,7	6,1
11	1,56	10,4	1,56	5,56

ТАБЛИЦА 2. Результаты расчета коэффициента отражения КРПМ

№ Вар.	Толщина РПМ, мм	Коэффициент отражения Г (%) для длин волн λ, см									
		1	2	3	4	5	6	7	8	9	10
1	1,8	3,4	5,0	2,3	3,5	6,0	5,9	6,5	7,0	8,5	9,8
2	1,9	3,1	5,4	2,5	3,6	5,0	5,8	5,7	6,9	8,3	9,8
3	2,0	3,0	5,0	1,8	3,0	4,9	6	4,9	6,5	8,0	9,2
4	2,1	3,4	5,4	4,0	4,1	4,9	5,9	6,0	6,8	7,9	9,1
5	2,2	3,1	5,3	4,4	4,5	5,1	6,0	6,1	6,7	7,8	8,9,

Способность материала поглощать электромагнитное излучение зависит от его состава и структуры и характеризуется лучшей поглощающей способностью при определенных диапазонах частот.

Список используемых источников

1. Ковалева Т. Ю., Ермаков А. В., Ковалева А. Г., Кирик Д. И., Иванов А. В. Селективные радиопоглощающие материалы // Сборник статей XXIV Всероссийской научно-технической конференции школы-семинара РАРАН. Москва, 2013 г. С. 272–287; С. 403–406.

2. Ковалева Т. Ю., Ермаков А. В., Иванов А. В. Результаты разработки селективных защитных материалов для подвижных объектов военной техники // Актуальные проблемы защиты и безопасности: труды XVI Всероссийская научно-практической конференции. Москва : РАРАН, 2014. Том 3. С. 379–385.

3. Ковалева Т. Ю., Ермаков А. В. Ковалева А. Г. Принципы моделирования и синтеза защитных покрытий промышленных объектов и объектов военной техники // Сборник статей XXII Всероссийской научно-технической конференции школы-семинара РАРАН. Москва : РАРАН. С. 262–264.

УДК 623.624

Т. Ю. Ковалева (кандидат технических наук, доцент, СПбГУТ)
Ю. И. Пустарнакова (студентка группы РК-51м, СПбГУТ)

ПОГЛОЩАЮЩИЕ МАТЕРИАЛЫ ДЛЯ СИСТЕМ СВЯЗИ

В работе представлены результаты разработки и исследования радиопоглощающих свойств защитных поглощающих материалов для радиоэлектронных систем и систем связи.

коэффициент отражения, магнитные и аэрированные диэлектрические наполнители, полимерная матрица.

В настоящее время все виды систем связи нуждаются в защите от влияния электромагнитного излучения. Одним из способов защиты данных систем является использование поглощающих материалов. Поглощающие материалы применяются в том случае, когда применение иных активных методов защиты нецелесообразно или невозможно.

При выборе поглощающего материала обязательно надо учитывать требуемый уровень поглощения электромагнитного излучения в определенном диапазоне частот, минимальный уровень отражения и места их расположения в технической системе связи [1]. Для определенного диапазона частот требуется определенный материал, позволяющий снизить уровень электромагнитного излучения до заданного значения. Если в разных диапазонах частот используется один тип материала, то в этом случае имеется возможность изменения толщины поглощающего материала, обеспечивающий необходимый уровень поглощения.

Поглощающие материалы состоят из неметаллической (чаще всего, полимерной) матрицы и наполнителей различных типов (например, мелкодисперсные, порошкообразные наполнители).

Были исследованы характеристики ряда материалов, состоящих из разных полимерных матриц и различных типов наполнителей (табл. 1).

ТАБЛИЦА 1. Модельные образцы композитных материалов для измерения коэффициентов отражения

№ модельного образца	**Наименование модельного образца**	**Толщина модельного образца *d*, мм**
1	Композитный материал на основе дисперсных магнитных наполнителей эпоксидной полимерной матрицы	3–3,5
2	Композитный материал на основе магнитных наполнителей и водоэмульсионной полимерной матрицы	2–3
3	Композитный материал на основе проводящих наполнителей и полиорганосилоксановой полимерной матрицы	3,5–4
4	Композитный материал на основе проводящих и аэрированных диэлектрических наполнителей и эпоксидной полимерной матрицы	3,3–3,9

Расчет коэффициента отражения осуществлялся в соответствии с формулой:

$$R_{otr} = R_0 + X_0^2 \cdot e^{i \cdot |k| \cdot 2 \cdot d},$$

где R_{otr} – полный коэффициент отражения электромагнитной волны от композиционного материала со слоистой структурой, безразмерная

комплексная величина; R_o – коэффициент отражения электромагнитной волны от границы «воздух–радиопоглощающее покрытие», безразмерная комплексная величина; k – волновое число, параметр электромагнитной волны, характеризующей распространение волны в среде, комплексная величина.

Результаты расчета коэффициента отражения по измеренным электромагнитным параметрам представлены в таблице 2.

ТАБЛИЦА 2. Таблица полученных расчетов радиофизических свойств поглощающего материала

№ расчета	Длина волны λ, см	Толщина экран *d*, мм	Коэффициент отражения *R*, %
1	2	0,5	2,6
2		1,0	3,2
3		1,5	8,1
4		2,0	9,7
5		2,5	7,6
6	3	0,5	4,3
7		1,0	6,3
8		1,5	9,4
9		2,0	8,4
10		2,5	2,5
11	5	0,5	1,3
12		1,0	8,5
13		1,5	9,2
14		2,0	5,1
15		2,5	3,1
16	8	0,5	4,2
17		1,0	5,9
18		1,5	9,7
19		2,0	9,8
20		2,5	5,9
21	10	0,5	3,6
22		1,0	5,5
23		1,5	9,6
24		2,0	9,7
30		2,5	7,1

Измерения диэлектрической и магнитной проницаемостей проводились на панорамных измерителях КСВ стандартными методами короткого замыкания и холостого хода. Результаты измерений коэффициента отражения по измеренным электромагнитным параметрам представлены в таблице 3.

ТАБЛИЦА 3. Результаты измерений коэффициента отражения модельных образцов

№ модельного образца	**Наименование модельного образца**	**Толщина модельного образца *d*, мм**	**Длина волны λ, см**	**Коэффициент отражения, %**
1	Композитный материал на основе дисперсных магнитных наполнителей эпоксидной полимерной матрицы	4	0,8	8,2
			2	11,0
			3,2	6,1
			5,6	9,1
			10,3	9,8
2	Композитный материал на основе магнитных наполнителей и водоэмульсионной полимерной матрицы	3	0,8	7,4
			2	10,5
			3,2	5,5
			5,6	6,6
			10,3	9,8
3	Композитный материал на основе проводящих наполнителей и полиорганосилоксановой полимерной матрицы	4	0,8	9,0
			2	11,9
			3,2	5,6
			5,6	6,1
			10,3	10,8
4	Композитный материал на основе проводящих и аэрированных диэлектрических наполнителей и эпоксидной полимерной матрицы	4	0,8	7,8
			2	10,8
			3,2	4,6
			5,6	9,7
			10,3	9,5

По результатам проведенного исследования следует, что сходимость результатов расчета и измерений коэффициента отражения составляет более 85 %.

Список используемых источников

1. Бабаевский П. Г., Виноградов В. М., Головкин Г. С., Гуняев Г. М., Кобец Л. П., Машинская Г. П., Тюкаев В. Н. Пластики конструкционного назначения / под ред. Е. Б. Тростянской. М. : Химия, 1974. 304 с.

УДК 681.3.06

В. Н. Коваленко (студент группы ИКТ-403, СПбГУТ)

МОДЕЛИРОВАНИЕ СОЛНЕЧНОЙ СИСТЕМЫ В MATLAB

В работе выполняется моделирование Солнечной системы в MATLAB. Приводится алгоритм работы написанной программы. Размеры планет, скорости их вращения, а также движение по орбите задаются по отношению к размерам, скорости вращения и орбите планеты Земля. Размеры Солнца были уменьшены. Демонстрируется моделирование системы в динамическом режиме. Приводятся функции для создания вращения вокруг своей оси и по заданной орбите.

MATLAB, function-файл, Солнечная система, полигональные объекты, матрица поворота и движения.

MATLAB – язык высокого уровня и интерактивная среда для программирования, численных расчетов и визуального представления результатов [1, 2]. С помощью MATLAB можно создавать модели реальных объектов.

Задачей данной работы было создание модели движения планет вокруг Солнца по разным орбитам и с разными скоростями, а также их вращения вокруг своей оси.

Создание программы выполняется в виде function-файл с названием SolarS. Function-файлом называют создаваемый пользователем М-файл, представляющий собой внешнюю функцию [3]. Начало описания function-файла:

```
function [ output_args ] = SolarS2( input_args )
```

Первым шагом необходимым для моделирования Солнечной системы будет создание черного фона (рис. 1). Используется функция figure:

```
figure('color','black'))
```

Рис. 1. Создание фона
Солнечной системы

Для создания объектов необходимо задать их оси:

ax=axes('Xlim',[−20 20],'Ylim',[-20 20],'Zlim',[−20 20]);)

Моделирование Солнца и планет будет происходить на основе модели сферы, изменяться будут только размеры по осям *x*, *y*, *z*. Задаются точки сферы:

t1=pi*(−10:1:10)/10; t2=(pi/2)*(−10:1:10)'/10;)

Следующий шаг – создание осей сферы используя коэффициенты для построения точек, синусы и косинусы, а также единичной матрицы, необходимой при построении оси *z*:

g=ones(size(t1)); – единичная матрица размером коэффициента *t*1
X=cos(t2)*cos(t1); Y=cos(t2)*sin(t1); Z=sin(t2)*g;

Моделирование Солнца и планет происходит с использованием функции plot3 (рис. 2). Размеры объектов задают коэффициенты перед осями. В круглых скобках – относительные размеры планет по отношению к Земле. Для того чтобы модель Солнечной системы была не слишком большой, вводятся дополнительные коэффициенты для размеров планет (1/4), а также значительно уменьшены размеры Солнца, так как оно в десятки раз больше планет Солнечной системы:

Sun=plot3(6/4*X, 6/4*Y, 6/4*Z,'y')
planet1=plot3((0.38)/4*X, (0.38)/4*Y, (0.38)/4*Z,'r'))

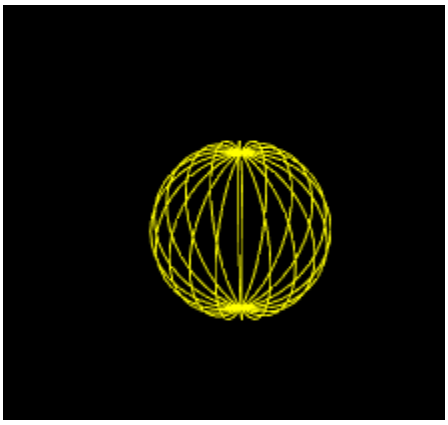


Рис. 2. Создание модели Солнца

Вывод всех объектов в одном окне осуществляется с помощью функции hold on.

Далее необходимо задать размеры графика – функция axis([−140 140 −140 140 −140 140]), где значение в скобках задают границы по осям *x*, *y*, *z*. Функция axis off – снимает обозначение осей [4], при этом все фигуры будут отображаться вместе с фоном нашей программы (рис. 3), иначе фон программы и фон для отображения объектов не будет совпадать (рис. 4).

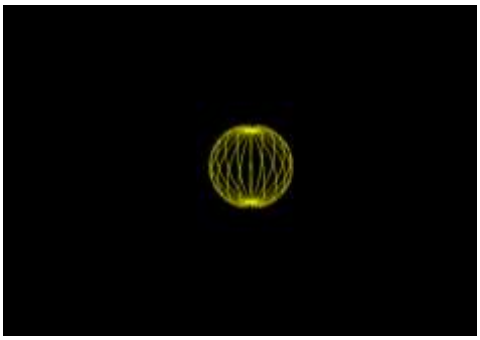


Рис. 3. Вывод объектов
с использованием axis off

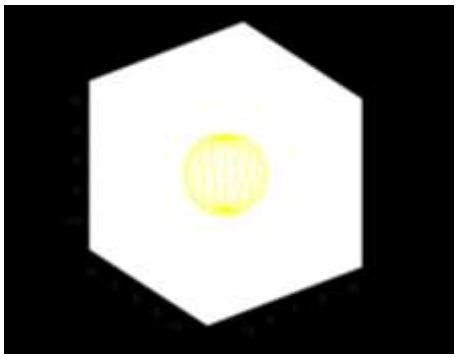


Рис. 4. Вывод объектов
без использования axis off

Для создания динамической модели необходимо создать полигональные объекты. Используются функции hgtransform, set:

```
p1=hgtransform('Parent',ax)
set (planet1,'Parent',p1)
```

Потом задаем цикл for для моделирования вращения планет и Солнца:

```
for t=0:1:17200
```

Переменная *t* задает длительность моделирования. Первое число используется для задания точки, с которой происходит начало моделирование (рис. 5 и 6).

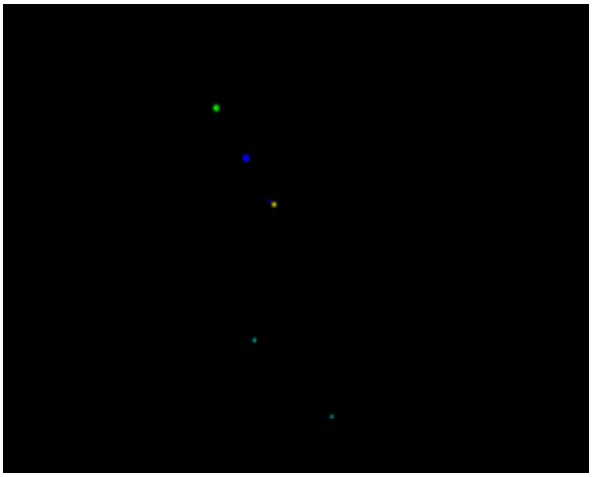


Рис. 5. Начало моделирования
с положения −100

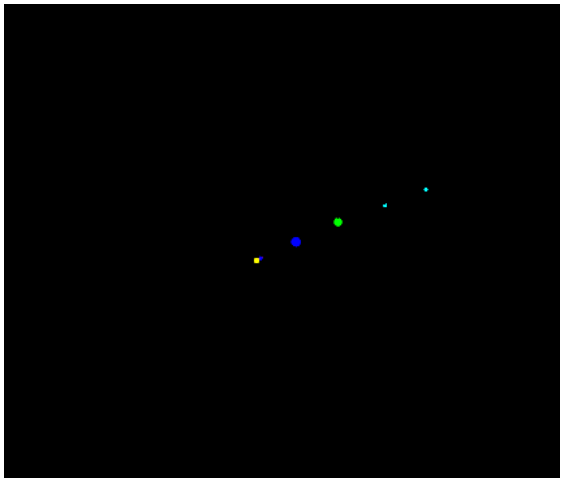


Рис. 6. Начало моделирования
с положения 0

Последним шагом будет задание матрицы поворота вокруг своей оси для Солнца и матрицы движения для планет в цикле for, 'zrotate' – поворот объектов вокруг своей оси, 'translate' – изменение положения объектов в пространстве

```
Mzr1=makehgtform('zrotate', deg2rad((−1/58.6)*t))
Mtr1=makehgtform('translate',[3.5*(0.38)*(cos(pi/30*t*1.61))
3.5*(0.38)*(sin(pi/30*t*1.61)) 3.5*(0.38)*(sin(pi/30*t*1.61))])
M1=Mtr1*Mzr1;
set(p1, 'Matrix',M1)
```

Значения в круглых скобках в функции изменения положения объектов – отношения орбит планет к орбите Земли, коэффициенты в функциях синуса и косинуса задают скорость вращения планет по орбите. Значение в скобках функции deg2rad задает скорость вращения планет и Солнца вокруг своей оси.

Матрица M1 объединяет функции вращения объектов и изменения положения. При этом M1 = Mtr1*Mzr1 и M1 = Mzr1* Mtr1 будут иметь разный результат.

Список используемых источников

1. MATLAB – высокоуровневый язык программирования [Электронный ресурс]. – Режим доступа: MATLAB.RU/PRODUCTS/MATLAB.

2. Степанов А. Б., Матиящук Д. К. Моделирование нейронной сети с произвольной функцией активации в MATLAB // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сб. ст. II-й международной научно-технической и научно-методической конференции, Санкт-Петербург 27–28 февраля 2013. – СПб. : СПбГУТ, 2013. С. 351–353.

3. Солонина А. И., Клинский Д. М., Меркурий Т. В, Персов С. Н. Цифровая обработка сигнала и MATLAB. СПб. : БХВ-Петербург, 2013. – 512 с.

4. Потемкин В. Г. Справочник по MATLAB [Электронный ресурс] // Графические команды и функции. URL: http://matlab.exponenta.ru/ml/book2/ chapter10/axis.php

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Степановым А. Б.

УДК 532.13

Н. А. Покровский (студент группы РК-21, СПбГУТ)

РАЗРАБОТКА ПОРТАТИВНОГО РОТАЦИОННОГО ВИСКОЗИМЕТРА

В условиях импортозамещения одной из важнейших задач становится развитие отечественного рынка измерительных приборов. Статья посвящена вопросам измерения вязкости в полевых условиях и созданию портативного прибора простого в использовании и экономически выгодного в производстве. В статье рассмотрен новый подход к приборам данного типа, а именно способ измерения вязкости.

ротационный вискозиметр, вязкость, измерение вязкости, вискозиметрия, реология.

На сегодняшний день одним из самых распространённых способов определения вязкости жидкости в промышленности и медицине является ротационный метод определения вязкости. Устройства данного класса на рынке представлены иностранными производителями (AND, Brookfield, Visco) и не имеют портативных аналогов для быстрого анализа образцов на месте взятия пробы. В условиях импортозамещения, одной из важнейших задач становится разработка простого в использовании и дешевого в производстве ротационного вискозиметра, способного измерять малые по объёму образцы жидкости (3–10 мл) и оперативно выдать результат.

Ещё одной из предпосылок к созданию портативного вискозиметра явилось то, что в последнее время в широкой медицинской практике возрастает интерес к экспресс анализу вязкости человеческой крови. Ведь при тяжёлых физических нагрузках и инфекционных заболеваниях происходит увеличение вязкости крови, а брюшной тиф и туберкулёз уменьшают её. Изменение вязкости крови сказывается на реакции оседания эритроцитов, что может свидетельствовать о протекании воспалительного процесса в организме [1].

Анализ вязкости крови вместе с другими анализами позволяет объективно оценить физическое состояние человека [1]. Это подразумевает под собой необходимость разработки портативного ротационного вискозиметра, удобного в применении и доступного по своим габаритам и техническим характеристикам для использования обычным пользователем, не обладающим специальными техническим и медицинским образованием.

Целью данного проекта являлось разработка портативного ротационного вискозиметра, способного измерять при небольших объёмах жидкости значение вязкости и обладающий конкурентными техническими, и экономическими параметрами.

Проект основывается на классических уравнениях гидродинамики и уравнениях, описывающих процессы, протекающие в электроприводе

постоянного тока. На основе теоретических выкладок была выведена формула для расчёта вязкости жидкости с использованием двигателя постоянного тока (1) [2, 3, 4, 5].

$$\eta = \frac{k \cdot \Phi \cdot \left(I_{н} - I_{хх}\right)}{44 \cdot \pi \cdot R_1^{\,2} \cdot \omega_1}, \qquad (1)$$

где k – это конструктивный параметр конкретного электродвигателя; Ф – суммарный магнитный поток; $I_н$ – ток нагрузки; $I_{хх}$ – ток холостого хода; R_1 – радиус измерительного шпинделя; ω – скорость вращения измерительного шпинделя, об/мин.

Разработанный прибор работает по следующей схеме (рис. 1):

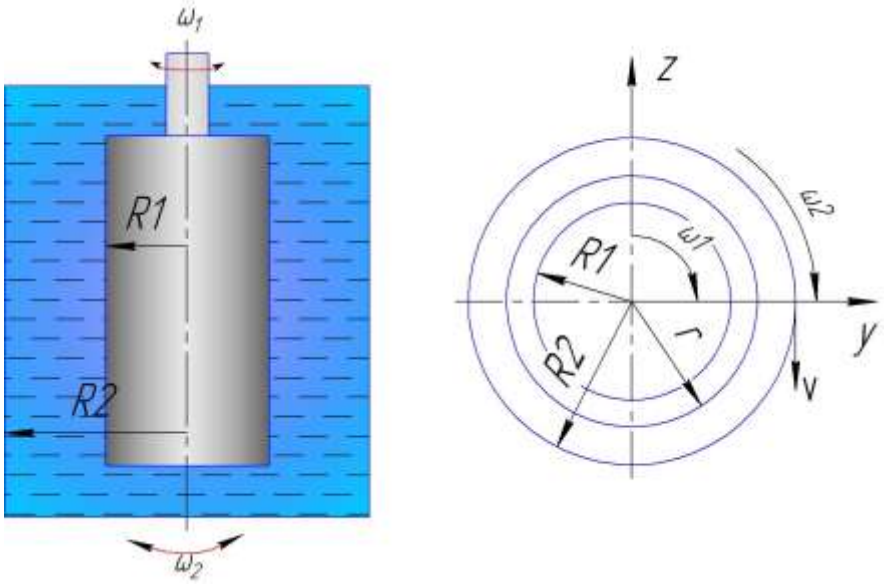


Рис. 1. Модель разработанного метода

В цилиндрический стакан наливают исследуемую жидкость, запускают электродвигатель постоянного тока и измеряют показания тока нагрузки на электродвигателе при вращении измерительного вала в исследуемой жидкости. Последующая стадия обработка результата на микроконтроллере и пересчёт полученного значения тока в значение коэффициента вязкости жидкости по формуле (1).

Разработанные и изготовленные по конструкторской документации измерительные шпиндели позволяют точно измерять при небольших объёмах жидкости коэффициент вязкости (рис. 2).

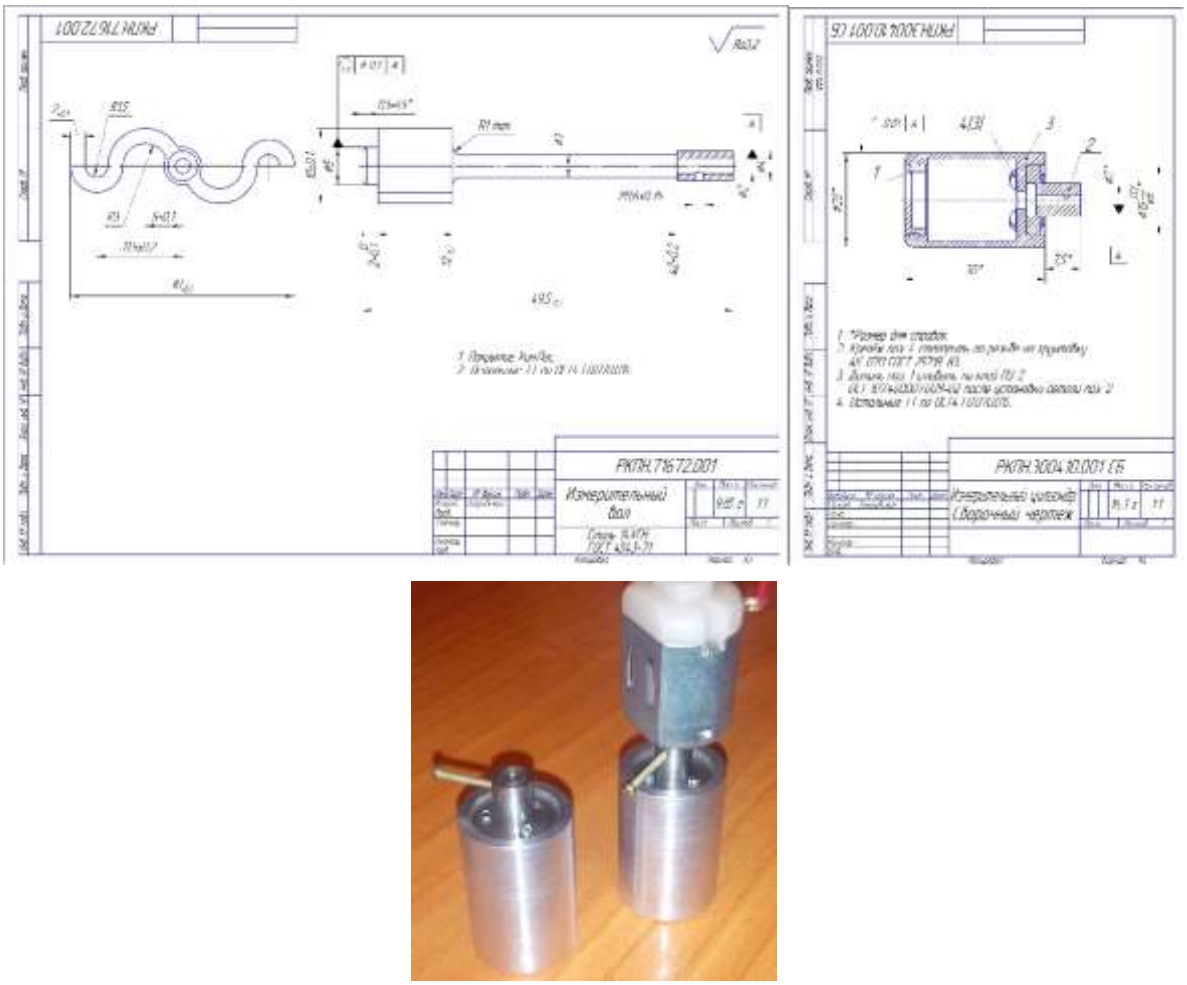


Рис. 2. Эскизы деталей и реальный образец

Спроектированная плата устройства обладает малыми габаритами (40×50 мм), что позволяет создать эргономичный корпус удобный для использования в полевых условиях (рис. 3).

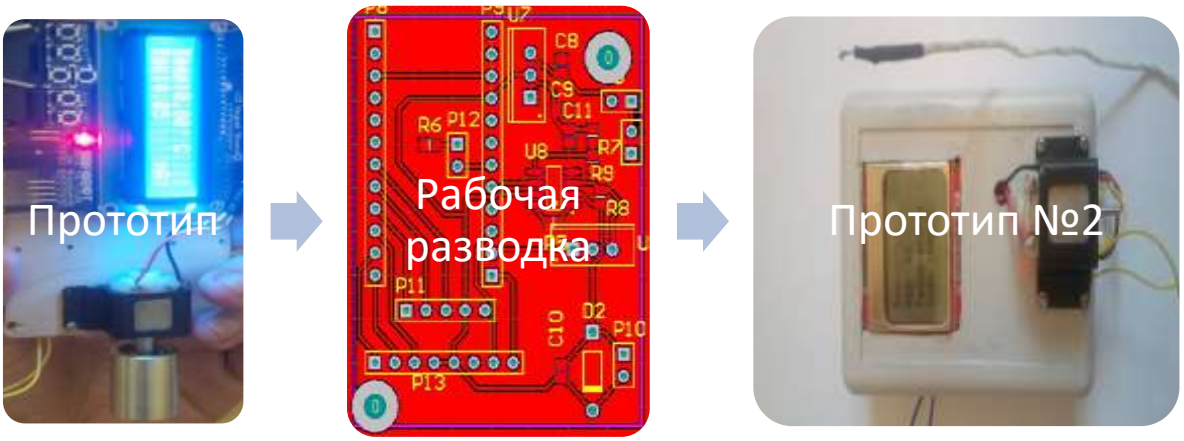


Рис. 3. Процесс разработки схемы устройства

С помощью рабочих прототипов были проведенны исследования зависимости вязкости жидкости от тока (рис. 4). Зависимость вязкости

жидкости от температуры и сравнение полученных значений вязкости разработанным прибором с табличными значениями (рис. 5) [4, 5].

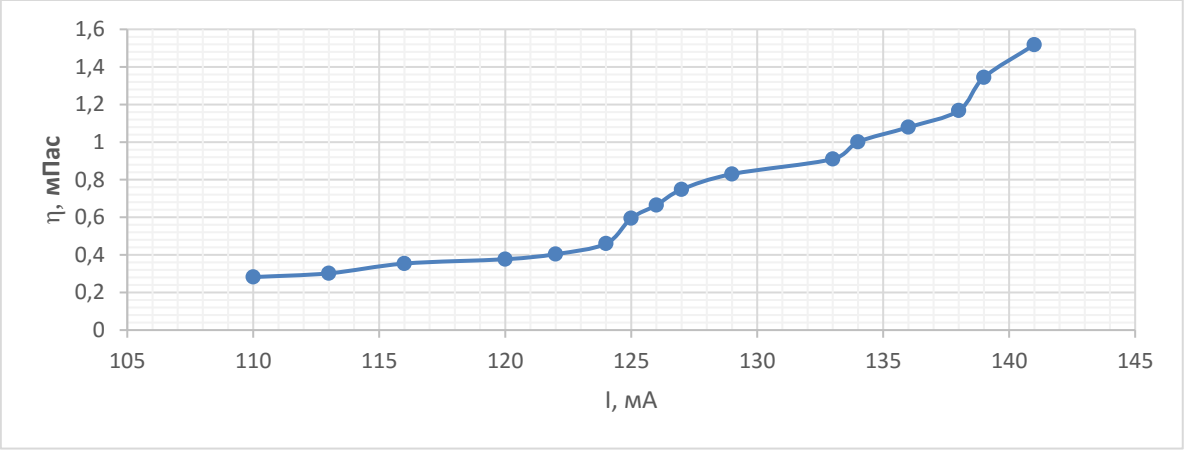


Рис. 4. Зависимость тока от вязкости жидкости (вода)

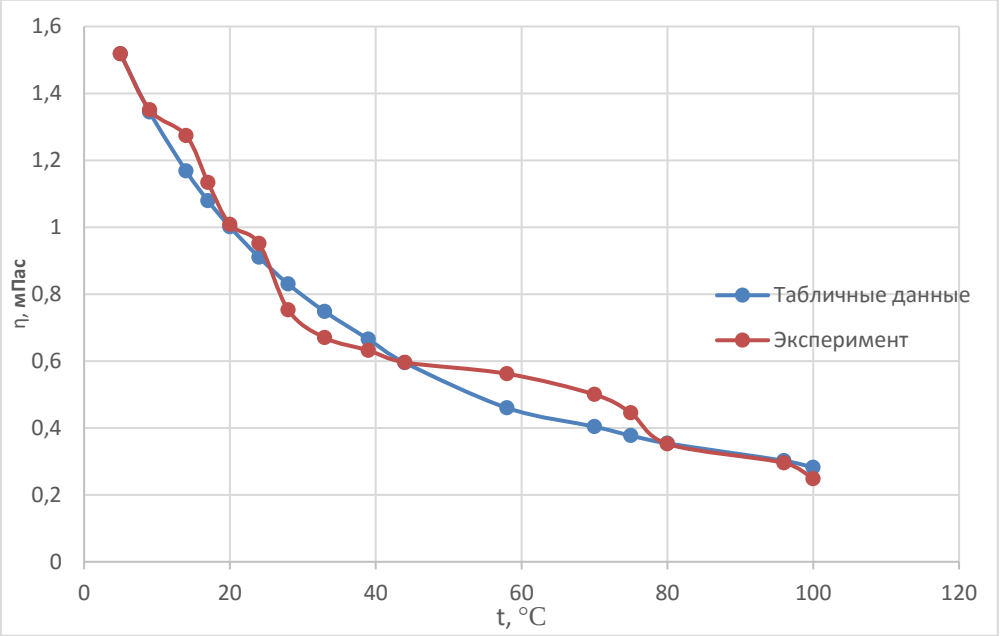


Рис. 5. Зависимость вязкости жидкости (вода) от температуры

Таким образом был спроектирован и реализован портативный в использовании прибор, с низким энергопотреблением и высокой точностью отображения приходящего сигнала. Данный прибор соответствует качественным требованиям, предъявляемым к классу подобных устройств, а также обладает достаточно низкой себестоимостью компонентов, что делает его конкурентоспособным.

В дальнейшем возможно улучшение характеристик прибора за счёт использования калиброванных электродвигателей и сопротивлений для получения высокой точности измерения вязкости.

Список используемых источников

1. Holsworth R. E., Cho Y. I. “Hyperviscosity Syndrome: A Nutritionally-Modifiable Cardiovascular Risk Factor.” Advancing Medicine with Food and Nutrients, Second Edition. Ed. Ingrid Kohlstadt. Boca Raton: CRC Press. 2012.
2. Валландер С. В. Лекции по гидроаэромеханике. Л. : Изд. ЛГУ, 1978. 296 с.
3. Чиликин М. Г., Сандлер А. С. Общий курс электропривода: учебник для вузов. 6-е изд, доп. и перераб. М. : Энергоиздат, 1981. 576 с.
4. Viscosity of Liquids: Theory, Estimation, Experiment, and Data. Dabir S. Viswanath, Tushar K. Ghosh, Dasika H. L. Prasad, Nidamarty V.K. Dutt, Kalipatnapu Y. Rani (auth.), Springer, 2007.
5. Таблицы физических величин : справочник / под ред. академика И. К. Кикоина. М. : Атомиздат, 1976. 1008 с.

Статья представлена научным руководителем,
кандидатом технических наук Уссом В. С.

УДК 534.842

А. И. Стеценко (студент группы РЦТ-22, СПбГУТ)

АКУСТИЧЕСКАЯ ОБРАБОТКА ПОМЕЩЕНИЯ ЭФИРНОЙ СТУДИИ РАДИОВЕЩАНИЯ РАДИОСТАНЦИИ «ЭХО МОСКВЫ» В САНКТ-ПЕТЕРБУРГЕ

Статья посвящена акустическим мероприятиям по коррекции акустики для эфирной студии. Целью проекта является оценка акустических условий и их улучшения для обеспечения помещений оптимальными акустическими характеристиками и параметрами. В студиях должны быть обеспечены все акустические характеристики: оптимальное время реверберации в разных частотных диапазонах, однородная структура звукового поля (время, энергия и направление прихода ранних отражений, степень диффузности, уровни энергии поздних отражений, структура распределения резонансов и т. д.), требуемый уровень шумов, а также другие объективные параметры, которые важны для слухового восприятия музыкальных и речевых программ.

речевая студия, акустика помещений, акустический расчет, время реверберации.

В общем комплекте электроакустического оборудования каналов звукового вещания студийные сооружения занимают особое место. Это объясняется тем, что, являясь первым звеном вещательного тракта, они в значительной мере определяют качество звучания передач в целом.

Основной величиной, характеризующей акустическое качество помещения, его пригодность для обеспечения хорошей слышимости речи или полноценного звучания музыки, является, как известно, время реверберации.

Опыт показывает, что существует оптимальное время реверберации, при котором звучание в закрытом помещении оказывается наилучшим с точки зрения слухового восприятия.

Оптимальное время реверберации в речевой студии должно быть небольшим, чтобы при быстром чередовании слогов каждый последующий слог был хорошо различим на фоне предыдущего.

Для обеспечения оптимальных акустических условий в помещении, согласно его функциональному назначению производится акустическая отделка студии.

Она включает в себя набор различных материалов, элементов и их комбинаций, применяемых при обработке студии, необходимых для создания требуемых характеристик звукового поля.

В данной работе разработаны акустические мероприятия по коррекции акустики в эфирной студии радиовещания радиостанции «Эхо Москвы» в Санкт-Петербурге для того, чтобы привести акустические параметры помещения к нормативным значениям. На рисунке 1 представлено помещение до акустической обработки.

Рис. 1. Помещение до акустической обработки

На рисунке 2 представлен план помещений аппаратно-студийного комплекса. Размеры пола помещения составляют 6×3,3 м. Высота потолка составляет 3,5 м. Общая площадь поверхностей помещения 104,7 м^2. Площадь пола 19,3 м^2. Объем помещения эфирной составляет примерно 69,3 м^3.

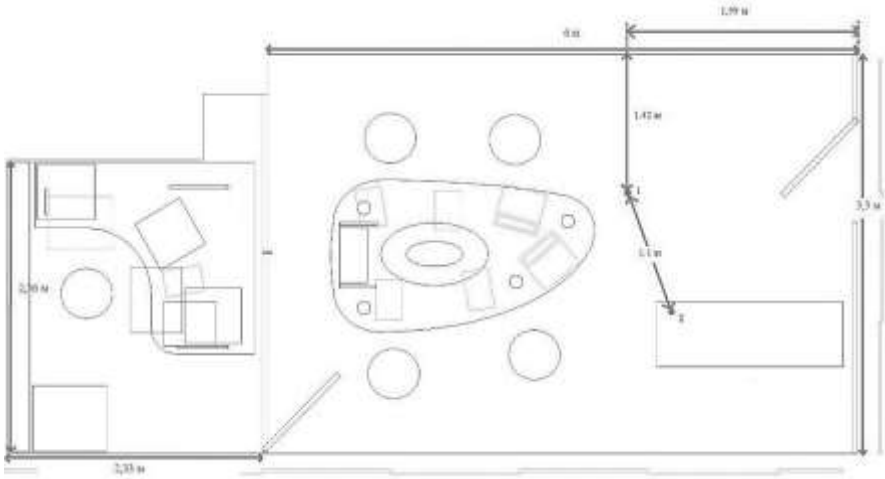


Рис. 2. План помещения АСК:
1 – измерительный микрофон, *2* – источник звука

Согласно ГОСТу 24146-89 «Метод измерения времени реверберации», были проведены измерения времени реверберации до акустической обработки помещения. Измерения проводились в полосах со средними геометрическими частотами от 125 до 4 000 Гц [1]. Расстояние от источника звука до измерительного микрофона равно радиусу гулкости помещения, который представляет из себя такое расстояние от центра источника звука, для которого уровень прямого звука равен уровню отраженного звука.

На рисунке 3 представлена блок-схема аппаратуры для измерения времен реверберации.

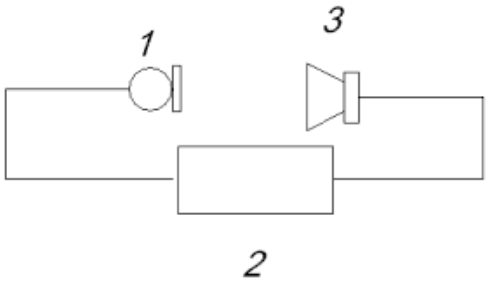


Рис. 3. Блок-схема аппаратуры для измерения времени реверберации:
1 – измерительный микрофон «Bayerdynamic MM1»,
2 – измерительная станция «Terrasonde ATB Audio Toolbox»,
3 – источник звука (громкоговоритель «Behringer Truth B2031»)

В качестве сигнала был использован белый шум. Белый шум – стационарный шум, спектральные составляющие которого равномерно распределены по всему диапазону задействованных частот. Согласно ГОСТу, измерения нужно проводить не менее, чем в трех точках помещения, помещения, однако, в связи с высокой загруженностью обрабатываемой эфирной студии радиовещания и сжатыми сроками выполнения работы, измерения были проведены только в одной контрольной точке. Располо-

жение контрольной точки соответствовало местоположению микрофона ведущего.

Согласно рекомендациям, среднее значение требуемого времени реверберации для малых речевых студий должно составлять около 0,35 с [2] (серая пунктирная кривая на рисунке 4).

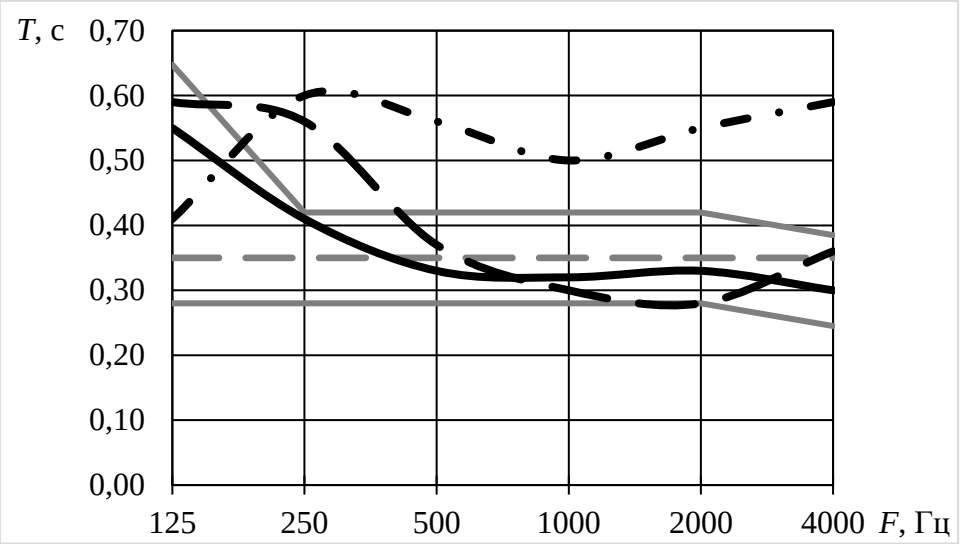


Рис. 4. Частотная зависимость времени реверберации

Результаты измерения частотной зависимости времени реверберации до акустической обработки студии представлены в таблице 1 и на рисунке 4 (черная штрих-пунктирная кривая).

ТАБЛИЦА 1. Частотная зависимость времени реверберации

F, Гц	125	250	500	1000	2000	4000
T, с до обработки (эксп.)	0,41	0,60	0,56	0,50	0,55	0,59
T, с после обработки (теор.)	0,55	0,41	0,33	0,32	0,33	0,30
T, с после обработки (эксп.)	0,59	0,56	0,37	0,30	0,28	0,36

Рекомендуемые допустимые пределы отклонения требуемого времени реверберации от среднего значения изображены на рисунке 4 серыми сплошными линиями. Подъём на низких частотах придает голосу «теплоту», при этом не снижая разборчивости речи [2].

Как видно, частотная зависимость времени реверберации, полученная до акустической обработки помещения, отличается от оптимальной почти во всем частотном диапазоне. Требуемое дополнительное звукопоглощение должно быть обеспечено во всех полосах частотного диапазона. В большей степени необходимо внесение материалов, имеющих эффективное поглощение на средних и высоких частотах.

Для решения задачи акустической обработки были проведены расчеты для определения количества единиц звукопоглощения в помещении. Для получения требуемой частотной зависимости времени реверберации были добавлены специальные акустические материалы, которые подбирались по нескольким критериям: акустические характеристики звукопоглощения, наличие сертификатов РФ, внешний вид, устойчивость к разрушению, удобство монтажа, стоимость единицы изделия, наличие на складе, быстрота поставки материалов на объект.

Список использованных звукопоглощающих материалов [3, 4]:

– «Heradesign Superfine» с заполнением мин. плитой «Шуманет-БМ»; площадь, занимаемая материалом S_1 = 10,8 м^2;

– «ЭхоКор» 20/600; площадь, занимаемая материалом S_2 = 5,4 м^2;

– «ЭхоКор» 50/600; площадь, занимаемая материалом S_3 = 5,4 м^2.

Результаты расчета времени реверберации приведены в таблице 1 и на рисунке 4 (черная сплошная кривая). Выбор элементов звукопоглощающей обработки эфирной студии, в целом, удовлетворяют нормативным требованиям по акустическим условиям звукопередачи.

Выбранные в результате расчета звукопоглощающие материалы были размещены в обрабатываемой студии. Результат размещения материалов представлен на рисунке 5.

После завершения монтажа были проведены повторные измерения времени реверберации согласно методике, описанной ранее. Полученные результаты, представлены в таблице 1 и на рисунке 4 (черная пунктирная кривая). Они вписываются в допустимые пределы отклонения частотной зависимости времени реверберации.

Рис. 5. Помещение после акустической обработки

Небольшие отличия результатов измерений от результатов теоретического расчета объясняются тем, что формальное соответствие расчётных

данных нормативным или заданным значениям акустических параметров ещё не гарантирует, а больше прогнозирует правильность выбранного решения и порядок величин, поскольку требуемые условия в помещении в большей степени обеспечиваются технологией размещения, монтажа и действительными по месту акустическими свойствами выбранных звукопоглощающих материалов и конструкций.

В целом, поставленная в рамках работы задача акустической обработки эфирной студии радиовещания радиостанции «Эхо Москвы» была выполнена успешно. Заказчик остался доволен результатом работы.

Список используемых источников

1. ГОСТ 24146-89. Метод измерения времени реверберации. М.: Издательство стандартов, 1989.
2. Walker, R. Acoustic criteria and specification. BBC Research and Development White Paper No. WHP 021, January 2002.
3. Heradesign: [сайт]. URL: http://www.heradesign.com (дата обращения 20.04.2016)
4. ЭхоКор: [сайт]. URL: http://echocor.ru (дата обращения 22.04.2016).

Статья представлена научным руководителем,
ассистентом Свиньиной О. А.

УДК 621.391.825

Э. Н. Сунгатуллин (аспирант, СПбГУТ)
В. М. Устименко (кандидат технических наук, профессор, СПбГУТ)

ФОРМИРОВАНИЕ ШИРОКОПОЛОСНЫХ ПОМЕХ

Широкополосные заградительные помехи в нисходящем канале (от базовой станции к мобильной) используются для обеспечения защиты от утечек информации по всем каналам сетей беспроводной мобильной радиосвязи. В докладе рассмотрен вариант цифрового формирования таких помех, более оптимальный по сравнению с аналоговым. При этом дальность блокирования связи зависит от расстояния до ближайшей базовой станции.

постановщик помех, мобильная радиосвязь, частотно-манипулированная шумовая (ЧМШ) помеха, 3G, цифро-аналоговый преобразователь (ЦАП), псевдослучайная последовательность (ПСП), управляемый напряжением генератор (ГУН).

При нынешнем широком распространении систем радиосвязи применение радиопомех чрезвычайно актуально в задачах радиоэлектронной борьбы (РЭБ). В коммерческих системах связи возможна несанкционированная утечка информации. Блокирование радиоканалов этих систем поз-

воляет предотвратить эту утечку или нежелательное использование систем связи в конкретных помещениях, зданиях или зонах местности.

Во многих случаях априорных данных о радиоканалах, частотах и сигналах, подлежащих блокированию, недостаточно, поэтому обычно подавлению подвергается весь диапазон радиочастот, в котором возможна работа радиолинии передачи информации или системы связи, т. е. используются *заградительные* по частоте помехи [1]. В противоположных случаях применяют *прицельные* (узкополосные) по частоте помехи.

Непрерывные шумовые помехи являются наиболее универсальными, так как обеспечивают принципиальную возможность маскировки полезных сигналов любой структуры и формы на временной и частотной оси, а также по направлению [2]. В зависимости от способа формирования непрерывные шумовые помехи подразделяются на *прямошумовые* (немодулированные), которые образуются в результате усиления собственных шумов, возникающих в электронных приборах (электровакуумных лампах, полупроводниковых диодах и транзисторах), и *модулированные*. *Прямошумовые* помехи не получили широкого применения из-за сравнительно низкой мощности источников первичного шума, необходимости его последующего многоступенчатого усиления и трудности сохранения высоких энтропийных свойств.

Модулированные формируются путём модуляции высокочастотных гармонических колебаний низкочастотным шумом по амплитуде (АМШ), частоте (ЧМШ), фазе (ФМШ) или одновременно по нескольким параметрам.

Для подавления связи необходимо выполнение условия (1) превышения отношения помеха/сигнал над коэффициентом подавления K_n на входе приемника мобильной станции (МС):

$$\frac{Pn}{Pc} > Kn, \qquad (1)$$

где Pn и Pn – мощности помехи и сигнала на входе приемника блокируемой системы соответственно [3].

Постановка такой помехи приводит к срыву управления мобильного телефона базовой станцией мобильной связи (происходит потеря сети мобильным телефоном) и, следовательно, к невозможности передачи информации. При этом на экране телефона значок уровня сигнала пропадает и появляется сообщение «Поиск сети».

Ранее [4] был рассмотрен способ формирования широкополосной заградительной помехи (рис. 1).

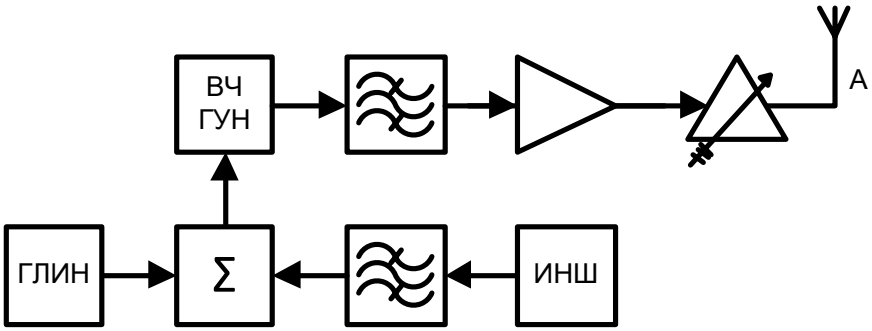


Рис. 1. Схема блокиратора стандарта связи UMTS2100
с широкополосной помехой с шумовой частотной модуляцией (ЧМШ)

Здесь с целью повышения эффективности помехового сигнала используется модуляция полосовым белым гауссовским шумом (БГШ) по частоте высокочастотного сигнала.

Генератор помех включает: высокочастотный генератор (ГВЧ) на базе генератора, управляемого напряжением, (ГУН); генератор линейно изменяющегося (пилообразного) напряжения (ГЛИН); источник низкочастотного шума (ИНШ); полосовой фильтр; усилитель мощности; согласующее устройство и антенну.

Для обеспечения требуемой эффективности работы блокиратора скорость изменения управляющего пилообразного напряжения должна быть довольно высокой. Например, у блокиратора связи в стандарте 3G UMTS2100 подобранный экспериментально оптимальный по энергетике период следования пилообразных импульсов составляет около 4 мкс [4].

Рассмотрим подробнее ИНШ. Наиболее простым способом формирования низкочастотного шума является аналоговый. В данном случае можно использовать тепловой шум в резисторе или лавинный шум обратно смещенного p-n-перехода (диода Шоттки или стабилитрона) с последующим его усилением и фильтрацией до необходимой полосы частот.

Существует также менее дорогой цифровой способ формирования полосового низкочастотного шума из псевдослучайной последовательности, полученной, например, в микроконтроллере и дальнейшим цифро-аналоговым преобразованием и фильтрацией.

Рассмотрим пример формирования широкополосной заградительной помехи системе связи UMTS2100.

На рисунке 2 приведена схема модели цифрового формирователя широкополосной помехи в системе автоматизированного проектирования Microwave Office.

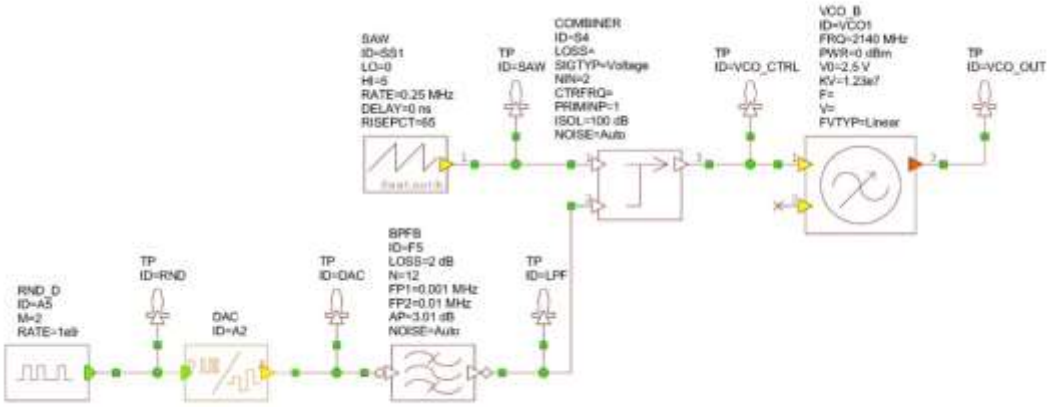


Рис. 2. Схема формирователя широкополосной заградительной помехи

Ниже (рис. 3) приведен спектр помехи, модулированной сгенерированным цифровым способом шумом полосой 9 кГц.

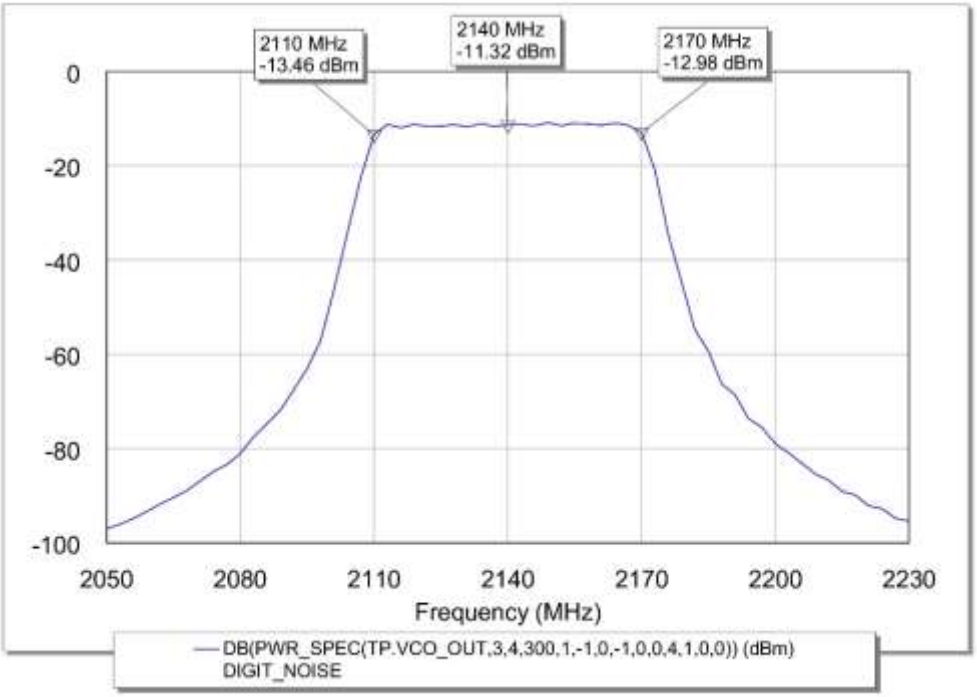


Рис. 3. Спектр моделированной помехи UMTS2100

Еще ниже (рис. 4) приведены спектры экспериментальной помехи, модулированной шумом полосой 5, 10 и 15 кГц соответственно.

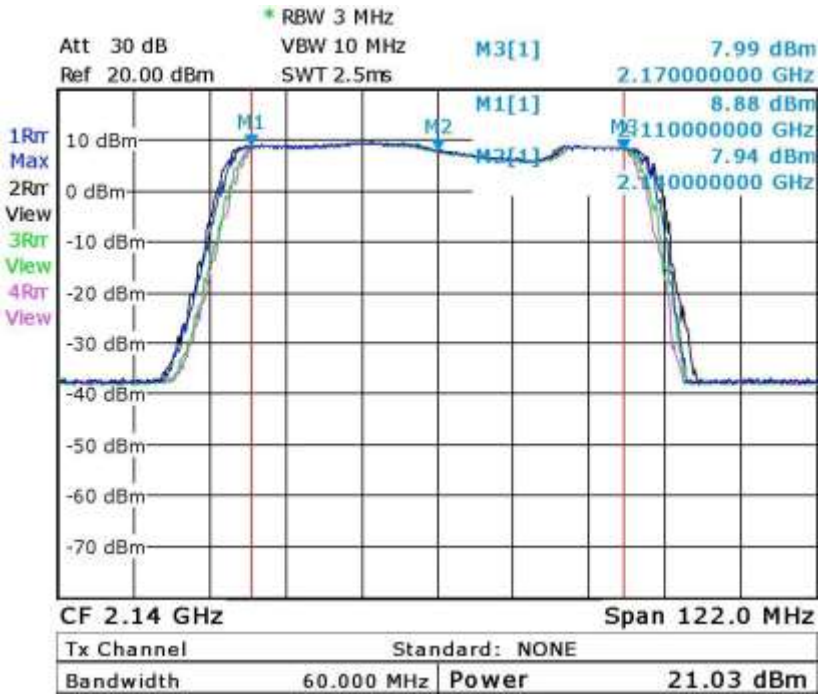


Рис. 4. Спектры экспериментальной помехи UMTS2100

При подавлении систем связи наиболее широко используют широкополосные помехи, модулированные шумом, поскольку у них наилучшие маскирующие свойства; кроме того, обычно не требуется большой точности совмещения несущей частоты передатчика помех с несущими частотами базовых станций.

Список используемых источников

1. Палий А. И. Радиоэлектронная борьба. 2-е изд., перераб. и доп. М. : Воениздат, 1989. 350 с.

2. Давыдова Н. С. Информационное подавление радиоэлектронных систем. Активные помехи, передатчики и станции активных помех : учебное пособие. М. : МАИ, 2002. 80 с.

3. Современная радиоэлектронная борьба. Вопросы методологии / под ред. В. Г. Радзиевского. М. : Радиотехника, 2006. 424 с.

4. Сунгатуллин Э. Н., Устименко В. М. Выбор помеховых сигналов блокираторов систем мобильной связи [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т., т. 1 / под ред. С. В. Бачевского. СПб. : СПбГУТ, 2015. С. 164–170. URL: http://sut.ru/doci/nauka/4.apino.2015.sut.pdf (дата обращения 04.04.2016).

УДК 621.372.63

А. В. Тумашов (студент группы РК-51М, СПбГУТ)

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЭКРАНИРОВАННОЙ РАМОЧНОЙ АНТЕННЫ ДЛЯ *N* – КОЛИЧЕСТВА ВИТКОВ

Данная статья посвящена антенне, которую можно отнести к классу пеленгаторных антенн. Рамочная антенна является дальнейшим развитием петлевого диполя. Само устройство относиться к области антенной радиотехники, которую можно применять в системах радиомониторинга, контроля электромагнитной обстановки в системах связи. Классическая рамочная антенна содержит один виток провода, но иногда используют и многовитковые рамочные антенны, имеющие число витков больше одного. Для того чтобы правильно подобрать входные параметры для данной пеленгаторной антенны не прибегая к созданию физического прототипа, стоит задача построения математической модели, которая свяжет геометрические и электродинамические параметры рамки.

рамочная антенна, рамка, четырехполюсник, многополюсник, волновое уравнение, матрицы Z, Y – параметров.

В технике и связи по проводам, передатчик и приемник соединены друг с другом парой проводов. Такая пара образует линию связи. Для решения большинства прикладных задач достаточно знать соотношения между напряжениями и токами на внешних зажимах линии и не интересоваться законами распределения напряжений и токов по длине линии, т. е. рассматривать линию как четырехполюсник.

Свойства четырехполюсника как системы для передачи энергии целиком определяются соотношениями, связывающие комплексы амплитуды напряжений и токов на двух парах зажимов четырехполюсника, которые называют уравнениями передачи четырехполюсника.

Уравнения, связывающие комплексные амплитуды напряжений и токов на внешних зажимах длинной линии, называют уравнениями передачи линии [1].

$$\dot{U}_0 = \dot{U}_1 \mathrm{ch}(\gamma l) + Z_{\text{В}} \dot{I}_1 \mathrm{sh}(\gamma l) \tag{1}$$

$$\dot{I}_0 = \frac{\dot{U}_1}{Z_{\text{В}}} \mathrm{sh}(\gamma l) + \dot{I}_1 \mathrm{ch}(\gamma l), \tag{2}$$

где $\dot{U}_0, \dot{I}_1$ – комплексные амплитуды напряжения и тока на входе приемника, $\dot{U}_1, \dot{I}_1$ – комплексные амплитуды напряжения и тока на входе приемника, γ – коэффициент распространения, $Z_{\text{В}}$ – волновое сопротивление, l – длина линии, $\mathrm{ch}(x)$, $\mathrm{sh}(x)$ – гиперболические функции косинуса и синуса.

Таким образом, линия является направляющей системой, вдоль которой распространяется электромагнитная энергия от передатчика к приемнику. Заключим, что параметры, характеризующие рамочную антенну, можно найти через уравнения передачи четырехполюсника, в котором коэффициенты будут определяться из уравнений передачи линии.

С учетом того, как протекают токи в рамке, будем рассматривать нашу антенну как сложную схему длинной линии, которая представляет собой шестиполюсник.

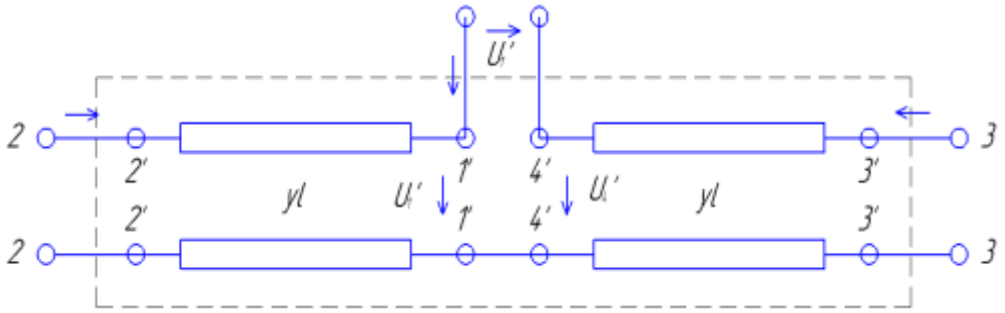


Рис. 1. Эквивалентная схема рамочной антенны с разрезом в середине трубы

Задача сводится к нахождению входных и выходных параметров антенны. В зависимости от решаемой задачи могут быть найдены *Y, Z, B, H, A, F* – параметры. Наиболее удобным способом нахождением коэффициентов воздействия и отклика системы, будет нахождение *Y*(*Z*) – параметров. Сначала находится матрица *Y*(*Z*) – параметров для одновитковой рамки, схема которой представлена выше. Затем мы рассматриваем *N* количество шестиполюсников, которые соединены параллельно – каскадно. Матрица такого соединения представлена ниже.

$$|Y| = |Z|^{-1} = \frac{1}{\rho}\begin{vmatrix} \mathrm{cth}(2N\gamma l) & -\dfrac{1}{\mathrm{sh}(\gamma l)} & \dfrac{-1}{\mathrm{sh}(2N\gamma l)} \\ -\dfrac{1}{2\mathrm{sh}(\gamma l)} & \dfrac{N}{2}\mathrm{cth}(\gamma l) & \dfrac{1}{2\mathrm{sh}(\gamma l)} \\ \dfrac{1}{\mathrm{sh}(2N\gamma l)} & \dfrac{2}{\mathrm{sh}(\gamma l)} & \mathrm{cth}(2N\gamma l) \end{vmatrix}, \qquad (3)$$

где *N* – количество витков в рамке, ρ – волновое сопротивление кабеля.

Как уже было сказано ранее, для решения многих прикладных задач достаточно знать соотношения между напряжениями и токами на внешних зажимах четырехполюсника. Т. е. схему рамочной антенны необходимо упростить с шестиполюсника до четырехполюсника, чтобы определенно точно знать воздействие и отклик системы. Для этого на входах 1–1 и 3–3

подключают симметрирующий трансформатор. Матрица такого четырехполюсника выглядит следующим образом.

$$\begin{bmatrix} Z_{11}^{\Sigma} = n^2\left(Z_{11} + Z_{33} - 2Z_{13}\right) \\ Z_{12}^{\Sigma} = Z_{21}^{\Sigma} = n\left(Z_{23} - Z_{12}\right) \\ Z_{22}^{\Sigma} = Z_{22} \end{bmatrix}, \qquad (4)$$

где $Z_{11}^{\Sigma} \ldots Z_{22}^{\Sigma}$ – элементы матрицы четырехполюсника, Z_{11}, $Z_{12} \ldots Z_{33}$ – элементы матрицы параллельно – каскадного соединения шестиполюсников, n – коэффициент трансформации.

Экран (труба) рамки без учета кабеля сам по себе, уже представляет антенну, со своим собственным сопротивлением. Для полного расчета сопротивления рамки, необходимо учесть и потери, которые вносит экран. Эта задача для экранированной рамочной антенны, была уже решена. Нам же необходимо выполнить пересчет сопротивления для нашей антенны, параметры которой мы задаем самостоятельно [2].

ТАБЛИЦА 1. Исходные данные рамочной антенны

Рабочий диапазон частот	10 кГц – 3 МГц
Радиус рамки	4,5 м
Радиус трубы	0,04 м
Окружающая среда	$\mu_0 = 4 \cdot \pi \cdot 10^{-7}$ $\varepsilon_0 = 8{,}854 \cdot 10^{-12}$

Рассчитанную антенну надо согласовать с приёмником. Для этого, внутреннее сопротивление приёмника (50 Ом) должно быть равным полному сопротивлению антенны и фидера. Пересчитаем полное сопротивление многовитковой антенны ко входным клеммам приёмника. Таким образом, в эквивалентной схеме, антенна представляет собой генератор, с внутренним сопротивлением Z_a, подключённый к четырёхполюснику, учитывающему потери в витках кабеля.

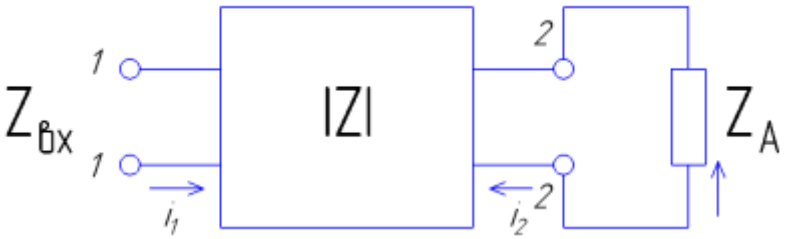


Рис. 2. Эквивалентная схема
экранированной рамочной антенны с подключенной нагрузкой

Сопротивление на входе приёмника будет равно:

$$Z_{\text{вх}} = Z_{11} - \frac{Z_{12}^2}{Z_a + Z_{22}}, \tag{5}$$

где $Z_{\text{вх}}$ – сопротивление на входе приемника, Z_a – сопротивление антенны(трубы), $Z_{11} \ldots Z_{22}$ – элементы матрицы сопротивлений четырехполюсника.

Для оценки полученных результатов обратимся к графикам, которые иллюстрируют изменяющиеся сопротивление на входе приемника в зависимости от увеличения количества витков.

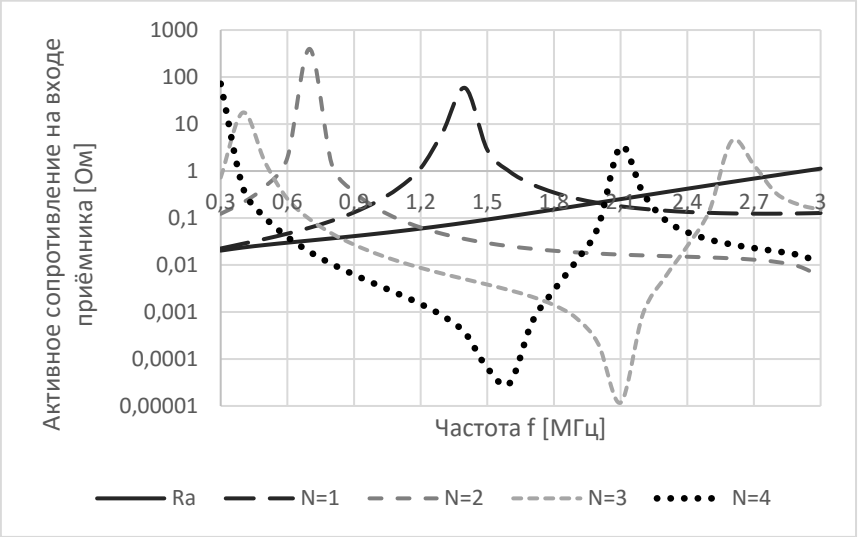


Рис. 3. Активная составляющая $Z_{\text{вх}}$ для антенн с N = 1, 2, 3, 4 количеством витков

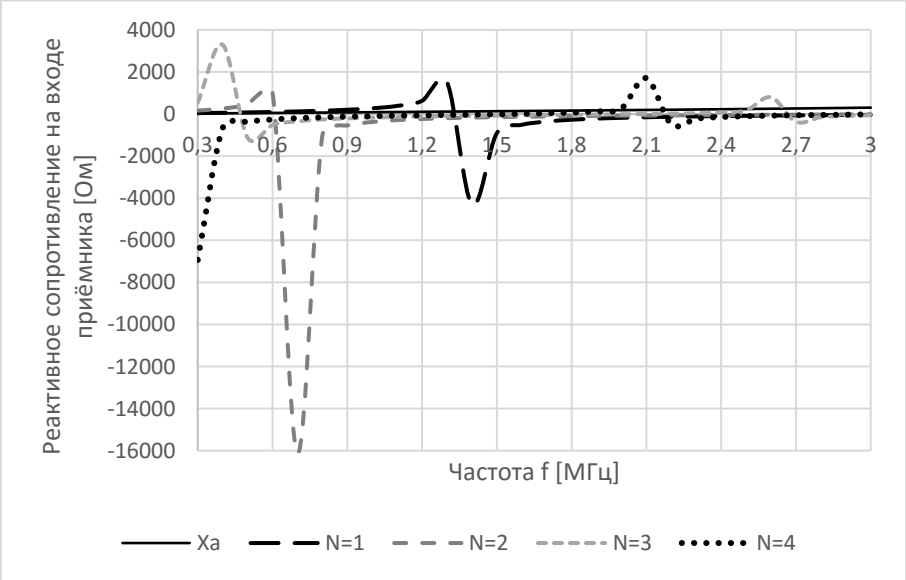


Рис. 4. Реактивная составляющая $Z_{\text{вх}}$ для антенн с N = 1, 2, 3, 4 количеством витков

Из графиков видно, что с увеличением количества витков возрастает $Z_{вх}$, как активная, так и реактивная ее составляющая. Из рисунков 3, 4 видно, что с увеличением количества витков уменьшается частота резонанса антенны, при этом, у антенн с N = 2, 3, 4 витками происходит увеличение число резонансных скачков. Адекватность математической модели можно оценить, сравнив экспериментальные данные, полученные с ранее созданных рамочных антенн.

Список используемых источников

1. Белецкий А. Ф. Основы теории линейных электрических цепей. М. : Связь, 1967. С. 353, 369–372, 402–411.
2. Кинг Р., Смит Г. Антенны в материальных средах. М. : Мир, 1984. С. 514.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Кириком Д. И.

УДК 681.848

А. И. Устинова (студентка группы 212, СПбГИКиТ)

НАНОМАТЕРИАЛЫ В СОВРЕМЕННОЙ АУДИОТЕХНИКЕ

Современные наноматериалы становятся очень популярными, и всё больше ученых находит им применение в самых неожиданных областях науки и техники. Так, открытый в 2010 году графен сейчас активно используется в исследованиях по электроакустике и даёт многообещающие результаты.

наноматериалы, электроакустика, громкоговорители, головные телефоны, микрофоны.

Графен представляет собой аллотропную модификацию углерода, образованную слоем атомов углерода толщиной в один атом, соединенных в двумерную гексагональную кристаллическую решетку. Он обладает хорошей электрической и тепловой проводимостями, низкой теплоёмкостью, оптической прозрачностью и низкими тепловыми шумами. Это всё делает графен привлекательным для аудиотехники. Кроме того, необычайная легкость материала обеспечивает хорошую звукопередачу на высоких частотах, а исключительная прочность способствует хорошему воспроизведению низких частот [1, 2, 3].

Далее будет рассмотрено несколько наиболее интересных работ, посвященных применению графена в современной аудиотехнике.

Учёные из Национального университета Сеула разработали пьезоэлектрический громкоговоритель с применением графена [3]. Он представляет собой поливинилиденфторидную пленку (ПВДФ), покрытую тонким слоем оксида графена, который в данном случае выполняет функцию электродов. При поступлении на них электрического тока от источника сигнала возникает обратный пьезоэлектрический эффект, вследствие чего полимерная пленка деформируется и образуются звуковые волны.

В ходе работы учёными были сняты амплитудно-частотные характеристики для разной толщины графеновых электродов – 60, 90 и 120 нм. Оказалось, что увеличение толщины электродов приводит к расширению частотного диапазона, в частности, средние частоты выражены намного сильнее при толщине в 120 нм, чем при толщине в 60 и 90 нм.

Также было проведено сравнение пленки на основе графена с пленкой, которая в настоящее время используется в промышленности и имеет аббревиатуру PEDOT:PSS. Исследования показали, что электроды из этой плёнки сильно уступают электродам из графена по передаче звука на всем интервале частот. Кроме того, графеновые громкоговорители хорошо себя зарекомендовали в качестве системы шумоподавления. Они позволяют создать колебания, равные по амплитуде, но противоположные по фазе тем колебаниям, которые необходимо подавить.

Необычный динамик был разработан в Техасском университете [4]. Его отличительной чертой является то, что он не содержит привычных составляющих: диффузора, подвижной катушки из проволоки, магнита и тому подобного. Более того, он тонкий, гибкий, прозрачный и до определенной степени растяжимый. Работает он на основе термоакустического эффекта, который заключается в том, что звуковые волны возникают благодаря переменному току, нагревающему проводник. Изменение температуры проводника приводит к колебанию температуры около него, а это в свою очередь ведет к изменению давления, т. е. к периодическому сжатию и разряжению окружающей среды. Данная идея сейчас очень актуальна, ведь обычная акустическая система занимает достаточно места, а современная техника стремится к тому, чтобы быть всё более и более компактной. Внедрение термоакустических динамиков позволит решить эту проблему и сэкономить место в телефонах, планшетах и тому подобном.

В своей работе [4] Чжи Вон Сук с коллегами исследовали в безэховой камере термоакустическую звуковую генерацию графена на подложках из разных материалов, таких как стекло, полиэтилентерефталат и полидиметилсилоксан. Полученные амплитудно-частотные характеристики показали, что уровень звукового давления на всех образцах увеличивается с ростом частоты. При этом важно отметить, что резонансные пики на характеристиках отсутствуют.

А совсем недавно на конференции в Сан-Франциско, 16 декабря 2014 года, группа ученых из Университа Цинхуа представила первые наушники-вкладыши, работающие на термоакустическом эффекте, с использованием графена. Особенность этих наушников в том, что они работают как в звуковом диапазоне (от 20 Гц до 20кГц), так и в ультразвуковом. Пока ученым удалось добиться уровня звукового давления в 70 дБ при мощности в 1 Вт. Дальнейшие исследования будут посвящены улучшению частотной характеристики в ультразвуковом диапазоне [4].

Калифорнийские ученые из университета Беркли предложили использовать многослойный графен в качестве диафрагмы для электростатических головных телефонов (наушников) [2]. Схематически такая система представляет собой диафрагму из многослойного графена, подключенную к источнику постоянного напряжения и зажатую между двумя кремниевыми электродами, покрытыми диоксидом кремния. На электроды подаётся переменный входной сигнал с разной полярностью, благодаря чему возникает электростатическое поле, и диафрагма начинает вибрировать, т. е. генерировать звук.

Из амплитудно-частотной характеристики экспериментальных наушников видно, что даже без специального акустического оформления они гораздо лучше передают высокие частоты, чем наушники коммерчески успешной модели Sennheiser MX-400 аналогичного размера. Они также обеспечивают лучшие показатели по чувствительности и отсутствию резковыраженных резонансов на высоких частотах. Кроме того, было замечено, что наушники с графеновой диафрагмой потребляют гораздо меньше энергии, что немаловажно в настоящий момент.

В Белградском университете группой ученых были проведены исследования, посвященные применению графена в качестве мембраны электростатического микрофона [1]. Его принцип работы аналогичен принципу работы электростатических головных телефонов (описан выше), однако работает в режиме генератора, а не двигателя. Для исследования был использован 30–60 слойный графен на никелевой фольге, суммарная толщина мембраны колебалась от 10 до 20 нм. Все расчеты и графики были смоделированы в специальной среде COMSOL. В ближайшее время ученые планируют реализовать физическую модель и проверить её на практике.

Конечно, чтобы рассмотренные устройства дошли до серийного производства, должно пройти какое-то время – ученым ещё предстоит решить ряд задач, связанных с возможностью получения листов графена большой площади и с понижением стоимости производства самого наноматериала. Однако уже сейчас мы имеем очень впечатляющие результаты, глядя на которые можно сказать, что в ближайшем будущем наноматериалы совершат революцию в аудиотехнике.

Список используемых источников

1. Todorovic D. Graphene microphone // Audio engineering society: the 136th convention 26–29 of April 2014.
2. Zhou Q., Zettl A. Electrostatic graphene loudspeaker // Applied physics letters. 2013. V. 102. N 22.
3. Shin K. Y., Hong J. Y., Jang J. Flexible and transperent graphene films as acoustic actuator electrodes using injekt printing // Chemical communications. 2011. V. 47. p. 8527–8529.
4. Suk J. W. Thermoacoustic sound generation from monolayer graphene for transparency flexible sound sources // Advanced materials. 2012. V. 24. N 47. p. 6342–6347.

Статья представлена научным руководителем,
кандидатом физико-математических наук, доцентом Мальцевой В. А.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 621.395

Д. Ю. Абраменкова (студентка группы ИКТК-35, СПбГУТ)

ПРОТОКОЛ ИНТЕРНЕТА ВЕЩЕЙ *CoAP*

В статье рассматривается протокол CoAP, его особенности, варианты применения, характерные процедуры. Приводится анализ информационных элементов и сообщений, обосновывается выбор протокола в зависимости от специфики планируемой сети Интернета Вещей. Актуальность данной темы обусловлена многообразием существующих протоколов, стандартов Интернета Вещей и отсутствием устоявшейся терминологии, описывающей концепцию в целом.

Интернет Вещей, протокол, CoAP, M2M, устройства, сеть, HTTP.

Всё больший интерес растёт к встроенным технологиям, с помощью которых можно устанавливать взаимодействие устройств друг с другом или с внешней средой. Известно более двадцати разработанных протоколов, позволяющих соединять и объединять устройства. Из них широтой использования выделяется протокол CoAP [2, 3, 4].

CoAP (*Constrained Application Protocol*) – это специализированный протокол передачи, предназначенный для использования в простых электронных устройствах, например, в датчиках малой мощности, выключателях, клапанах, которые должны управляться или контролироваться удаленно через сеть Интернет.

Протокол находится на прикладном уровне модели OSI. Предназначен для простого соединения с сетью с соблюдением специальных требований, например: поддерживание многоадресной рассылки, низкие накладные расходы, простота при использовании в среде с ограниченными возможностями, что позволяет применять его в Интернете Вещей и в устройствах с межмашинным взаимодействием (M2M), которые имеют маленький запас памяти и вычислительной мощности (рис. 1).

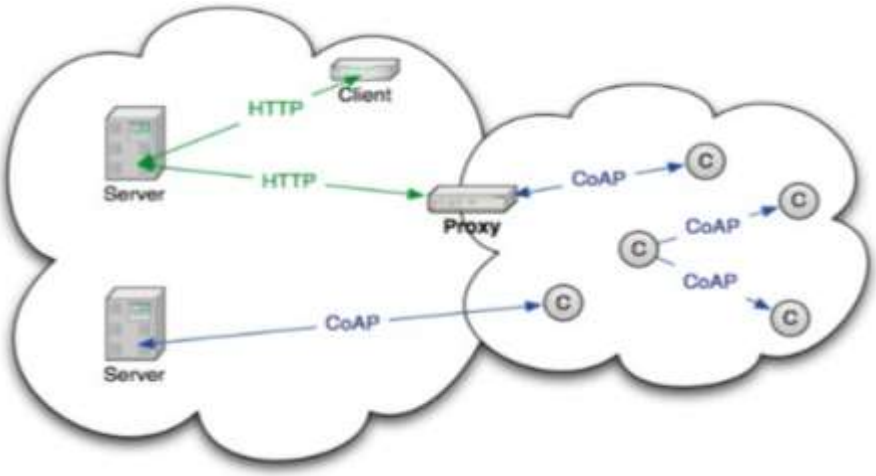


Рис. 1 Взаимодействия CoAP

CoAP разработан рабочей группой *The Internet Engineering Task Force* (IETF) *Constrained RESTful* environments (CoRE). Стандарт описан в RFC 7252.

В CoAP используются 4 типа сообщений:

Confirmable (CON): сообщения требующие подтверждения. Когда пакеты не теряются, каждое сообщение *Confirmable* вызывает ровно одно ответное сообщение подтверждения или сброса.

Non-confirmable (NON): сообщения не требующие подтверждения. Передаются регулярно, например. показания от датчика.

Acknowledgement (ACK): подтверждает, что пришло сообщение *Confirmable*. Само сообщение *Acknowledgement* не означает успех или неудачу любого запроса, содержащегося в сообщении *Confirmable*.

Reset (R): указывает на то, что конкретное сообщение (*Confirmable* или *Non-confirmable*) было получено, но некоторая часть текста отсутствует и невозможно правильно его обработать. Такая ситуация обычно возникает, когда принимающий узел перегружен и сбросил состояние, которое потребуется, чтобы понять сообщение. Посылка этого сообщения (например, отправив пустое сообщение *Confirmable*) также полезна в качестве проверки доступности узла ("COaP *ping*").

Все эти сообщения CoAP кодируются в простом двоичном формате. Формат сообщения изображен на рисунке 2, он начинается с фиксированного размера заголовка 4 байта. За этим следует значение маркера переменной длины, который может быть от 0 до 8 байт. После этого либо отсутствуют, либо приходят операций COaP с необязательной последующей полезной нагрузкой, которая занимает остальную часть дейтаграммы.

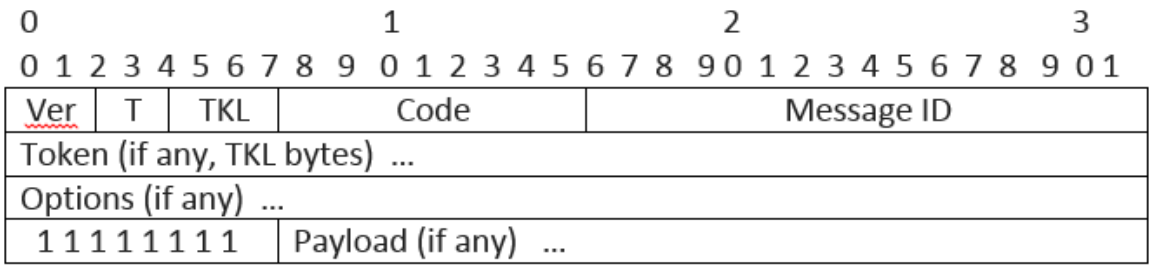


Рис. 2. Формат сообщения

Поля в сообщении определяются следующим образом:

Версия (*Version*) (Ver): двухразрядное целое число без знака. Указывает номер версии CoAP.

Тип (*Type*) (T): двух битовое целое число без знака. Указывает, является ли это сообщение типа *Confirmable* (0), *Non-confirmable* (1), *Acknowledgement* (2), или *Reset* (3)

Длина маркера (*Token Length*) (TKL): четырёхразрядное целое число без знака. Указывает длину поля *Token* переменной длины (0–8 байт). Длины от 9 до 15 зарезервированы и не должны быть посланы, иначе они будут обработаны как ошибка формата сообщения.

Код (*Code*): восьми битное целое число без знака, делится на трёх битовый и пяти битовый класс. Задокументирован как "*c.dd*", где "*c*" это цифра от 0 до 7 для трёх битного подполя и "*dd*" две цифры в диапазоне от 00 до 31 для пяти битного подполя. Класс может указывать на запрос (0), успешный ответ (2), ошибка клиента (4), или ошибка сервера (5). В частном случае, код 0.00 указывает на пустое сообщение. В случае запроса, поле код указывает на метод запроса; в случае ответа, код ответа.

Идентификатор сообщения (*Message ID*): - шестнадцатиразрядное целое число без знака. Используется для обнаружения дублированных сообщений.

За заголовком следует значение *Token*, которое может составлять от 0 до 8 байт, как указано в поле TKL. Значение *Token* используется для определения соотношения запросов и ответов.

Далее следуют опции (*Options*). *CoAP* определяет варианты опций, которые могут быть включены в сообщение.

CoAP работает над UDP. Клиенты и серверы взаимодействуют путём датаграмм без установления соединения. Повторы и переупорядочение реализованы в стеке приложений. CoAP позволяет использовать UDP-вещания и многоадресную передачу, которая используется для адресации.

Одна из главных характерностей CoAP – это взаимодействия с *HTTP*. Рассмотрим их взаимодействия на примере запроса устройством температуры с датчика (рис. 3).

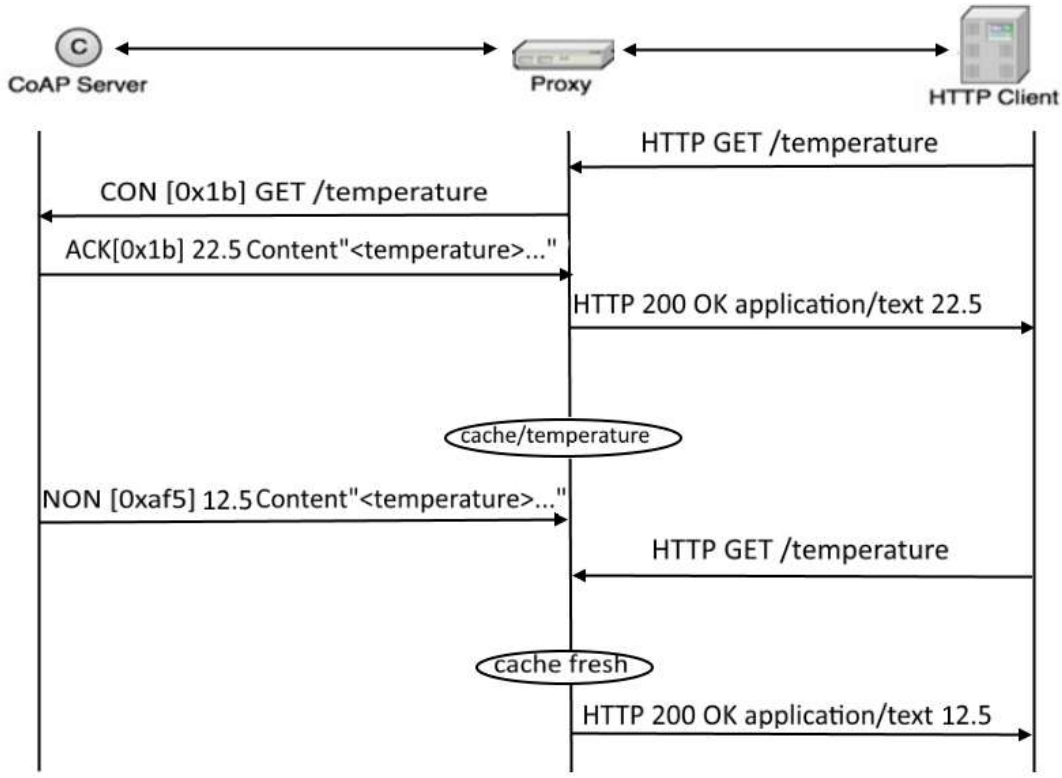


Рис. 3. Сценарий взаимодействия

HTTP *Client* посылает сообщение GET, в котором содержится запрос на получение температуры. Сообщение придёт на *proxy*, который преобразует HTTP запрос в запрос по протоколу CoAP. Далее информация о требовании параметра температуры передаётся в сообщении CON, и ему будет присваивается идентификатор сообщения, такой же идентификатор будет уже в ответном сообщении ACK, которое несёт в себе требуемую информацию. Данные температуры придут на прокси, запишутся в его кэш, и отправятся клиенту. Кэш будет обновляться новыми значениями температуры из сообщения NON, поступающего через некоторые интервалы времени. Когда HTTP *Client* снова отправит запрос о температуре, он получит уже быстрый ответ, в котором информация уже будет просто взята из свежей информации в кэше.

Почему же стоит выбрать CoAP, а не что-то другое? В преимущества этого протокола входит то, что у него маленькая величина сообщений, простые алгоритмы обработки, он идеален для ограниченных сетей с ограниченным количеством устройств, он специализирован на M2M приложения и легко взаимодействует по прокси к/от HTTP. При этом CoAP не является заменой или сжатой версией HTTP, он предназначен для автономных изолированных сетей, у которых отсутствует соединение с сетью.

Список используемых источников

1. Стандарт RFC 7252 [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc7252 , свободный. Яз. англ.

2. Росляков А. В., Ваняшин С. В., Гребешков А. Ю. Интернет Вещей: учебное пособие. Самара: ПГУТИ, 2015. 200 с.
3. Ovidiu Vermesan, Peter Friess Internet of Things – From Research and Innovation to Market Deployment. River Publishers, 2014. 356 p.
4. Internet of Things: Standards and Guidance from the IETF [Электронный ресурс]. – Режим доступа: https://www.internetsociety.org/publications/ietf-journal-april2016/internet-things-standards-and-guidance-ietf, свободный. Яз. англ.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Гойхманом В. Ю.

УДК 621.398

М. В. Авраменко (студент группы ИКТК-27, СПбГУТ)

АНАЛИЗ СУТОЧНЫХ ИЗМЕНЕНИЙ АТМОСФЕРНЫХ ЯВЛЕНИЙ ПРИ ПОМОЩИ РАЗРАБОТАННОГО M2M РЕШЕНИЯ ДЛЯ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА ОКРУЖАЮЩЕЙ СРЕДЫ

У технологии межмашинных коммуникаций есть огромный потенциал для улучшения охраны окружающей среды и экологической обстановки. Регулярные измерения состояния воздуха в крупных мегаполисах помогут жителям не только понять состав и качество воздуха, но и помочь экологическим организациям в борьбе с опасными загрязнениями. В статье рассматриваются результаты исследования суточных изменений атмосферных явлений от сенсорного узла.

machine-to-machine, интернет вещей, межмашинные коммуникации, носимые устройства, качество воздуха, атмосферные явления.

Постановка задачи

Проникновение в нашу жизнь устройств Интернета Вещей усиливается с каждым годом. Носимая электроника становится всё популярнее: пользователи смартфонов приобретают умные часы, браслеты, чтобы получить дополнительные функции [1]. Обеспечение экологической безопасности и внедрение современных технологий мониторинга экологической обстановки является одной из актуальных задач. У технологии межмашинных коммуникаций или M2M (*Machine-2-Machine*), являющейся составной частью концепции Интернета Вещей, есть огромный потенциал для улучшения охраны окружающей среды, она может приносить пользу различным формам сельского хозяйства, контролировать состав воздуха, влажность почвы [2]. Разрабатываемый проект нацелен решить задачи мониторинга окружающей среды, а так же иметь минимальную сложность

интеграции устройств и отображать данные от датчиков с любых устройств в режиме реального времени.

Целью данной работы является анализ данных полученных от сенсорного узла для выявления закономерности в изменениях атмосферных явлений для последующей доработки устройства в передачи данных при изменении показателей.

Для исследования суточных изменений атмосферных явлений, необходимо создать макет M2M-сети и сенсорный узел. На рисунке 1 приведена схема разработанного макета сети. Она состоит из четырех основных компонентов:

1) веб-сервер Apache 2 под управлением ОС Linux;
2) сервер базы данных под управлением СУБД MySQL;
3) web-приложение, которое визуализирует необходимую информацию для пользователя;
4) макет сенсорного узла.

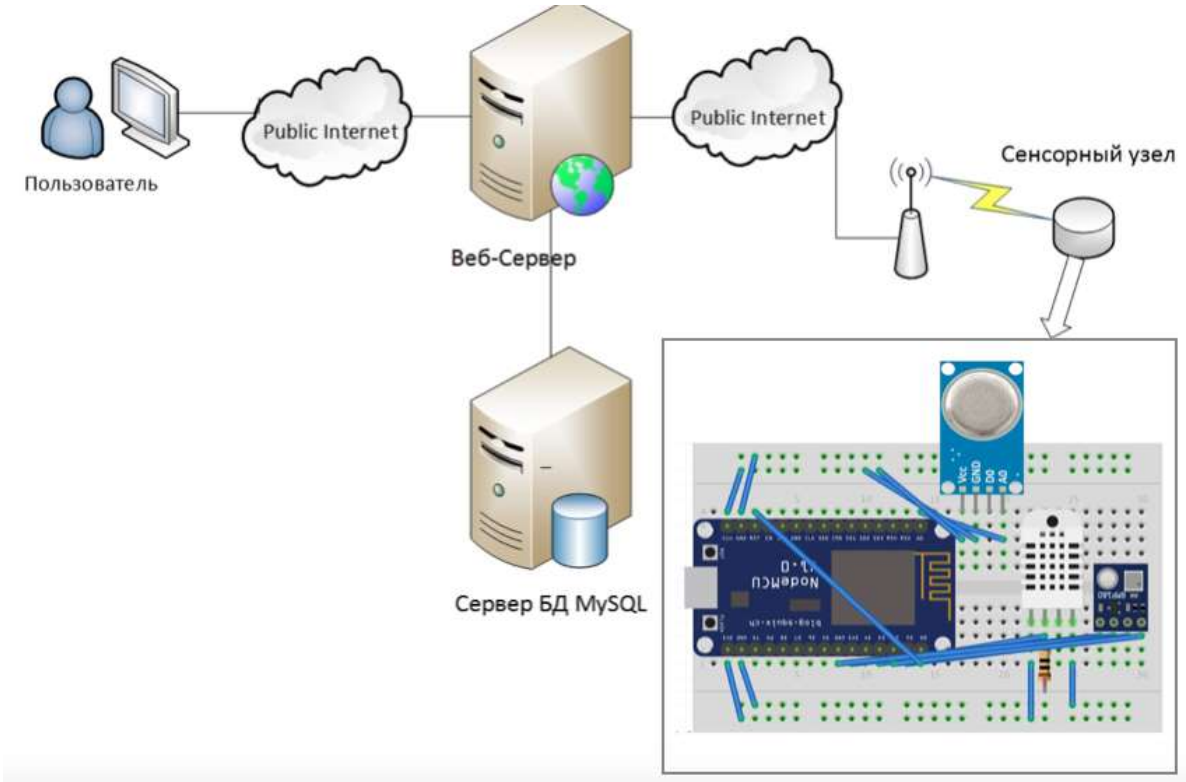


Рис. 1. Схема макета M2M-сети

При разработке макета сенсорнго узла стоит уделить внимание его относительно малой стоимостью по сравнению с уже существующими модулями, а так же минимальные габариты. Макет сенсорного узла состоит из:

– датчика температуры и влажности DHT22,
– датчика давления BM180,
– датчика качества воздуха MQ135.

Управляющим устройством служит Wi-Fi модуль ESP8266 версии ESP-12/NodeMCU, объединяющий в себе функции микроконтроллера и имеющий PCB антенну с дальностью до 400 м на открытом пространстве. В модуле полностью реализован TCP/IP стек, что позволяет использовать для передачи данных на удаленный сервер любой протокол, работающий поверх транспортного уровня.

После разработки модели M2M-сети и обеспечении связности, необходимо разработать алгоритм работы сенсорного узла для проведения замеров в разных районах города Санкт-Петербурга.

Алгоритм работы сенсорного узла представлен блок-схемой на рисунке 2, начинающейся с инициализации сенсорного узла, далее запускается таймер. В течении определенного времени осуществляется сбор данных от датчиков. После остановки таймера, полученные данные анализируются путем применения алгоритма нахождения грубых выбросов. При нахождение значений выходящих за пределы допустимых границ, они передаются брокеру при помощи организации Wi-Fi канала между точкой доступа и узлом. По окончанию передачи данных на сервер процедура повторяется.

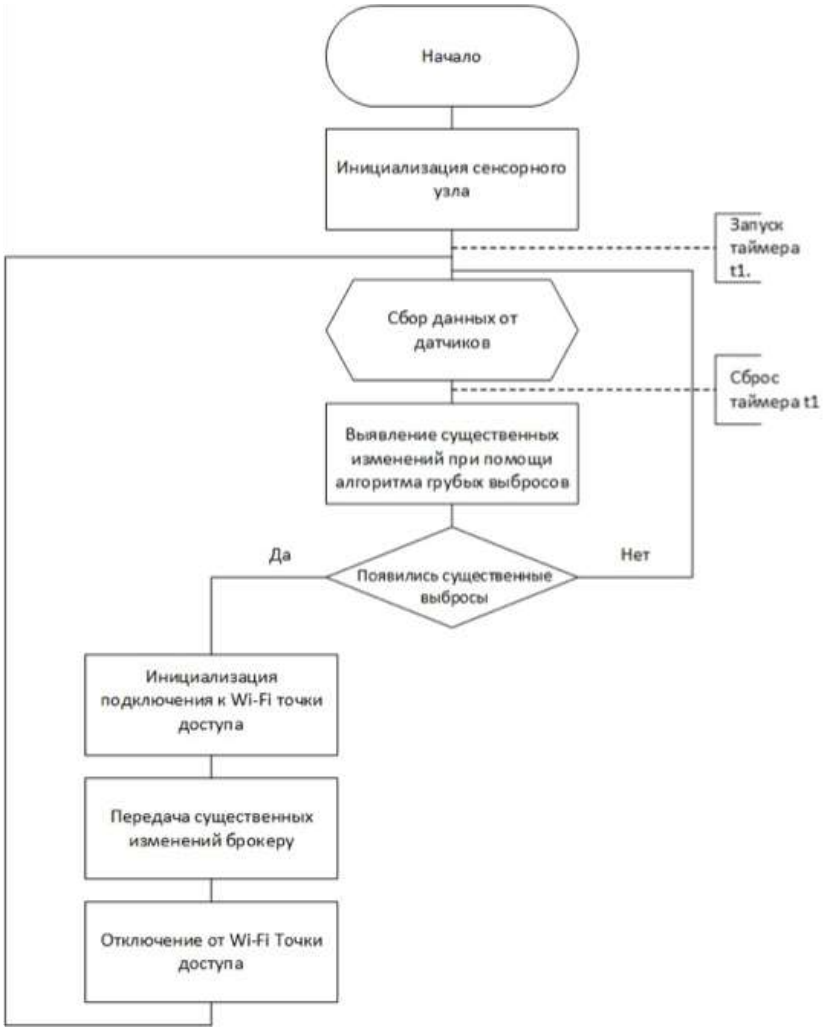


Рис. 2. Алгоритм работы сенсорного узла

Для проведения эксперимента были выбраны пять дней: 18 мая, 1, 3, 5 и 7 июня 2016 г. Сенсорный узел был установлен в пяти районах соответственно: Василеостровском, Приморском, Калининском и Невском г. Санкт-Петербурга и измерял четыре основных показателя: температуру (градусы Цельсия), влажность (проценты), атмосферное давление (мм.рт.ст.), качество воздуха (ppm, миллионные доли).

На рисунке 3 приведены результаты эксперимента по Калининскому району, так как по остальным районам наблюдается схожая тенденция. На данном графике отображена зависимость миллионной доли (ppm) от времени (сутки). За день было передано 241 значение.

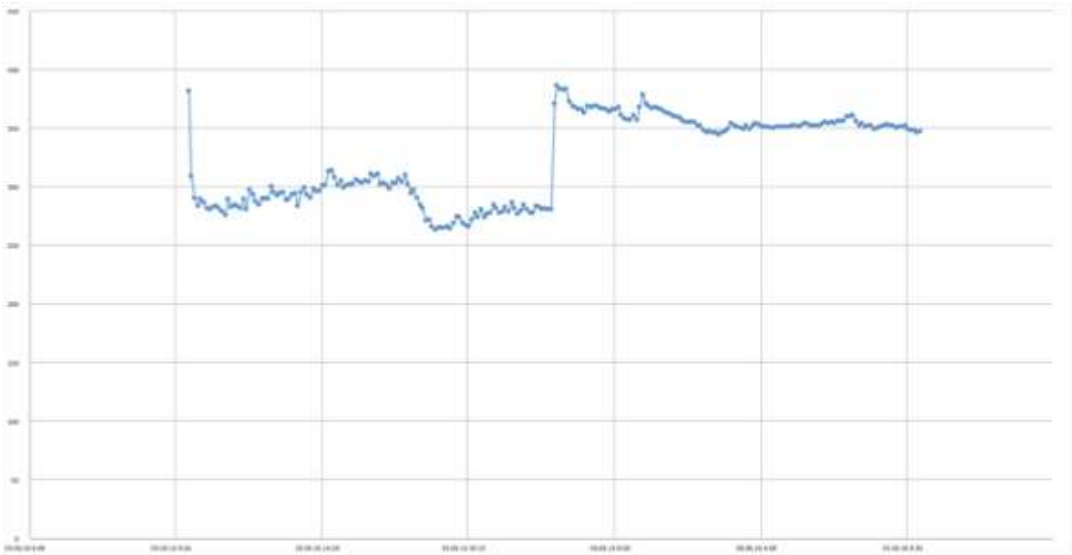


Рис. 3. Суточные изменения качества воздуха в Калининском районе

На рисунке 4 отображена зависимость интервалов между двумя смежными значениями (качества воздуха, выраженной в ppm) и времени (сутки). По результатам после применения алгоритма нахождения грубых выбросов было передано 33 значения. Двумя прямыми показан «коридор значений», в который вошли значения не критичные для передачи.

После проведения экспериментов, для анализа трафика, порождаемого сенсорным узлом, необходимо построить распределение интервалов времени между пакетами. Каждый переданный пакет – это один атмосферный показатель. Полученное распределение качества воздуха по всем пяти районам приведено на рисунке 5.

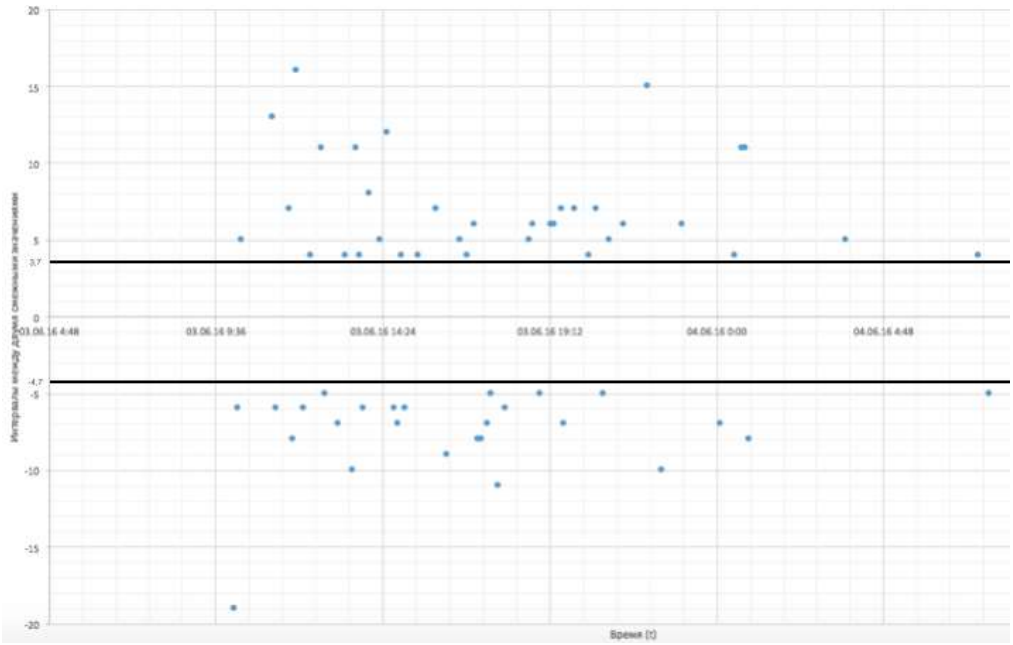


Рис. 4. Суточные изменения качества воздуха в Калининском районе после применения алгоритма нахождения грубых выбросов

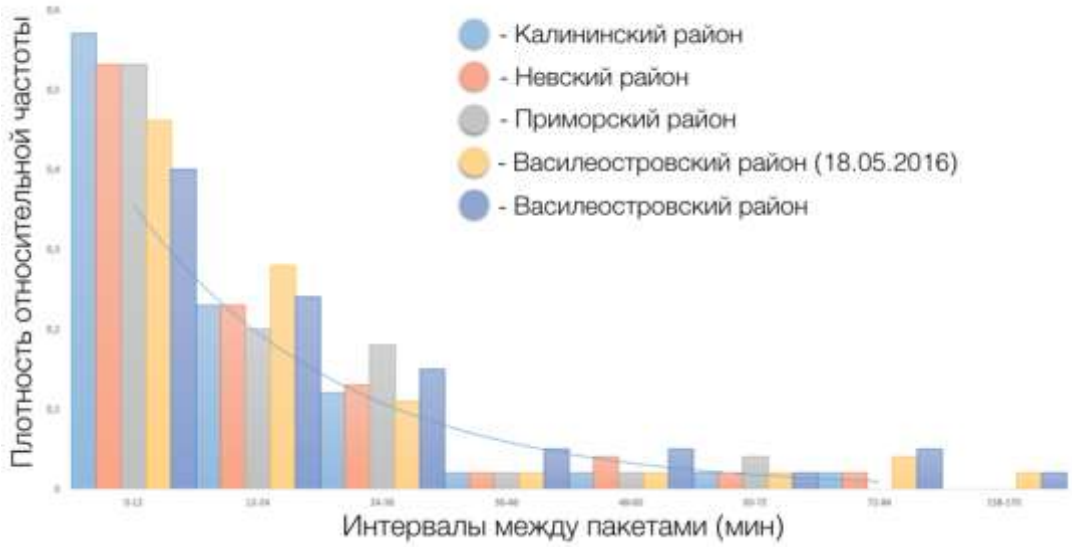


Рис. 5. Гистограмма распределения интервалов между пакетами

Выводы

Выводом данной работы, можно указать, что после применения алгоритма нахождения грубых выбросов и разработки алгоритма получения данных от сенсорного узла, основной межпакетный интервал по всем атмосферным показателям приходится в среднем на интервал 0–18 мин., так как изменения между двумя смежными значениями, превышающими критический порог, происходят минимальными интервалами, что свидетельствует о инерционности датчиков.

На основе этих данных можно предположить, что сенсорному узлу требуется осуществлять передачу данных в среднем не чаще чем раз в 20 минут, что, во-первых, влияет на расчет энергопотребления сенсорнго узла, а во-вторых, влияет, в будущем, на анализ общего трафика, так как подобных M2M-устройств в сети ожидаются миллионы.

Список используемых источников

1. Гольдштейн Б. С., Кучервый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с. ISBN 9785977509008.

2. Stryjak J., Sharma A. Analysis Agricultural machine-to-machine (Agri M2M): a platform for expansion [Электронный ресурс] // GSMA. 2015. URL: http://www.gsma.com/ mobilefordevelopment/wp-content/uploads/2015/03/Agricultural-M2M.pdf

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Гойхманом В. Ю.

УДК 65.011.56

В. А. Акишин (системный аналитик, ООО «НТЦ Аргус»)

ПОДХОДЫ К ВНЕДРЕНИЮ КОНЦЕПЦИИ CUSTOMER EXPERIENCE MANAGEMENT

Customer Experience Management (CEM) – концепция, включающая в себя совокупность процессов, методов и технологий, ориентированных на управление впечатлениями, которые клиент получает от взаимодействия с компанией. Существуют разные трактовки того, как и с помощью каких инструментов должна реализовываться данная концепция в рамках работы современного оператора связи. В статье рассматриваются подходы к внедрению CEM решений в общую архитектуру OSS/BSS решений, а также ключевые задачи и структура инструментов, реализующих концепцию CEM в инфокоммуникационной специфике оператора связи.

Customer Experience, Customer Experience Management, OSS/BSS, TMForum.

В условиях современной конкуренции на рынке телекоммуникаций операторы связи уделяют большое внимание решениям по управлению опытом и лояльностью клиентов, которые позволили бы выстроить эффективные бизнес-процессы обслуживания клиентов, тем самым снизить отток абонентов и преумножить доходы компании. В связи с этим, все больше набирает популярность применение концепции *Customer Experience Management*, в частности имплементация данной концепции в общую инфокоммуникационную специфику оператора связи.

Customer Experience (CE) – понятие включающее в себя совокупность всех ощущений и впечатлений, получаемых клиентом в процессе взаимодействия с компанией на протяжении всего жизненного цикла клиента, начиная от поиска информации об услуге и до окончания ее использования. *Customer Experience Management* (CEM) – совокупность процессов, методов и технологий, которые позволяют отследить, измерить и повлиять на уровень *Customer Experience* клиента [1].

При внедрении концепции CEM рассматривают не только соответствующую информатизацию деятельности компании, но и подход к взаимоотношениям с клиентами в целом: т. е. имплементируя CEM компания должна достигнуть определенного уровня зрелости [2]. Однако на сегодняшний день нет формальных границ, описывающих, где начинается и заканчивается CEM. Рассмотрев *Enhanced Telecom Operations Map (*eTOM*)*, можно сделать вывод, что CEM охватывает все домены бизнес-процессов оператора связи – от работы с клиентами до эксплуатации сетевых элементов [3].

Согласно проведенному исследованию TM *Forum* в 2011 г., на основании данных двадцати крупнейших поставщиков услуг, внедрение *CEM*-решения позволяет оператору изменить в лучшую сторону значение следующих показателей:

– сократить расходы;
– сократить отток клиентов;
– повысить удовлетворенность клиентов;
– увеличить доходы компании;
– повысить качество предоставляемых услуг;
– ускорить время вывода из эксплуатации услуг.

Конечная цель оператора, использующего CEM-решение – это создание ценного отношения с клиентами, за счет которого клиент на долгое время остается пользователем услуг. CEM-решения, позволяют оператору привлекать дополнительных клиентов за счет собственной рекламы, а также позволяют поднимать рейтинг бренда компании [4].

Изначально, CEM не ориентирован на специфику инфокоммуникационых услуг и отталкивается от такой области маркетинга как *Customer Relationship Management (*CRM*)* – управление взаимоотношениями с клиентами. Однако актуальное состояние концепции определяется вовлечением в нее большого количества различных информационных систем управления и хранения данных об абонентах. В связи с этим, первоочередной задачей внедрения CEM является определения оптимального подхода реализации задач концепции, с учетом текущих планов оператора, его масштабов и инфокоммуникационной специфики.

На текущий момент выделяют следующие основные подходы реализации целей и задач концепции CEM:

– имплементация отдельной самодостаточной системы (CEM-комплекса) в общую OSS/BSS архитектуру оператора связи;

– реализация CEM, как набора плагинов к существующим CRM решениям.

Первый подход – имплементация отдельной самодостаточной системы (CEM-комплекса) в общую OSS/BSS архитектуру оператора связи, потребует решения двух типовых задач, связанных с внедрением любой новой системы в существующую архитектуру

– каким образом подобная система должна вписываться в общую модель OSS/BSS стека оператора связи;

– какие функции должна выполнять данная система и в чем ее концептуальное отличие от систем, выполняющих задачи концепции CRM.

С точки зрения общей OSS/BSS архитектуры оператора связи CEM-комплекс должен выступать как единый агрегатор данных о *Customer Experience* клиента от всех систем OSS/BSS комплекса оператора связи, а также внешних источников знаний о клиенте, таких как социальные сети. При этом часть систем будет обогащаться обработанными данными о CE для решения узких прикладных задач взаимодействия с клиентом.

Вопрос функциональности самодостаточного CEM-комплекса, решается с помощью выделения нескольких уровней системы. При этом верхние уровни могут использовать результаты обработки информации о *Customer Experience* клиента, получаемые на более низких уровнях:

– уровень API. Служит единой точкой входа для информации о *CE* клиента из систем OSS/BSS комплекса, а также внешних источников данных;

– *Data Aggregation* – уровень агрегации данных. Функциональность данного уровня позволяет обрабатывать массивы информации о CE клиента получаемые из различных источников, в т. ч. преобразование количественной информации в качественную;

– *Analytics* – аналитический уровень. Данный уровень должен реализовывать задачи анализа и визуализации агрегированной информации о CE клиента для решения задач в рамках операционного управления, а также сегментировать клиентскую базу на основе CE клиента для работы верхних уровней;

– *Cusomer Interaction Management* – уровень управления взаимодействиями с клиентом. Уровень реализует инструменты, позволяющие влиять и отслеживать CE клиента, на основе совокупности знаний о клиенте в рамках каждого конкретного прецедента взаимодействия с компанией.

– *Application* – прикладной уровень. Данный уровень определяет то, каким образом до пользователя доводиться функционал, реализуемый на предыдущих уровнях модели, например, мобильное приложение или *Web*-интерфейс и т. д.

На рисунке 1 в виде функциональной карты визуализированы слои и высокоуровневые возможности CEM-комплекса:

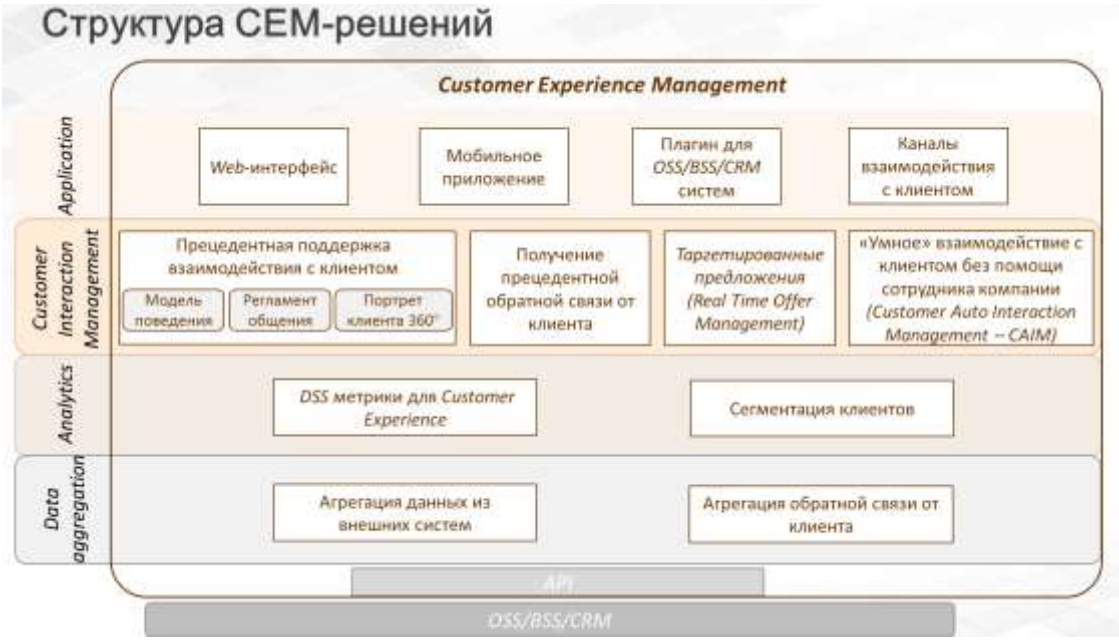


Рис. 1. Функциональная структура CEM-комплекса

Иной подход к внедрению концепции CEM – реализация набора плагинов к существующим CRM решениям. Классическая концепция CRM предполагает наличие ряда клиент-ориентированных транзакций, которые реализуются в т. ч. в системах OSS/BSS комплекса. Успешность выполнения данных транзакций определяется соблюдением установленных нормативов (KPI) и фактом успешного завершения взаимодействия с клиентом (например, клиенту выдана справка). При таком определении CRM, внедрение CEM, предполагает, что в одной или нескольких информационных системах оператора должен быть реализован набор плагинов или надстроек, которые позволят оператору получить измеряемую сверх выгоду от клиент-ориентированных транзакций. Сверх выгода для оператора, в данном случае, должна выражаться:

– в увеличении лояльности клиента,
– в снижении степени оттока клиентов,
– дополнительной прибыли (увеличение дохода/снижение издержек),
– улучшение имиджа оператора в глазах клиента.

Сравнивая два вышеописанных подхода, стоит отметить их преимущества и недостатки. Внедрение CEM-комплекса как полноценной системы в рамках общей архитектуры – это сложная и трудоемкая задача. Она несет в себе ряд сложностей в части организации взаимодействия другими системами OSS/BSS ландшафта. Но при этом, данных подход позволяет оператору в полной мере реализовывать задачи концепции CEM в рамках инфокоммуникационной прослойки бизнеса. В связи с большими

издержками, максимальная эффективность данного подхода может реализовываться только для инфокоммуникационной специфики крупных операторов связи.

Альтернативный подход – внедрение CEM как набор плагинов к существующим системам. Данный подход потребует нецелевых доработок в смежных системах OSS/BSS комплекса, что усложняет их поддержку и функционирование. Также стоит отметить, что второй подход в меньшей степени позволяет реализовывать цели и задачи концепции CEM. При этом внедрение набора плагинов является гораздо менее трудоемкой задачей, чем внедрение масштабного CEM-комплекса. Именно этот фактор обуславливает популярность данного подхода у предприятий малого и среднего бизнеса, в т. ч. в области телекоммуникаций.

Список используемых источников

1. Бутчер Стефан А. Программы лояльности и клубы постоянных клиентов. М. : Вильямс, 2004. 272 с. ISBN 5-8459-0614-8

2. Gary Mak, Srinivas Guruzu. Hibernate Recipes: A Problem-Solution Approach. Apress, 2010. 313 p. ISBN 1430227966, 978-1430227960.

3. ETSI Technical Report (TR) 188 004 V1.1.1 (2005-05) Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; OSS vision.

4. TM FORUM. GB921CP. Business Process Framework (eTOM). Concepts and Principles. Release 13.0. TM Forum; August 2013.

Статья представлена научным руководителем,
кандидатом технических наук Кисляковым С. В.

УДК 004.725.5

А. С. Викулов (студент группы М-02з СПбГУТ)

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В ПЛАНИРОВАНИИ СЕТЕЙ Wi-Fi ВЫСОКОЙ ПЛОТНОСТИ

Основная проблема сетей высокой плотности (СВП) заключается в быстром росте требований пользователей к качеству беспроводной сети в больших помещениях, где простое радиопокрытие с достаточным уровнем сигнала всей площади более не отвечает требованиям сетевых сервисов. Несмотря на все современные достижения в развитии технологии, произошедшие в последние годы, сама физическая радиочастотная суть сетей Wi-Fi изменений не претерпела. Основной задачей сетей СВП является увеличение числа клиентов сети, физически размещенных на небольшой площа-

ди. Далее будут рассмотрены наиболее актуальные на сегодняшний день факторы, влияющие на построение СВП.

локальные сети, абонент, Wi-Fi, высокая плотность, радиопланирование.

Рассмотрим ключевые критерии радиопланирования:

- Скорость передачи является первейшей для абонента характеристикой в сети скорости передачи данных. К сожалению, при проектировании, скорость передачи данных – это очень плохой критерий оценки радиопокрытия. В зависимости от множества факторов скорость может значительно меняться.
- Уровень сигнала. Минимальные требования к уровню сигнала должны быть обязательным критерием проектирования беспроводной сети. С другой стороны, в реалиях СВП требование по уровню сигнала обычно выполняется с большим запасом, поэтому само по себе не может быть определяющим.
- Соотношение сигнал/шум+интерференция (SINR) является другой важной метрикой. Рекомендованное значение для WLAN передающих только данные: 15 дБ или лучше. Для сетей, поддерживающих передачу голоса и видео, рекомендованные значения SINR: 20 дБ или лучше [1].
- Число доступных точек доступа (ТД). Если поставить себя на место клиента, то, несмотря на то, что ему видна только одна ТД на каждом канале, в пределах видимости клиента должно быть больше одной точки доступа для обеспечения сервиса. Как много их должно быть – зависит от используемых приложений. Например, в случае приложений, передающих голос, каждому устройству должна быть доступна основная ТД на уровне минус 65 дБм и еще одна на уровне не хуже минус 77 дБм [2].
- Эфир. В некотором смысле, эфирное время – это тоже важнейший ресурс, который необходим принимать во внимание при планировании сети, поскольку в пределах домена коллизий СВП одновременно передавать может только одно из множества устройств. Некоторые клиенты могут быть подключены на низких скоростях, поэтому совокупная пропускная способность этого канала на точке доступа может стремительно падать в те моменты, когда эфир предоставляется этим клиентам. Этот эффект значительно усиливается, когда такой клиент физически находится на пределе досягаемости ТД.
- Размер ячейки. Для больших объектов с СВП необходимо достижение высоких показателей емкости и таким образом необходимо иметь значительно больше ТД, чем на аналогичном объекте с традиционным Wi-Fi. Следовательно, целью должно являться уменьшение размеров ячейки сети СВП.

Важнейшими для СВП нововведениями стандарта 802.11ac являются:

- Больший вычислительный ресурс ТД поддерживающих новый стандарт является несомненным достоинством, поскольку в процессе де-

модуляции и декодирования сигнала в средах СВП точке доступа требуются серьезные вычислительные ресурсы.

- Поэтапный переход клиентов на работу с MIMO, поскольку позволит более оперативно обрабатывать пиковые нагрузки и быстрее освобождать эфир.
- TxBF. Улучшает SINR в обоих направлениях, улучшает CSI.
- MU-MIMO является крайне актуальным для СВП нововведением, поскольку позволяет точке доступа работать с несколькими клиентами одновременно.

Сеть Wi-Fi стандарта 802.11n может работать с каналами шириной 40 МГц, путем агрегирования двух 20 МГц каналов. Для стандарта 802.11ac доступны уже каналы шириной 80 и 160 МГц. Агрегирование каналов является довольно привлекательной возможностью, поскольку увеличивается пропускная способность для клиентов, поддерживающих такую конфигурацию [3].

Для СВП, возможность повторного использования каналов и сегментирование клиентских устройств в домены коллизий меньшего размера– это факторы гораздо большего значения, нежели значение пиковой пропускной способности в расчете на клиентское устройство. Снижение числа каналов, путем увеличения их ширины – путь к снижению емкости сети.

Фактически в российских реалиях, агрегирование каналов до ширины 40 МГц даст на выходе только 4 непересекающихся канала (36–40, 44–48, 52–56 и 60–64) что сведет к нулю привлекательность диапазона 5 ГГц с позиции частотного планирования. Использование же каналов шириной 80 и 160 МГц принципиально невозможно, поскольку полностью исключает возможность, какого бы то ни было радиопланирования. Что касается диапазона 2,4 ГГц, то в нем говорить об агрегировании каналов в принципе бессмысленно. В общем случае предпочтительнее иметь 50 пользователей в каждом из двух каналов HT20, чем 100 пользователей в одном канале HT40. Плюс ко всему не все из абонентских устройств используют все возможности каналов HT40 из-за своей слабой вычислительной мощности. Другим недостатком агрегированных каналов является ужесточение требований к SINR – в случае каналов 40 МГц – на 3 дБ, а для каналов 80 МГц – на 6 дБ.

Таким образом, предпочтение должно быть отдано каналам HT20 с целью получения максимальной пользовательской емкости.

MIMO использует SDM для передачи не просто одной и той же последовательности данных, а для передачи множественных последовательностей, которые при приеме будут объединены в один общий сегмент данных. В документе Aruba Networks [4] показано, что при условии поддержки на стороне клиентского устройства, увеличение числа пространственных потоков пропорционально увеличивает пропускную способность. Необходимо отметить, что данный эффект не меняется в широ-

ком диапазоне как числа клиентских устройств, так и сетевой нагрузки. Это особенно важно, поскольку многие преимущества стандарта 802.11ac второй волны сильнейшим образом зависят от того, насколько оправдаются надежды, возлагаемые на технологию MIMO.

Но есть и обратная сторона. Применение MIMO для СВП не несет однозначной выгоды. Радиомодули с поддержкой MIMO разработаны специально для работы в условиях множественных переотражений сигнала. Однако, в сетях СВП целью является минимизация эффектов переотражений, в особенности, если речь идет о больших пространствах с точно подобранными и сориентированными внешними антеннами [4].

Несмотря на заметный эффект, масштабируемость этой технологии пока ограничена. MIMO – это долгосрочное вложение. В то же время эффект с точки зрения покрытия заметен сразу, в основном за счет более производительных процессоров, используемых этими ТД, которые позволяют более эффективно демодулировать слабый сигнал.

Однако, самая большая проблема на данный момент – отсутствие поддержки MIMO на клиентских устройствах. Тому есть три основные причины:

- стоимость чипсетов, поддерживающих MIMO;
- низкая потребность пользователей в высоких скоростях;
- ограниченность работы от батареи, ввиду высокого энергопотребления процессоров в этих режимах.

В сетях 802.11n и 802.11ac первой волны MIMO может быть использовано для работы только с одним пользователем в каждый конкретный момент времени. В 802.11ac второй волны эта ситуация меняется, поскольку вводится принцип MU MIMO – Multi User MIMO. Эта технология, представляющая собой пример SDMA, дает возможность точке доступа с 802.11ac передавать два или более пространственных потока к двум или более клиентским устройствам одновременно. Таким образом, возможности по повышению емкости сети СВП теоретически увеличиваются. В стандарте 802.11ac wave 2 поддерживается передача данных 4 клиентам одновременно в нисходящем потоке (и только в нем).

MU-MIMO работает следующим образом. ТД с задействованным функционалом MU-MIMO периодически посылает зондирующие сигналы. Клиенты отвечают на них кадром, содержащим CSI с учетом полученного зондирующего сигнала. Точка, получив CSI от каждого клиента, вычисляет необходимую фазу и уровень передачи для каждой своей антенны. После этого ТД передает потоки данных нескольким устройствам за одну передачу. При этом раздельная передача в сторону клиентов выражается в пространственном разнесении лучей передачи (TxBF).

Преимуществами подхода MU-MIMO (для поддерживающих его клиентов) для задач СВП являются снижение времени ожидания передачи и более эффективное использование эфира и спектра. Следствием являются

более высокие скорости передачи данных, рост емкости сети, повышение эффективности работы дешевых клиентов, и косвенно – лучшая работа клиентов старых версий стандарта 802.11.

Важно помнить, что MU-MIMO работает только в диапазоне 5 ГГц и дополнительно усложняет логику работы ТД необходимостью планировать эфирное время с учетом потребностей клиентов SU/MU-MIMO.

В работе [5] приведен список чипов клиентских и инфраструктурных устройств, поддерживающих стандарт 802.11ac wave 2. Поэтому на этапе планирования пока не стоит всерьез рассчитывать на прирост емкости от эффектов MU-MIMO.

Многие производители стараются улучшить характеристики принимаемого сигнала на клиентском устройстве путем формирования луча в его направлении. В стандарте 802.11ac была стандартизирована технология формирования луча TxBF. Из проприетарных технологий, имеющих ту же цель, особо стоит выделить: Cisco ClientLink и Ruckus BeamFlex.

Технология Cisco ClientLink увеличивает избирательность для клиентов с 802.11a/g OFDM. Поскольку такие клиенты не поддерживают тех преимуществ, которые дает 802.11n, они являют собой наименее эффективных клиентов в сети. Использование ClientLink в СВП позволяет точке доступа улучшить SINR примерно на 3–6 дБ для клиента, запрашивающего подобный сдвиг. Для СВП сети основанной на решениях Cisco Systems это очень заметное дополнение к сетевой архитектуре.

В противовес Cisco Systems, использующим неявное формирование луча «на чипе», Ruckus Wireless применяет формирование луча «на антенне» – технологию под названием “BeamFlex”. По своей сути BeamFlex использует массив антенн – фазированную антенную решетку. При необходимости, ТД с BeamFlex может настроить массив антенн в любую из возможных комбинаций, отслеживая соединения в реальном времени и модифицируя лучи, чтобы они соответствовали динамически изменяющимся условиям. Следуя логике MRC, антенны усиливают полезные сигналы и гасят ненужные. Это позволяет получить прирост мощности сигнала до 10 дБ по направлению целевого луча, а также подавление помех на величину до 17 дБ на задних лепестках диаграммы направленности.

Однако, поскольку пока клиент не имеет возможности делать аналогичное формирование луча, принципиальным недостатком всех подобных решений является вносимый дисбаланс в линк клиент-ТД. Поэтому уровни на которых клиент и точка «слышат» друг друга в результате применения этих технологий могут заметно разниться. Это, хоть и в разной мере, но – априори плохо для сетей 802.11 и в свою очередь может привести к заметному несовпадению скоростей передачи как минимум control трафика, что может быть критичным для передачи данных в ряде конкретных приложений.

Стандарт 802.11ax, как результат дальнейшей эволюции 802.11ac будет использовать модуляцию 256-QAM, с OFDMA (orthogonal frequency division multiple access) с дальнейшим повышением числа клиентов одновременно принимающих данные. Будет увеличиваться спектральная плотность мощности в расчете на пользователя и как следствие увеличиваться совокупная пропускная способность сети. Помимо этого, стандарт также внесет возможность работы с MU-MIMO в восходящем канале. Номинальные скорости соединения в 802.11ax ожидаются от 10 до 14 Гбит/с. Энергетический бюджет увеличится на 9 дБ с соответствующим увеличением дальности работы. Предполагается увеличение максимального числа MU-MIMO потоков до 8. Также стандарт внесет возможность работы с MU-MIMO в диапазоне 2.4 ГГц. Утверждение спецификаций 802.11ax в IEEE ожидается в 2019 году, однако первые устройства с поддержкой 802.11ax могут появиться с конца 2017 года [5].

Список используемых источников

1. Ruckus Wireless. Deploying very High Density Wi-Fi. Design and Configuration Guide for Stadiums. 2012.
2. Meru Networks. Best Practices Guide for High-Density Design and Deployment. 2012.
3. Cisco Systems. Wireless LAN Design Guide for High Density Environments in Higher Education. 2011.
4. Chuck Lukaszewski. VHD 802.11ac Networks VRD. Theory Guide v1. Aruba. 2015.
5. Strategy Analytics. 802.11ac Wave 2 with MU-MIMO: The Next Mainstream Wi-Fi Standard. 2015.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Гришиным И. В.

УДК 65.011.56

Л. А. Виткова (аспирант, СПбГУТ)
М. Н. Дудникова (студент группы ИКТЗ-23, СПбГУТ)

ИССЛЕДОВАНИЕ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БАНКИНГА ДЛЯ ФИЗИЧЕСКИХ ЛИЦ

Развитие IT-технологий породило бесчисленное множество удобств, как для физических, так и для юридических лиц. Актуальность данной статьи обусловлена тем, что с ростом услуг, которые предоставляются через интернет, появился новый сектор экономики – электронная коммерция, частью которого является электронный

банкинг. В данной статье анализируются существующие уязвимости, угрозы и методы защиты в сфере электронного банкинга.

информационная безопасность, угрозы, уязвимость, электронный банкинг.

Введение

Развитие IT-технологий ежедневно открывает новые возможности и горизонты для общества. Интернет стал универсальной средой, он предоставил возможность повышения качества и скорости взаимодействия как для физических, так и для юридических лиц. Число пользователей глобальной компьютерной сети стремительно растёт. На современном этапе развития науки и техники, информатизации различных областей жизни общества, появились новые технические возможности проведения денежных расчётов и взаимозачетов. В нынешних условиях коммерческие банки стремятся предоставлять своим клиентам усовершенствованные банковские услуги, которые связаны с электронными системами расчетов.

Актуальность данной статьи обусловлена тем, что количество сервисов и услуг растёт, глобальная сеть Интернет стала универсальной коммерческой средой, ежедневно между серверами банков, электронными сервисами и клиентами происходят миллиарды транзакций, ведется активная финансовая деятельность. Как следствие, появляются новые уязвимости и угрозы информационной безопасности в новом секторе экономики, в частности в электронной коммерции, частью которой является электронный банкинг. В сфере ЭБ существует и такая проблема, как не разработанность методических аспектов обеспечения информационной безопасности для физических лиц.

В сфере электронного банкинга наиболее уязвимыми для преступников являются такие формы бизнеса, как информационно-развлекательные сервисы, электронная коммерция, интернет-банкинг и онлайн-торговля. В кибермошенничестве под кражей понимается хищение и присвоение не материальных вещей или денег, а конфиденциальной информации, которая и наносит урон организации или человеку, а уже в дальнейшем, с помощью этой информации преступник может и украсть деньги [2].

Сегодня в России угрозам информационной безопасности противостоят тысячи профессионалов, сотни компаний, государственные службы, банки, но халатность и не осведомленность пользователя сервисов наносит не меньший ущерб. Угрозы были и остаются одной из наиболее распространенных причин ущерба конфиденциальности, целостности и доступности информационных систем, и все же, несмотря на огромные усилия технического и экспертного сообщества, убытки, приносимые инцидентами информационной безопасности в электронном банкинге, продолжают расти.

Анализ

Согласно Базельскому комитету по банковскому надзору электронный банкинг получил такое определение: «электронное банковское дело или электронный банкинг (e-banking), включает в себя предоставление розничных и незначительных по объёму банковских продуктов, услуги через электронные банковские каналы, а также значительные по объёму электронные платежи и другие оптовые банковские услуги электронным способом».

Рынок электронных платежей стремительно растёт с каждым годом, вместе с ним растёт число компьютерных преступлений. Ежедневно тысячи людей становятся жертвами сетевых аферистов.

Сейчас наиболее востребованным способом безналичных расчетов является осуществление платежей через банковские карты. В нашей стране число дебетовых карт превышает численность граждан почти в 2 раза. На январь 2016 г. их количество составило 243 929 тыс. ед.

Из статистики ЦБ РФ за 2015 г. следует, что мошенники чаще всего пытаются украсть суммы от 10 до 50 тыс. рублей, количество инцидентов с каждым кварталом 2015 года росло, и только во втором квартале удалось предотвратить 21 % от суммы нелегально выводимых денежных средств [3].

Рост популярности систем электронного банкинга, не только в западных странах, но и в России, еще раз подтверждает, что у этого вида банковских услуг появился устойчивый и платёжеспособный спрос.

Идентификация угроз информационной безопасности в сфере электронного банкинга приводит к очень большому числу сценариев возможных инцидентов. В статье приведён анализ угроз с более высокими уровнями рисков. Формально риск можно определить следующим образом: *риск = угроза * уязвимость* [4].

Таким образом, устранение уязвимости и уменьшение вероятности реализации угрозы непосредственно приводят к снижению риска.

Синтез

Для оценки и анализа существующих угроз информационной безопасности в сфере электронного банкинга для мобильных устройств использован один из инструментов выбора и оценки решения – метод Дельфи. Метод характеризуется меньшей предвзятостью, субъективностью и влиянием авторитета отдельных участников. При оценке коэффициента уязвимости была введена шкала баллов от 0 до 10, где 10 – наиболее часто встречающаяся по мнению экспертов угроза.

Экспертные оценки опираются на авторское исследование конъюнктуры информационной безопасности, на базе статистики представленной Лабораторией Касперского на виртуальной карте угроз для России и для

мира. Период первый квартал 2016 г., четвёртый квартал 2015 г., третий квартал 2015 г., второй квартал 2015 г. [5].

В целях дальнейшего вычисления уровня риска каждой угрозы, введён коэффициент угрозы, по шкале от одного до трёх, где «3» – максимальный уровень угрозы, то есть последствия её реализации – это нарушение целостности, нарушение доступности, нарушение конфиденциальности. Коэффициент «1» в этой шкале означает, что в последствиях этой угрозы может быть только одно из вышеприведённых нарушений.

В таблице 1 приведён перечень рассмотренных детектируемых угроз из банка данных угроз ФСТЭК [6].

ТАБЛИЦА 1. Перечень угроз из БДУ и их коэффициентов

№ УБИ в БДУ	Название угрозы	Коэффициент угрозы
УБИ.173	Угроза «спама»	1
УБИ.170	Угроза неправомерного шифрования информации	1
УБИ.127	Угроза подмены действия пользователя путём обмана	3
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	1
УБИ.036	Угроза исследования механизмов работы программы	2
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	2
УБИ.042	Угроза межсайтовой подделки запроса	3
УБИ.172	Угроза распространения «почтовых червей»	3
УБИ.006	Угроза внедрения кода или данных	3

В таблице 2 показаны выставленные экспертами оценки для каждой вышеописанной угрозы методом Дельфи.

ТАБЛИЦА 2. Выставленные экспертами оценки

	УБИ 173	УБИ 127	УБИ 116	УБИ 086	УБИ 036	УБИ 042	УБИ 172	УБИ 170	УБИ 006
Эксперт 1	10	6	4	2	3	1	2	1	2
Эксперт 2	10	8	7	3	3	2	2	1	1
Эксперт 3	10	7	6	4	8	1	5	1	1
Эксперт 4	8	6	5	3	10	2	2	1	1
Эксперт 5	7	2	2	6	4	7	6	4	2
Эксперт 6	10	5	6	4	2	5	3	2	2

Результаты рассчитанного риска угроз представлены в таблице 3.

ТАБЛИЦА 3. Полученные коэффициенты и риск угроз

Средняя оценка	УБИ 173	УБИ 127	УБИ 116	УБИ 036	УБИ 086	УБИ 172	УБИ 042	УБИ 170	УБИ 006
Коэффициент уязвимости	9,2	5,7	5	5	3,6	3,3	3	1,7	1,5
Коэффициент угрозы	1	3	1	2	2	3	3	1	3
Риск	**9,2**	**17,1**	**5**	**10**	**7,2**	**9,9**	**9**	**1,7**	**4,5**

Проанализировав полученные результаты, видим, что наиболее опасной угрозой является угроза подмены действий пользователей путём обмана.

Следует отметить, что из года в год совершенствуются техники обмана пользователей. Так, в последних версиях Android при отправке текстового сообщения на премиум-номер система спросит у пользователя разрешения. Изобретатели SMS-троянца Tiny поверх этого диалогового окна выводят свое, которое не перекрывает при этом кнопки оригинального окна.

Вторыми наиболее опасными являются угрозы УБИ.036 и УБИ.172.

Через «почтовые черви», к которым и относятся загрузчики, нарушитель устанавливает вредоносное ПО на устройство пользователя, когда risktool же часто помогают вышеперечисленным вредоносным программам оставаться незаметными легально, посредством выключения тех или иных процессов, приложений.

Угроза «спама» на сегодняшний день находится на третьем месте. Количественно её очень много, но угрозы как таковой она не представляет.

УБИ.042, угроза межсайтовых подделок запросов на четвёртом месте.

Банкеры напрямую крадут учётные данные от систем интернет-банкинга, мобильного банкинга и платёжных систем.

УБИ.086 на пятом месте.

Основная функция – перенаправить SMS-транзакции, осуществляемые во время оплаты пользователем контента или продуктов приложениях так, чтобы средства ушли на счёт к злоумышленнику. На сегодняшний день Triada – самый сложный зловред данного типа.

Угроза перехвата данных, передаваемых по вычислительной сети занимает всего лишь шестое место, на общем фоне угроз.

Сюда же входят spy-трояны, которые воруют персональные данные пользователей, в том числе входящие SMS (mTAN) от банков.

Остальные угрозы на общем фоне обладают наименьшим риском для физических лиц.

Вывод

Ключевым преимуществом электронного банкинга является возможность доступа к счетам в любое время и из любого места. Клиенту теперь не обязательно посещать банк для выполнения платежей или получения выписки – он может всё это сделать, не отходя от своего рабочего места и имея под рукой лишь телефон, с выходом в интернет.

В сфере информационной безопасности электронного банкинга используются различные решения, число которых очень велико. Многие банки предлагают своим клиентам такие услуги, как мобильный банк, позволяющий отслеживать все движения по счету, 3D-Secure, как двухфакторную аутентификацию, выпуск виртуальной карты, и открытие дополнительного накопительного счета. Но на сегодняшний день все эти решения не обеспечивают гарантированную защиту. Универсального «способа защиты от мошенничества» нет, как и нет действенного способа защиты от обмана вообще. Возможно, что высокая степень защищённости от мошеннических операций может быть достигнута за счет следования тактике, основанной на общепринятых принципах безопасного поведения совместным использованием специализированных механизмов. Современные методические аспекты в области обеспечения информационной безопасности для физических лиц требуют доработки и совершенствования. Защите в сфере информационной безопасности электронного банкинга сейчас крайне необходимы преобразовании и инновация.

Список используемых источников

1. Волков Д. Кибермошенничество в России: эволюция угроз // Банковские технологии. 2015. № 1. С. 26–28.

2. Статистика Центрального Банка Российской Федерации по ДБО за 2015 год [Электронный ресурс]. – URL: http://www.cbr.ru/statistics/ (дата обращения: 03.05.2016).

3. Мастяева И. Н., Мирзаханян Р. Э. Методы и модели рисков в различных областях // Фундаментальные исследования. 2014. № 9–2. С. 399–402.

4. Интерактивная карта киберугроз // Касперский [Электронный ресурс]. – URL: https://cybermap.kaspersky.com/stats/ (дата обращения: 10.05.2016).

5. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю [Электронный ресурс]. URL: http://bdu.fstec.ru/threat (дата обращения 01.05.2016).

Статья представлена научным руководителем,
доктором технических наук, профессором Карцевым И. И.

УДК 004.72

С. А. Высоцкий (студент группы ИКТМ-54М, СПбГУТ)
В. С. Елагин (кандидат технических наук, доцент, СПбГУТ)
В. С. Пряжников (студент группы ИКТМ-54М, СПбГУТ)
В. А. Сорокин (студент группы ИКТМ-54М, СПбГУТ)

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ И ДАЛЬНЕЙШЕГО ПРИМЕНЕНИЯ DPI НА SDN СЕТЯХ

Технологии стремительно развиваются. Появляются новые стандарты и типы сетей. SDN сети – новый виток в сфере инфокоммуникаций. Ввиду недостаточного развития сети отсутствуют многие услуги на данной сети. В статье описывается возможность применения технологии DPI для расширения функционала сети.

программно-конфигурируемые сети, трафик, глубокий анализ пакетов.

В настоящее время технологии стремительно развиваются. Одним из перспективных направлений являются SDN сети [1]. SDN *(Software Defined Networking)* – программно-конфигурируемые сети, технология построения архитектуры сетей связи, основанная на принципе разделения функций управления и функций передачи данных. Технология определяет два вида устройств: контроллеры и коммутаторы. Концепция предполагает, в отличие от традиционных сетей связи, вынести функции управления в отдельное устройство контроллер, а коммутаторам оставить только функцию передачи трафика, минимальный функционал устройства должен снизить их стоимость [2]. Такой подход может существенно снизить затраты на масштабирование и обслуживание сети, однако сейчас концепция не выполняет из-за того, что SDN-коммутаторы стоят достаточно дорого. Декомпозиция может быть, как физическая, так и логическая (в целях тестирования). К контроллеру подключены все коммутаторы в сети, соответственно контроллеру известны все процессы, проходящие на каждом коммутаторе, таким образом, контроллер имеет возможность оперативной работы с таблицами коммутаторов, в том числе может и конфигурировать маршрут передачи данных в зависимости от загруженности конкретного коммутатора, т. е. выполнять балансировку нагрузки. Таким образом, достигается оптимальное распределение ресурса, в SDN сетях. Контроллер общается с каждым коммутатором по протоколу OpenFlow. В настоящее время последняя версия протокола *v*1.5, однако стабильной является версия *v*1.3. Обмен данными между контроллерами и коммутаторами осуществляется за счёт двух типов сообщений: *of_packet_in, of_packet_out*.

На момент проведения исследований уровень развития SDN сетей остается на достаточно низком уровне. Вследствие чего возникают проблемы при реализации дополнительных сервисов, таких как: контекстная

реклама, сервисы обеспечения безопасности и им аналогичные. Решения на базе технологии DPI позволят существенно расширить список дополнительных сервисов и услуг.

Проблема применения функций этих сервисов состоит в том, что структура и функционал сетей SDN существенно отличается от тех, которые существуют сейчас и использовать технические средства для обеспечения этих функций в традиционном виде будет нельзя.

DPI *(Deep Packet Inspection)* – система глубокого анализа пакетов [3]. Исходя из специфики сетей SDN можно заметить, что существует несколько возможных мест установки DPI. Так как в SDN сетях весь трафик идет через контроллер, то мы можем установить DPI на нем (рис. 1).

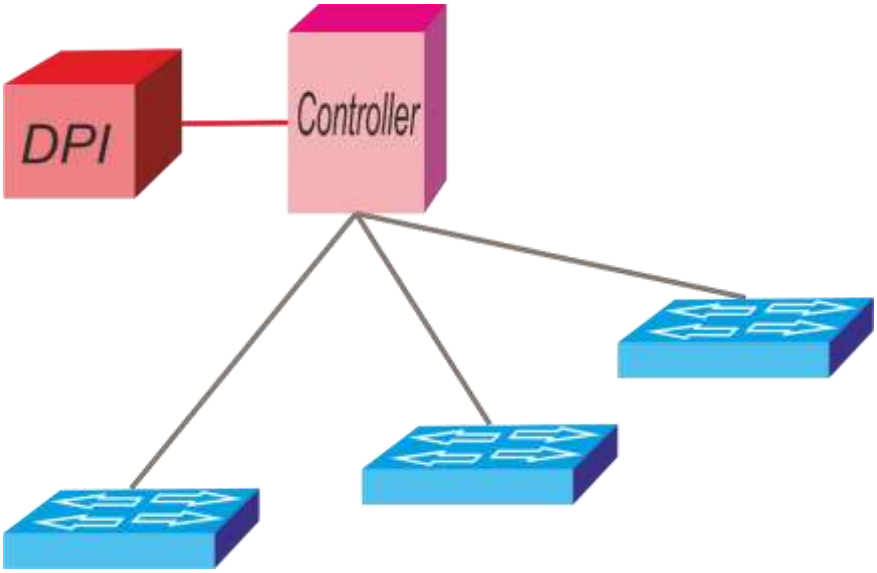


Рис. 1. Установка DPI с подключением в контроллер

Это даст доступ к информации о всем трафике сети, но с небольшим исключением: мы можем лишь просматривать информацию о трафике. DPI на контроллере дает возможность отследить все источники и пункты назначения трафика, определить MAC-адреса на канальном уровне, определить транспортный протокол и его порты, определить прикладные протоколы, если такие имеются и порты на них. Исходя из этих данных можно полностью идентифицировать хост-отправитель и его цель в сети, а также следить за всеми его сессиями.

Второй метод размещения DPI на сети SDN – это установка его в разрыв между контроллером и коммутаторами сети (рис. 2). Можно было бы рассмотреть установку на каждом коммутаторе, но при таком методе рушится концепция сети SDN, т. к. ее суть в том, чтобы сделать коммутаторы наиболее «глупыми» и как следствие более дешевыми. В данном случае мы имеем возможность полностью контролировать потоки трафика, следить за их источниками, а также, при необходимости модифицировать отдельные пакеты или целые сессии.

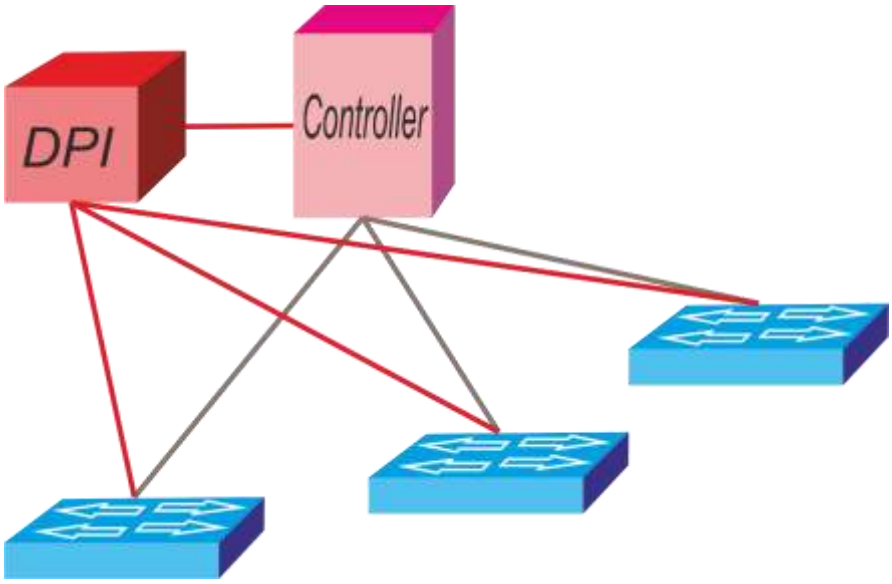


Рис. 2. Установка DPI в разрыв между контроллером и коммутаторами

Была развернута виртуальная SDN сеть с помощью эмулятора Mininet. Так же был написан скрипт на ЯП Python с применением библиотеки Scapy, реализующий функционал DPI. Целью скрипта являлось нахождение и выделение из общего потока трафика OpenFlow потоков. Также была реализована сигнатура (рис. 3) для OpenFlow трафика, поскольку в библиотеке Scapy готовой сигнатуры не было. OpenFlow пакеты имеют некоторые постоянной длины, что и позволило реализовать сигнатуру.

```
def pkt_callback(pkt):
    n_time = int(time() * 1000000)
    if TCP in pkt and Raw in pkt:

        pkt_n = pkt.getlayer(Raw)
        try:
            pkt_n =  pkt_n.load.encode('HEX')

            l_pkt = len(pkt_n)/2

            v = pkt_n[:1]
            type = pkt_n[2:4]
            lenght = pkt_n[4:8]
            id = pkt_n[8:16]

            if l_pkt == int(lenght, 16):
                print '\nOpenFlow: v: %s type: %s lenght: %s id: %s' % (v, type, lenght, id)
                k_time = int(time() * 1000000)
                print '\nTime: %d\n' % (k_time - n_time)
            else: pass
        except: pass
```

Рис. 3. Сигнатура OpenFlow пакетов

Данная сигнатура определяет пакеты OpenFlow, а также считает сколько времени ушло на обработку пакета. Было проведено тестирование

сигнатуры на виртуальной сети SDN. Обнаруженные скриптом пакеты были отсортированы по времени обработки и представлены в виде графика.

Рис. 4. График времени обработки пакетов

На графике (рис. 4) видно, что основной объем пакетов обрабатывается в промежутке от 312 до 319 микросекунд. Это означает, что использование DPI на сети повлечет за собой появление задержек.

На данный момент были реализованы только примитивные функции DPI на SDN сетях. В дальнейшем исследовании ставятся следующие задачи:

1. Анализ вероятностно-временных характеристик при работе с DPI. Как видно из результатов эксперимента, представленных на графике (рис. 4) вмешательство в работу сети, привносит некоторые задержки, соответственно необходимо провести исследование этих задержек и проанализировать, не являются ли они критическими для работы сети.

2. Исследовать возможность модернизации трафика. Поставленная задача довольна обширная, в неё входят:

2.1 Изменение сигнального трафика, например, для преднамеренного изменения маршрута, на не оптимальный.

2.2 Попытка подмены не зашифрованных пользовательских данных, с целью борьбы с пиратством.

2.3 Добавление контекстной рекламы, информация для которой будет собираться посредством DPI, а также вырезание контекстной рекламы, на уровне оператора.

Внедрение любых из вышеописанных в этом пункте возможностей, также привнесёт в сеть задержки, которые соответственно необходимо учесть.

Список используемых источников

1. Сетевые технологии SDN – Software Defined Networking [Электронный ресурс]. URL: https://habrahabr.ru/company/muk/blog/251959/
2. Software-Defined Networking (SDN) Definition [Электронный ресурс]. URL: https://www.opennetworking.org/sdn-resources/sdn-definition
3. Высоцкий С. А., Матвеев П. С., Пряжников В. С., Сорокин В. А. Исследование систем для мониторинга и анализа сетевого трафика NTOPNG и NDPI [Электронный ресурс] // 69 региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2015»: сб. науч. ст. / под ред. К. В. Дукельского. СПб. : СПбГУТ, 2015. С. 105–108. URL: http://www.sut.ru/doci/ nauka/69rntk.pdf

УДК 004.9

В. Ю. Гойхман (кандидат технических наук, доцент, СПбГУТ)
А. А. Савельева (студентка группы ИКТК-26, СПбГУТ)

КЛАССИФИКАЦИЯ И АНАЛИЗ ПРОТОКОЛОВ ИНТЕРНЕТА ВЕЩЕЙ

В статье рассматриваются протоколы Интернета Вещей, приводится анализ их особенностей на основе рассмотрения сообщений и выполняемых с их помощью процедур. Сопоставляются процедуры и варианты применения протоколов, производится классификация. Актуальность данной темы обусловлена многообразием существующих протоколов, стандартов Интернета Вещей и отсутствием устоявшейся терминологии, описывающей концепцию в целом.

Интернет Вещей, IoT, Протоколы IoT, M2M, XMPP, SOAP, COAP, STOMP, MQTT, DDS.

Цель настоящей статьи – анализ существующих протоколов, их классификация. Для наиболее эффективного достижения цели было необходимо последовательно выявить особенности протоколов, этапы их взаимодействия, выделить ключевой признак для классификаций.

После первичного рассмотрения [1], представленных далее протоколов, была составлена следующая таблица (табл. 1), где главный критерий – назначение протокола. Данная информация была взята в качестве отправной точки в исследовании.

Далее, после детального изучения спецификаций [2, 3, 4, 5, 6, 7], было принято решение рассматривать протоколы на предмет выполняемых функций, которые реализуются с помощью наборов сообщений-методов (табл. 2).

ТАБЛИЦА 1. Сравнительная таблица

Протокол	Трансп.	Назначение	Особенность
XMPP	TCP	Для адресации в небольшой персональной сети	Для идентификации пользователей используются JID, по формату похожие на адреса электронной почты (username@jabber.ru)
SOAP	TCP	Для распределённой вычислительной среды	Поддерживает два механизма доступа SOAP RPC и SOAP Message
STOMP	TCP	Для сети, в которой есть вероятность использования нескольких комбинаций разных протоколов, нуждающейся в простом протоколе передачи сообщений через брокера	Взаимодействие со многими языками, платформами и брокерами
COAP	UDP	Для сети с ограниченными ресурсами, низким энергопотреблением	Учитывает различные вопросы среды реализации в ограниченных сетях
MQTT	TCP	Для загруженных сетей с большим количеством устройств и брокером	Использование механизма очередей сообщений
DDS	UDP	Для сетей, нуждающихся в распределении нагрузки	Реализует прямую шинную связь между устройствами на базе реляционной модели данных

ТАБЛИЦА 2. Сообщения протоколов Интернета Вещей

Протокол	Архитектура	Шаблон	Метод	Сообщения	Кол-во сообщений
XMPP	Клиент-Сервер	Bus-based	-	XML-потоки (строфы)	-
SOAP	Клиент-Сервер	Broker–based	Запрос-Ответ	Get; SOAPAction, SOAPActionResponse	3
STOMP	Издатель-подписчик	Broker–based	Запрос-Ответ	SEND SUBSCRIBE UNSUBSCRIBE BEGIN COMMIT ABORT ACK NACK DISCONNECT	9

Протокол	Архитектура	Шаблон	Метод	Сообщения	Кол-во сообщений
COAP	Клиент-сервер	Broker-based	Запрос-Ответ	GET PUT HEAD POST DELETE CONNECT	6
MQTT	Издатель-подписчик	Broker-based	Запрос-Ответ	CONNECT CONNACK PUBLISH PUBACK PUBREC PUBREL PUBCOMP SUBSCRIBE SUBACK UNSUBSCRIBE UNSUBACK PINGREQ PINGRESP DISCONNECT	14
DDS	Издатель-подписчик	Bus-based	Запрос-Ответ	Entity Class WaitSet Class Condition Class Publisher Class DataWriter Class Subscriber Class DataReader Class ReadCondition Class QueryCondition Class И другие	13 классов

Как видно из таблицы (табл. 2), для дальнейшего сравнения протоколы XMPP и DDS не подходят, поскольку нецелесообразно сопоставлять протоколы, основанные на потоках и классах с протоколами, основанными на сообщениях-методах. Очевидно, что из-за схожей структуры сообщений, оставшиеся протоколы можно соотнести с методами протокола HTTP [8], не анализируемого ранее, но подходящего для составления сравнительной таблицы (табл. 3). Методы OPTIONS и TRACE протокола HTTP не включены, поскольку не имеют аналогов в исследуемых протоколах.

ТАБЛИЦА 3. Сопоставление с методами протокола HTTP

HTTP	SOAP	STOMP	COAP	MQTT
GET	+		+	+
HEAD			+	
POST	+		+	+
PUT		+	+	+
DELETE			+	
CONNECT		+		+

Основываясь на сообщениях, выделим далее процедуры, реализуемые с помощью представленных сообщений, и подчеркнем отличительные особенности, заявленные в спецификациях (табл. 4). Таким образом, акцентируя внимание на свойствах протоколов, возможно разработать рекомендации по их использованию.

Также было необходимо обратиться и к уже существующим решениям, следовательно, осознать оптимальность выбора протокола (табл. 5). Заявленные в таблице варианты применений были заимствованы в различных разрозненных источниках, так как чаще всего данная информация не распространяется и не предоставляется производителями, как неориентированная на широкий круг пользователей, либо носящая конфиденциальный характер.

ТАБЛИЦА 4. Процедуры, выполняемые анализируемыми протоколами

Протокол	Процедуры	Отличительная особенность
XMPP	Процедуры запроса информации, получения данных, установки новых значений или замещения существующей величины.	● XML-потоки и XML-строфы обеспечивают быстрый асинхронный обмен; ● Схема адресации JID – набор элементов, образующих доменный идентификатор, идентификатор узла или ресурса.
SOAP	Удаленный вызов методов; Процедуры запроса параметров.	● Возможность удаленного вызова методов/функций с помощью механизма доступа SOAP RPC; ● Нейтрален к платформе.
STOMP	Процедуры публикации\подписки; Операции с транзакциями.	● Поддерживает операции с транзакциями; ● Поддержка большого количества совместимых библиотек.
COAP	Процедуры записи и получения необходимых конкретных параметров.	● Представляет собой двоичную версию протокола HTTP, упрощённую под задачи транспортировки данных по линиям с ограниченной пропускной способностью [9].
MQTT	Процедуры обработки публикаций/подписки.	● Поддерживает различные классы QoS (1–3); ● Поддерживает механизм очередей.
DDS	Процедуры получения и отправки данных.	● Реализует прямую шинную связь; ● «Хранение истории» – наличие кэша; ● Поддерживает механизм контроля «жизнеспособности» (Keepalive и Lifecycle)

ТАБЛИЦА 5. Примеры использования протоколов в конкретных решениях

Протокол	Примеры применения
XMPP	Philips Hue gateway, «умная техника» Nest Labs, RabbitMQ
SOAP	API Яндекс.Директ, Платформа .NET Framework; Реализован в Apache сервере, внедрен в IIS и Windows DNA 2000. Продукты поддерживающие SOAP: Voyager (Object Space), Zope – the Python Application Server (Digital Creations), Frontier groupware product (User Land).
STOMP	RabbitMQ, OpenMQ, HornetQ и другие
COAP	IoTivity, DS18B20 (датчик температуры), Проект Ньютон (умный дом)
MQTT	Mosquitto для Intel Edison, Платформа Eurotech Everyware Cloud (EDC), микроброкер IBM Lotus Expeditor, RabbitMQ
DDS	RTI, Система помощи водителю от VW, NAV Canada (аэронавигационная служба Канады)

Проанализировав полученные данные, возможно подвести итог по применению каждого из протоколов:

- **XMPP** – в системах освещения, а так же для адресации устройств в небольших персональных сетях; предусмотрена работа с Брокером.
- **SOAP** – поддерживает обслуживание Web-сервисов и обеспечивает совместную работу платформы и Internet-приложений.
- **STOMP** – ориентирован на обеспечение работы брокера сообщений. Используется в брокерах объектов «Умной индустрии».
- **COAP** – для устройств с ограниченными ресурсами и для сетей с низким энергопотреблением. К примеру, в системах датчиков температуры и других датчиков «Умного дома».
- **MQTT** – поддерживает обмен сообщениями в корпоративных системах и служит для подключения сенсорных узлов, а также в облачных платформах; ориентирован на работу Брокера.
- **DDS** – в автоматизированных системах управления движением, а также энергетике и финансовой сфере.

Сопоставив полученную информацию, можно составить упрощенные топологии, иллюстрирующие оптимальное применение определенного протокола на различных отрезках сети, с учетом особенностей каждого из них (рис. 1). Подразумевается, что Broker-сервер, который принимает информацию от источников и передает ее соответствующим получателям, в сложных системах может выполнять также различные операции, связанные с анализом и обработкой данных [9]. Под Devices понимаются устройства-датчики, объединённые работой микроконтроллера, а под Application – клиентское приложение, установленное на персональном устройстве.

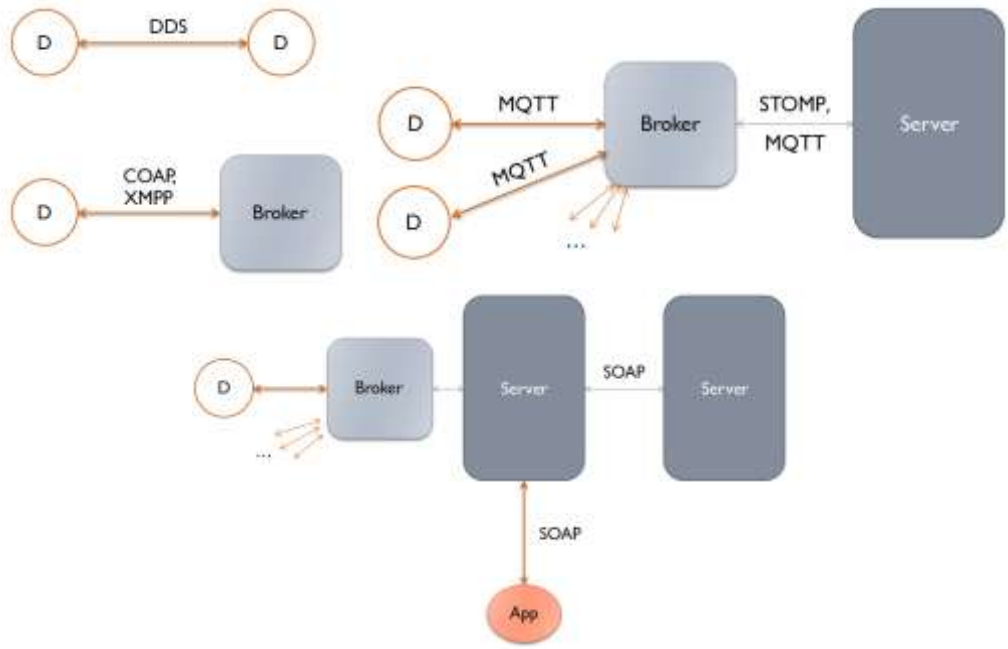


Рис. 1. Топологии, иллюстрирующие применение анализируемых протоколов

Согласно представленным топологиям, можно классифицировать протоколы по их направленности – для обеспечения связей между Датчиками/Узлами, Брокерами, либо Серверами/Приложениями пользователя. Такая классификация позволяет абстрагироваться от конкретного решения по применению протокола и сфокусироваться на его целевом назначении. Приведенный пример классификации является первичными. Учитывая, что существуют и перекрывающиеся области применения протоколов, вероятно, необходимо применять альтернативный подход к рассмотрению их особенностей и к составлению классификации.

Ключевые особенности протоколов зависят от их предполагаемого применения в условиях реализуемой сети. Основные задачи протоколов различны, различны архитектуры и возможности. Поэтому к выбору оптимального протокола для своего приложения нужно подходить основательно, объективно взвешивать все положительные и отрицательные свойства каждого из них, исходя из конкретных потребностей.

Список используемых источников

1. Гойхман В. Ю., Савельева А. А. Протоколы Интернета вещей // «Актуальные проблемы инфокоммуникаций в науке и образовании». V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. / под ред. С. В. Бачевского. СПб. : СПбГУТ, 2016.

2. Extensible Messaging and Presence Protocol (XMPP): Core // RFC-3920 // 2004.

3. Simple Object Access Protocol (SOAP) 1.1 / W3C / Don Box, David Ehnebuske, Gopal Kakivaya // 2000.

4. STOMP Protocol Specification, Version 1.2 // licensed under the Creative Commons Attribution v2.5 license // 2012.

5. The Constrained Application Protocol (CoAP) / RFC 7252 – Proposed Standard // 2014.

6. MQTT V3.1 Protocol Specification // International Business Machines Corporation (IBM) Eurotech / 2015.

7. OMG (Object Management Group) DDS v1.4 – the DDS specification // 2015.

8. Hypertext Transfer Protocol (HTTP/1.1) / RFC 2068 – Draft Standard// 1999.

9. Росляков А. В., Ваняшин С. В., Гребешков А. Ю. Интернет вещей. Самара: ПГУТИ, 2015. С. 107–109.

УДК 654.739

В. С. Голубев (студент группы МБИ-21, СПбГУТ)

РАЗРАБОТКА ПРИНЦИПОВ УПРАВЛЕНИЯ АДАПТИВНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

В статье рассматривается способы представления элементов функционирования программ управления для адаптивных систем. Исходя из представленных способов, следует вывести модель представления с целью выведения технических характеристик работы программного обеспечения. Данный программный элемент предназначен для защиты программного обеспечения и управления программами в рамках единой адаптивной системы.

адаптивные системы, экспертные системы, программы управления, клиент-серверная архитектура, защита информации.

Введение

Разработка ЭС в корне отличается от разработки обычного программного продукта. Сложность, новизна и неформализуемость задач, для решения которых предполагается разработать ЭС, приводит к невозможности заранее детально спланировать все шаги по ее созданию и разработать ее законченный прототип. Наиболее приемлемый выход из этого положения заключается в постепенном развитии системы. При этом используется концепция "быстрого прототипа", суть которой заключается в следующем:

Разработчик не пытается сразу создать законченный продукт или даже представить на начальном этапе архитектуру всей будущей системы. Как только разработчик приобретает достаточно знаний для реализации решения хотя бы ряда простых задач, он создает действующую модель-прототип системы, которая решает некоторые задачи конкретного приложения. Анализ модели-прототипа позволит оценить корректность выбранного подхода, определить следующие шаги по развитию системы. Поэтому попытаемся определить идеи, основные понятия и концепции, лежащие в основе ее построения.

Описание головного проекта

Проект **RPA** (лат. *rationabile progressio aggredi* [*умеренная программа для решения*]) – проект, объединяющий в себе несколько программных средств, аппаратно-программных средств и все ЭВМ, включенные в одну ЛВС. Цель **RPA** обеспечить адаптивную защиту выделенной ЛВС. Однако, в целом, вся адаптивная система не будет ограничиваться одной лишь защитой ЛВС. Среди списка ее задач будет следующее:

1. Содержание гибкой базы данных (знаний), накопление информации;
2. Саморазвитие, реализация адаптивных функций;
3. Успешная защита от:
   a. НСД;
   b. нарушения целостности;
   c. нарушения конфиденциальности...
4. Успешная "проактивная" защита:
   a. преследование нарушителя, "заброс" вредоносных файлов;
   b. содержание вредоносных элементов;
   c. шифрование файлов;
   d. создание стеганограм.

Определив основные идеи проекта была попытка начать разрабатывать первую версию RPA – A_RPA.

Программа *"***A_RPA***"* разбивается на следующие компоненты:

1. *Medic_RPA* (Санитар) – данное программное предназначенное для восстановления и поддержки всего ПО "A_RPA". Включает в себя следующие возможности:
   a. создание резервных копий;
   b. шифрование данных;
   c. встроенный стегокодер.
2. *Worker_RPA* (Рабочий) – специальное программное обеспечения для осуществления поисковой работы общего ИИ. Включает в себя:
   a. универсальный и совершенствуемый поисковик;
   b. Анализатор + Синхронизатор (для БД) выбранной/найденной информации.
3. *Solder_RPA* (Солдат) – главная причина создания A_RPA в целом, инструмент защиты и атаки. Включает следующие элементы:
   a. антивирус (карантинная область, удаление вредоносных кодов);
   b. шпион – перехватчик информации (принцип DLP-систем, различных снифферов и кейлогиров);
   c. бекдор – важный инструмент для реализации скрытного захода не только на удаленные машины, но и на рабочие станции ЛВС;
   d. дешифратор – использование набора известных методов криптоанализа и стегоанализа (может разделяться на два элемента);
   e. заразитель – элемент подбора вирусных атак для контратаки нарушителя. Должен будет включать в себя знания о различных типах вирусов и элементов их рассылки (спам).

Любая экспертная система имеет клиент-серверную архитектуру, разобравшись с ее серверной составляющей, перейдем к клиенту.

Клиентская часть RPA это программа управления RPA manage, осуществляющая взаимодействие со всей системой: с серверной ее частью

непосредственно, с «ульем» опосредовано через серверную. Функции RPA manage:

- Аутентификация.
- Взаимодействие с базами данных.
- Наличие редактора кода и возможность загружать/сохранять исходники модулей улья с целью их ручного редактирования – это необходимо на первых этапах для первоначального обучения агентной НС и для последующего ее контроля.
- Логирование событий в программе.
- Вывод лога с сервера о произошедших событиях.
- Отображение кластеров защищаемой сети с конечными машинами в визуально информативной форме, для мониторинга состояния обеспечения защищенности.

Это полный перечень функций, которые на данный момент необходимо реализовать в проекте.

Программа RPA manage будет разрабатываться с расчетом на то, что ее можно будет использовать для управления экспертными системой. Реальность такова, что RPA будет разрабатываться параллельно с программой управления. Это значит, что требования к программе могут меняться в процессе разработки. Необходима гибкость при разработке. Ее можно достигнуть применением такого шаблона проектирования как MVC, что расшифровывается как *model-view-controller* (модель-представление-контроллер). Схема шаблона представлена на рисунке 1.

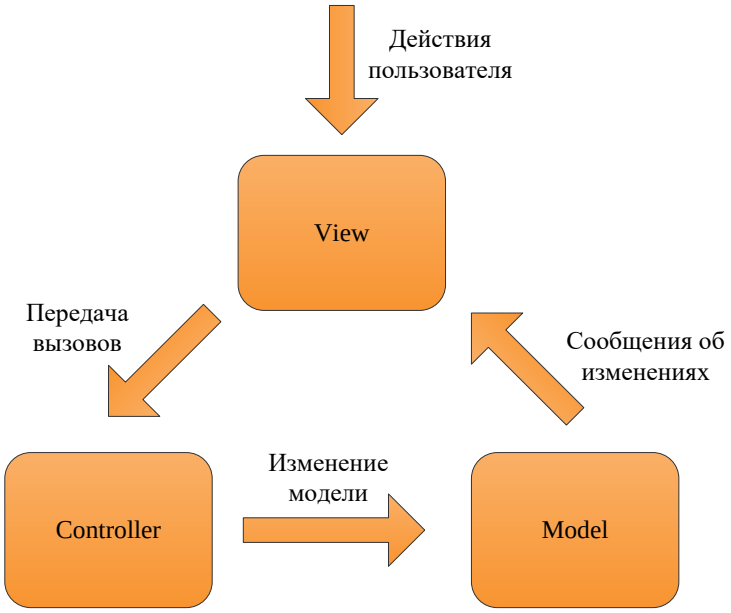


Рис. 1. Схема шаблона проектирования MVC

Шаблон проектирования MVC предполагает разделение данных приложения, пользовательского интерфейса и управляющей логики на три от-

дельных компонента: модель, представление, контроллер, таким образом, что модификация каждого компонента может осуществляться независимо.

Модель (*Model*) предоставляет данные предметной области представлению и реагирует на команды контроллера, изменяя свое состояние.

Представление (*View*) отвечает за отображение данных предметной области (модели) пользователю, реагируя на изменения модели.

Контроллер (*Controller*) интерпретирует действия пользователя, оповещая модель о необходимости изменений.

Модель может представлять собой объект, реализующий переключатель. В простейшем случае данная модель характеризуется состоянием: выключен или включен – и, кроме того, позволяет изменять его – объект модели имеет метод изменения состояния:

– выключить,
– включить.

Представление отображает на дисплее состояние переключателя с помощью определенной текстовой или графической формы. Например, представление может отображать текстовую метку, которая при изменении состояния модели переключателя отобразит соответствующий текст:

– выключен,
– включен.

Помимо отображения представление позволяет пользователю изменять состояние переключателя с помощью графических примитивов, к примеру, двух кнопок с надписями:

– включить,
– выключить.

Представление умеет только отображать состояние модели переключателя, для изменения представление обращается к контроллеру.

Контроллер представляет собой объект, который в нашем случае умеет только изменять состояние модели переключателя.

Разработав такой примитивный шаблон нам будет очень просто вносить изменения в панель управления и производить ее модификацию.

Выбранный итеративный подход к разработке, оказался единственным правильным решением, так как блоки системы развиваются параллельно и, поэтому для лучшей согласованности разработки проекта необходимо проводить ревизию требований к каждому из блоков часто.

Также это значит, что в каждой итерации каждый из блоков будет дорабатываться «понемногу» и на первой итерации разработки нужно как можно быстрее получить прототип программы, чтобы было с чем работать в дальнейшем; что улучшать.

Прототип RPA manage (рис. 2) будет реализовывать необходимый минимум функций для работы с удаленным приложением, а именно ЭС. Вот этот список функций:

- Идентификация пользователя с последующей аутентификацией на сервере (аутентификацию пока что можно реализовать в самой программе).
- Логирование событий.
- Возможность удаленной работы с базой данных, формируемой на сервере.
- Наличие консольной строки ввода.

Рис. 2. Прототип программы управления

Заключение

В расчете закона управления используется принцип работы программ управления, и полученные управляющие значения обеспечивают так называемое «проактивное управление», что позволяет заранее принимать эффективные меры противодействия распространению потенциальных угроз, а не реагировать на ситуацию только после очередного шага злоумышленника или угроз нарушения доступа.

Список используемых источников

1. Кучер В. А., Атрощенко В. А., Видовский Л. А., Трофимов В. М. Модель информационной безопасности процессов управления вычислительными сетями [Электронный ресурс] // Научный журнал КубГАУ. 2009. № 110 (06). URL: http://ej.kubagro.ru/2015/06/pdf/117.pdf

2. Rohloff K. Stochastic Behavior of Random Constant Scanning Worms// Computer Communications and Networks, 2005. ICCCN 2005. – Proceedings. 14th International Conference on 17–19 Oct. 2005.

3. Захарченко А. А. Черводинамика: причины и следствия // Защита информации. Конфидент. 2004. № 2. С. 50–55.

4. Андрианов В.И., Романов Г.Г., Штеренберг С.И. Экспертные системы в области информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая

конференция: сборник науч. ст. в 2 т. / под ред. С. В. Бачевского. СПб. : изд. СПбГУТ, 2015. Т. 1. С. 193–197.

5. Штеренберг С. И. Методика построения поисковой системы для примитивной программы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 52–57.

Статья представлена научным руководителем,
аспирантом Штеренбергом С. И.

УДК 004.78

И. Д. Григорьев (студент магистратуры группы М091501(72) МТУСИ)

КЛАССИФИКАЦИЯ СЕРВИСОВ ПРИКЛАДНОГО УРОВНЯ В СИСТЕМЕ *CNS/ATM*

В статье описаны компоненты авиационной системы и их функции, а также обоснована актуальность рассматриваемых вопросов. На основании стандартизирующих документов определены основные типы работающих приложений и параметры качества обслуживания. Реализация механизмов качества обслуживания требуется для корректной работы приложений в системе и установления возможности расширения системы.

авиационные системы, беспроводные системы, гражданская авиация, приложения, качество обслуживания, наблюдение.

В начале 1980-х годов, ИКАО (Международная организация гражданской авиации) признала усиливающиеся ограничения существующей навигационной системы и потребность в улучшениях. В 1983 году ИКАО создала FANS (*Committee of Future Air Navigation Systems*) с целью изучения и внедрения новых концепций и методов. FANS занялась разработкой новых систем CNS (*Communications, Navigation and Surveillance*) для управления воздушным движением (ATM) для организации связи земля-воздух преимущественно средствами цифрового канала передачи данных. ИКАО разработала архитектуру систем связи, которая удовлетворяла бы нуждам пользователей (авиакомпаниям и государствам).

Основой для внедрения и работы такой системы служит авионика. Авионикой называются электронные системы, располагающиеся на борту авиационного судна. Она занимается коммуникацией, навигацией, управлением множеством систем и является неотъемлемой частью современных летательных аппаратов.

В настоящее время данная архитектура частично внедрена в эксплуатацию [1]. В системе существует 6 главных компонентов:

1. Интерфейс пилота должен быть эффективным и простым во взаимодействии с системой передачи данных, помимо этого, организация взаимодействия пилот-контроллер требуют наличия крайне быстрого механизма. Использование цифрового канала передачи для предоставления интерфейса требует разработки таких процедур, при работе которых были бы минимизированы системные ошибки ввода.

2. Электроника авиалайнера является основой для работы цифровой системы передачи данных. Оборудование должно обрабатывать данные, принимаемые от интерфейса пилота, сенсоров и системы управления полетом, и направлять информацию в цифровой канал передачи данных в реальном времени. Оборудование также должно обрабатывать входящие извне сигналы от авторизованных источников.

3. Канал передачи данных воздух-земля и земля-земля может быть, как ATN-совместимым, так и спутниковым, либо другим, соответствующим требованиям для работы с системой передачи. При передаче системой авиалайнера будет выбран наиболее подходящий путь на основании изменяющихся во времени параметров: географическое положение, стоимость передачи, задержка, пропускная способность и доступность соединения [2].

4. Канал воздух-земля будет соединен с системой управления воздушным движением через существующую наземную сеть связи. Сеть должна быть совместима с наборов протоколов, используемых в концепции ATN. Для передачи любых сообщений наземные ATN-маршрутизаторы должны выбрать наиболее подходящий канал.

5. Наземная система должна осуществлять связь и распространение информации о местоположении с минимальным участием диспетчера. Мониторинг совместимости, избегание коллизий, обработка ошибок и большое количество других функций, связанных с безопасностью и эффективностью управления воздушным трафиком выполняет наземная система.

6. Интерфейс взаимодействия с контроллером содержит требуемые инструменты для композиции сообщений канала воздух-земля. Провайдеры авиационных систем проектируют и разрабатывают интерфейсы контроллеров, которые бы удовлетворяли их нуждам.

В рамках данной системы работает большое количество приложений, каждое из которых стандартизировано [3]. *Data Link Initiation Capability* (DLIC) предоставляет необходимую информацию для установки канала между наземной станцией и авиалайнером. Запуск приложения инициируется авиалайнером. Приложение выполняет следующие функции: вход в систему, выполнение инструкций по связи с наземными системами другого типа, локальное распространение информации, продвижение информации о входе в систему на земле.

Automatic Dependent Surveillance (ADS) – автоматическое зависимое наблюдение, данное приложение отвечает за наблюдение за положением воздушных судов, находящихся в океаническом пространстве и других зонах, где обеспечивается контроль управления трафиком без использования радара.

Controller-Pilot Data Link Communications (CPDLC) отвечает за организацию двустороннего обмена данными между авиадиспетчером и пилотом. Отправка CPDLC сообщения начинается с выбора адреса, выбора и, если необходимо, дополнения сообщения в отображаемом меню, либо другими способами, которые позволили бы организовать быструю компоновку сообщения и начало передачи. Сообщение может включать в себя разрешения на вход в воздушное пространство, ожидаемые разрешения, запросы, отчеты и иную информацию. Наиболее важным преимуществом работы данного приложения является снижение нагрузки на голосовой канал связи, поскольку эти данные в настоящее время передаются преимущественно с использованием аналогового голосового канала.

Data Link Flight Information Services (FIS) позволяет передавать информацию о полете, которая может быть предоставлена авиалайнеру в дискретной форме, например информация о погодных условиях, аэродромах и т.д. Такая информация поможет пилоту, усилив безопасность полета и улучшив ситуационное оповещение.

ATS *Interfacility Data Communication* (AIDC) обрабатывает информацию о приближающихся рейсах, границе района полетной информации. Также приложение занимается координацией условий пересечения границы и контролем трансфера.

Automatic Dependent Surveillance – Broadcast (ADS-B) – приложение наблюдения, занимающееся передачей таких параметров, как позиция и идентификация, широковещательным каналом для приема таких данных любыми наземными или воздушными пользователями.

На основании теоретических данных о распределении трафика для каждого из видов приложений можно определить эталонные требования к качеству обслуживания, указанные в таблице 1. Вдобавок к указанным условиям, всем приложениям требуется:

- вероятность потери отправленного сообщения должна быть меньше или равна 10^{-6};
- вероятность того, что после потери сообщения в системе, уведомление о потере не будет доставлено источнику должна быть меньше или равна 10^{-9};
- вероятность ошибочного направления сообщения к получателю должна быть равна или меньше чем 10^{-7}.

ТАБЛИЦА 1. Требования к системам связи для различных типов приложений

Приложение	Доступность (%)	Целостность	Надежность (%)	Непрерывность (%)
DLIC	99,9	10^{-6}	99,9	99,9
ADS	99,996	10^{-7}	99,996	99,996
CPDLC	99,99	10^{-7}	99,99	99,99
FIS	99,9	10^{-6}	99,9	99,9
AIDC	99,996	10^{-7}	99,9	99,9
ADS-B	99,996	10^{-7}	99,996	99,996

В таблице 2 отображены различные уровни производительности системы связи, которые могут быть выбраны для предоставления вышеописанных сервисов в рамках существующей системы. В зависимости от предоставляемого уровня сервиса, любое государство может определить производительность, требуемую в рамках данной области, руководствуясь такими факторами как распределение авиалайнеров в воздушном пространстве (эшелонирование), плотность трафика и пути его следования.

ТАБЛИЦА 2. Требования ко времени задержки передачи

Уровни производительности	Рекомендованная задержка передачи в режиме «точка-точка», сек	Задержка в 95 % случаев в режиме «точка-точка», сек	Задержка в 99,996 % случаев в режиме «точка-точка», сек
A	0.5	0.7	1
B	1	1.5	2.5
C	2	2.5	3.5
D	3	5	8
E	5	8	12.5
F	10	15	22
G	12	20	31.5
H	15	30	51
I	30	55	90
J	60	110	180

Можно также определить рекомендацию, при которой ни одно сообщение в соединении «точка-точка» не должно передаваться от источника к получателю дольше, чем 30 секунд. Исключением могут служить исключительные ситуации: природные катаклизмы, террористическая атака.

Развитием и разработкой CNS/ATM системы в настоящее время непрерывно занимаются ученые по всему миру, совершенствуя как аппаратную, так и программную базу, стандартизируя и внедряя новые элементы системы. Количество приложений, работающих в системе увеличивается, и в связи с этим, вопросы организации качества обслуживания выходят на первый план. Вышеописанное является достоверным признаком появления в ближайшем времени новых методов, которые позволят эффективнее и надежнее передавать данные в авиационных системах.

Список используемых источников

1. ICAO Doc 9750-AN/963, Глобальный аэронавигационный план на 2013–2018 гг., изд. 4-е. Канада : Монреаль, 2013.
2. ETSI EN 302 842-1 VHF air-ground and air-air Digital Link (VDL) Mode 4 radio equipment; Technical characteristics and methods of measurement for aeronautical mobile (airborne) equipment, 2010.
3. ICAO Doc 9694-AN/955 Manual of Air Traffic Services Data Link Applications, 1st edition, 1999.

Статья представлена научным руководителем
кандидатом технических наук, доцентом Орловым В. Г.

УДК 004.042

Н. Ю. Гричиненко (студент группы ИКПИ-32, СПбГУТ)
В. В. Громов (студент группы ИКПИ-32, СПбГУТ)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБРАБОТКИ ДАННЫХ С ДАТЧИКОВ ГАЗА И ТЕМПЕРАТУРЫ ПРИ ПОМОЩИ МИКРОКОМПЬЮТЕРА RASPBERRY PI 2B

В статье рассматривается взаимосвязь компонентов сложной системы, в которой неразрывно связаны такие понятия как удаленная обработка данных на WEB-сервере и программирование микроконтроллеров. Такая статья интересна тем, что реализация задачи охватывает очень широкий аспект работы компьютерной техники, где результат зависит от функционирования физической цепи питания и калибровкой датчиков, заканчивая работой баз данных сервера в сети Интернет.

Raspberry Pi, Raspbian, датчики, MySQL, Python, PHP, Google Charts.

Теоретическая справка

Разработка представляет собой заготовку для системы мониторинга за окружающей средой в режиме реального времени с отображением информации в сети Интернет. Главными компонентами системы являются:

- Микрокомпьютер *Raspberry Pi*, работающий под операционной системой *Raspbian*.
- Датчики для измерения температуры и показаний концентрации углекислого газа.
- *WEB-сервер*, который занимается сбором информации, которую передает микрокомпьютер.

Пользователь такой системы может дистанционно зайти на генерируемую страницу *WEB-сайта* и посмотреть показания датчиков в режиме реального времени. Подобные системы используются в “Умных” домах, где владелец может посмотреть различные показания датчиков, которые отображают полезную информацию, например, показания температуры, газа, счетчика воды, электричества и т. д.

Общая схема взаимодействия представлена на рисунке 1.

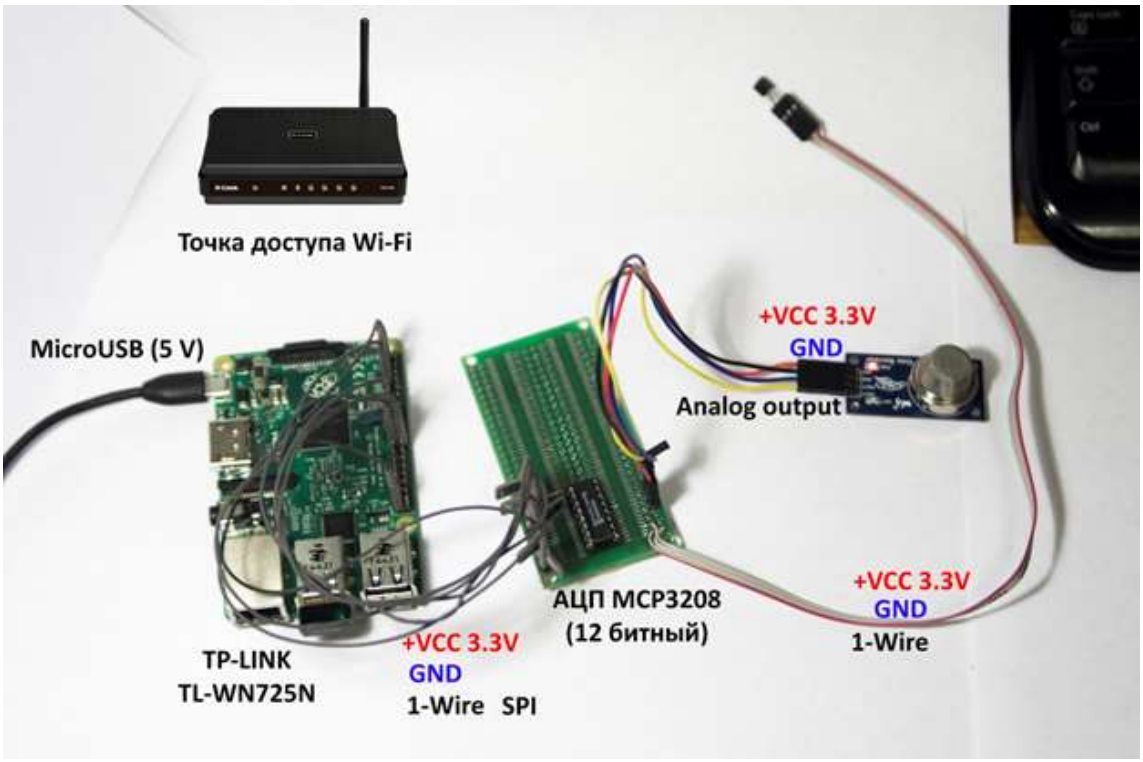


Рис. 1. Интерфейс взаимодействия составных частей системы

Микрокомпьютер *Raspberry Pi 2B* является миниатюрным компьютером, работающим под операционной системой *Raspbian*, которая основана на дистрибутиве *Linux Debian*. Также для микрокомпьютера доступны и другие адаптированные версии операционных систем: *Windows 10*, *FreeBSD* и т. д.

Raspberry Pi 2B также может выполнять роль микроконтроллера, поскольку имеет 40 пинов для ввода/вывода с различных датчиков и устройств. Выходы *Raspberry Pi 2B* поддерживают множество интерфейсов для ввода/вывода, такие как *GPIO*, *1-Wire*, *SPI*, *i2C*, *UART* и т. д.

Плата-контроллер *Raspberry Pi 2B* считывает данные с датчика температуры *DS18b20* и датчика концентрации углекислого газа *CO2 SNS-MQ135* в интервале один раз в минуту. Полученную информацию микроконтроллер, который подключен к сети Интернет при помощи Wi-Fi-*роутера* по беспроводному соединению Wi-Fi, передает на сервер.

Датчики подключены через интерфейсную схему с аналоговым цифровым преобразователем (АЦП), поскольку датчик концентрации газа на выходе имеет аналоговый сигнал, тогда как микрокомпьютер *Raspberry Pi 2B* не располагает встроенным АЦП.

Датчик концентрации газа *MQ135* передает данные о концентрации газа на *Raspberry Pi* и имеет следующие характеристики:

- Рабочая температура: от −10 до +45 градусов.
- Влажность: не менее 95 % *Rh*.
- Стандартная концентрация кислорода: 21 %.
- Концентрация кислорода может влиять на чувствительность, минимальная концентрация составляет 2 %.
- Чувствительность датчика: концентрация газов в пределах – аммиак 10–300 *ppm*, бензин 10–1000 *ppm*, спирт 10–300 *ppm*.

Для корректной работы датчика газа необходима калибровка датчика. Для этого требуется «прогревание» датчика газа на 24 часа с последующими математическими расчетами. В данной работе рассматривались приблизительные значения датчика, а для расчета были использованы значения других пользователей, которые прогревали датчик на 24 часа и снимали с него показания.

Датчик температуры DS18b20 может работать в температурных диапазонах от −55 до +125 градусов и имеет погрешность +/− 0,5 градусов на интервале от −10 до +85 градусов. Датчик отправляет данные (9, 10, 11, 12-битное число в зависимости от настройки) по интерфейсу 1-Wire и имеет 64-битный код для идентификации датчика.

Для снятия данных с двух датчиков на стороне микроконтроллера была разработана программа на языке Python, которая опрашивала датчик температуры и снимала показания с внешнего АЦП, после чего отправляла данные на сервер.

Отправка данных на сервер

После обработки показаний углекислого газа и температуры происходит их отправка на сервер с установленной системой управления базами данных *MySQL*. Сервер может быть установлен непосредственно

на *Raspberry Pi*, однако более логичным представляется его расположение на удаленной машине.

Поскольку обработка данных происходит в файле со скриптом Python-программы, дальнейшая отправка на сервер осуществляется в нем же. Это становится возможным благодаря драйверу python-mysqldb, устанавливаемому на Raspberry Pi. В общем виде подключение к базе данных и создание курсора (объект для работы с ней) выглядит следующим образом

```
db= MySQLdb.connect(host="IP",user="username",passwd="password",
db="database_name")
cursor= db.cursor()
```

IP – *IP* адрес хоста,
username – логин,
password – пароль,
database_name – название базы данных.

Далее осуществляется SQL-запрос в таблицу *gas*, расположенную в базе данных *server*, со вставкой данных, а именно – времени (*datetime*), когда произошло снятие данных, и показания концентрации газа (*gas*). Завершается код исполнением запроса и применением изменений в базе данных.

```
sql = ("""INSERT INTO server.gas (datetime,gas) VALUES (%s,%s)""",
(datetime,gas))
try:
  cursor.execute(*sql)
  conn.commit()
except:
  conn.rollback()
    exit (0)
```

Стоит отметить, что для показаний температуры процедура отправки данных в виде SQL-запросов аналогична.

Отображение данных на сайте

Для наглядного отображения данных с показаниями датчиков температуры и углекислого газа можно прибегнуть к созданию обычной страницы на сервере, где будет расположен скрипт от *Google Charts* для вывода графиков.

Значения для графиков берутся путем php запроса к базе данных с указанием IP-хоста, логина и пароля, а также базы данных и нужной таблицы. После этого создается таблица данных для *Google Charts*, куда передаются необходимые данные.

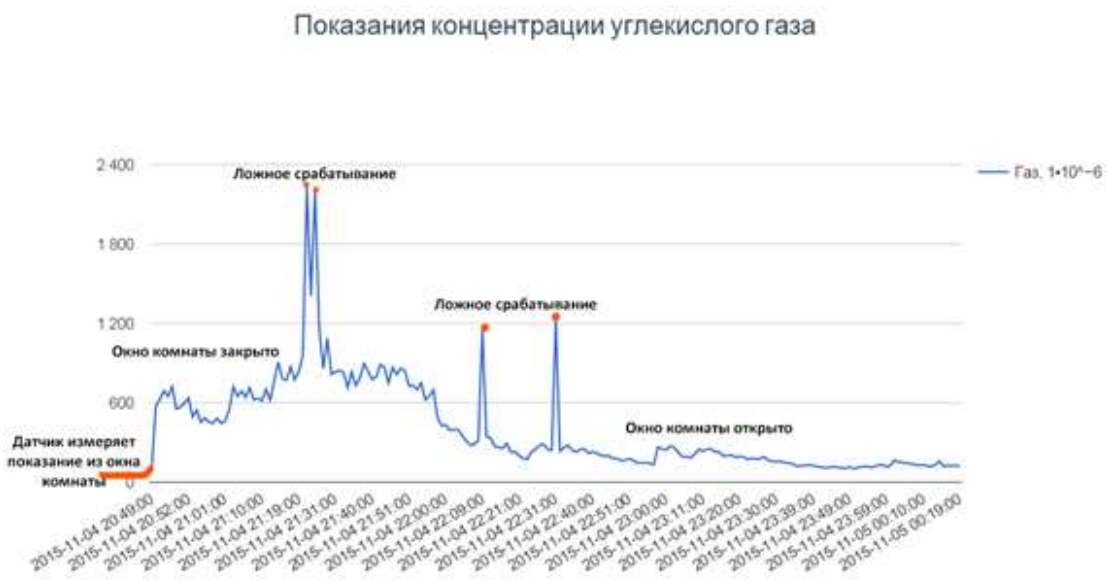


Рис. 2. График с показателями концентрации углекислого газа

На данном графике видно, как в самом начале датчик снимает показание газа на улице, после чего происходит повышение показателей вследствие того, датчик находился в комнате с закрытым окном (при этом имеются два ложных срабатывания), а далее – понижение концентрации газа из-за того, что окно закрыли.

Как можно заметить, датчик иногда выдает ложные показания. Для исправления ложных показаний требуется уменьшить интервал срабатывания датчика до нескольких секунд, после чего компенсировать аномальные результаты. Такой подход требует сканировать обстановку окружения чаще, чем несколько раз в минуту.

Заключение

Была изучена заготовка для системы мониторинга за окружающей средой в режиме реального времени, включающая в себя реализацию отправки данных, полученных с датчиков на *Raspberry Pi*, на удаленный *WEB-сервер* с дальнейшим просмотром информации через обычную *WEB*-страницу.

Список используемых источников

1. Документация по работе с модулем MySQLdb для Python [Электронный ресурс]. – Режим доступа: http://mysql-python.sourceforge.net/MySQLdb.html

2. Документация по подключению к MySQL с помощью PHP [Электронный ресурс]. – Режим доступа: http://php.net/manual/ru/pdo.connections.php

3. Вывод графиков с помощью Google Charts [Электронный ресурс]. – Режим доступа: https://developers.google.com/chart/

Статья представлена научным руководителем,
начальником центра НОЦ "ТИОС" Уссом В. С.

УДК 004.042

Н. Ю. Гричиненко (студент группы ИКПИ-32, СПбГУТ)

ТРАНСЛЯЦИЯ ВИДЕОПОТОКА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

В данной статье рассматривается возможность реализации передачи видеотрафика по сети Wi-Fi с динамического объекта, управлением которого занимается микроконтроллер (микрокомпьютер) Raspberry Pi, на планшетный компьютер с операционной системой Android, который может выступать в роли пульта управления объектом. В ходе выполнения работы был проведен анализ выбора библиотек для трансляции и приема видеопотока с Raspberry Pi на планшетный компьютер соответственно.

Raspberry Pi, Android, Raspbian, видеопоток, LibVLC, MJPG-Streamer, планшетный компьютер.

Компоненты и их взаимодействие

Главным компонентом в системе выступает микрокомпьютер Raspberry Pi 2B, который представляет собой одноплатный микроконтроллер с четырехъядерным процессором Cortex A7 и работающий на частоте 900 МГц. Благодаря наличию USB портов становится возможным подключение через стандартный разъем самых обыкновенных камер, а также в качестве альтернативы может выступить модуль-камера, подключается которая непосредственно к плате через разъем *Camera Serial Interface*.

С помощью такого функционала на Raspberry Pi не составит труда реализовать целый ряд задач: собрать бюджетный видеорегистратор или создать передвигающего робота, который сможет совершать видеосъемку и передавать трафик на пульт управления в режиме реального времени. Возможность реализации задачи по передачи видеотрафика и является темой рассмотрения данной статьи.

Адресатом при передаче видеотрафика становится планшет, работающий под операционной системой *Android*. При наличии подключения Raspberry Pi к Wi-Fi точке трафик передается по локальной или глобальной сети, в зависимости от нужд пользователя и настроек сети.

Конкретизировать модели камеры, WiFi-модуля для Raspberry Pi и планшетного компьютера в рамках рассматриваемой системы не имеет смысла по той причине, что реализация данной задачи не требует специфического функционала от данных устройств. Единственный критерий – наличие на планшетном компьютере версии ОС Android не ниже чем 4.0.

В общем виде последовательность взаимодействия компонентов следующая:

1. Обработка данных микроконтроллером с последующей трансляцией в сети (например, локальной) по определенному порту микрокомпьютера.

2. Подключение планшетного компьютера к узлу по заданному порту и просмотр данных.

Разработка приложения для планшетного компьютера

Первоочередной целью при конструировании данной системы является разработка приложения для возможности приема и просмотра видеотрафика на планшетном компьютере. В качестве среды разработки выбор падает на Android Studio – IDE для работы с платформой Android.

Создание приложения сводится по большому счету к выбору необходимой библиотеки, позволяющей воспроизводить видео на планшете, и дальнейшим с ней манипуляциям. Поскольку передача и просмотр трафика происходят в режиме реального времени, то, в первую очередь, важна минимизация задержки.

В результате работы были рассмотрены наиболее популярные библиотеки для видеотрансляции (табл. 1), и для дальнейшей работы была использована библиотека MjpegView.

ТАБЛИЦА 1. Выбор библиотеки

Библиотека	Задержка в радиусе 10 метров	Функционал
MediaPlayer	2–3 секунды	Средний
libVLC	1–2 секунды	Большой
MjpegView	0,1–0,3 секунды	Малый

В то же время библиотека MjpegView имеет ограниченный функционал, однако использование кодека MJPEG обеспечило существенно более низкую по сравнению с другими библиотеками задержку даже без изменений каких-либо исходных параметров.

Библиотеки MediaPlayer и в особенности libVLC располагают обширным функционалом, однако не обходятся без буфера, который применяется для погашения неравномерности скорости воспроизведения видео. И, если MediaPlayer не подразумевает сокращение размера буфера вообще, то использование в libVLC даже минимально допустимых значений (в противном случае буфер переполняется) в результате приводит к немалой задержке, избежать которую не представляется возможным.

Использование кодека MJPEG

Motion JPEG – цифровой видеоряд, состоящий из последовательности отдельных изображений JPEG. Отображение 16 или более кадров в секун-

ду воспринимается зрителем как видеоизображение. Отображение 30 (NTSC) или 25 (PAL) кадров в секунду воспринимается как полномасштабное видео.

Одним из достоинств данного метода сжатия является то, что каждому кадру в последовательности гарантируется качество, получаемое на уровне сжатия, выбранном для сетевой камеры или видеокодера. Другим преимуществом можно назвать то, что потеря одного кадра во время передачи не повлияет на качество остального видеоряда.

Однако задействование данного кодека влечет собой неиспользование технологий сжатия видеоизображения для сокращения объема данных, чего нельзя сказать о более современных кодеках MPEG-4 и H.264.

Как следствие приходится либо обеспечивать высокую скорость передачи, либо применять низкое качество сжатия.

Впрочем, поскольку приводимая модель подразумевает передачу данных преимущественно по локальной сети, причем объем остального трафика не велик в рамках рассматриваемой модели, кодек MJPEG удовлетворяет потребностям при выполнении задачи.

Еще одним достоинством MJPEG в контексте данной системы является то, что, поскольку видеоряд состоит из статичных кадров, их можно анализировать независимо от других, а, значит, становятся проще выполнимыми такие теоретические задачи, как, например, измерить расстояние от динамического объекта с *Raspberry* на борту до препятствий или обнаружить человеческие лица.

Реализация передачи видеопотока на Raspberry

Осуществить трансляцию видеопотока по сети с Raspberry при использовании кодека MJPEG, который выбран при разработке приложения, способен мультимедийный фреймворк *gstreamer*.

Взаимодействие с ним происходит через командную строку, и для удобства можно написать скрипт, запуск которого будет влечь за собой программное использование тех или иных компонентов фреймворка.

Подобный скрипт будет включать в том числе и указание *IP* хоста (источника, т. е. в данном случае Raspberry Pi), порта хоста, разрешения кадров и их количества в минуту.

Использование нижеприведенных команд позволяет запустить *gstreamer* и начать транслирование потока:

```
gst-launch v4l2src ! ffmpegcolorspace ! video/x-raw-
yuv,width=640,height=480,framerate=30/1 ! jpegenc ! tcpserversink
host=$192.168.0.101 port=5555 sync=false
```

Указать IP, порт и разрешение кадров необходимо и на стороне приемника, коим в данном случае выступает планшетный компьютер. Функ-

ционал выбранной библиотеки *mjpegview* при написании приложения является достаточным для того, чтобы указать эти параметры для начала приема трафика.

Потенциальное сокращение задержки

Как было написано выше, библиотека *mjpeg* и фреймворк при базовых настройках обеспечивают задержку в районе 0.1–0.3 секунд в радиусе до 10 метров. Существует множество способов для сокращения задержки, однако можно ограничиться основными:

1. Изменение параметров TCP на стороне источника (Rasperry Pi), с чем справляется команда *sysctl*, отвечающая за управление параметрами ядра. Например, увеличение размера буфера позволит передавать дейтаграммы более высокого размера и, таким образом, избежать или хотя бы снизить фрагментацию.
2. Не всегда имеет смысл использовать высокую частоту кадров, и зачастую можно сократить ее с 60 до 30 кадров в минуту.
3. Как следствие, можно прибегнуть к меньшему кодированию кадров MJPEG и передавать их по сети без существенного сжатия.
4. Увеличение пропускной способности сети при помощи замены оборудования и сетевых настроек.

Заключение

Был произведен выбор библиотеки для воспроизведения видео с последующим написанием соответствующей программы в интегрированной среде разработки Android Studio. Кроме того, была рассмотрена реализация трансляции видеопотока непосредственно от Raspberry Pi благодаря использованию фреймворка *gstreamer*.

Список используемых источников

1. Учебник по Android Studio [Электронный ресурс]. URL: http://startofandroid.com/
2. Петин В. А. Микрокомпьютеры Raspberry Pi. Практическое руководство. СПб. : БХВ-Петербург, 2015. 240 с. ISBN 978-5-9775-3519-9
3. Документация по фреймворку gstreamer [Электронный ресурс]. URL: https://gstreamer.freedesktop.org/documentation/

Статья представлена научным руководителем,
начальником центра НОЦ "ТИОС" Уссом В. С.

УДК 004.042

Н. Ю. Гричиненко (студент группы ИКПИ-32, СПбГУТ)

РАЗРАБОТКА ПО ДЛЯ ОБРАБОТКИ ДАННЫХ С ДАТЧИКОВ НА ЯЗЫКЕ SWI-PROLOG

Целью данной работы является проведение исследования на тему возможного применения академического языка программирования Prolog в современных технических системах на базе микрокомпьютера Raspberry Pi в рамках дисциплины "Логические и функциональные языки программирования". В частности, рассматривается возможность реализации программного обеспечения на языке SWI-PROLOG, которое позволит на микроконтроллере Raspberry Pi обработать данные с подключенных датчиков: датчика температуры и датчика газа.

Raspberry Pi, SWI-Prolog, Raspbian, датчики.

Теоретическая справка

Prolog – язык и система логического программирования, основанные на языке предикатов математической логики дизъюнктов Хорна, представляющей собой подмножество логики предикатов первого порядка.

SWI-Prolog – это свободная реализация языка программирования Prolog. Эта реализация языка программирования постоянно развивается, начиная с момента создания в 1987 году.

Python – высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода. Синтаксис ядра Python минималистичен. В то же время стандартная библиотека включает большой объём полезных функций.

Raspberry Pi 2B – Одноплатный компьютер на базе процессора ARM Cortex-A7 с тактовой частотой 900 MHz.

Raspbian – это операционная система, которая основана на дистрибутиве Linux Debian и оптимизирована для микрокомпьютера Raspberry Pi.

Введение

При проведении данной исследовательской работы был определен ряд требований к написанной программе, что было вызвано ограничениями как среды SWI-Prolog и языка Prolog, так и функциональностью датчиков и Raspberry.

- Обработка данных должна выполняться в среде SWI-Prolog;
- Непосредственное снятие данных с датчиков может происходить на других языках программирования;
- Использование микроконтроллера Rapsberry Pi 2B;

- Работа Rapsberry должна происходить под управлением операционной системы Raspbian.
- Программа на SWI-Prolog должна выполнять следующие функции:
  - нахождение промежутков, где температура больше или меньше заданного числа;
  - вычисление максимального и минимального значений температуры и газа;
  - нахождение среднего значения температуры или газа.

Описание системы

Данную систему можно рассматривать как заготовку системы для умного дома, поскольку все параметры можно снимать при помощи контроллера Raspberry Pi.

Имеются датчик концентрации углекислого газа SNS-MQ135, а также датчик температуры DS18b20, для работы с которыми была разработана интерфейсная схема с внешним аналоговым преобразователем, поскольку в Raspberry Pi не имеется встроенного АЦП, тогда как датчик концентрации углекислого газа выдает показания в аналоговом сигнале.

Raspberry Pi 2B считывает данные с датчиков с интервалом в одну минуту. Интервал времени для запроса формируется по готовности снятия данных с датчиков температуры, поскольку важно снимать показания с датчиков одновременно. С датчика газа информация снимается почти без задержек, поэтому идет привязывание к готовности снятия параметров с датчика температуры (интервал задержки между показаниями датчика температуры составляет одна-две секунды). Датчик температуры DS18b20 осуществляет передачу информации по интерфейсу 1-Wire, тогда как датчик концентрации углекислого газа – при помощи интерфейса SPI.

Снятие данных происходит при помощи программы, написанной на языке Python.

Взаимодействие программного обеспечения

Поскольку Raspberry Pi – микрокомпьютер, работающий под операционной системой Raspbian, которая позволяет получить доступ к более чем десяти тысячам бинарных пакетов Debian, у разработчика появляется возможность производить работу с написанием и выполнением программ на языках Prolog и Python непосредственно на самой плате.

Первоначально имеется Prolog-программа (файл с расширением .pl), состоящая лишь из базовых правил, которые впоследствии позволят пользователю обращаться к программе и получать необходимую информацию.

Множество правил и фактов в Прологе задают отношения между объектами в конкретной прикладной области, образуя тем самым программу.

Такие отношения принято называют предикатами, тогда как связанные подобными отношениями объекты имеют название аргументы.

В исходной Prolog-программе имеются следующие предикаты:

- *tempMore* (X) – предикат, который выводит те факты (в данном случае это данные вида Информация (Время (минуты), время (секунды), показания датчика газа, показания датчика температуры)), в которых показания датчика температуры выше входного аргумента X;
- *temples* (X) – аналогичен вышенаписанному предикату и отличается лишь тем, что выводит те факты, в которых показания датчика температуры ниже входного аргумента X;
- *maxGas* – предикат, который выводит максимальное показание датчика газа;
- *minGas* – предикат, который выводит минимальное показание датчика газа;
- *maxTemp* – предикат аналогичен maxGas с той лишь разницей, что приводится информация с датчика температуры;
- *minTemp* – предикат аналогичен minGas с той лишь разницей, что приводится информация с датчика температуры;
- *averageTemp* – предикат, который выводит среднюю температуру;
- *averageGas* – предикат, который выводит среднее показание с датчика газа;
- *all_inf* – предикат, который поочередно вызывает все вышенаписанные предикаты и, таким образом, выводит всю информацию.

Кроме того, в этой программе присутствует комментарий вида *%end of block*, на место которого *Python*-программа, обработав данные с датчиков, позднее записывает их в виде недостающих фактов. Конечная программа будет представлять собой новый файл и являть собой гибрид исходной программы и фактов, созданных при помощи написанной программы на языке Python.

Что касается непосредственно самих фактов, то они, как было написано выше, представляют собой предикаты вида

Информация (Время(минуты), время(секунды), показания датчика газа, показания датчика температуры)).

Например:

info(28, 39, 50.2045051249, 26.375).

Взаимодействие пользователя с программой

Конечный файл с программой имеет расширение *.pl* и может запускаться в среде *SWI-Prolog*, где пользователь имеет возможность ввести необходимый предикат и увидеть на экране соответствующую информацию.

Редактирование программы в операционной системе Raspbian возможно как в среде SWI-Prolog, так и при помощи любого текстового редактора.

К примеру, при вызове предиката *tempMore* (26) среда выведет такие данные:

time = 28 minutes 39 seconds. Temp = 26.375 gas(ppm) = 50.2045051249
time = 28 minutes 42 seconds. Temp = 26.437 gas(ppm) = 50.2045051249
time = 28 minutes 44 seconds. Temp = 26.312 gas(ppm) = 50.2045051249
time = 28 minutes 47 seconds. Temp = 26.312 gas(ppm) = 50.2045051249
time = 28 minutes 50 seconds. Temp = 26.25 gas(ppm) = 50.2045051249
time = 28 minutes 52 seconds. Temp = 26.437 gas(ppm) = 50.2045051249
time = 28 minutes 55 seconds. Temp = 26.5 gas(ppm) = 50.2045051249
time = 28 minutes 58 seconds. Temp = 26.5gas(ppm) = 50.2045051249
time = 29 minutes 00 seconds. Temp = 26.562 gas(ppm) = 50.2045051249

Заключение

Было проработано взаимодействие существующего макета со средой разработки для академического языка Пролог с применением полученных знаний в рамках изученной дисциплины.

Список используемых источников

1. Губанова Т. В. Логическое и функциональное программирование: учебное пособие. СПб. : СПбГУТ, 2014. 96 с.
2. Хабаров С. П. Интеллектуальные информационные системы. PROLOG – язык разработки интеллектуальных и экспертных систем: учебное пособие. СПб. : СПбГЛТУ, 2013. 138 с.
3. SWI-Prolog [Электронный ресурс]. URL: http://www.swi-prolog.org/

Статья представлена научным руководителем,
старшим преподавателем Губановой Т. В.

УДК 004.7

В. В. Громов (студент группы ИКПИ-32, СПбГУТ)

ОБЗОР И АНАЛИЗ КОМПОНЕНТОВ ДЛЯ ИНТЕРНЕТ-МАГАЗИНА НА БАЗЕ CMS JOOMLA

В статье рассматриваются основные аспекты создания небольшого интернет-магазина на базе бесплатных компонентов и модулей с использованием системы управления контентом CMS Joomla. На основе проведенного анализа даются подробные рекомендации по созданию интернет-магазина и оптимизации бюджета проекта.

CMS Joomla, Интернет-магазин, JoomShopping, VirtueMart, HikaShop.

Введение

В настоящее время одной из наиболее распространенных задач для WEB-разработчика является создание интернет-магазина для индивидуальных предпринимателей.

Каждый проект создания подобных ресурсов имеет свои особенности, которые нужно учитывать WEB-разработчику: целевая аудитория сайта, бюджет проекта, продвижение и администрирование сайта, взаимодействие ресурса с базами данных заказчика, и т. д.

В статье описывается создание интернет-магазина для небольших фирм на основе готовых компонентов, поскольку это ускоряет разработку сайта и требует меньших материальных затрат.

Создание небольшого интернет-магазина можно разбить на следующие подзадачи:

1) Выбор необходимого хостинга (выбор сервера, где будет храниться сайт).
2) Выбор службы предоставления доменов (регистрация доменного имени сайта).
3) Выбор необходимой CMS (система управления контентом).
4) Выбор необходимых компонентов и модулей для построения интернет-магазина.
5) Заполнение сайта контентом.
6) Продвижение сайта в поисковых системах Yandex и Google.

Выбор хостинга

Хостинг – услуга по предоставлению ресурсов для размещения информации на сервере, постоянно находящемся в сети (обычно Интернет). Существует множество критериев для выбора хостинга.

Ниже приведена таблица, в которой описаны основные характеристики, которыми можно руководствоваться при выборе фирмы и тарифа, предоставляющей услуги хостинга.

Было рассмотрено два популярных недорогих хостинга с разными тарифами (табл. 1).

В результате анализа был выбран хостинг HOSTLAND.

ТАБЛИЦА 1. Выбор хостинга

Параметр	HOSTLAND	Интернет Хостинг Центр
Время работы	с 2003 года	с 2009 года
Стоимость	от 119 руб/мес.	от 159 руб/мес.
Ограничения	до 3 % *CPU*, 2 *GB* памяти на хранение сайта	

Параметр	HOSTLAND	Интернет Хостинг Центр
Поддержка	круглосуточная	
бесплатный период работы	1 месяц	7 дней
Оплата за год	от 99 руб. мес. + домен в зоне *.ru* бесплатно на год.	от 132 руб. мес. + домен в зоне *.ru* бесплатно на год.

Выбор службы предоставления доменов

Так как выбор домена заказчиком произошел в зоне *.org*, то главным условием выбора фирмы, предоставляющей услуги по регистрации доменов, была стоимость (табл. 2). В итоге была выбрана фирма *godaddy.com*.

ТАБЛИЦА 2. Выбор регистратора домена

Параметр	*Nic.ru*	*godaddy.com*	*reggi.ru*	*reg.ru*
Стоимость	990 руб/год	662 руб/год	829 руб/год	878 руб/год

Рекомендации при выборе хостинга и службы предоставления доменов

При выборе службы предоставления доменов, а также хостинга не желательно пользоваться бесплатными сервисами, которые предоставляют соответствующие услуги, поскольку это может повлиять на доступность сайта. Бесплатные хостинги не будут нести ответственность за то, что сайт может быть безвозмездно утерян. Также рекомендуется делать бекапы (резервные копии) сайта.

Выбор необходимой системы управления контентом (*CMS*)

CMS – это программа, предоставляющая инструменты для добавления, редактирования, удаления информации на сайте.

Большинство современных CMS имеет модульную архитектуру, что позволяет администратору самому выбирать и настраивать те компоненты, которые ему необходимы.

При выборе CMS необходимо обратить внимание на возможность её обновления и стоимость.

Обновление и поддержка CMS должны обязательно присутствовать, поскольку постоянно обнаруживаются уязвимости в CMS, при помощи которых можно взломать сайт. Если вовремя обновлять сайт, то можно уберечься от несанкционированного доступа в работу сайта, а также предотвращать появление вирусов.

Ниже рассмотрены наиболее популярные CMS. Сравнительную характеристику CMS (табл. 3).

ТАБЛИЦА 3. Сравнительная характеристика CMS

Параметры	**Joomla**	**WordPress**	**OpenCart**	**1С-Битрикс**
Стоимость	бесплатно	бесплатно	бесплатно	**35000 в год**
Обновления	да	да	да	**1 год**
Поддержка	сообщество	сообщество	сообщество	круглосуточная
Русский язык	да	да	да	да
Особенности			встроенный интернет магазин	установленный интернет магазин

В результате была выбрана CMS Joomla. Также наиболее подходящим претендентом на CMS для интернет-магазина является OpenCart. В CMS OpenCart встроен интернет-магазин, который остается только заполнить товаром. Выбор CMS Joomla был обусловлен тем, что CMS является бесплатной, её можно применять для создания сайтов разных тематик, имеются обновления, и существует большое сообщество поддержки.

Выбор расширений для построения интернет-магазина

Поскольку в CMS Joomla нет встроенного расширения интернет-магазина, то были рассмотрены специальные компоненты для *Joomla*, позволяющие создать интернет-магазин.

Существует множество компонентов для построения интернет-магазина, причем большинство из них условно-бесплатные.

Зачастую условно-бесплатные компоненты в дальнейшем для развития сайта требуют оплаты. Это связано с тем, что в бесплатных версиях компонента интернет-магазина могут отсутствовать критически важные функции для его работы. Отсутствие необходимого функционала обнаруживается обычно на этапе заполнения данными сайта.

Сравнительные характеристики компонентов (табл. 4).

ТАБЛИЦА 4. Сравнение компонентов интернет-магазина для *CMS Joomla*

Параметр	**JoomShopping**	**HikaShop**	**VirtueMart**	**IPrice calculator LIGHT**
Стоимость	условно-бесплатные			
Нагрузка на сервер	средняя	средняя	большая	малая
Возможность импорта товаров (CSV)	да	да	да	да
Наличие корзины товара	да	да	да	**нет**
Возможность заказа товара без регистрации	да	**нет**	да	да

Параметр	JoomShopping	HikaShop	VirtueMart	IPrice calculator LIGHT
Вывод товара	плиткой	плиткой и списком	плиткой	список
Возможность модернизации кода компонента	да	?	**затруднительна**	да
Обновления	да	да	да	**3 месяца**
Раскрутка сайта при помощи компонента	да	?	?	?
Стоимость полной версии	-	**50$**	Бесплатно	**150$**

В IPrice calculator LIGHT нет корзины, т. е. заказ товаров из разных категорий совершить нельзя. В платной версии корзина есть, но поддержка обновлений происходит только в течение 3-х месяцев.

VirtueMart сильно нагружает сервер, причем он реализован так, что оптимизировать код компонента для определенных задач проблематично.

В бесплатной версии HikaShop заказ товара возможен после длительной регистрации. В платной версии такого ограничения нет.

В JoomShoping есть ограничение на импорт товара: импортировать можно не все характеристики товара из .CSV таблицы. Но это ограничение можно убрать путем небольшого видоизменения исходного кода. Решение этой проблемы есть на форумах.

В результате был выбран компонент JoomShopping, а также установлены для компонента JoomShopping бесплатные модули и плагины: фильтр товаров, автоматическое построение меню, модуль для распродаж, плагин для поиска товара.

Также были установлены другие модули для CMS Joomla: бесплатный модуль-форма «позвоните мне» Call me back, модуль меню Smart Scroll Menu, модуль меню AS MENU, бесплатный простой шаблон для сайта.

Редактирование разметки и CMS сайта

После установки всех необходимых расширений и заполнения сайта информацией часто необходимо редактировать разметку и дизайн сайта, а в некоторых случаях и оптимизировать работу движка.

Для редактирования разметки и дизайна сайта необходимы навыки CSS и HTML. Для изменения ядра CMS и работы расширений сайта необходимы навыки работы с PHP и MySQL. Также подобные знания могут пригодиться для создания собственных модулей и компонентов сайта.

“Раскрутка” сайта в поисковых системах

Перед добавлением сайта в поисковые системы необходимо заполнить сайт оригинальным контентом, создать карту сайта, заняться внутренней оптимизацией: добавить метатеги, включить SEF-*ссылки* (*search engine friendly*) посредством стандартных настроек или сторонних расширений и т. д.

Заключение

В результате работы проведен обзор компонентов для интернет-магазина на базе CMS Joomla, проработаны основные аспекты создания небольшого сайта для интернет-магазина.

Список используемых источников

1. Версии модуля Hikashop [Электронный ресурс]. URL: hikashop.com/ extensions/compare-versions.html //
2. Русскоязычный сайт разработчиков Joomshopping [Электронный ресурс]. URL: joomshopping.pro
3. Иностранный сайт разработчиков Joomshopping [Электронный ресурс]. URL: webdesigner-profi.de
4. Сайт с шаблонами для Joomla [Электронный ресурс]. URL: joomla24.com
5. Официальные расширения для Joomla [Электронный ресурс]. URL: extensions.joomla.org

Статья представлена научным руководителем,
старшим преподавателем Губановой Т. В.

УДК 004.042

В. В. Громов (студент группы ИКПИ-32, СПбГУТ)

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ МИКРОКОНТРОЛЛЕРА ATMEGA128 ДЛЯ СНЯТИЯ ДАННЫХ С ЦИФРОВОГО КОМПАСА ПО ШИМ СИГНАЛУ

При изучении микроконтроллеров семейства AVR и STM одним из важнейших аспектов для изучения является работа с системными прерываниями и таймерами. В данной статье рассмотрена реализация программы, использующая таймер и системные прерываниями на микроконтроллере Atmega128, при помощи которых будет обрабатываться сигнал широтно-импульсной модуляции (ШИМ).

ШИМ, ATmega128, AVR RISC-архитектура, CMPS03.

ATmega128 представляет собой 8-разрядный микроконтроллер, основанный на расширенной AVR RISC-архитектуре.

За счет выполнения большинства инструкций за один машинный цикл ATmega128 достигает производительности 1 млн операций в секунду/МГц, что позволяет проектировщикам систем оптимизировать соотношение энергопотребления и быстродействия.

В качестве источника ШИМ сигнала используется электронный компас CMPS03, который выдает значение отклонения от севера в градусах по ШИМ-сигналу.

CMPS-03 – оценочная плата на базе магниторезистивного сенсора KMZ51. Работа сенсоров происходит под управлением микроконтроллера PIC16F872.

Интерфейс данной платы представлен на рисунке 1.

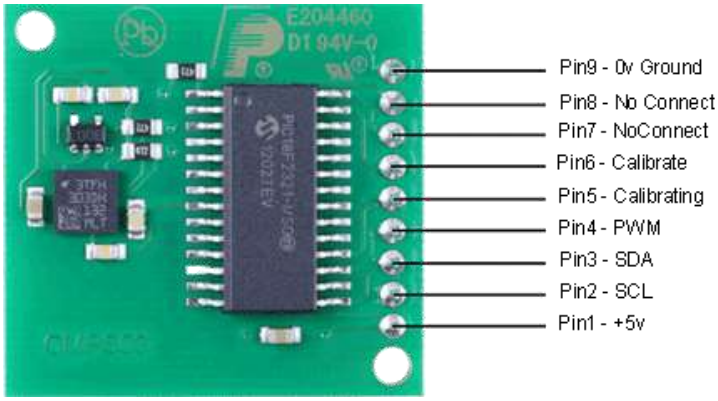


Рис. 1. Интерфейс электронного компаса CMPS03

Отладка данной схемы производилась на отдельном контроллере, основанном на базе микропроцессора Atmega128.

Плата компаса подключена к контроллеру Atmega128 следующим образом:

- Pin 1 подключается к питанию контроллера с напряжением +5 V.
- Pin 2, 3 подключаются к питанию с напряжением +5 V через резистор номиналом 4.7 k, так как для использования широтно-импульсной модуляции требуется задать необходимый режим плате через Pin 2, 3. Pin 2, 3 подключаются к ножкам микроконтроллера PC4 и PC5.
- Pin 4 подключается к выходу ножки таймера микроконтроллера ISC70.
- Pin 5, 6 не используются, так как на данном этапе калибровка не требуется.
- Pin 7, 8 не подключены, так как это не предусмотрено производителем.
- Pin 9 подключается к земле.

Плата CMPS03 имеет два интерфейса для вывода данных: PWM и I2C.

PWM – это широтно-импульсная модуляция (ШИМ), сигнал, который передается по одному каналу. В зависимости от значения на выходе устройства длительность единичного импульса может изменяться в пределах, установленных производителем. В данном случае 0 градусам соответствует длительность единичного импульса 10 мс, а 360 градусам соответствует значение в 100 мс.

Снять значение длительности фронта можно двумя случаями:

a) использование стандартной библиотеки для работы с ШИМ,

b) работа с таймерами.

Для получения практического опыта была создана программа для 8-битного таймера, который работал с переполнением значения счетчика.

I2C – двухпроводный последовательный интерфейс, разработанный корпорацией Philips. В данной работе он не рассматривался.

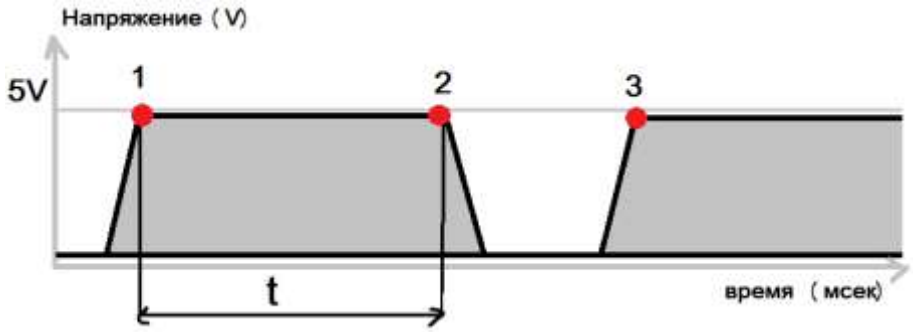


Рис. 2. Диаграмма работы ШИМ

Программа для микроконтроллера работает следующим образом:

Как писалось выше, в зависимости от длительности импульса (интервал между точками 1 и 2, рис. 2), формируется выходное значение. Чем больше время такого интервала, тем больше значение компаса соответственно.

Микроконтроллер может различать на входе сигнала восходящий и спадающий фронт. На рисунке 2 представлены восходящие фронты 1 и 3, спадающий – 2 фронт. Контроллер, в свою очередь, может по фронту сигнала сделать прерывание, то есть запустить функцию, которая написана программистом. В функции, которая обрабатывает прерывание, необходимо либо запускать, либо останавливать таймер, чтобы узнать время единичного фронта сигнала, после чего в зависимости от времени фронта можно было вычислить цифровое значение компаса.

Частота работы микроконтроллера 1 МГц, т. е. микроконтроллер может сделать 1 миллион операций в секунду. В данном случае значение на выходе счетчика за одну секунду будет равно 1 млн. Максимальное значение длительности импульса ШИМ платы CMPS03 равняется 100 мс. Тогда максимальное значение счетчика таймера будет достигать на выходе 100 тыс. при максимальном значении компаса, равном 359 градусам.

Сама плата CMPS03 не способна выполнять настолько точные измерения, чтобы имелось 100 тыс. измерений на весь фронт времени, поэтому можно понизить частоту работы таймера микроконтроллера на 8. Тогда максимальное значение на выходе таймера будет равняться 12 500, что входит в пределы значения int.

Таймеры в микроконтроллере Atmega128 бывают 8-битные и 16-битные. То есть значение счетчика может достигать максимального значения $2^8 = 256$ или $2^{16} = 65\,536$, причем каждый таймер привязан к определенному выходу (ножке) микроконтроллера.

Для уменьшения аппаратных затрат был использован 8-битный таймер с переполнением. Для этого потребовалась дополнительная переменная типа int count1, которая увеличивалась на 256 при переполнении 8-битного таймера, после чего 8-битное значение самого таймера TCNT0 обнулялось. Также отдельное значение таймера count1 увеличивалось по спадающему фронту, только в таком случае инкрементировалось значение таймера на значение TCNT0. Таким образом, в count1 хранится длительность единичного сигнала, а TCNT0 используется для работы с таймером (в котором может храниться часть длительности сигнала).

Фактически count1 может измеряться в пределах от 0 до 65 536, в то время как значение TCNT0 меняется в пределах от 0 до 256.

Стоит отметить, что, если бы использовался 16-битный таймер, стало бы возможным считывать значение, минуя переполнение при спадающем фронте сигнала.

Отладочная плата для программы выглядит следующим образом: к самому контроллеру подключено 6 светодиодов, которые в зависимости от положения компаса загораются. При самом меньшем значении (когда компас указывает на север) включен один светодиод, при наибольшем значении (когда компас указывает на юг) – все шесть. В промежуточных значениях включены от одного до шести светодиодов.

Работа светодиодов описывается в функции powerLed(), тогда как count приравнивается значению count1, умноженному на коэффициент 0,0028.

Ниже рассмотрены основные аспекты программы, написанной на языке Си в среде разработки AVR Studio:

1) Инициализация портов для вывода светодиодов для отладки платы. Здесь записываются данные в соответствующий регистр DDRA. Программирование выходов микроконтроллера для подачи напряжения на светодиоды.

```
DDRA| = (1<<PA0) | (1<<PA1) | (1<<PA2) | (1<<PA3) | (1<<PA4).
```

Также инициализируются порты для подачи логической единицы (напряжение +5 V) на входы цифрового компаса.

```
DDRA| = (1<<PC4) | (1<<PC5).
```

2) Инициализация таймера микроконтроллера.

TCCR0|= (0<<CS02) | (0<<CS01) | (0<<CS00).

Установка таймера TCNT0, где задается делитель частоты.

TIMSK |= (1<<TOIE0);

TIFR |= (1<<TOV0).

Установка разрешения прерывания по переполнению счетчика таймера.

TCNT0 = 0.

Установка 8-разрядного счетного регистра в ноль. Именно этот регистр инкрементируется при каждом такте микроконтроллера.

3) Инициализация портов для запуска и остановки таймера.

Установка регистра внешних прерываний, который задает прерывания в зависимости от фронтов сигнала широтно-импульсной модуляции.

EICRB |= (1<<ISC71) | (1<<ISC70).

Задает прерывания по обоим фронтам сигнала с входа микроконтроллера INT7 (ISC*n*1, где *n* – номер порта).

EIMSK |= (1<<INT7).

Разрешение прерывания с порта INT7.

4) Обработка прерывания по ШИМ сигналу для запуска и остановки таймера.

ISR(INT7_vect){

if(EICRB & (1<<ISC70)){ //Если обнаружен нарастающий фронт ШИМ сигнала: сигнал на входе таймера равен логической единице (1<<ISC70) и до этого таймер не был запущен (EICRB).

TCCR0 |= (1<<CS02) | (0<<CS01) | (1<<CS00);

EICRB &= ~(1<<ISC70); //Запуск таймера.

TCNT0 = 0; //Счет счетчика начинается с нуля.

count1 = 0; //Обнуление значения глобальной переменной.

}else { //Попался спадающий фронт сигнала count = (count1+TCNT0) * 0,0028;

В переменной count хранится цифровое значение с компаса в градусах.

EICRB |= (1<<ISC70); //Для возможности при нарастающем фронте заново запустить таймер.

TCCR0 |= (0<<CS02) | (0<<CS01) | (0<<CS00); //Остановка таймера.

TCNT0 = 0; count1 = 0;}} //Обнуление значения счетчика.

5) Инкрементирование переменной count1 при переполнении 8-битного счетчика таймера.

ISR(TIMER0_OVF_vect){TCNT0 = 0; count1 += 256;}

Соответствующие установки регистров можно посмотреть в описании микроконтроллера Atmega128.

Заключение

В результате работы была написана программа, которая обрабатывала данные, полученные по ШИМ сигналу. Были получены практические навыки в программировании микроконтроллера Atmega128, а также рассмотрена работа цифрового ШИМ сигнала.

Список используемых источников

1. ATMEGA128 Datasheet [Электронный ресурс] // Документация для микроконтроллера Atmega128. – URL: http://lib.tixer.ru/datasheets/ac/ic/mcu/avr/ ATmega128A_Russian_Datasheet.pdf
2. Описание работы электронного компаса [Электронный ресурс]. URL: robot-electronics.co.uk //.
3. Блог об электронике и микроконтроллерах [Электронный ресурс]. URL: easyelectronics.ru
4. Сайт о разработке приложений для микроконтроллеров. URL: microtechnics.ru

Статья представлена научным руководителем,
начальником центра НОЦ "ТИОС" Уссом В. С.

УДК 621.395

А. Д. Дремина (студентка группы ИКТК-26, СПбГУТ)

АНАЛИЗ ТРАФИКА ТАРГЕТИРОВАННОЙ РЕКЛАМЫ СОЦИАЛЬНЫХ СЕТЕЙ

Статья посвящена анализу объема сетевого трафика сервисов сбора статистики и таргетированной рекламы социальной сети «Вконтакте». В ходе проведения эксперимента с помощью утилиты Wireshark был захвачен трафик, возникающий при загрузке фотографии в онлайн-сервис с помощью различных браузеров (Google Chrome, Mozilla Firefox, Opera, Internet Explorer). В результате анализа получены данные об изменении объемов трафика сервисов сбора статистики и рекламных объявлений.

Wireshark, Google Chrome, Mozilla Firefox, Opera, Internet Explorer, vk.com, статистический анализ сетевого трафика, таргетированная реклама, социальные сети.

Введение

По данным интернет агентства ASTDESIGN [1] 94 % россиян имеют аккаунт в какой-либо социальной сети и 80 % используют его регулярно.

Среднестатистический пользователь проводит не менее 2 часов в сутки за просмотром новостей в социальной сети. Подобного рода онлайн-сервисы также является хранилищем различного рода информации о каждом отдельно взятом пользователе: интересы, личные фотографии, сведения о посещаемых сообществах и прочее. Таким образом, социальные сети являются мощным инструментом для маркетинга. В представленной статье речь пойдет о сетевом трафике сервисов сбора статистики и таргетированной рекламы социальной сети «Вконтакте». Таргетированная реклама представляет собой объявления, нацеленные на группы пользователей, объединенных по различным параметрам, например, интересы, пол, возраст, географическое положение, социальное положение и другие. Статья является продолжением исследования статистического анализа сетевого трафика [2], возникающего при загрузке фотографии в социальные сети.

Целью статьи является исследование объемов трафика сервисов сбора статистики и рекламных объявлений.

Описание лабораторного стенда

В ходе проведения экспериментов были использованы 4 широко распространенных (по версии интернет-проекта Openstat [3]) браузера, доступных для персонального компьютера: Google Chrome, Mozilla Firefox, Opera и Internet Explorer.

Используемое оборудование:

- роутер фирмы D-LINK с макс. скоростью беспроводного соединения 54 Мбит/с и стандартом беспроводной связи 802.11g,
- ноутбук (далее PM) HP Pavilion dv6, с операционной системой Windows 7.

На PM было установлено следующее программное обеспечение:

a) утилита для захвата сетевого трафика Wireshark (версия 2.0.1);

b) браузеры:
   - Google Chrome (48.0.2564.116 m),
   - Mozilla Firefox (44.0.2),
   - Opera (35.0.2066.92),
   - Internet Explorer (11.0.9600.1780).

Описание проводимого эксперимента

До начала проведения экспериментов, на PM были отключены работающие службы, являющиеся источником фонового трафика.

Исследование представляет собой проведение экспериментов по захвату трафика, возникающего в результате поочередной загрузки изображения в социальную сеть с помощью четырех браузеров, в утреннее (11 ч) и вечернее (23 ч) время каждого из 5 последовательных дней одного меся-

ца. Эксперименты были проведены в марте и мае 2016 г. В процессе проведения каждого эксперимента фиксировались следующие события:

- открытие браузера;
- переход на главную страницу социальной сети;
- авторизация;
- переход во вкладку «фотографии»;
- начало загрузки изображения;
- окончание загрузки, выход из учетной записи;
- закрытие вкладки социальной сети, закрытие браузера;
- остановка Wireshark.

Для обработки полученных данных была написана программа на языке программирования PHP. Захваченный трафик проходил следующие этапы обработки:

- *Выявление сессий*. На данном этапе пакеты сортируются по номерам сессий (tcp.stream).
- *Отбраковка неполных сессий*. Сессии, открытые до начала проведения эксперимента, отбрасываются.
- *Сопоставление доменным именам*. Следующим шагом с помощью интернет-ресурса bgp.he.net [4] IP-адреса сопоставлялись с доменными именами для последующей сортировки.
- *Подсчет объемов*. И, наконец, заключительным этапом являлся подсчет объемов входящего и исходящего трафика.

Результаты

Сервисы сбора статистики

На этапе сопоставления IP адресов доменным именам, в социальной сети «Вконтакте», помимо адресов, относящихся к онлайн платформе и браузерам, были найдены адреса, принадлежащие следующим сервисам сбора статистики:

TNS Gallup – является поставщиком данных мониторинга рекламы и СМИ в России, также занимается оценкой затрат на рекламу.

Liveinternet.ru – сервис сбора и обработки данных, предоставляющий отчет об основных показателях посещаемости (количество загрузок сайта, посетителей, используемые браузеры и прочее).

Mail.ru Group – также представляет сервис сбора статистики посещаемости сайтов. На данный момент является единственным владельцем социальной сети «Вконтакте».

На рисунке 1 представлен график средних значений (Кбайт) объемов трафика сервисов сбора статистики за исследуемый период (исходящий трафик – красный, входящий – синий).

Рис. 1. Объем трафика сервисов сбора статистики

На основании полученных результатов можно сделать следующие выводы:

- в ходе анализа трафика, полученного при загрузке фотографии с помощью браузера Mozilla Firefox, адреса сервисов сбора статистики не были обнаружены;
- объем трафика сервисов сбора статистики составляет десятки Кбайт;
- объем исходящего трафика сервисов TNS Gallup и liveinternet.ru в браузерах Google Chrome и Opera на 25–30 % больше входящего;
- наибольший объём трафика у сервиса Mail.ru

Таргетированная реклама

Таргетированная реклама представляет собой объявления, нацеленные на определенные группы пользователей, объединенных по различным параметрам: интересы, демографическое, географическое или социальное положение и прочие. Главной особенностью такого вида рекламы является возможность продемонстрировать сообщение только той аудитории пользователей, которую оно заинтересует.

Социальная сеть «Вконтакте» отображает объявления, которые, как правило, представляют собой, 1–3 блока, каждый из которых состоит из изображения, размером (90×120 px или 145×165 px), с заголовком (до 25 символов) и текстом описания (до 60 символов). Размещаются подобные блоки в левой части окна браузера.

В результате более тщательного анализа захваченного трафика, было обнаружено, что часть данных передается посредством протокола HTTP, в структуре которого был обнаружен путь к ресурсам рекламы.

С помощью функции просмотра сетевых запросов (вкладка «Network») в исследуемых браузерах, было выяснено, что часть рекламных объявлений загружается с интернет-портала Яндекс.

На рисунке 2 изображены графики изменения объема трафика таргетированной рекламы социальной сети «Вконтакте» (штрихпунктирная – исходящий, сплошная – входящий).

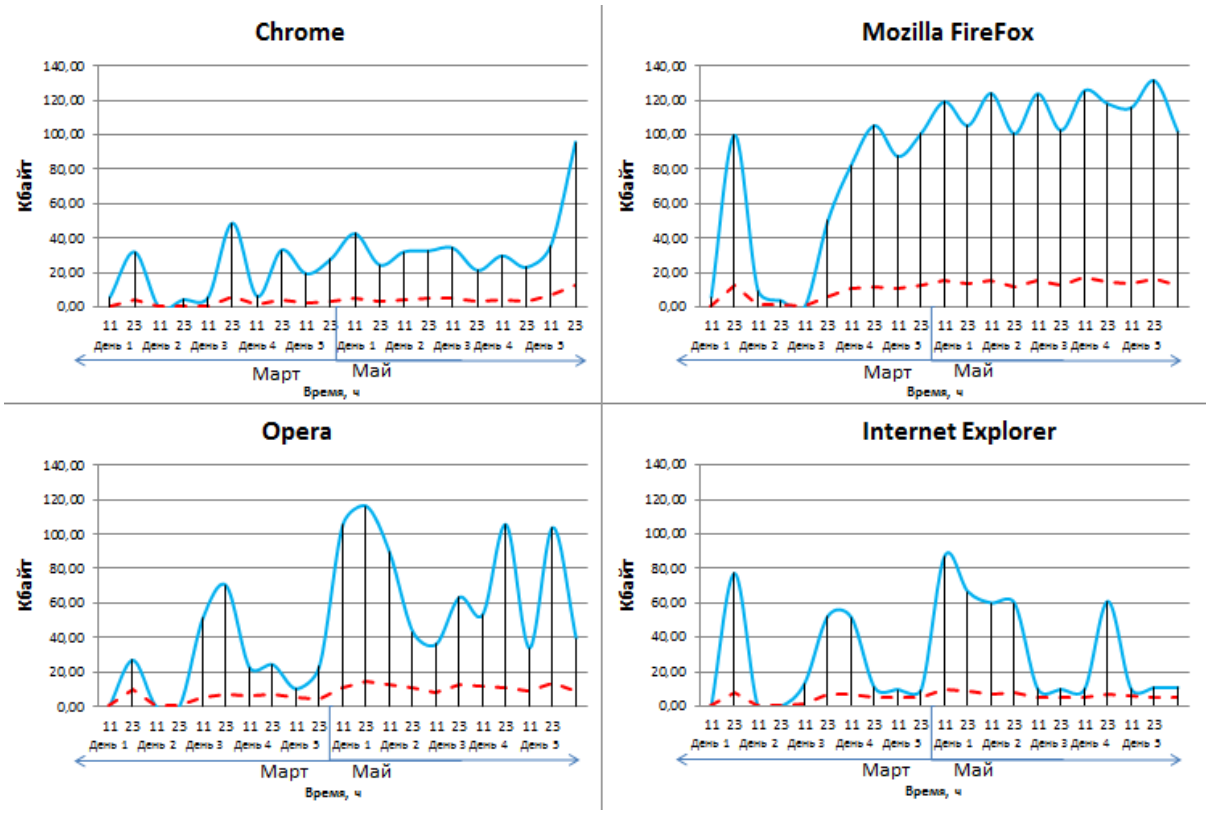


Рис. 2. Объем трафика таргетированной рекламы

На рисунке 3 представлена столбчатая диаграмма средних значений объема трафика для каждого браузера (исходящий – красный, входящий – синий).

В результате анализа полученных данных было выявлено, что изменения объема входящего трафика имеет нелинейный характер, что объясняется разным количество показываемых объявлений в отдельно взятое время. Объем исходящего трафика в среднем до 20 Кбайт.

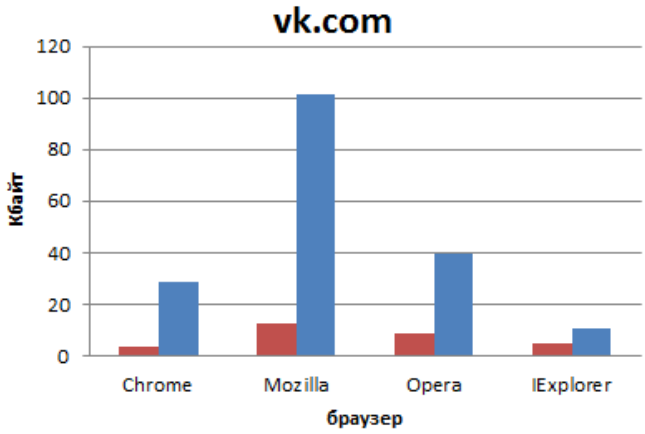


Рис. 3. Диаграмма средний значений объема трафика

Заключение

В процессе проведения исследования были получены следующие результаты:

- объем трафика сервисов сбора статистика и таргетированной рекламы составляет десятки Кбайт (сотни в случае с рекламными объявлениями в браузере Mozilla Firefox);
- наибольший объем входящего и исходящего трафика у сервиса Mail.ru, ведущего статистику посещаемости сайтов;
- объем входящего трафика таргетированной рекламы превышает исходящий в 2–10 раз;
- зависимость объема трафика от типа браузера и времени проведения эксперимента не была найдена.

Список используемых источников

1. Интернет-агентство ASTDESIGN [Электронный ресурс]. URL: http://www.astdesign.ru/ (дата обращения: 14.06.16)

2. Дремина А. Д. Статистический анализ трафика при загрузке фотографии в социальные сети // «Актуальные проблемы инфотелекоммуникаций в науке и образовании». V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. / под ред. С. В. Бачевского. СПб. : СПбГУТ, 2016.

3. Сервис Openstat [Электронный ресурс]. URL: https://www.openstat.com/ (дата обращения: 14.06.16)

4. Интернет-сервис bgp.he.net [Электронный ресурс]. URL: http://bgp.he.net/ (дата обращения: 14.06.16)

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Гойхманом В. Ю.

УДК 004.72

В. С. Елагин (кандидат технических наук, доцент, СПбГУТ)
А. В. Онуфриенко (студент группы ИКТК-26, СПбГУТ)

ТЕХНОЛОГИЯ ГЛУБОКОЙ ИНСПЕКЦИИ ПАКЕТОВ В ПРОГРАММНО-КОНФИГУРИРУЕМОЙ СЕТИ

Программно-конфигурируемые сети приобретают все большую популярность в связи с возможностью решения проблем независимости от производителя оборудования, снижения стоимости оборудования, упрощения администрирования сетью, однако при передаче данных возникает потребность в технологии глубокой инспекции пакетов.

программно-конфигурируемая сеть, глубокая инспекция пакетов, DPI, Mininet.

Введение

Сегодня наиболее актуальным для операторов стало обеспечение видимости, того какой трафик проходит через сеть, для обнаружения изменения поведения пользователей на раннем этапе.

До сих пор в центре внимания были канальный и сетевой уровни, а не транспортный, представительный и уровень приложений. Тем не менее, нет никаких сомнений в том, что уровни 4–7 станут основным направлением для будущего изучения. Ведь, если в программно-конфигурируемых сетях физическое оборудование будет уходить на второй план, то потребности приложений и абонентов переместятся на первый план. Предполагается, что сами приложения будут запрашивать определенные возможности в сети, и в связи с этим будут формироваться определенные сетевые ресурсы. Политики для каждого приложения будут установлены в момент разработки приложения и перенесены на платформу, как услуга, и будут охватывать, например, производительность, требования соответствия уровня надежности. В данном вопросе DPI является технологией, которая как раз справится с этими вопросами: она определяет конкретные приложения в режиме реального времени при определенных ключевых узловых точках, применяет политику. Политики могут включать в себя блокирование, оптимизации, определения приоритетов [1].

Так же система глубокого анализа может предоставить подробные данные, для информирования контроллера о состоянии сети и потоках ее трафика. Это позволяет рассматривать сеть как целостный ресурс, а не различные группы устройств. В конечном счете, внедрение DPI-систем позволит применять политики контроля и автоматизации для всей сети в целом.

Экспериментальная часть

Для проведения исследования была использована среда *Mininet*. *Mininet* близко эмулирует реальную физическую сеть, путем воссоздания операционного окружения.

Развернуть простую сеть *Openflow* в эмуляторе *Mininet* можно в консоле локальной машины с использованием удаленного контроллера на виртуальной машине (графический интерфейс показан на рис. 1):

$ sudo mn –-controller=remote, ip=172.16.117.231, port=6653 --switch ovsk, protocols=OpenFlow13 –topo=tree, depth=1, fanout=2,

где *mn* – это главный исполняемый файл *Mininet*. Ключ *topo* создает топологию (дерево), опцией *switch* указывается тип коммутатора (*ovsk* – встроенный). Тип контроллера – удаленный (*controller remote*).

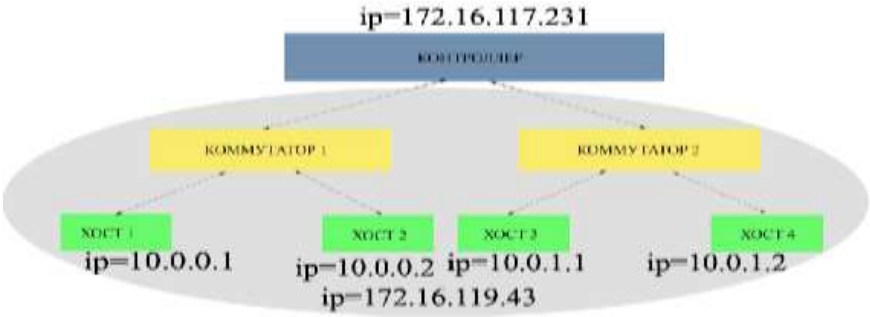


Рис. 1. Схема, развернутая в *Mininet*

В программно-конфигурируемых сетях для связи контроллера с коммутатором используются сообщения протокола *OpenFlow*, в то время как внутри самой сети используются различные протоколы [2]. Важным является детальное рассмотрение верхних уровней в модели *OSI*, а не физического, канального и сетевого. Рассмотрим на примере, указанном на рисунке 2, реакцию сети на протоколы прикладного уровня при взаимодействии между объектами нашей сети.

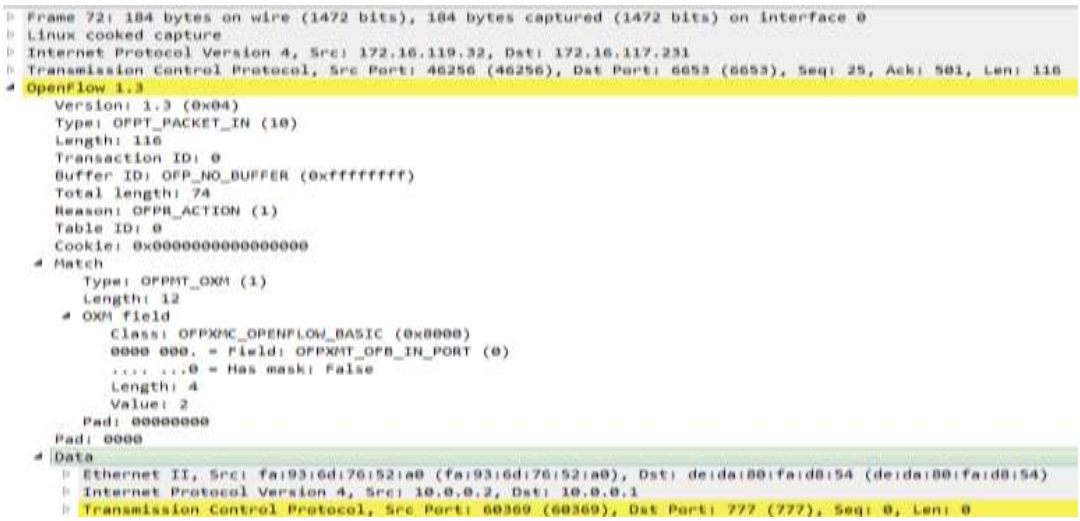


Рис. 2. Сообщение протокола *OpenFlow* при работе с протоколом HTTP

Можно заметить, что в сообщениях *OpenFlow* был виден трафик транспортного уровня, а трафик прикладного уровня при передаче HTTP пакетов в сообщениях *OpenFlow* не может быть распознан. Чтобы устранить этот эффект, можно использовать системы глубокого анализа, как инструмент статистического анализа.

Благодаря системам глубокого анализа оператор связи может узнать, как используются ресурсы сети и при необходимости применить требуемые политики. Статистика, собираемая системой, может помочь своевременно обнаруживать проблемы, знать какой тип трафика преобладает на сети, выявить самых пользователей, наиболее посещаемые пользователями сайты [3].

Рассмотрим особенности размещения DPI систем на разных уровнях:

1) Уровень приложений.

С относительной легкостью, программное обеспечение DPI может быть встроено на уровне бизнес-приложений. Тем не менее, некоторым приложениям может потребоваться минимизированное влияние узких мест, созданных длительным путем передачи данных. Учитывая возможность задержек, это развертывание DPI лучше всего работает для не критичных ко времени использования сетевых приложений, таких как аналитика.

2) Уровень управления.

Программное обеспечение DPI может быть развернуто в контроллере. Тем не менее, часть неопознанного коммутаторами трафика должна быть отправлена на DPI-систему для опознания, что может привести к проблемам масштабируемости и производительности. После этого все последующие потоки одного и того же типа не отправляются на коммутатор, что может привести к тому, что будут пропущены «опасные» пакеты.

3) Уровень инфраструктуры.

Сетевые устройства тоже могут запустить программное обеспечение DPI, и после идентификации приложений и метаданных, они могут либо применять предварительно определенную политику, либо отправить эту информацию в контроллер, а затем получить обратно политику или правило.

Реализации DPI в слое узла минимизирует задержку. Однако этот подход является дорогостоящим, поскольку он требует наибольшее количество экземпляров в сети.

Реализация системы DPI на коммутаторе очень выгодна в том случае, если у нас есть жесткое требование к ограничению какого-либо трафика, так как абсолютно все пакеты пройдут через систему и будут подвергнуты тщательной проверке. К сожалению, такое воздействие повлияет на производительность сети, и привести к задержкам.

Рассмотрим этот вариант подробнее.

В качестве DPI-системы была использована утилита для создания и работы с сетевыми пакетами *Scapy*.

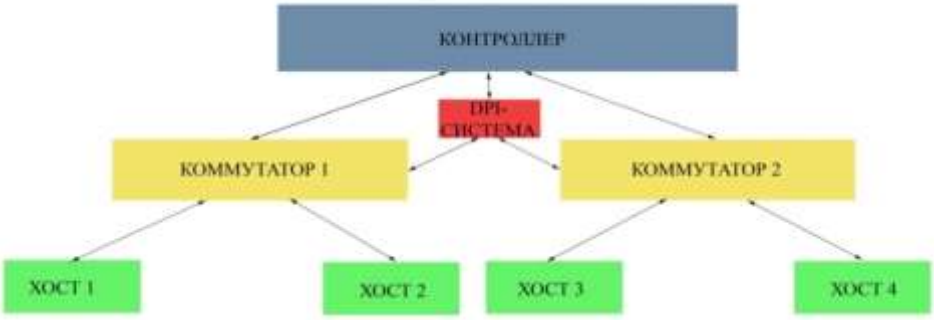


Рис. 3. Схема программно-конфигурируемой сети с внедрением DPI-системы

В ходе исследования пакетов OpenFlow была выделена постоянная часть пакета, которую и решено было взять как сигнатуру протокола OpenFlow.

Благодаря централизованному построению маршрутов и контролю всего сетевого трафика подозрительный поток при необходимости может быть отправлен на существующие средства DPI для анализа.

Результаты

При исследовании взаимодействия системы, были вычислены задержки при обработке пакетов OpenFlow, которые были занесены на график распределений задержек, указанный на рисунке 4.

Для анализа эксперимента было выбрано 10 416 значений.

Максимальное время обработки пакета составило 14 424 мкс.

Минимальное время обработки составило 210 мкс.

Среднее время обработки – $\dot{x} = \frac{\sum_{i=0} x_i}{n} =$ 439,173675 мкс.

Мера разброса значений времени обработки пакета – $D = \frac{\sum_{i=0} \left(x_i - \dot{x} \right)^2}{n-1} =$ 77 186,36 мкс

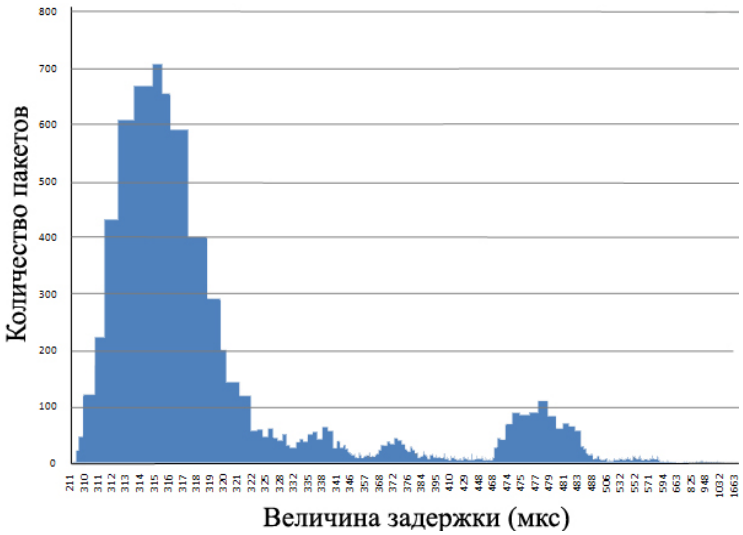


Рис. 4. График расределения задержек

В графике ярко выделяются 2 экстремума, необходимо дальнейшее исследование, чтобы оценить (не) зависимость второго экстремума от оборудования, на котором проводился эксперимент.

Заключение

В результате проведённого анализа можно сделать вывод, что внедрение DPI-системы является необходимым действием для наилучшего функционирования сети, улучшения сетевых характеристик путем контролирования трафика, а так же для внедрения новых услуг. Однако из-за появления задержек, необходимо перед установкой системы провести дополнительное исследование сети и применять DPI-систему, которая будет соответствовать требованиям данной сети. Так же применение такой системы в настоящее время может сдерживаться следующими факторами: нарушением неприкосновенности частной жизни, применением не корректных политик, а так же препятствие заключается в дороговизне приобретения и установке DPI-системы.

Список используемых источников

1. Елагин В. С. СОРМ в сетях пост-NGN. Модели и технологии [Электронный ресурс] // Вестник связи. 2015. № 06. С. 47–49. URL: http://files.iks.sut.ru/publications/2015-010-pp.pdf (дата обращения 21.05.2016).
2. Программно-конфигурируемые сети [Электронный ресурс] // Открытые системы. СУБД. 2012. № 09. URL: http://www.osp.ru/os/2012/09/13032491/ (дата обращения 20.05.2016).
3. Зачем нужен DPI [Электронный ресурс] // Telekomza [сайт]. URL: http://telekomza.ru/2012/03/26/zachem-nam-nuzhen-dpi/ (дата обращения 20.05.2016).

УДК 004.042:004.9;351.9

Д. В. Журкин (студент группы ИКТБ-58М, СПбГУТ)
О. Н. Рябова (консультант, Управление Роскомнадзора по СЗФО)
Д. В. Сахаров (кандидат технических наук, доцент, СПбГУТ)

ОТКРЫТЫЕ ДАННЫЕ В СОВРЕМЕННОМ ОБЩЕСТВЕ: АНАЛИЗ МОДЕЛЕЙ РАЗВИТИЯ

В работе осуществлен анализ понятия открытых данных – даны определения; описаны структура и форматы. Рассматривается актуальность концепции открытых данных, ее роль в глобальных технологиях открытости государства и качества жизни граждан. Приводятся примеры использования, а также возможные перспективы использования на основе мирового опыта. Приводится исследование существующих приложений на основе наборов открытых данных. Высказываются предложения по новым приложениям с использованием существующих наборов данных, размещенных на официальных сайтах ФОИВ.

открытые данные, стандарт открытости, общедоступные данные, открытое правительство, приложения на основе открытых данных, порталы открытых данных.

Открытые данные – информация о деятельности государственных органов и органов местного самоуправления, размещенная в сети «Интернет» в виде массивов данных в формате, обеспечивающем их автоматическую обработку в целях повторного использования без предварительного изменения человеком (машиночитаемый формат), и на условиях ее свободного (бесплатного) использования [1].

Основные принципы открытых данных: первичность, полнота, актуальность, пригодность к машинной обработке, отсутствие дискриминации по доступу, отсутствие проприетарных форматов, лицензионная чистота. В соответствии с этими принципами, для упрощения использования открытых данных используются специальные лицензии CC-BY *(Creative Commons)* и ODC-BY *(Open Knowledge Foundation)*, базирующиеся на подходе «*some rights reserved*» – «некоторые права сохранены», в отличие от стандартного подхода «все права сохранены». Так, пользователь без заключения договора с владельцем ОД может использовать (в том числе повторно) открытые данные свободно, бесплатно, бессрочно, безвозмездно и без ограничения территории использования, в том числе имеет право копировать, публиковать, распространять открытые данные, видоизменять открытые данные и объединять их с другой информацией, использовать открытые данные в некоммерческих и коммерческих целях, использовать для создания программ для ЭВМ и приложений. Но при использовании открытых данных пользователь обязан: использовать открытые данные только в законных целях; не искажать открытые данные при их использовании; сохранять ссылку на источник информации при использовании открытых данных.

Наборы открытых данных публикуются в следующих форматах: при визуальном представлении – в формате HTML или RDFa (модель описания метаданных *Resource Description Framework in attributes*). Также должно быть обеспечено файловое представление в форматах CSV (формат представления табличных данных *comma-separated values*) или XML (язык разметки *Extensible Markup Language*). В формате CSV рекомендуется публиковать данные, имеющие плоскую табличную форму, при этом в содержании записи не допускается использование символа перевода строки. Сложные иерархические данные рекомендуется публиковать в форматах XML. Кроме того, вместе с данными, публикуемыми в формате XML, должны публиковаться файлы структурного описания формата в виде схемы XSD (язык описания структуры XML *Schema*). Вместе с данными, публикуемыми в формате CSV, должны публиковаться файлы структурного описания формата в виде текстового файла (*txt, csv*), имеющего спецификацию в виде открытого стандарта.

К структуре публикуемых наборов открытых данных выдвигаются следующие требования:

а) структура наборов открытых данных должна представлять описание каждого информационного поля набора данных.

б) при изменении структуры набора открытых данных должна обеспечиваться версионность структуры и соответствие данной версии последующим наборам открытых данных

в) количество хранимых версий структуры набора данных определяется на основании ресурсных возможностей для хранения с учетом потребности пользователей набора данных;

г) каждая версия структуры наборов открытых данных должна иметь постоянную гиперссылку;

д) в случае предоставления доступа к набору данных через программный интерфейс, указывается гиперссылка на файл, содержащий описание такого интерфейса и условия использования [2].

Схема публикации файлов открытых данных выглядит следующим образом: Владелец переводит набор данных в формат, в котором этот набор данных подлежит публикации, публикует паспорт набора данных, добавляет необходимую информацию на страницу публикации открытых данных своего веб-сайта (реестр наборов открытых данных, опубликованных государственным органом) и ссылку на страницу соответствующего паспорта набора данных, проверяет доступность опубликованного набора данных для пользователей веб-сайта, передает в виде файла в формате CSV или XML запись об опубликованном наборе данных, выгруженную из реестра наборов данных, открытых, в рабочую группу федерального уровня, ведущую единый реестр открытых данных. Рабочая группа федерального уровня обновляет единый реестр открытых данных, а также другую информацию об опубликованных наборах государственных данных, которую она ведет на портале открытых данных Российской Федерации: *http://data.gov.ru*.

Публикуются открытые данные в рамках реализации постановления Правительства Российской Федерации от 10 июня 2013 года № 583 "Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети "Интернет" в форме открытых данных" и согласно распоряжению Правительства Российской Федерации от 10 июля 2013 года № 1187-р «О перечнях информации о деятельности государственных органах, местного самоуправления, размещаемой в сети Интернет в форме открытых данных».

Существует немало областей, где «открытые данные» весьма полезны, а также много примеров того, как они используются и обеспечивают значительный эффект. Так, благодаря наличию «Открытого правительства» (т. е. открытой государственной информации) граждане могут принимать более информированные решения и совершать более обоснованный выбор относительно получения доступа к ресурсам общества и их ис-

пользования, может поощряться более активная гражданская позиция населения. Концепция «Открытого правительства» обеспечивает гласность благодаря свободному и неограниченному доступу к государственным данным и информации; иными словами, благодаря ей люди знают, чем занимается правительство от их имени.

Кроме того, наличие открытой государственной информации открывает возможности для представителей предпринимательских кругов: обеспечивается доступ к разнообразным массивам полезных данных, способным стимулировать создание инновационных предприятий и услуг, многие из которых представляют общественную и коммерческую ценность.

В перспективе рассматривается использование открытых данных при планировании городской инфраструктуры на основании статистических данных о численности населения и перемещении людских потоков в течение дня. Это позволяет определять необходимое количество социально значимых коммерческих структур. В случае публикации плана развития города в формате открытых данных государство получает возможность вступать в диалог с бизнесом и совместно моделировать максимально удобную для граждан инфраструктуру, что может значительно сократить издержки на ее обслуживание [3].

В настоящее время, существует множество полезных, с социальной и образовательной точки зрения, приложений, использующие наборы ОД, и их количество с каждым днём становится всё больше. В Российской федерации они размещаются на портале *http://data.gov.ru*. На данном портале также присутствуют средства разработки. Также проводятся различные конкурсы по разработке приложений на основе открытых данных. Рассмотрим зарубежные модели развития.

На едином портале ОД США публикуются государственные и негосударственные данные. Первые находятся в свободном и бесплатном доступе. Наборы данных, публикуемые от имени других лиц, могут распространяться по лицензии, информация о которых должна указываться в описании конкретного набора данных. В США открытые данные не содержат информации, доступ к которой может быть ограничен законодательством о государственной или иной тайне. Сфера открытых данных активно развивается и является востребованной обществом, что иллюстрируется следующими примерами использования открытых данных:

Сайт *http://www.opensecrets.org* позволяет гражданам США отслеживать формирование и расходование бюджетных средств в стране и их влияние на выборы и государственную политику. Например, можно отслеживать финансирование отдельных комитетов или привлечение средств отдельными конгрессменами.

Портал общественных петиций https*://wwws.whitehouse.gov/ petitions/* - граждане выкладывают свои обращения, и петиции, набравшие 25 тыс. голосов отправляются на рассмотрение в Белый Дом.

Сайт *http://votesmart.org* – представляет структурированные и визуализированные данные о политиках США [4].

В Великобритании Создан единый портал ОД, на котором размещаются государственные и негосударственные открытые данные. Также портал выступает агрегатором данных, которые могли быть размещены ранее. Для получения доступа к данным разработан пакет лицензий на использование информации государственного сектора в следующих случаях: бесплатное пользование и повторное использование информации государственного сектора для любых целей (как коммерческих, так и некоммерческих); бесплатное пользование и повторное использование только в некоммерческих целях; платное повторное использование.

Непосредственно социальный эффект от использования открытых данных в Великобритании можно охарактеризовать проектами:

Проект «*Fix My Street*», представляющем собой услугу по обсуждению и уведомлению властей о проблемах, возникающих вокруг городских дорог и на улицах.

Сайт криминальной статистики (*http://www.ukcrimestats.com*) – позволяет детализировать её до улиц и подразделений полиции.

http://www.police.uk/ – сервис картографирования информации о преступлениях и их раскрытии по всей стране. Например, по городу Лондон представлена статистика по месяцам, по типам происшествий, по улицам, по количеству преступлений на 1 000 человек.

http://data.gov.uk/ideas – каталог идей и предложений на сайте открытых данных Великобритании [5].

На основе анализа существующих на российских порталах наборов, предлагается создать приложение – **Персональные данные под защитой**. Суть проекта заключается в следующем: довольно часто мы оставляем свои данные, заполняя всевозможные анкеты или участвуя в акциях, так же собирают информацию о нас учреждения здравоохранения, операторы мобильной связи, различные автосалоны, страховые компании, банки и другие структуры. На сайте Роскомнадзора публикуется набор в формате открытых данных: Реестр операторов, осуществляющих обработку персональных данных. На его основе можно создать приложение, позволяющее, прежде чем заполнить какую-либо анкету или просто ответить на вопросы о себе, убедиться в том, что интервьюер включен в Реестр операторов ПД. Как минимум, это даст уверенность в том, что он обязан соблюдать требования по защите персональных данных граждан. Прежде чем использовать, а тем более передавать третьим лицам информацию, оператор должен получить от вас письменное согласие на обработку данных в рамках трудового договора, контракта, договора на оказание услуг. В это же приложении можно включить хранение списка операторов, которым Вы предоставили свои персональные данные, и предоставить возможность

отправлять отзыв на согласие обработки тем юр. лицам, чьи услуги Вас больше не интересуют, отследить, если произошла утечка.

Список используемых источников

1. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 № 149–ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. – 2006. – 29 июля.

2. Методические рекомендации по реализации принципов открытости в федеральных органах исполнительной власти (утверждены протоколом заседания Правительственной комиссии по координации деятельности открытого правительства от 29 мая 2014 г. N АМ-П36-89пр) [Электронный ресурс]. URL: http://data.gov.ru/ metodicheskie-rekomendacii-po-realizacii-principov-otkrytosti-v-federalnyh -organah-ispolnitelnoy.

3. Артамонов Р. Е., Датиев С. Б., Жулин А. Б. Оценка социально-экономического эффекта публикации открытых данных на примере данных общественного транспорта Москвы / Артамонов Р. Е., Датиев С. Б., Жулин А. Б. [и др.] / Нац. исслед. ун-т «Высшая школа экономики», Центр анализа деятельности органов исполнительной власти. М. : изд. дом Высшей школы экономики, 2015. 92 с. ISBN 978-5-7598-1266-1

4. Открытые государственные данные: российский и зарубежный опыт. Информационный обзор / Центр технологий электронного правительства НИУ ИТМО. Серия «Развитие информационного общества и электронного правительства». 2012. Вып. 3. 8 с.

5. Стырин Е. М. Государственное управление на основе открытых данных: перспективы развития : препринт WP8/2012/01 / Нац. исслед. ун-т «Высшая школа экономики». М. : Изд. дом Высшей школы экономики, 2012. 32 с.

УДК 004.056

П. Ю. Захарова (студентка группы МБИ-22, СПбГУТ)
С. И. Штеренберг (аспирант, СПбГУТ)

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОМОЩИ DLP-СИСТЕМ

Статья посвящёна проблеме расследования инцидентов информационной безопасности в компаниях. Выделены необходимые условия, цели и этапы проведения расследования. Особое внимание обращено на использование возможностей DLP-систем для решения поставленной проблемы.

инцидент информационной безопасности, расследование инцидента, внутреннее расследование, DLP-система.

В современных компаниях существует большое количество различных информационных потоков, полный контроль которых невозможен. Рано или поздно в любой компании возникают инциденты информацион-

ной безопасности. В свою очередь, компании стремятся минимизировать возможные убытки или постараться предотвратить инцидент на стадии его формирования. Для достижения поставленной цели необходимо организовать процесс управления инцидентами.

Для построения процесса управления инцидентами информационной безопасности необходимо сформировать жизненный цикл управления инцидентом информационной безопасности [1]. Его схема представлена на рисунке 1.

Рис. 1. Жизненный цикл управления инцидентом информационной безопасности

На схеме можно наблюдать, что цикл содержит 4 шага: обнаружение, регистрация, устранение видимых причин и последствий инцидента, его расследование и корректировка всей системы безопасности. В данной статье подробно рассмотрен третий шаг.

Процедуру расследования можно разделить на два этапа, каждый из которых преследует свою цель. Первым этапом является сбор данных. На этом этапе восстанавливается хронология событий, собираются доказательства. В случае выхода процедур за рамки внутреннего расследования, производится сбор юридически значимых материалов. Целью данного этапа является определение виновных в инциденте и степени их вины. Вторым этапом является анализ собранных данных. Выявляются причины и условия возникновения инцидента, оцениваются последствия инцидента. Для этого этапа целью является формирование предложений по совершенствованию системы организации для предотвращения повторения подобных ситуаций в будущем. Таким образом, благодаря постоянному совершенствованию, поддерживается надёжность всей системы.

Для успешного проведения расследования внутри организации необходимы определённые условия. Прежде всего, должна быть разработана соответствующая документация: политика реагирования на инциденты, процедура обработки инцидентов. Команда по расследованию инцидентов должна иметь налаженные контакты с определёнными работниками внутри организации (юристы, узкопрофильные специалисты, служба безопасности и т. д.). Важную роль имеет техническое оснащение команды.

Частью технического оснащения может стать DLP-система (*Data Leak Protection*). Работа DLP-систем строится на перехвате и последующем анализе потоков данных, циркулирующих внутри защищаемой корпоративной сети или выходящих за её пределы [2]. Изначально такие системы создавались для предотвращения, фиксирования утечек информации и оперативного оповещения службы безопасности. Со временем разработчики внедрили функционал расследования внутрь самих систем.

Современные DLP-системы могут предоставлять следующий функционал расследования:

- граф связей сотрудников;
- система уровня доверия к сотрудникам;
- сохранение переписки сотрудников;
- различные виды поисков: по ключевым словам, регулярным выражениям, поиск «похожих» и т. п.;
- отслеживание перемещений файлов;
- отчёты по различным параметрам, в том числе статистические;
- «личные дела» или «досье»;
- снимки/видеозаписи экрана, просмотр рабочего стола в режиме реального времени;
- аудио/видеозапись сотрудников;
- контроль рабочего времени: какие программы были запущены, как долго, какое окно является «активным»;
- посещаемость сотрудником различных сайтов.

В совокупности с широкими возможностями DLP-систем по перехвату и анализу данных, приведённых выше инструментов достаточно для проведения большинства внутренних расследований в компаниях. Общую схему работы с DLP-системой можно увидеть на схеме (рис. 2).

Для более полного понимания возможностей DLP-систем необходимо привести примеры расследуемых инцидентов. Такими инцидентами могут быть копирование всех доступных данных увольняющимся сотрудником, пересылка секретарём протоколов совещаний на внешний почтовый ящик и т. п.

Показательным является следующий пример реального инцидента, предоставленный компанией SearchInform. Системный администратор, ответственный за работу почтового сервера компании, настроил себе копию писем всех корпоративных почтовых ящиков, получив доступ ко всей переписке компании. Инструмент отчётности, входящий в состав DLP-системы, отразил резко возросшее количество писем и показал, что наибольшее количество писем получает системный администратор. Таким образом, система позволила оперативно устранить утечку информации до того, как компании был нанесён существенный ущерб.

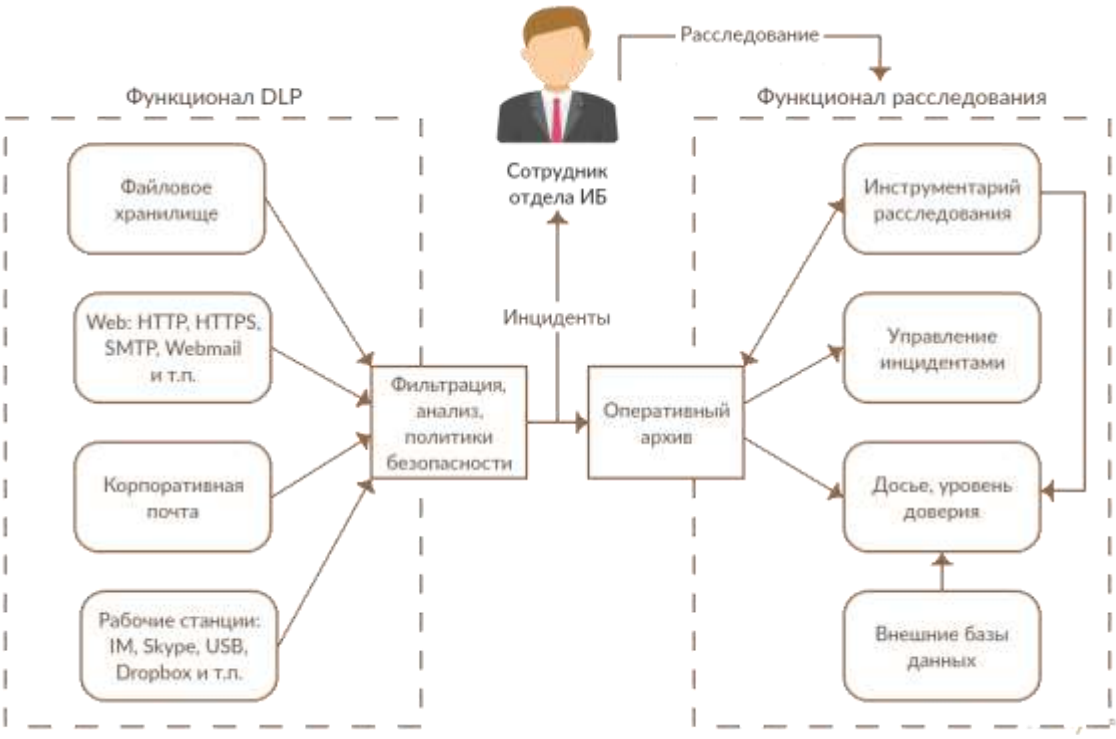


Рис. 2. Схема работы с DLP-системой для сотрудника, ответственного за проведение расследований

Согласно исследованию компании SearchInform, внедрение DLP-системы позволяет увеличить скорость расследования инцидента в 4,6 раза, а также снизить их количество в 2,5 раза. Особенно эффективны данные системы в крупных компаниях, где контроль действий сотрудников сильно осложнён в связи с их количеством. При использовании DLP-систем один сотрудник отдела информационной безопасности может осуществлять контролировать 1 000–1 500 сотрудников [3].

Внедряя DLP-систему, компания получает возможность как проводить внутренние расследования, так и собирать юридически-значимые доказательства для защиты своих интересов в суде.

Список используемых источников

1. Управление инцидентами информационной безопасности [Электронный ресурс] // Открытые системы. СУБД. 2006. № 10. URL: http://dsec.ru/ipm-research-center/article/information_security_incident_management/

2. Решения в части защиты конфиденциальной информации от утечки (DLP-системы) [Электронный ресурс] // Интернет-портал Ramec security. URL: http://security.ramec.ru/resheniya/resheniya-v-chasti-zashhityi-konfidenczialnoj-informaczii-ot-utechki-dlp-sistemyi.html

3. Практические аспекты реализации системы информационной безопасности в российских компаниях. Из опыта работы SearchInform [Электронный ресурс] // CNews. 2013. URL: http://www.cnews.ru/reviews/ppt/forum_2013/safety/7_Matveev.pdf

УДК 004.056.53

Е. Н. Золотарева (студентка магистратуры группы Р-4152, ИТМО)
К. Н. Золотарева (студентка магистратуры группы Р-4152, ИТМО)

УМЕНЬШЕНИЕ ИНФОРМАЦИОННЫХ РИСКОВ ОРГАНИЗАЦИИ С ПОМОЩЬЮ МЕХАНИЗМОВ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

В данной статье рассматривается вопрос об уменьшении информационных рисков, основанный на механизмах контроля привилегированных пользователей с помощью специализированных систем. Показаны перспективы применения данных систем для крупного и среднего бизнеса.

привилегированные пользователи, контроль, информационные риски.

Успешная деятельность организации и конкурентоспособность напрямую зависит от того, насколько защищены ее активы и информационная безопасность имеет определяющее значение. Так как за последние десятилетия подходы к ее обеспечению изменились, необходимо исследовать новые подходы к обеспечению информационной безопасности и снижению рисков.

Для обеспечения информационной безопасности в автоматизированных системах управления, построения эффективной системы защиты информации, не достаточно выявить каналы утечки информации, проанализировать возможные угрозы, последствия их реализации и оценить потери. Необходимо хорошо представлять облик нарушителя и выявить причины деструктивных действий. Нарушителями в рамках данной статьи являются привилегированные пользователи.

Для того чтобы понять кого надо контролировать, ознакомимся с понятием привилегированный пользователь.

Привилегированный пользователь (ПрП) – пользователь, обладающий расширенными правами доступа к системе, называемый администратором или root. Он может иметь права на доступ к любому файлу и на выполнение любой программы.

Причинами деструктивных действия привилегированных пользователей являются:

- Любопытство или стремление доказать, на что они способны. Многие внутренние пользователи не считают свои действия «вредоносными». Они расценивают их как брошенный вызов – мобилизацию своего опыта, терпения, а также сочетания стратегического и тактического мышления Месть (обиженные сотрудники). Внутренние инициаторы атак, подталкиваемые жаждой мести, испытывают враждебные чувства по отношению к вполне конкретным сотрудникам, а не к компании в целом. Действия та-

ких людей особенно опасны, потому что они проявляют выдержку и видят перед собой четкую цель. К данной категории чаще всего относятся бывшие сотрудники, считающие, что их несправедливо уволили.

- Финансовые мотивы. Внутренние пользователи, преследующие финансовые цели, крадут конфиденциальную информацию для заинтересованных третьих лиц.

Но реальные возможности нарушителя информационной безопасности во многом определяются в том, как организована информационная безопасность: состоянием объекта защиты, наличием потенциальных каналов утечки информации, качеством средств защиты информации.

От надежности системы защиты информации зависят и действия нарушителя, так как для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определённые ресурсы. Если информационная безопасность достаточно высока, его затраты будут чрезмерно велики, и он откажется от своего замысла. В связи с этим целесообразно определить в качестве показателя эффективности системы защиты информации вероятность обнаружения и своевременной реакции на каждый вид нарушения.

В связи с выше перечисленным появляются следующие возможные риски, связанные с неправомерными действиями привилегированных пользователей.

В таблице 1 представлены потенциальные неправомерные действия привилегированных пользователей.

ТАБЛИЦА 1. Потенциальные неправомерные действия привилегированных пользователей

Привилегированные пользователи	**Активы**	**Неправомерные действия**
1. Системные администраторы. 2. Администраторы безопасности. 3. Руководители ИТ-службы.	Windows, Linux, Unix и мэйфреймы	1. Чтение, копирование и изменение данных. 2. Изменение настроек безопасности. 3. Создание и удаление учетных записей. 4. Разрешение и запрет общего доступа к файлам. 5. Запуск программ.
1. Администраторы безопасности. 2. Руководители ИТ-службы.	Каталоги служб	1. Чтение, копирование и изменение данных пользователей. 2. Добавление и удаление пользователей. 3. Изменение полномочий пользователей. 4. Разрешение удаленного доступа.
1. Администраторы приложений. 2. Разработчики приложений. 3. Веб-мастера 4. Внештатные разработчики.	Уровни приложений	1. УЗ для обслуживания. 2. Файлы конфигурации 3. Выполнение приложений под указанной учетной записью. 4. Подключение к БД.

Привилегированные пользователи	Активы	Неправомерные действия
1. Администраторы БД. 2. Разработчики приложений. 3. Администраторы приложений. 4. Внештатные разработчики.	Базы данных	1. Чтение и изменение строк БД. 2. Доступ к транзакционным данным. 3. Изменение конфигурации и схемы БД. 4. Добавление и изменение хранимых процедур.
1. Сетевые администраторы. 2. Администраторы безопасности.	Устройства защиты сети	1. Изменение настроек. 2. Изменение политик безопасности и качества обслуживания. 3. Разрешение и запрет доступа к сети. 4. Доступ к каналам данных. 5. Включение и выключение мониторинга.
1. Системные администраторы. 2. Операторы резервного копирования. 3. Сетевые администраторы.	Инфраструктура резервного копирования и обслуживания.	1. Потеря каталога резервного копирования и потеря сохраненных данных. 2. Нарушение целостности данных.

Помимо отчетов о подключении внешних привилегированных пользователей, большую озабоченность вызывает необходимость выдачи реальных административных паролей для целевой системы или даже класса систем (например, аккаунт root для Unix/Linux систем или аккаунт администратора для Windows Server) [1, 2].

Но основной проблемой является то, что даже правильно настроенная отчетность на шлюзе удаленного доступа и отчетность на целевой системе, не могут сопоставить в реальном времени одни данные с другими.

Зная данные о том, кто, когда и откуда подключился к сети (отчет о соединении) или даже какие команды он выполнял в течение сессии, нельзя оперативно посмотреть действия этого человека на целевой системе, т. к. никто не мешает администратору зачистить все следы, и наоборот, по отчетам целевой системы нельзя понять, кто и откуда это делал. В итоге будут существовать несколько типов отчетов, которые придется как-то сопоставлять друг другу.

Если даже сопоставить данные из нескольких журналов постфактум, то это станет непростой задачей. Время в системах может быть не синхронизировано. При большом потоке данных журналы становятся огромны. Физически работа по анализу логов вручную затягивается, и поэтому практически не используется при анализе действий пользователей.

Так как много возможных рисков, связанных с ПрП и сложно работать с отчетностью на шлюзе удаленного доступа и целевой системы, то для облегчения работы и достижения большей безопасности можно использовать системы контроля привилегированными пользователями, а так

же ряд организационных и технических мероприятий, для снижения уязвимостей.

Системы контроля привилегированных пользователей (СКПрП) предназначены для централизованного управления правами на доступ к информации, учетными записями, паролями и другими атрибутами в информационных системах, что позволяет автоматизировать процессы управления правами доступа, снизить риски информационной безопасности и оптимизировать затраты на администрирование ИТ инфраструктуры.

Данная система предоставляет отчетность обо всех учетных записях и правах доступа ПрП организации в интегрированных с системой КПрП информационных системах.

Данные системы выгодны крупным компаниям, в частности руководству и самим привилегированным пользователям.

Во-первых, можно будет по результатам внутренней проверки однозначно указать, кто совершил ошибку и предъявить доказательства, причем не косвенные, а визуальные и понятные, не только техническим специалистам, но и остальным сотрудникам (при убытках компании, для возбуждения уголовного дела доказательства очень важны).

Во-вторых, данные системы повысят уровень ответственности администраторов различных систем, т.к. они будут знать, что производимые ими действия, в важных системах, пишутся в журнал событий (в текстовом и видео форматах).

В-третьих, отдельные операции можно будет проводить в 4 глаза.

В-четвертых, привилегированные пользователи смогут избежать наказания если при разборе конфликтной ситуации выяснится, что они все делали верно и в соответствии с нормативными документами.

В-пятых, легче наладить смену административных паролей.

В-шестых, безопасный удаленный доступ привилегированных пользователей к серверам организации.

Кроме того, привилегированные пользователи не смогут войти в систему со стороннего компьютера, т. к. помешает контроль со стороны ИБ за исполнением требований политики и правила "раздачи" ip адресов и регистрации компьютеров в AD.

Так же в данных системах реализована «защита от дурака» (от некоторых команд, при вводе которых система разрывает соединение и не дает ее выполнить). Например, создание пользователя в Cisco или Unix сервере.

Кроме того, такие системы позволяют выявить недостатки сопроводительной документации, инструкций, ведется протоколирование действий и сокращается время разбора инцидентов (не более 1 часа).

Но данное решение достаточно дорогостоящее, поэтому стоит хорошо оценить необходимость системы (данные системы являются отличным решением для организаций с большой ИТ – инфраструктурой). Так же, прежде чем внедрять выбранную системы контроля привилегированных

пользователей необходимо проверить ее на соответствие требованиям POC (Proof of Concept – Проверка Концепции).

Список используемых источников

1. Прозоровский А. Управление привилегированными учетными записями [Электронный ресурс] // Информационное агентство bankir.ru: [сайт]. URL: http://bankir.ru/publikacii/20140407/upravlenie-privilegirovannymi-uchetnymi-zapisyami-10004868/ (дата обращения 20.06.2016).

2. Стонеф Крис Общие сведения об управлении паролями привилегированных учетных записей [Электронный ресурс] // TechNet: сетевой журн. 2008. Сентябрь. URL: https://technet.microsoft.com/ru-ru/magazine/2008.09.passwords.aspx (дата обращения 23.06.2016).

Статья представлена научным руководителем,
доктором технических наук, доцентом Лебедевым И. С.

УДК 004.056

А. С. Исаков (студент группы ИКТЗ-24, СПбГУТ)

РАЗВЕРТЫВАНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА НА ОС UNIX (LINUX) ДЛЯ ОБЕСПЕЧЕНИЯ ПОДДЕРЖКИ PKI

На консультации по вопросам формирования цифрового пространства ЕАЭС с экспертами и представителями бизнеса членом Коллегии (Министром) по внутренним рынкам, информатизации и информационно-коммуникационным технологиям ЕЭК была определена необходимость формирования единого цифрового пространства ЕАЭС. Основной акцент был сделан на обеспечение информационной безопасности в платежных системах, используемых, для обслуживания цифровых рынков стран Союза. Построение сервисов доверенной третьей стороны должно осуществляться с использованием программного обеспечения преимущественно отечественной разработки и производства.

инфраструктура открытых ключей, удостоверяющий центр, сертификат, открытый ключ.

Основной вопрос, связанный с использованием средств ЭЦП, к которым предъявляются требования по высокой отказоустойчивости заключается в повышенных мерах обеспечения информационной безопасности при доверии к службам ДТС международного информационного обмена.

Как известно, операционные системы отечественного производства базируются на открытых кодах ОС типа Linux и прошли оценку соответствия согласно федеральному законодательству Российской Федерации,

поэтому наиболее актуален вопрос развертывания удостоверяющего центра (УЦ) в среде именно этих операционных систем.

Для реализации этой идеи, необходимо развернуть УЦ для обеспечения поддержки Инфраструктуры Открытых Ключей (рис. 1) [1], по выдаче сертификатов открытых ключей.

Рис. 1. Инфраструктура открытых ключей

Для развёртывания УЦ на ОС Unix (Linux) был сделан выбор в пользу УЦ на TinyCA.

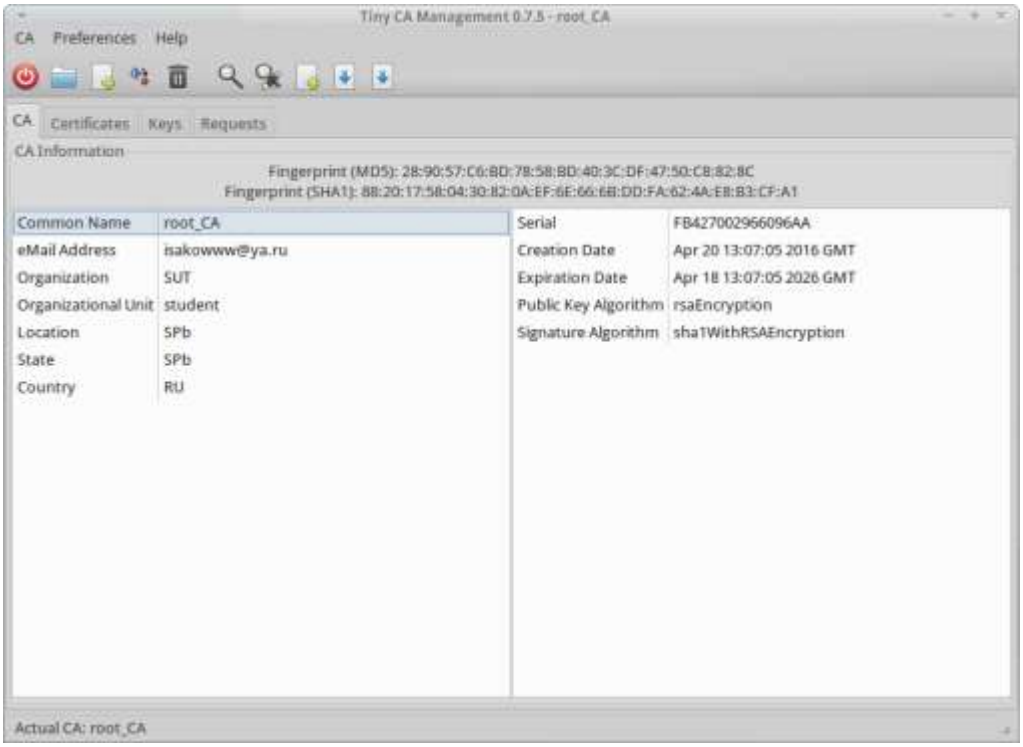


Рис. 2. Графический интерфейс TinyCA

TinyCA решает задачи управления сертификации (УЦ). Интерфейс (рис. 2) TinyCA, обеспечивает расширенные функции по выпуску сертификатов, среди которых стоит отметить [2]:

- Создание неограниченного количества УЦ: возможность работать с несколькими УЦ (выбор производится при открытии приложения или с помощью элемента интерфейса);
- возможность создания и управления иерархической древовидной структуры корневого и подчинённых УЦ;
- создание и аннулирование сертификатов в формате X.509, выпускаемых по шаблонам S/MIME, SSL Client, SSL Server;
- импорт и обработка запросов на выпуск сертификатов;
- экспорт сертификатов в форматы PEM, DER, PKCS # 12 и текстовый формат;
- интеграция в УЦ любых криптопровайдеров имеющих стандартизованный программный интерфейс (в т. ч. соответствующих требованиям национальных стандартов на СКЗИ).

Структура взаимодействия программных модулей и интерфейса ПО, показана на рисунке 3, она состоит из:

1) графический интерфейс *GUI*;
2) ядро процессинга обработки запросов и взаимодействия графического интерфейса ПО TinyCA с ПО OpenSSL – CA.pl;
3) подключаемые компоненты ПО OpenSSL;
4) конфигурационные файлы ПО TinyCA;
5) файлов журнала регистрации событий работы УЦ.

Последовательность Развертывания УЦ с использованием ПО TinyCA состоит из следующих действий:

1) Установка и первоначальная настройка ПО TinyCA согласно эксплуатационной документации.
2) Создание корневого УЦ, путем выбора соответствующего пункта в интерфейсе TinyCA и настройки полей его сертификата. При этом УЦ выпускает свой самоподписанный сертификат, после чего УЦ считается развёрнутым.

Для выпуска сертификата пользователя необходимо создать запрос с помощью утилиты certmgr Windows и экспортировать его на съемный носитель, для дальнейшей его передачи и импорта в TinyCA.

Для создания сертификата открытого ключа в TinyCA, необходимо импортировать ранее выполненный запрос сертификата пользователя, на основе которого, будет выпущен сертификат открытого ключа пользователя, сформировавшего запрос в УЦ TinyCA. После выпуска сертификата пользователя, он импортируется в хранилище сертификатов ОС Windows.

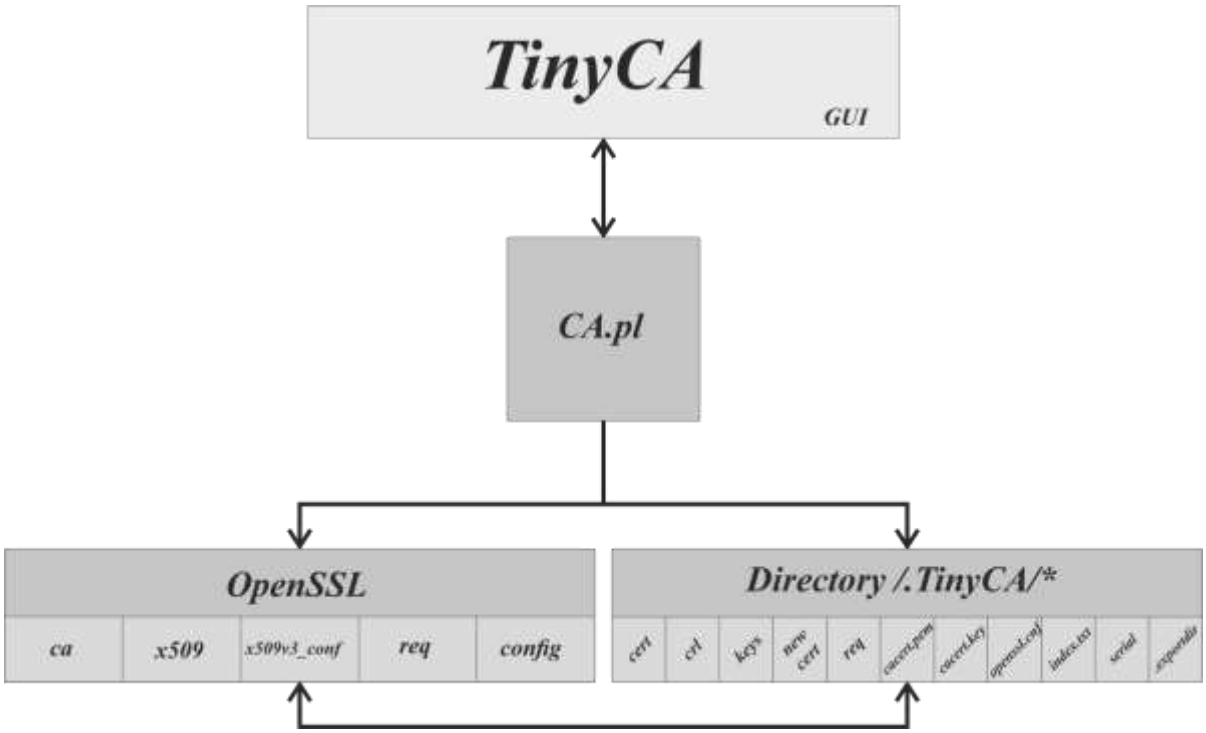


Рис. 3. Структура взаимодействия программных модулей и интерфейса ПО

Как видно из рисунка 4, что выпущенный сертификат, был сформирован путем подписания на секретном ключе УЦ TinyCA пользовательского запроса на сертификат в соответствии с требованиями стандарта X.509 [3].

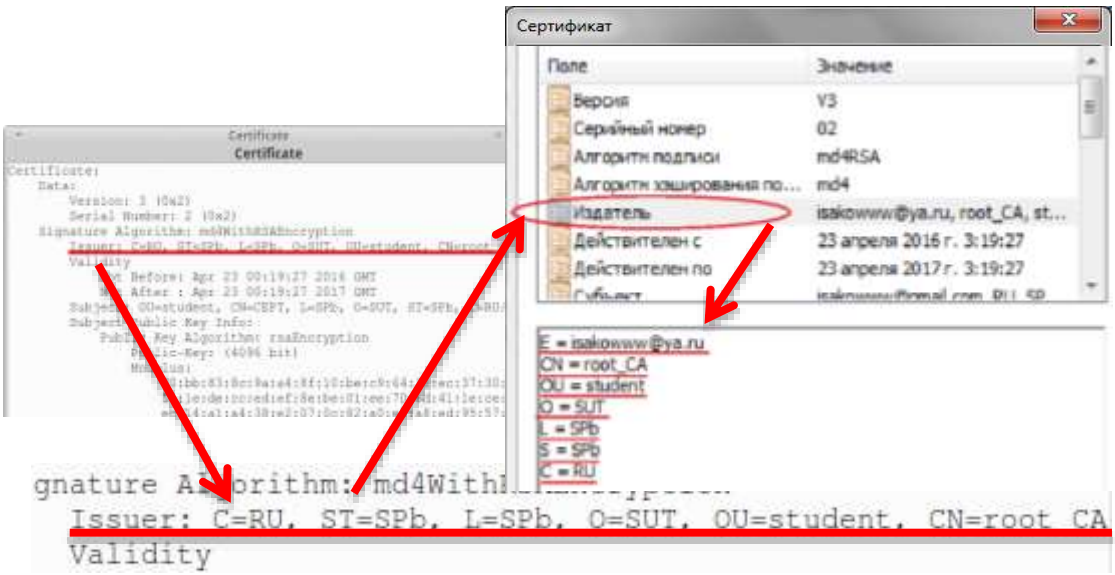


Рис. 4. Демонстрация подписанного сертификата в TinyCA и в certmgr Windows

В заключение стоит отметить, что TinyCA, позволяет выпускать сертификаты соответствующие стандарту X.509, открытые ключи, ЭЦП, обрабатывать запросы на сертификаты, формировать базы открытых ключей

и списков отозванных сертификатов, что соответствует большинству задач выполняемых на Windows УЦ.

Список используемых источников

1. Cooper D., Santesson S., Farrell S., Boeyen S., Housley R., Polk W., Yee P. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
2. Stephan Martin TinyCA – OpenSSL Front end. URL : http://tinyca.sm-zone.net/
3. Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key certificates and attribute certificates.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Юркиным Д. В.

УДК 004.021

И. В. Кропивко (студент группы ИКТБ-58м, СПбГУТ)

ИССЛЕДОВАНИЕ АУДИОСТЕГОСИСТЕМЫ, ПОСТРОЕННОЙ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ЭХО-СИГНАЛОВ С ПЕРЕДАЧЕЙ ИХ ЧЕРЕЗ АКУСТИЧЕСКУЮ СРЕДУ С ВНЕШНИМИ ШУМАМИ

Теоретически и экспериментально исследуется стегосистема при передаче информации на различные расстояния в акустической среде при наличии посторонних шумов. Показывается, что при использовании метода, основанного на эхо-сигналах, и адекватном выборе параметров вложения, стегосистема обеспечивает достоверный прием информации при достаточном удалении передатчика и приемника друг от друга и при наличии значительных шумов в акустической среде.

стегосистема, эхо-сигналы, кепстральный анализ, акустические шумы.

Стеганография – это семейство методов, при помощи которых некоторая дополнительная информация погружается в основное сообщение (так называемое покрывающее сообщение) при сохранении хорошего качества покрывающего сообщения.

В работе были исследованы методы построения такой стегосистемы, параметры которой позволяли бы передавать скрытую информацию с помощью аудиосигнала через акустическую среду. Данную стегосистему можно применять при передаче скрытой информации с помощью аудиосигналов, которые будут воспроизводиться с помощью мегафона. Также данный метод возможен для использования в качестве цифрового водяного

знака с целью сохранения прав собственности на аудио продукцию, к примеру, на концертных выступлениях. Схема работы исследуемой стегосистемы изображена на рисунке 1.

Рис. 1. Схема работы аудио стегосистемы

В качестве используемого метода вложения в исследуемой стегосистеме предлагается использовать метод, основанный на эхо-сигналах. Он заключается в добавлении «эхо» (сдвинутого по времени сигнала) к основному аудио сигналу. При этом данная «добавка» воспринимается человеком не как добавление аддитивного шума, а как появление дополнительной звуковой «окраски» (рис. 2).

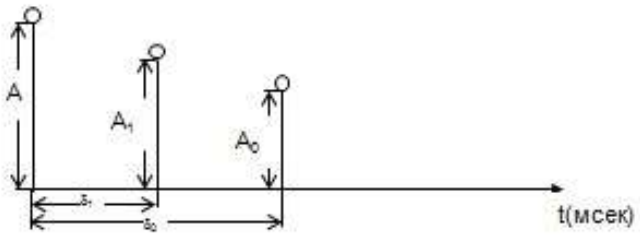


Рис. 2. Параметры вложения информации с использованием эхо-сигналов:
A – амплитуда исходного сигнала,
A_1 – амплитуда эхо-сигнала, соответствующая вложению «1»,
A_0 – амплитуда эхо-сигнала, соответствующая вложению «0»,
δ_1 – задержка эхо-сигнала, соответствующая вложению «1»,
δ_0 – задержка эхо-сигнала, соответствующая вложению «0»

В качестве метода обнаружения подобной стегосистемы предлагается использовать кепстральный метод приема. Основная идея кепстрального анализа заключается в том, что свёртка двух сигналов ($x(n) = S(n) * h_b(n)$) соответствует сумме их кептремов:

$$\tilde{x}(n) = \tilde{S}(n) + \tilde{h}_b(n), \quad n = 1,2,\ldots, \tag{1}$$

где $S(n)$ – исследуемый аудиосигнал, h_b – отклик фильтра на вложенный бит $b = (0,1)$, «~» – означает представление в виде кеструме.

При этом корреляционный прием сигналов, основанный на кепстреме, определяется следующей известной формулой:

$$\sum_n \hat{x}(n) \cdot \hat{h}_0(n) \underset{b=1}{\overset{b=0}{\gtrless}} \sum_n \hat{x}(n) \cdot \hat{h}_1(n), \tag{2}$$

Одним из ключевых факторов при выборе данного метода извлечения является тот факт, что в кепстральной области не имеет значения абсолютное значение амплитуды сигнала, которое меняется на протяжении всего сигнала и мешает выбрать порог для правила решения с использованием автокорреляционной функции.

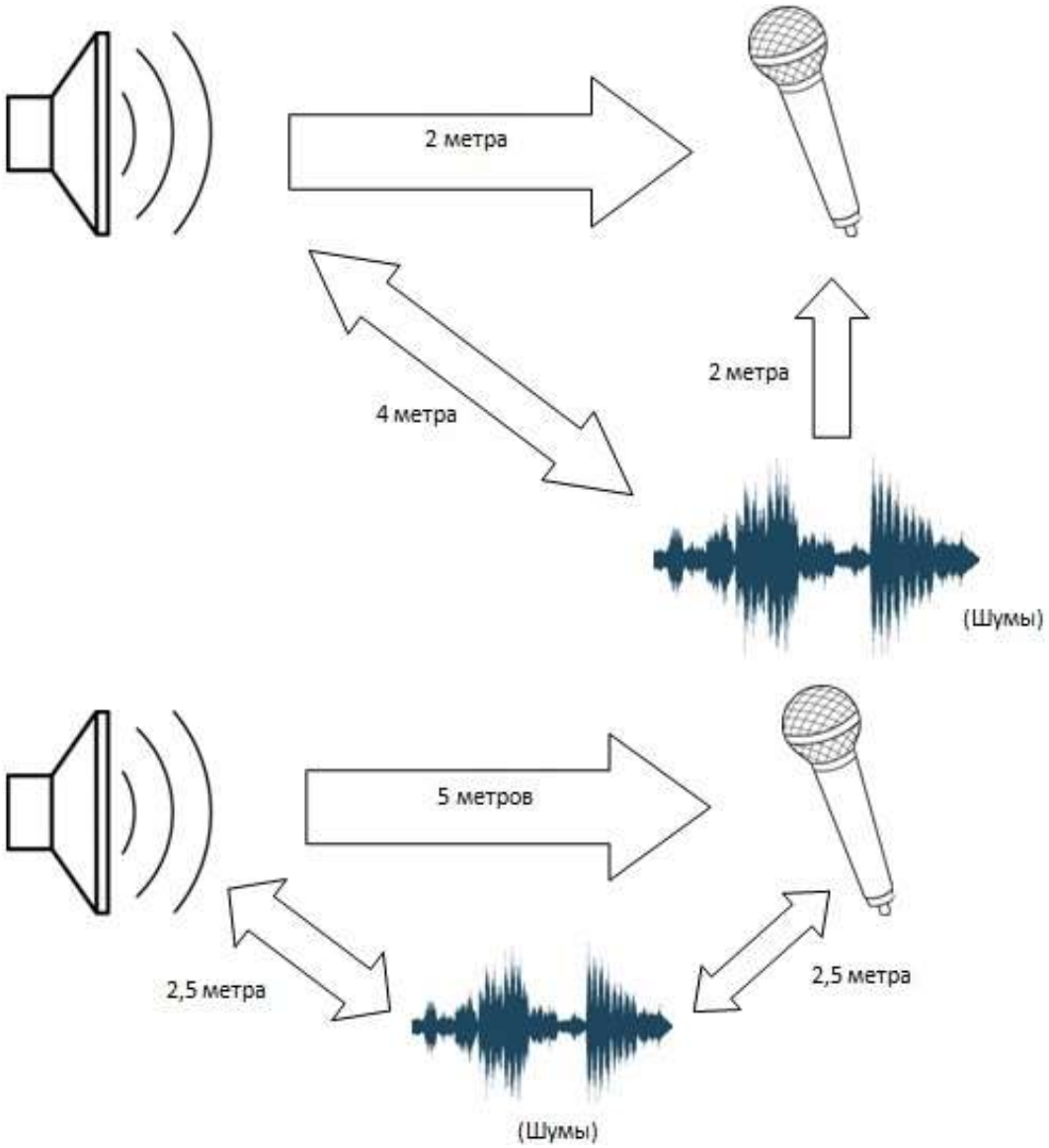


Рис. 3. Схема эксперимента с акустическими шумами

В ходе исследования был проведен следующий эксперимент. В три различных аудиосигнала было произведено вложение с использованием эхо-сигналов с одними и теми же параметрами вложения (глубина вложения 0,5; задержка сигнала – 32 и 37 отсчетов; количество бит, использующихся для вложения одного информационного бита – 10 000). Затем аудиосигнал проходил через акустическую среду, причем сначала в среде не было явных источников акустического шума, а затем они были добавлены согласно схеме, представленной на рисунке 3.

После прохождения акустической среды аудиосигнал с вложенной информацией подвергался кепстральному анализу. Результаты эксперимента представлены в таблицах 1–3 (аббревиатуры в таблицах – музыкальные файлы: Champions League – CL, Queen We Are The Champions – QWATC, inf – infinity, «бесконечность»).

ТАБЛИЦА 1. Результаты исследования при удалении источника и приёмника при отсутствии шума (расстояние в 2 м)

Расстояние в 2 м от приёмника	CL	QWATC	Penelope
Вероятность ошибки (%)	0,8	1,6	2
Максимальный уровень сигнала (дБ) на приёме	−8,8	−10,6	−3,3
Средний уровень сигнала (дБ) на приёме	−inf	−inf	−90,3

ТАБЛИЦА 2. Результаты эксперимента при максимальном уровне шума в −19,3 дБ

Шум			
Средний уровень сигнала (дБ)	−90,3		
Максимальный уровень сигнала (дБ)	−19,3		
Шум расположен на расстоянии в 2 м от приёмника и 4 м от источника			
Расстояние в 2 м от приёмника	CL	QWATC	Pen
Вероятность ошибки (%)	1,2	8,4	9,2
Максимальный уровень сигнала (дБ) на приёме	−13,3	−12,1	−10,8
Средний уровень сигнала (дБ) на приёме	−90,3	−90,3	−90,3
Шум расположен на расстоянии в 2,5 м от приёмника и 2,5 м от источника			
Расстояние в 5 м от приёмника	CL	QWATC	Pen
Вероятность ошибки (%)	10	16	13,6
Максимальный уровень сигнала (дБ) на приёме	−17,2	−11,6	−14,0
Средний уровень сигнала (дБ) на приёме	−inf	−inf	−inf

ТАБЛИЦА 3. Результаты эксперимента при максимальном уровне шума в −21,9 дБ

Шум			
Средний уровень сигнала (дБ)	−inf		
Максимальный уровень сигнала (дБ)	−21,9		
Шум расположен на расстоянии в 2 метра от приемника и 4 метра от источника			
Расстояние в 2 м от приемника	CL	QWATC	Pen
Вероятность ошибки (%)	0,4	3,2	2,8
Максимальный уровень сигнала (дБ) на приеме	−13,2	−10,8	−11,3
Средний уровень сигнала (дБ) на приеме	−90,3	−90,3	−90,3
Расстояние в 5 м от приемника	CL	QWATC	Pen
Вероятность ошибки (%)	1,2	6,8	6,4
Максимальный уровень сигнала (дБ) на приеме	−18,7	−17,3	−18
Средний уровень сигнала (дБ) на приеме	−inf	−inf	−90,3

Как видно из приведенных выше таблиц, при удалении источника и приемника сигналов друг от друга происходит незначительное ухудшение достоверности приема сигнала. Также стоит отметить, что даже при наличии сильного акустического шума (см. табл. 2) для аудиосигнала, при обработке которого легче других происходит синхронизация, вероятность ошибки возросла незначительно, в то же время для других аудиосигналов достоверность приема оставалась на удовлетворительном уровне. Наиболее показательными являются результаты, приведенные в таблице 3, так как шумовой фон в этом случае считается наиболее приближенным к реальной ситуации – передаче информации в местах с большим количеством побочных источников различного рода шумов. Как видно из таблицы 3, достоверность сигнала, несмотря на наличие шумов, остается на достаточно хорошем уровне.

Подводя итоги, следует отметить, что выбранная стегосистема, использующая вложение информации при помощи эхо-сигналов, подтвердила свою состоятельность при удалении источника информации от приемника при отсутствии и наличии шумов на расстоянии в два и пять метров. Достоверность информации во всех исследуемых схемах эксперимента оставалась на хорошем уровне. В дальнейшем планируется увеличить расстояние между источником и приемником сигналов до 50 метров и использовать при передаче речи мегафон в качестве устройства воспроизведения.

Список используемых источников

1. Коржик В. И., Алексеев В. Г., Федянин И. А. Выделение цифровых “водяных” знаков из аудиосигналов с использованием методов кепстрального анализа // 63 науч-

но-техническая конференция профессорского-преподавательского состава, научных сотрудников и аспирантов : материалы / ГОУВПО СПбГУТ. СПб., 2011. С. 225.

2. Bender W., Gruhl D., and Lu A. “Echo Hiding” Lecture Notes in Computer Science, 1996.

3. Donald G. Childers, fellow, IEEE, David P. Skinner, member, IEEE, and Robert C. Kemerait, member, IEEE „The Cepstrum: A Guide to Processing”, Proceedings of IEEE, VOL. 65, NO 10. OCTOBER 1977.

Статья представлена научным руководителем,
доктором технических наук, профессором Коржиком В. И.

УДК 004.056.53

К. А. Кудрявцева (студентка группы Р-4152, ИТМО)
Н. С. Ральникова (студентка группы Р-4152, ИТМО)

УПРАВЛЕНИЕ РИСКАМИ НА ПРЕДПРИЯТИИ, ИСПОЛЬЗУЮЩЕМ ВОЛОКОННО-ОПТИЧЕСКИЕ ЛИНИИ СВЯЗИ

Современное правовое, нормативное и методическое обеспечение безопасности информации в волоконно-оптических коммуникациях явно недостаточно, оно охватывает только государственные и военные объекты, оставляя личность и предпринимательство без должного внимания. Так как передаваемый по таким сетям трафик всегда носит конфиденциальный характер, оценке рисков информационной безопасности на предприятии, использующим волоконно-оптические линии связи, необходимо уделить должное внимание.

оценка рисков, оптоволокно, информационная безопасность, конфиденциальность.

Оптическая кабельная инфраструктура объекта информатизации может включать не только локальную сеть, но и сети телефонной связи, кабельного телевидения, систем видеонаблюдения, различных измерительных систем и другие кабельные системы. Передаваемый по ОК трафик носит конфиденциальный характер и имеет важное значение для функционирования объекта независимо от вида сети. Трафик может подвергаться различным опасностям, таким как нарушение конфиденциальности, целостности и доступности.

Конфиденциальностью обладает не только внутренний и внешний трафик, но и внутри объекта информатизации информация ограниченного доступа циркулирует в виде речи сотрудников или различных звуков работающего оборудования.

Таким образом, можно выделить две главные угрозы безопасности информации, передаваемой по ВОЛС:

1) Угроза перехвата трафика.

2) Угроза перехвата речевой информации.

Информация на предприятии может быть перехвачена, модифицирована или удалена при подключении к ВОЛС, что принесет предприятию убытки в денежном эквиваленте, часто не малые.

Оценка рисков информационной безопасности необходимый элемент в работе службы безопасности на предприятии, оценка рисков поможет проанализировать правильность выбранных методов защиты с экономической точки зрения.

Управление рисками представляет собой последовательность согласованных действий по руководству компанией и контролю ее деятельности в ситуации, вызванной наличием риска. Так же подразумевает систематическое выявление и оценку рисков, принятие необходимых мер и доведение информации о рисках до всех сотрудников компании.

Анализ рисков – обязательное требование стандарта СТО-БР ИББС по обеспечению информационной безопасности в банковской сфере. При прохождении сертификации на соответствие требованиям стандарта ИСО/МЭК 27001 эта процедура так же необходима [1].

Наиболее известные методы оценки: качественный и количественный анализ.

Суть качественного анализа рисков заключается в оценке значений риска экспертами. Данный метод используется, когда сам риск не может быть измерен количественно и описан математически.

Количественный анализ может производиться аналитически или графически. Он предполагает численное определение величин отдельных рисков и риска проекта в целом. Количественная оценка рисков позволяет четко рассчитать и аргументировать инвестиции в безопасность, но она крайне трудоемка [2].

Среди качественных методов оценки риска информационной безопасности часто используется экспертная оценка. Метод экспертных оценок риска – это метод прогнозирования и анализа рисков, которые основаны на заключениях экспертов, имеющих опыт реализации проектов.

Рассмотрим некоторые из существующих видов такой оценки, а так же их методологию [3].

Первая группа экспертных оценок – это индивидуальные оценки. Данная группа включает в себя следующие методы.

1) Интервью. Эксперт и опрашивающий находятся в непосредственном контакте. Необходимая информация извлекается в ходе беседы.

2) Анкетный опрос. Эксперту предлагается для заполнения анкета, содержащая набор вопросов, каждый из которых логически связан с центральной задачей исследования.

3) Аналитический метод. Эксперт проводит логический анализ какой-либо прогнозной ситуации, и результатом его деятельности является аналитическая докладная записка.

Вторая группа экспертных оценок – коллективные оценки. В эту группу входят следующие методы.

1) «Мозговой штурм». Метод является очень эффективной технологией генерирования новаторских идей. Отбирается группа квалифицированных экспертов, но оценки и выводы делаются в ходе заседания. Все эксперты делятся на две группы: первая генерирует идеи (выставляет оценки), а вторая – их анализирует.

2) Метод векторов предпочтений. Применяется, когда необходимо провести ранжирование объектов. Эксперт анализирует каждый из рассматриваемых объектов и выбирает предпочтительный в форме ранжирования.

3) Метод Дельфи. Последовательное анкетирование мнений экспертов по интересующей организаторов экспертизы проблеме. Метод предполагает серию опросов экспертов, не имеющих возможности вступать друг с другом в непосредственный контакт и получающих информацию о заключениях других лишь по их письменным отчетам. После чего определяется степень согласованности экспертов.

4) Дискуссия. Проводится как открытое коллективное обсуждение рассматриваемой проблемы, основной задачей которого является всесторонний анализ всех факторов, положительных и отрицательных последствий, выявление позиций участников.

К эксперту предъявляют следующие требования:

1) Стаж.
2) Креативность.
3) Эвристичность.
4) Интуиция.
5) Предикативность.
6) Независимость.
7) Всесторонность [4].

Проведя анализ методов экспертной оценки, можно сделать вывод о том, что так как сфера защиты волоконно-оптических коммуникаций пока не развита, то сложно будет остановиться на мнение одного эксперта, поэтому остановимся на выборе коллективной оценки. А именно на методе Делфи, так как такой опрос не требует личного присутствия эксперта, можно использовать электронную почту, а так же нет доминирования мнения одного из экспертов.

Приведем пример анкеты для экспертов – определение вероятности реализации угрозы (табл. 1).

Угрозы:

1) Перехват трафика контактным методом с разрывом ОК.

2) Перехват трафика контактным методом с прямым доступом к ОК.

3) Перехват трафика контактным методом оптического туннелирования.

4) Перехват трафика дистанционным методом на основе параметрических методов.

5) Перехват трафика дистанционным методом путем регистрации побочных излучений.

6) Изменение параметров ОВ.

7) Перехват речевой информации в действующем ОК.

8) Перехват речевой информации в недействующем ОК.

Тогда анкета будет выглядеть следующим образом, где 1–8 соответствующие угрозы, представленные выше:

ТАБЛИЦА 1. Пример анкеты для экспертной оценки

	Угрозы							
Эксперты	1	2	3	4	5	6	7	8
Иванов И. И								
Петров П. П.								
…								

Эксперт должен оценить вероятность реализации угроз на конкретно рассматриваемом объекте. Возможные варианты ответа:

– вероятность реализации угрозы высокая,
– вероятность реализации угрозы средняя,
– вероятность реализации угрозы низкая.

После этого, проводится анализ всех оценок экспертов с целью выделения среднего или медианы и крайних значений оценок. Экспертам сообщаются результаты обработки первого тура опроса с указанием расположения оценок каждого эксперта. Если оценка эксперта сильно отклоняется от среднего значения, то его просят аргументировать свое мнение или изменить оценку. После чего процедура повторяется [1]. Таким же образом проводятся последующие туры.

В качестве заключения можно отметить, что для оценки рисков организации целесообразно выбрать качественную оценку рисков, а именно экспертную оценку, так как обеспечивает наглядность и не требует больших затрат на организацию и проведение. Экспертные оценки помогут выявить наиболее вероятные угрозы системы информационной безопасности, касательно ВОЛС. На их основании можно сделать вывод о том, чему конкретно стоит уделять особое внимание и какие угрозы необходимо минимизировать в первую очередь.

Список используемых источников

1. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М. : Стандартинформ, 2008. 31 с. – URL: http://protect.gost.ru/ document.aspx? control=7&id=129018 (дата обращения: 03.04.2016)
2. Зайцева Н. М. Количественный анализ информационных рисков // Материалы VI межвузовской научно-практической конференции аспирантов, студентов и курсантов «Современные тенденции и перспективы развития водного транспорта России» 14 мая 2015 года. СПб. : ГУМРФ им. адм. С.О. Макарова, 2015. 472 с.
3. Лукичёва Л. И., Егорычев Д. Н., Анискина Ю. П. Управленческие решения : учебник по специальности «Менеджмент организации». 4-е изд., стер. М. : Издательство «Омега-Л», 2009. 383 с.
4. Лаптева Н. А., Морозова Т. Ф. Оценка рисков при реализации инвестиционно-строительного проекта на примере бизнес-центра // Magazine of civil engineering. 2011. № 2. С. 48–51.

Статья представлена научным руководителем,
доктором военных наук, профессором Каториным Ю. Ф.

УДК 004.056.53

К. А. Кудрявцева (студентка группы Р-4152, ИТМО)
Н. С. Ральникова (студентка группы Р-4152, ИТМО)

АНАЛИЗ БИОМЕТРИЧЕСКИХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Достоинства биометрических идентификаторов на основе уникальных биологических, физиологических особенностей человека, однозначно удостоверяющих личность, привели к интенсивному развитию соответствующих средств. Для использования тех или иных биометрических систем контроля и управления доступом, необходимо проведение их анализа.

информационная безопасность, биометрика, система контроля и управления доступом.

Основой системы информационной безопасности любого предприятия является система контроля и разграничения доступа. Различные системы контролируемого обеспечения доступа можно разделить на три группы в соответствии с тем, что человек собирается предъявлять системе: секретные данные (пароль, PIN), персональный идентификатор (пластиковая карта, токен), либо свои персональные характеристики – биометрические данные.

Согласно результатам исследований, треть пользователей записывает пароли, а это означает, что любые носители информации о пароле (как правило, это обычный листок бумаги, оставленный в ящике стола) могут быть доступны другим лицам. Большинство экспертов приходит к выводу, что компаниям следует использовать новые методы обеспечения безопасности, в частности биометрию. Биометрические системы доступа являются очень удобными для пользователей. В отличие от паролей и носителей информации, которые могут быть потеряны, украдены, скопированы биометрические системы доступа основаны на человеческих параметрах, которые всегда находятся вместе с ними, и проблема их сохранности не возникает.

Основные рекомендации заключаются в использовании биометрических технологий, причем по прогнозам разработчиков, биометрические сканеры и вычислители вскоре будут встраиваться непосредственно в компьютер. Использование биометрической идентификации в службе информационной безопасности предприятия, в первую очередь, позволит ограничить доступ к компьютерам (рабочим станциям и серверам), к базам данных либо их частям, обеспечит контроль личности оператора в реальном режиме времени.

Биометрические системы контроля доступа делятся на два класса:

- системы, использующие статические методы, основанные на физиологических характеристиках человека, т. е. на уникальных характеристиках, данных ему от рождения (рисунки папиллярных линий пальцев, радужной оболочки глаз, геометрия руки и т. д.);
- системы, использующие динамические методы, основанные на поведенческих характеристиках людей, то есть основаны на характерных для подсознательных движений в процессе воспроизведения или повторения какого-либо обыденного действия (почерк, голос и особенности речи, ритм работы на клавиатуре и т. д.).

Все биометрические системы работают практически по одинаковой схеме. Принцип работы таких систем основан на получении изображения со сканера биометрического считывателя и его преобразовании в некий шаблон, который затем сравнивается с имеющейся базой.

В момент сравнения полученного изображения с шаблоном возможно появление ошибок: ошибки первого рода – когда сканер не может распознать зарегистрированного пользователя и ошибки второго рода – когда незарегистрированный пользователь определяется системой как зарегистрированный.

Динамические методы биометрической аутентификации основываются на поведенческой (динамической) характеристике человека, то есть построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия.

1) По рукописному почерку. Как правило, для этого вида идентификации человека используется его роспись (иногда написание кодового сло-

ва). Сложность метода заключается в том, что при каждом подписывании автором могут добавляться некоторые фрагменты подписи, так же как некоторые фрагменты могут сливаться там, где в образце этого нет. Также серьезной проблемой является сильная зависимость параметров системы от психологического состояния людей и стабильности их почерка.

2) По клавиатурному почерку. Возможность аутентифицировать клавиатурный почерк человека появляется при вводе в качестве пароля фразы, состоящей из достаточно большого количества букв. Система фиксирует времена нажатия клавиш и интервалы между нажатиями и отпусканиями клавиш (контрольные параметры) [1]. Достоинством данного метода является то, что для идентификации личности не требуется никакого дополнительного оборудования кроме стандартной клавиатуры.

3) По голосу.

Существует достаточно много способов построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик голоса. Система анализирует несколько произношений контрольной фразы, на основе чего создается биометрический эталон, который, по сути, предсказывает наиболее вероятные значения характерных функций. Недостатком системы служит невозможность сохранения контрольной фразы в тайне. Поэтому современные ожидания эффективности систем аутентификации по голосу базируются на предположении о возможности такой аутентификации при произнесении произвольной фразы [1].

Статические методы биометрической аутентификации основаны на физиологических характеристиках человека, присутствующих от рождения и до смерти, находящиеся при нём в течение всей его жизни, и которые не могут быть потеряны, украдены и скопированы.

1) Отпечатки пальцев. Идентификация по отпечаткам пальцев – это наиболее распространенный биометрический метод идентификации личности. Каждый человек имеет уникальный папиллярный узор на кончиках пальцев, благодаря чему и возможна идентификация. Особенности папиллярного узора преобразовываются в уникальный код, который сохраняет информативность изображения отпечатка [2]. Преимущества использования аутентификации по отпечаткам пальцев – легкость в использовании, быстрота и удобство, а также сравнительно маленькая стоимость оборудования. К недостаткам же данного метода относятся невозможность идентификации при царапинах, порезах и ожогах пальцев, а также недостаточная защищенность от подделки, что связано с широким распространением данного метода.

2) Радужная оболочка глаза. Это тонкая подвижная диафрагма глаза у позвоночных с отверстием (зрачком) в центре. Радужная оболочка образовывается ещё до рождения человека, и не меняется на протяжении всей жизни. По текстуре она напоминает сеть с большим количеством окружа-

ющих кругов и рисунков, которые могут быть измерены компьютером, рисунок радужки очень сложен, это позволяет отобрать порядка 200 точек, с помощью которых обеспечивается высокая степень надежности аутентификации. Поэтому данный метод является наиболее точным [3]. К недостатком данного метода можно отнести высокую стоимость оборудования, а к достоинствам – высокую точность метода и отсутствие физического контакта со сканером.

3) Сетчатка глаза. Метод идентификации по сетчатке глаза основывается на уникальности рисунка кровеносных сосудов глазного дна. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, направленное через зрачок к кровеносным сосудам на задней стенке глаза. Из полученного сигнала выделяется несколько сотен особых точек, информация о которых сохраняется в шаблоне [3]. Подобные системы требуют чёткого изображения и, как правило, чувствительны к неправильной ориентации сетчатки. Поэтому требуется смотреть очень аккуратно, а наличие некоторых заболеваний может препятствовать использованию данного метода. Также к недостатком относится высокое время обработки. К достоинствам можно отнести очень низкую вероятность ошибок.

4) Геометрия лица. Существует множество методов распознавания по геометрии лица. Все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. Эта область биометрии многим кажется привлекательной, потому что мы узнаем друг друга в первую очередь по лицу [2].

5) Карта вен. Данный метод идентификации является наиболее новым. Инфракрасная камера делает снимки внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК излучение. В результате, степень отражения уменьшается, и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку [3]. Достоинство – не требуется контакта человека со сканирующим устройством. Многие возрастные заболевания могут затруднить идентификацию, привести к ошибке второго рода – это явный недостаток данного метода.

Выше были рассмотрены различные методы, применяющиеся в биометрических системах контроля и управления доступом. Каждый из них имеет как преимущества, так и недостатки, и могут применяться в зависимости от поставленной задачи. Например, самый быстрый метод – метод сканирования отпечатков пальцев, однако он не достаточно надежный, и если необходима более надежная система, то следует использовать метод распознавания по радужной оболочке, однако этот метод будет более дорогостоящим. Для массового распознавания людей лучше всего подходят методы идентификации по геометрии лица.

В качестве примера рассмотрим систему для контроля физического доступа сотрудников на предприятие. Для этого вполне подойдет система, использующая метод идентификации по отпечатку пальца. Проходная объекта может быть оборудована следующей системой:

- ZKTeco MA300 – биометрический контроллер-считыватель. Модель представляет собой небольшой терминал в котором объединены такие компоненты как: считыватель бесконтактных карт EM-marine, биометрический датчик и функциональный контроллер доступа в помещение.
- Турникет-трипод настенный ОМА-26.461**.** Турникет предназначен для управления потоками людей в системах управления и контроля доступа. Турникет предотвращает несанкционированный вход и выход людей при проходе через зоны контроля с двухсторонним движением.

Недостатки методов парольной аутентификации, а также методов с использованием физических идентификаторов, привели к осознанию необходимости использования биометрических систем контроля и управления доступом. В данной статье был проведен анализ методов биометрических систем контроля и управления доступом, выявлены преимущества и недостатки различных методов, а также представлено решение оборудования проходной предприятия с использованием биометрической системы для контроля физического доступа.

Список используемых источников

1. Черкезов Р. Динамические методы биометрической аутентификации личности: эссе [Электронный источник]. URL: http://re.mipt.ru/infsec/2006/essay/2006_ Dynamic_ biometric_ authentification__Cherkezov.pdf

2. Мальцев А. Современные биометрические методы идентификации [Электронный ресурс] // habrahabr.ru: [сайт]. URL: http://habrahabr.ru/post/126144/.

3. Попов М. Биометрические системы безопасности [Электронный ресурс] // БДИ 2002. № 1 (41). URL: http://www.bre.ru/security/12571.html.

Статья представлена научным руководителем,
доктором военных наук, профессором Каториным Ю. Ф.

УДК 004.724.3

М. С. Кулаков (аспирант, МТУСИ)

РАЗРАБОТКА ПРОТОКОЛА МАРШРУТИЗАЦИИ САМООРГАНИЗУЮЩЕЙСЯ AD HOC СЕТИ ДЛЯ СИСТЕМ АЗН-В

Интенсивный рост числа транспортных средств, как наземных, так и авиационных создал в некоторых регионах большую нагрузку на системы контроля и управления

движением. На сегодняшний день, комбинирование различных инфокоммуникационных технологий и внедрение их в транспортную среду является одной из задач, решение которой может быть использовано для множества практических применений. Являясь неотъемлемой частью инфокоммуникационных технологий телекоммуникационные сети передачи данных предоставляют уникальную возможность обмена информацией между пользователями, где бы они не находились в рамках этой сети. Использование мобильных Ad Hoc сетей является одним из перспективных методов повышения ситуационной осведомленности транспортных систем, т.к. данный вид сетей обладает несколькими важными свойствами: автоконфигурацией, самооптимизацией и самовосстановлением.

АЗН-В, самоорганизующиеся сети, маршрутизация, Ad Hoc.

Создание интеллектуальных коммуникационных систем контроля и управления движением различных транспортных средств является перспективной тематикой для исследований и разработок. По данным компании *exxonmobil* число личных автомобилей вырастет к 2040 году более чем в 2 раза по сравнению с 2010 годом, и составит 1 600 млн легковых автомобилей [1]. В соответствии с прогнозом компании *Boeing* авиакомпании разных стран мира в период с 2007 до 2026 г. приобретут 28 600 новых самолетов, что также обозначает прирост числа самолетов примерно в 2 раза. Следует отметить, что большинство специалистов отрасли считают прогнозы компании *Boeing* наиболее точными и заслуживающими внимания [2]. Ситуация усугубляется приростом числа летательных аппаратов (ЛА) малой авиации (частной) и развитием сфер применения беспилотных летательных аппаратов (БПЛА).

Современные тенденции развития телекоммуникаций ориентированы на создание сетевых структур для организации обмена данными различного типа. Телекоммуникационная сеть – это сложная система, представляющая собой совокупность абонентских узлов и средств связи, и выполняющая различные функции обмена и обработки информации. Не исключением являются и авиационные системы связи, в общей сложности, состоящие из большого числа участников и отдельных элементов. Однако, на данный момент, не существует полноценной реализации авиационной сетевой структуры, причины в этом следующие:

1) высокая интенсивность изменения топологии сетевых элементов, т. к. ЛА движутся с высокой скоростью и на разных высотах;

2) существенные ограничения по используемому УКВ-диапазону авиационной связи;

3) возможность использования других частотных диапазонов(выше по частоте) чревато: во-первых, перекрытием диапазонов, являющимися специфичными для разных регионов мира, а во-вторых, увеличением мощности и габаритов приемопередатчиков.

4) сложность в реализации сетевой маршрутизации с помощью традиционных алгоритмов маршрутизации;

5) большая длительность периода внедрения новых систем авионики.

С развитием средств авионики в дополнение к существующим системам контроля и управления воздушным движением стали внедряться технологии автоматического зависимого наблюдения вещательного (АЗН-В): системы 1090ES [3] и VDL Mode 4 [4], позволяющие вести обмен местоположением и намерениями всех участников движения, в том числе и на земле.

Функционал VDL Mode 4 благодаря особому методу доступа к среде имеет ряд преимуществ, для создания на его основе самоорганизующейся сети, по сравнению с системой 1090ES. Каждый приемопередатчик VDL Mode 4, используя несколько различных алгоритм, имеет возможность самому выбрать временной слот (канальный интервал), в котором он будет вести передачу с малой вероятностью коллизии.

Для решения задачи обеспечения ситуационной осведомленности в транспортных сетях перспективным подходом является построение мобильной самоорганизующейся Ad Hoc сети между участниками движения, а также их контрольными пунктами.

Мобильные Ad Hoc сети (MANET) – это самоорганизующиеся сети передачи данных, с переменной топологией и не имеющие постоянной структуры, которые предназначены для связи между подвижными объектами [5]. Таким образом, в данной сети каждое устройство может двигаться независимо, в любом направлении и, соответственно, будет менять соединения с другими узлами достаточно часто. При этом каждый узел может являться ретранслятором трафика в независимости от собственного назначения. Термин «*Ad Hoc*» означает особенность или специализированность такой сети, т. е. её направленность на решение одной конкретной или ряда задач.

В рамках работы по исследованию самоорганизующихся авиационных сетей, с помощью пакета моделирования OMNET++ [6], были смоделированы несколько сценариев возможности развертки самоорганизующейся сетевой структуры на Дальнем Востоке, Ямале и в Северо-Атлантическом океане. При моделировании учтены такие параметры, как: расстояние между объектами (по трем координатам) мощность передатчика, чувствительность приемника, затухание при распространении, диаграмма направленности, уровень шума и др. [7]. На рисунке 1 показан один из примеров времени обзора маршрутов ЛА.

При разработке протокола маршрутизации следует учесть множество факторов, которые в конечном итоге могут повлиять на общую производительность сети. Таким образом, исследователи выделяют несколько базовых классов алгоритмов маршрутизации в MANET сетях, которые лежат в основе различных протоколов:

1. Алгоритмы маршрутизации, основанные на топологии сети. Такие алгоритмы определяют метод нахождения маршрута от источника до адре-

сата и поэтому распадаются на два подкласса: реактивные (маршрут строится только в том случае, когда источнику требуется отправить данные) и проактивные (узлы в сети время от времени рассылают по сети актуальную информацию о состоянии маршрутов и записывают её в таблицу).

2. Географические алгоритмы, использующие информацию о местоположении узлов в сети для маршрутизации данных.

3. Гибридные алгоритмы маршрутизации. Данный вид алгоритмов комбинирует методики маршрутизации географических и топологических алгоритмов.

4. Кластерные алгоритмы маршрутизации. Такие алгоритмы делят по тем или иным признакам сетевые узлы на кластеры и обеспечивают внутрикластерную и межкластерную маршрутизацию данных.

5. Алгоритмы *data fusion*, использующие анализ различных данных получаемых с сетевых узлов для решения задачи нахождения маршрутов.

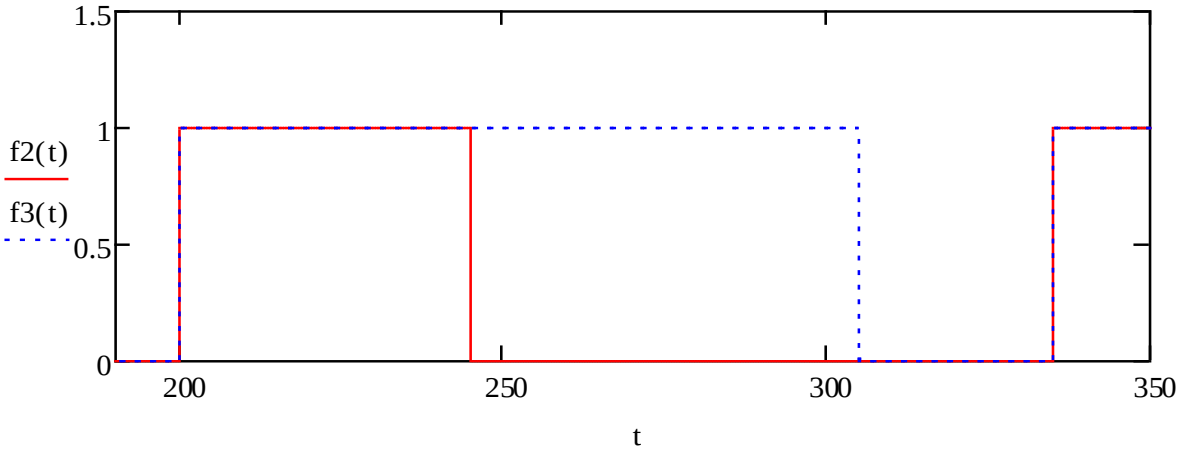


Рис. 1. Оценка времени обзора
для маршрута 25414 Салехард – Сабетта (выигрыш около 70 %).
Красным – время в прямой видимости наземной станции,
синим – наблюдение через сеть

При рассматриваемой топологии сети, дальности радиовидимости и ограниченных канальных ресурсах эффективной техникой маршрутизации может являться семейство географических протоколов маршрутизации.

С учетом рассмотренных выше особенностей сетей MANET и области их возможного применения предполагается использовать протокол маршрутизации, состоящий из следующих этапов функционирования:

- периодическое вещание местоположения и намерений узлами сети, как в зоне собственной радиовидимости, так и за её пределами, для обеспечения остальных узлов сети информацией для маршрутизации;
- использование поля жизни сетевого пакета, как ограничителя расстояния распространения сообщения, так и метки пройденных интервалов;

- поиск маршрутизатора производится только при необходимости передачи данных, при этом текущее местоположение адресата вычисляется исходя из данных полученных от него;
- использование жадного алгоритма (выбирается ближайший узел к адресату) для выбора маршрутизаторов среди узлов, от которых пришли пакеты с наименьшим и одинаковым временем жизни, что в свою очередь обеспечит оптимальность работы жадного алгоритма;
- пассивное прослушивание при ретрансляции сообщения, что позволит выявить ошибки маршрутизации без каких-либо дополнительных процессов обмена данными.

Разработанный гибридный протокол маршрутизации для многоинтервальной передачи данных между приемопередатчиками БЛА и контрольными пунктами использует информацию о местоположении узлов сети. Суммарно, рассматриваемый подход позволяет:

- использовать служебные сетевые сообщения, занимающие несколько десятков бит, что позволит обмениваться информацией относительно большому числу узлов без перегрузки сети;
- функционировать с малым количеством служебных сообщений;
- использовать простой алгоритм маршрутизации, что обеспечит эффективную обработку сетевых сообщений на узлах с малыми энергозатратами, что может быть эффективно применено для операций поиска и спасания и для малогабаритных БЛА.

В дальнейшем протокол будет промоделирован в симуляторе OMNeT++ и получены оценки его производительности.

Применение технологии самоорганизующихся сетей в интеллектуальных транспортных системах может повысить уровень ситуационной информированности всех участников движения, тем самым повысить и безопасность движения, как и в авиационной среде, так и наземной. Способность сети справляться с потоками данных при том условии, что данный вид трафика является очень чувствительным и к времени, и к вероятности доставки. Эффективность работы интеллектуальных транспортных систем с применением протоколов самоорганизующихся сетей зависит от метода доступа к среде передачи данных, что требует тщательного анализа и моделирования различных сценариев работы.

Список используемых источников

1. Exxonmobil [Офиц. сайт]. URL: http://corporate.exxonmobil.com/ en/energy/ energy-outlook/charts/light-duty-fleet-by-type-chart?parentId=8b22b63c-0329-4e0f-a820-9845 ea 41 be7b (дата обращения 28.11.13).

2. АвиаПорт.Ru – авиация и бизнес. Новостной ресурс. URL: http:// www.aviaport.ru/ digest/2007/08/22/126752.html (дата обращения: 29.11.13).

3. Technical Provisions for Mode S Services and Extended Squitter – ICAO Doc 9871 AN/460, Second Edition, 2012. 352 p.

4. Manual on VHF Digital Link (VDL) Mode 4 – ICAO Doc 9816 AN/448, First Edition, 2004. 406 p.

5. Varga A. The ONMeT++ discrete event simulation system // in Proceeding of European Simulation Multiconference, 2001.

6. Azzedine Boukerche Algorithms and protocols for wireless and mobile ad hoc networks // University of Ottawa, Canada, 2009, p. 9.

7. Кулаков М. С. Анализ сценариев развертки мобильных Ad Hoc сетей на базе режима VDL Mode 4 // INTERMATIC – 2013. / Материалы международной научно-практической конференции. Часть 4. М. : МИРЭА, 2013. С. 49–53.

Статья представлена научным руководителем,
доктором технических наук, профессором Шавриным С. С.

УДК 004.056.52

М. В. Левин (аспирант, СПбГУТ)
Е. С. Фостач (студентка, СПбГУТ)

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ ИТ-ИНФРАСТРУКТУРОЙ

В процессе развития отрасли телекоммуникации сложилось так, что в гетерогенно организованной сети необходимо наличие отдельных инструментов для управления сетевым оборудованием. Данная потребность связана с архитектурными особенностями проектируемых сетей связи и технической реализацией сетей, которые в свою очередь должны решать свои задачи, опираясь на различные сетевые механизмы, протоколы и стандарты.

механизм Single-Sign-On, микросервисная архитектура, аутентификация.

При решении задачи унифицированного управления необходимо руководствоваться рекомендациями и стандартами отрасли, которые позволят избежать ошибок при проектировании и эксплуатации. Стоит отметить весомый вклад таких организаций как ITU-T, DTMF и IETF. На примере последней, можно рассмотреть показательную инициативу RFC 3535 [1].

На основании RFC 3535 можно сказать, что управление сетевой инфраструктурой заключается в конфигурировании параметров, как элементов сети, так и сети в целом. Для каждого элемента сети путем конфигурирования определяются сетевые адреса, идентификаторы, географическое положение и прочие параметры. Для сети в целом управление конфигурацией начинается с построения топологической схемы, то есть с отображения реальных связей между элементами сети и связей между элементами

сети, иллюстрирующих образование новых физических и логических каналов, изменение таблиц коммутации и маршрутизации.

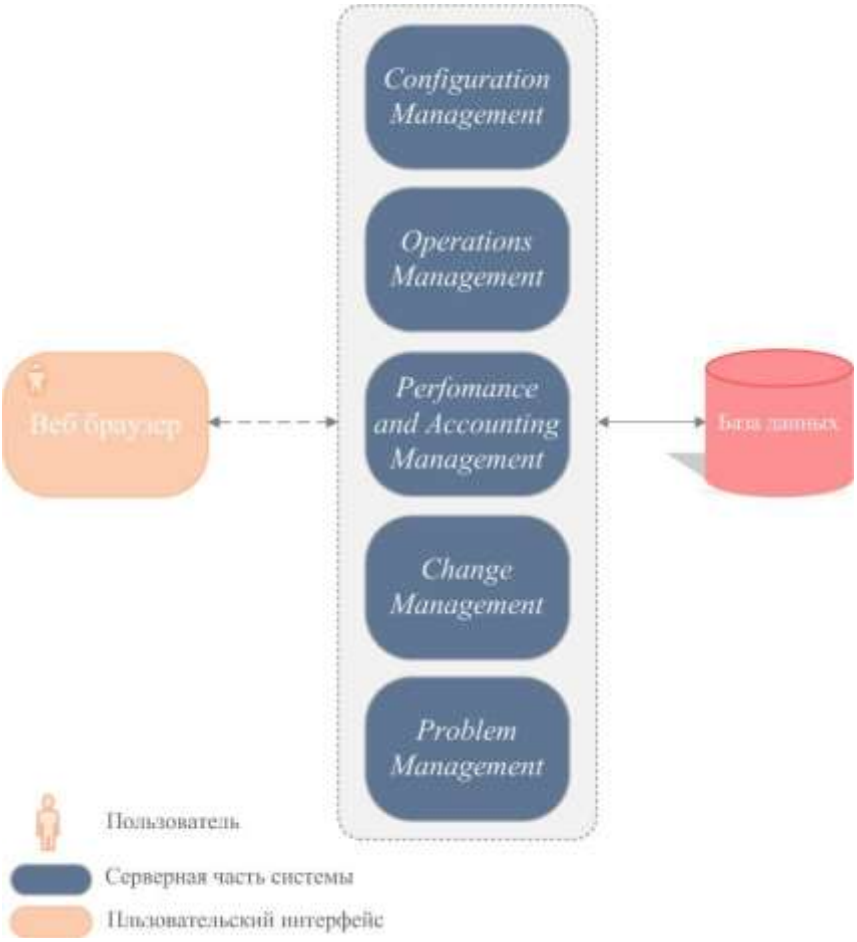


Рис. 1. Логическая архитектура системы

Для того чтобы реализовать систему управления конфигурацией сетевой инфраструктурой, а так же элементами ИТ-инфраструктуры (для управление параметрами питания, охлаждения и т. п.), необходимо выделить основные функциональные области управления:

- *configuration management* (управление конфигурацией) – идентифицирует ресурсы физических и логических систем и обеспечивает управление их взаимоотношениями;
- *perfomance and accounting management* (управление производительностью и учетом использования ресурсов) – обеспечивает квалификацию, измерение, сообщение и управление реакцией, доступностью, утилизацией и использованием компонентов сети;
- *problem management* (управление проблемами) – обеспечивает обнаружение, диагностику, решение, а также средства отслеживания и управления проблемой;

- *operations management* (управление операциями) – обеспечивает средства для запроса и управления распределенными сетевыми ресурсами из центрального пункта;
- *change management* (управление изменениями) – обеспечивает планирование, управление и применение и модификаций в аппаратном обеспечении, микрокодировании и программном обеспечении системы.

Таким образом, на рисунке 1 показаны основные элементы логической архитектуры системы управления ИТ-конфраструктурой:

1) Система управления базой данных – система, предназначенная для управления и манипулирования некоторым набором перманентных данных.

2) Серверная часть системы – обеспечивающая логику работы системы и представлена набором функциональных областей управления.

3) Пользовательский веб-интерфейс – предназначенный для работы пользователя с системой.

Отметим, что системы управления конфигурацией оборудования реализуются как программные системы, которые требуют рассмотрения с учетом подходов ИТ-отрасли и современных требований к архитектурам программного обеспечения. Одним из таких динамично развивающихся подходов является микросервисный подход.

Для поддержки микросервисного подхода необходимо понимать каким образом будут реализованы механизмы аутентификации и авторизации пользователя в контексте самого приложения и доступа пользователя к ресурсам.

Для обеспечения единого безопасного доступа к данным каждого микросервиса применяется унифицированное средство управления доступом на основе технологии однократной аутентификации *Single-Sign-On* (SSO).

SSO – это механизм, с помощью которой приложение (*Service Provider,* SP) делегирует функцию аутентификации пользователей другому приложению (*Identity Provider,* IdP). Такой подход позволяет пользователю свести множество своих учетных данных в разных системах к единому профилю и экономит время пользователя за счет отсутствия необходимости повторных регистраций.

Таким образом, при создании единого входа требуется уделять повышенное внимание к защите учетных данных пользователя.

На общем уровне, процесс выглядит следующим образом (рис. 2):

1) Клиент аутентифицируется в IdP одним из способов, специфичным для него (пароль, ключ доступа, сертификат, Kerberos, и т. д.).

2) Клиент просит IdP предоставить ему токен для конкретного *SP*-приложения. IdP генерирует токен и отправляет его клиенту.

3) Клиент аутентифицируется в SP-приложении при помощи этого токена.

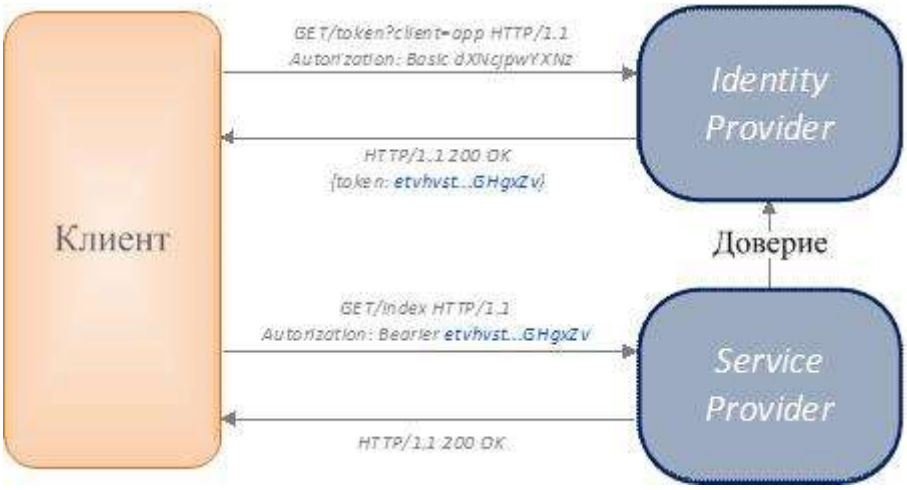


Рис. 2. Аутентификация активного клиента при помощи токена

Исходя из описанных ранее принципов работы механизма *SSO*, можно сделать вывод – аутентификация пользователей в отдельных экосистемах должна быть реализована в виде отдельного сервиса, аккумулирующего в себе данные из нескольких сервисов, с помощью которого пользователь осуществляет вход в систему, и предоставляющий эти данные другим микросервисам для дальнейшей работы пользователя (рис. 3).

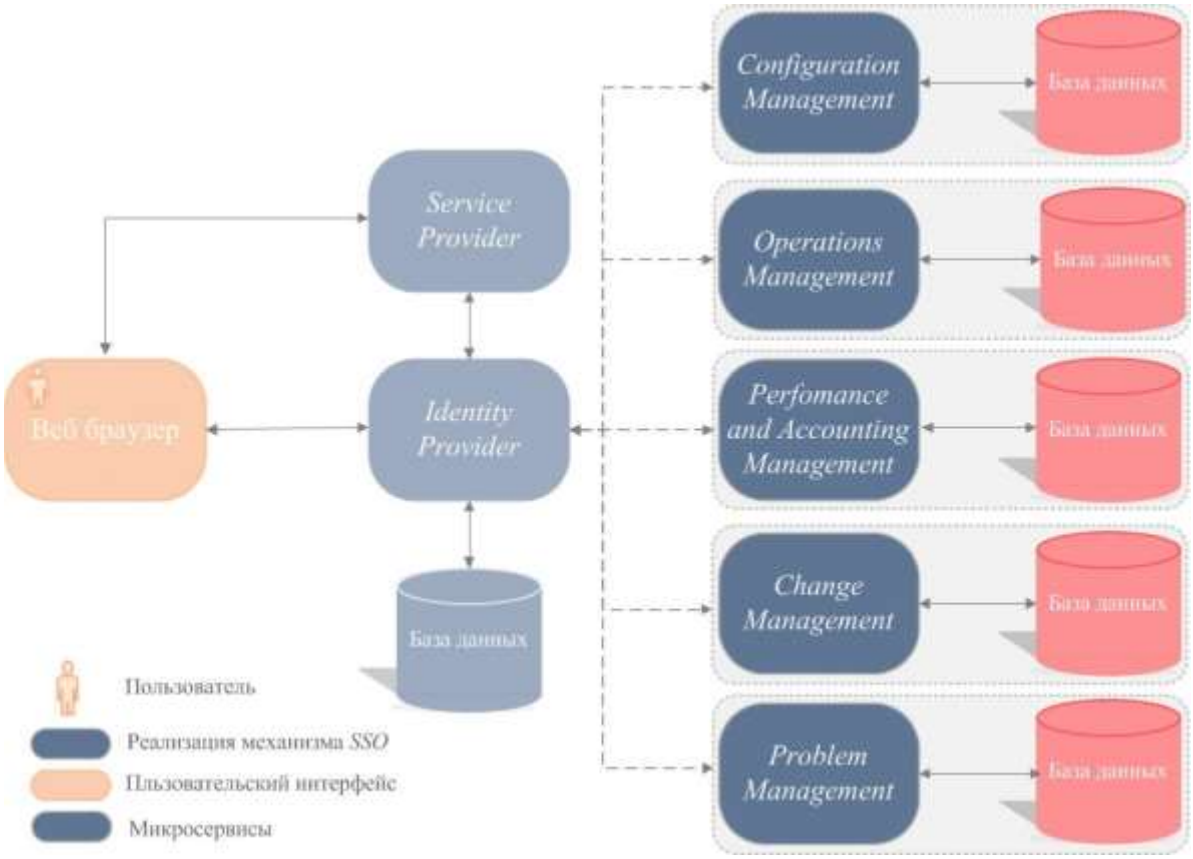


Рис. 3. Архитектура системы с применением механизма SSO

Для того чтобы реализовать механизм единого входа, существует протокол OAuth (*Open Authorization*). Это открытый протокол авторизации, позволяющий предоставлять клиенту ограниченный доступ к защищенным ресурсам сервера от имени владельца ресурса. Владельцем ресурса может быть другой клиент или конечный пользователь.

Последняя версия стандарта OAuth 2.0, опубликована в 2012 г. в документе IETF RFC 6749 [2]. OAuth 2.0 позволяет сторонним приложениям получать доступ от своего имени или ограниченный доступ к HTTP-службе от имени владельца ресурса, организовав процесс согласования взаимодействия между владельцем ресурса и HTTP-службой. Наличие прав определяется токеном, который может быть один и тот же для разных клиентов, либо у одного клиента могут быть разные токены в разное время. Права клиенту предоставляются в обмен на предоставление токена.

Стандарт не определяет формат токена, который получает приложение, поэтому токен сам по себе не может быть использован для аутентификации пользователя. Соответствующие возможности в данной области предоставляются OpenID Connect. OpenID Connect является стандартом, возникшим в качестве конкретной реализации OAuth 2.0 и основанным на способах управления технологией единого входа. В нем используются простые REST-вызовы (используются методы HTTP GET, POST и перенаправления, протокол позволяет конечным пользователям предоставить доступ к ресурсам третьей стороне, не раскрывая свои идентификационные данные) [3].

Таким образом, применение механизма SSO дает следующие преимущества:

1) Снижение количества точек регистрации, необходимых для каждого микросервиса.

2) Повышение безопасности за счет единой точки входа в систему.

3) Снижение нагрузки на сеть, связанной с многократными процедурами аутентификации.

Список используемых источников

1. RFC 3535. Overview of the 2002 IAB Network Management Workshop [Электронный ресурс] / J. Schoenwaelder. [2003]. URL: https://tools.ietf.org/html/rfc3535 (дата обращения 15.05.2016).

2. RFC 6749. The OAuth 2.0 Authorization Framework [Электронный ресурс] / D. Hardt. [2012]. URL: https://tools.ietf.org/html/rfc6749 (дата обращения 15.05.2016).

3. Sam Newman, Building Microservices . O'Reilly Media, 2015. 280 с.

Статья представлена научным руководителем,
кандидатом технических наук, профессором Красовым А. В.

УДК 004.932

Д. М. Марданов (студент группы ИКПИ-41, СПбГУТ)

РЕАЛИЗАЦИЯ РАЗДЕЛЬНОГО СЖАТИЯ ПОЛЯ ОСОБЫХ ТОЧЕК И ОСТАТОЧНОГО ПОЛЯ НА ОСНОВЕ ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЯ В ВИДЕ СКАЛЯРНЫХ ПОЛЕЙ

Было произведено раздельное сжатие в программном комплексе, предназначенном для редактирования изображения. Отдельно сжимается поле особых точек, что позволяет с удобством анализировать изображение. Также отдельно сжимается сглаженное поле изображение. Более того, присутствует возможность сжать оба компонента изображения.

сжатие изображения, скалярные поля, остаточное поле, поле особых точек.

Рассматриваемая программная система, имеет сложную структуру. Она состоит из пяти проектов, каждый из которых выполняет определенную функцию. Все эти проекты должны объединиться в один общий, что приводит к некоторым сложностям, связанным с соединением проектов. Программная система расширяема, что позволяет добавлять в нее новые возможности и дополнять функционал.

В приложении для операционной системы Windows, которое обеспечивает редактирование изображения пользователем, а также построение сглаженных полей и полей особых точек, необходимо реализовать раздельное сжатие поля особых точек и сглаженного поля.

Информация о сжатом поле особых точек должна сохраняться в файл. Также в файл должна сохраняться информация о сглаженном поле. Данные, записанные в файлах, должны обладать полнотой информации, для того, чтобы их можно было использовать в дальнейшем.

Таким образом, будет организовано сжатие двух частей изображения – поля особых точек и сглаженного поля, и эти части смогут применяться самостоятельно.

В данном приложении сжатие особых точек производится на основе сжатия кромок. Следовательно, следует записать информацию об объеме кромок. Данная информация будет достаточно полной, чтобы впоследствии можно было иметь всю информацию о сжатом изображении.

Для сглаженного поля необходимо записать усредненные матрицы для каждого цвета, что позволит иметь полную информацию о сглаженном поле.

Ниже представлен список файлов, которые должны формироваться при решении задачи:

1) файл, хранящий длину кромки для поля особых точек через сглаженное поле;

2) файл, хранящий длину кромки для поля особых точек через цепочки;

3) файл, хранящий длину кромки для поля особых точек напрямую;

4) файл, хранящий усредненную матрицу для красного цвета;

5) файл, хранящий усредненную матрицу для зеленого цвета;

6) файл, хранящий усредненную матрицу для синего цвета.

Приведенная стратегия решения задачи позволит максимально гибко использовать сохраненную в файлы информацию и использовать ее.

Так как при вычислении особого поля происходит сначала компрессия, а затем и декомпрессия кромок, необходимо сохранять данные в момент между двумя этими процессами, то есть после компрессии кромок. Компрессия происходит в два этапа:

- компрессия до байтов,
- компрессия до битов.

Таким образом, после компрессии до битов необходимо записать объем кромки.

Данную операцию необходимо для всех трех вышеуказанных способов построения поля особых точек.

Ниже приведен код компрессии и декомпрессии кромок:

```
<Компрессия>
unsigned long kromkaLength;
unsigned char *compressedKromka = oper.BeginCompressKromka(b, nKromkaSizeR,
kromkaLength);
unsigned long sortkromkaLength;
unsigned char *twocompressedKromka =
oper.TwoStageCompressKromka(compressedKromka , kromkaLength, sortkromkaLength);
std::ofstream out("RGBKromkaSize.txt");
out << sortkromkaLength;
out.close();
unsigned long _kromkaLength;
unsigned char *_sortkromkaLength =
oper.TwoStageDeCompressKromka(twocompressedKromka , sortkromkaLength,
_kromkaLength);

unsigned long KromkaSize;
unsigned char *decompressedKromka=oper.EndDecompressKromka(_sortkromkaLength,
_kromkaLength,KromkaSize);
b=&decompressedKromka[0];
nKromkaSizeR=KromkaSize;
<Декомпрессия>
unsigned long  nKromkaSizeG, nKromkaSizeB,Length,SaveKr7,numL=0;

SaveKr7=nKromkaSizeG=nKromkaSizeB=nKromkaSizeR;

unsigned char *wholeKr = new unsigned char[h * w * 30+ 1];
```

```
unsigned char fg,fb,*Begb,*Begkr;
Begb=b;  Begkr=wholeKr;
```

При построении сглаженного поля необходимо из матриц цветности составить усредненные матрицы: матрицу размера H×W для каждого цвета преобразовать в матрицу размера h×w, записывая в сжатую матрицу средние значения.

Обеспечив сжатие матрицы для каждого из трех цветов, необходимо записать эти матрицы в файл.

Ниже приведен код алгоритма сжатия сглаженного поля:

```
int h = smoothedRGB.getHeight();
int height = theColorField->getHeight();
int w = smoothedRGB.getWidth();
int width = theColorField->getWidth();
int mean_r = 0;
int mean_g = 0;
int mean_b = 0;
int size = zwin*sizeof(unsigned char);


std::ofstream meanR("meanR.txt");
std::ofstream meanG("meanG.txt");
std::ofstream meanB("meanB.txt");



for (int i = 0; i < h; i++)
{
	for (int j = 0; j < w; j++)
	{
		mean_r = 0;
		mean_g = 0;
		mean_b = 0;
		for (int m = 0; m < height/h; m++)
		{
			for (int n = 0; n < width/w; n++)
			{
				mean_r += linearedImageR[n + m*width + j*height/h +
i*width*height/h];
				mean_g += linearedImageG[n + m*width + j*height/h +
i*width*height/h];
				mean_b += linearedImageB[n + m*width + j*height/h +
i*width*height/h];
			}
		}
		meanR << mean_r / ((height / h)*(width / w)) << " ";
		meanG << mean_g / ((height / h)*(width / w)) << " ";
		meanB << mean_b / ((height / h)*(width / w)) << " ";
```

```
            }
            meanR << "\n";
            meanG << "\n";
            meanB << "\n";
        }
        meanR.close();
        meanG.close();
        meanB.close();
```

Рис. 1. Оригинал изображения

Рис. 2. Восстановление изображения после сжатия предикативного и сглаженного поля со степенью сжатия = 4

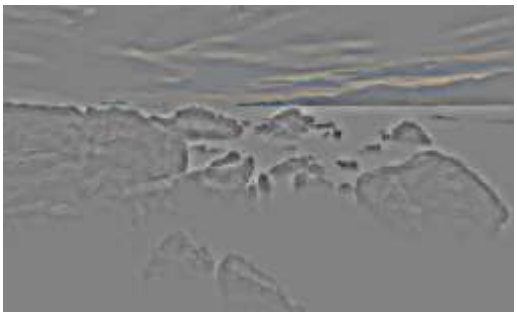


Рис. 3. Поле особых точек изображения

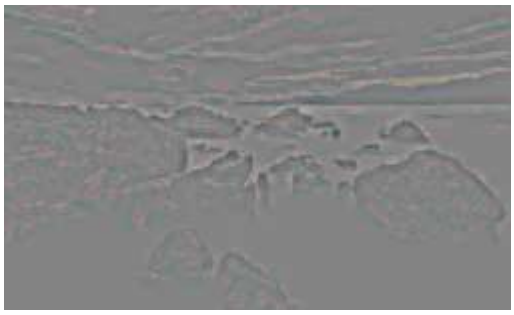


Рис. 4. Восстановленное поле особых точек после сжатия со степенью сжатия = 4

Рис. 5. Сглаженное поле

Рис. 6. Восстановленное сглаженное поле после сжатия со степенью сжатия = 210

На рисунках 1 и 2 показаны результаты восстановления изображения после суммарного сжатия поля особых точек и сглаженного поля.

На рисунках 3 и 4 показаны результаты восстановления поля особых точек после сжатия. На рисунках 5 и 6 показаны результаты восстановления сглаженного поля после сжатия.

Таким образом, было организовано хранение информации о сжатом поле особых точек и сглаженном поле, что позволяет работать с этой информацией, комбинируя ее необходимым образом. Например, сжатое поле особых точек может быть использовано для анализа изображения, а также распознавания образов. Описанными выше возможностями, была повышена функциональность программы. Поставленная задача была выполнена.

Список используемых источников

1. Болтов Ю. Ф. Выделение контуров изображений на основе функции Грина // Телекоммуникации. М. : Наука и технологии, 2009. № 5. С. 27–32.
2. Болтов Ю. Ф., Волков И. А. Сглаживание изображений на основе решения краевой задач // Телекоммуникации. М. : Наука и технологии, 2010. № 5. С. 24–33.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Болтовым Ю. Ф.

УДК 004.056

А. В. Масюкайте (студентка группы ИКТК-26, СПбГУТ)

ИССЛЕДОВАНИЕ ПРИНЦИПОВ ОРГАНИЗАЦИИ ВИРТУАЛЬНЫХ СЕТЕВЫХ ФУНКЦИЙ НА БАЗЕ OPENSTACK NETWORKING (NEUTRON)

На сегодняшний день огромную роль в бизнесе играет то, с какой скоростью компания способна адаптироваться под бизнес-процессы, партнеров и клиентов. Здесь многое зависит от используемых сетевых технологий. Традиционные сети устаревают и требует замены на более динамичные. Для решения этой задачи на современном этапе внедряются принципиально новые технологии, в частности, NFV (Network Function Virtualization), которые изменяют традиционные принципы управления инфокоммуникационными сетями. В основе этих концепций лежит программное управление.

виртуализация сетевых функций, Network Function Virtualization (NFV), OpenStack, Neutron.

Network Functions Virtualisation (NFV) – виртуализация сетевых функций (сервисов) – это принцип отделения сетевых функций от аппаратных средств, на которых они осуществляются, за счёт применения виртуальной аппаратной абстракции.

С помощью NFV становится возможным объединение различных типов сетевого оборудования на стандартных мощных серверах, коммутаторах и системах хранения, которые могут располагаться в датацентрах, сетевых узлах и в помещениях конечных пользователей.

На сегодняшний день разработкой спецификаций для технологий NFV занимается отраслевая группа (NFV ISG) при Европейском институте телекоммуникационных стандартов (ETSI).

NFV предусматривает реализацию сетевых функций в качестве только программного обеспечения, работающего поверх инфраструктуры NFV (NFVI). На высокоуровневом NFV фреймворке (рис. 1) можно выделить три рабочих компонента [1]:

1) Виртуализированные сетевые функции– Virtualized Network Functions (VNF), которые являются программной реализацией сетевых функций, работающей поверх NFVI.

2) Инфраструктура NFV – NFV Infrastructure (NFVI). Является совокупностью программных и аппаратных компонентов, которые образуют основу для развертывания и управления виртуализированными сетевыми функциями.

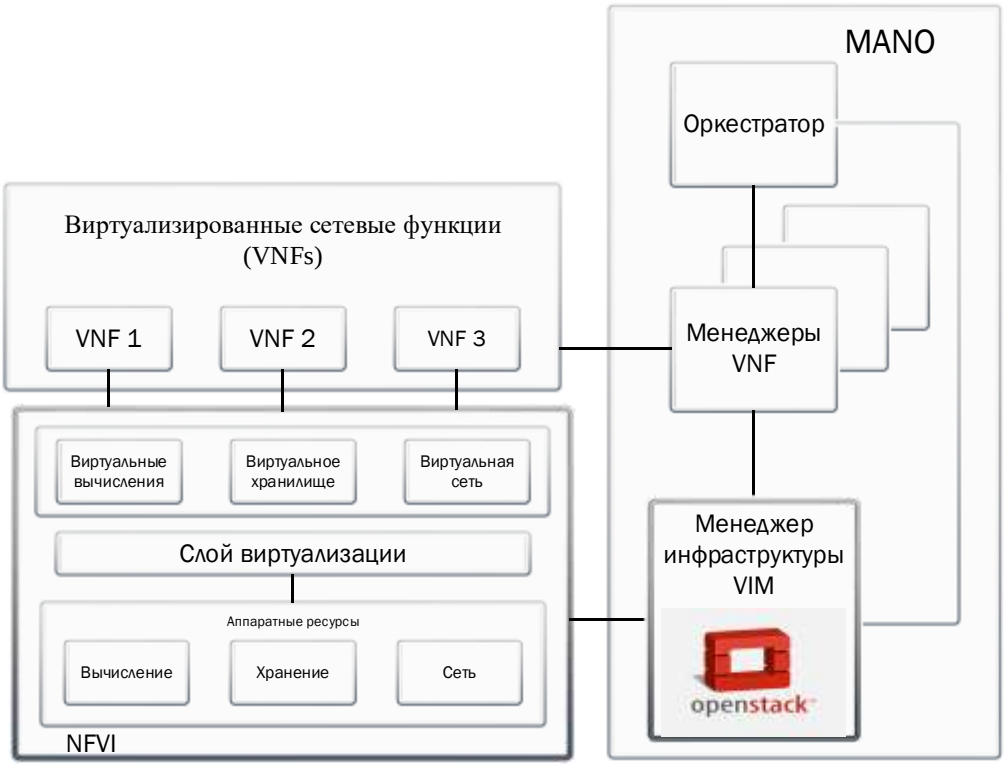


Рис. 1. Архитектура NFV

С точки зрения виртуализированной сетевой функции VNF, слой виртуализации и аппаратные ресурсы выглядят как единое целое, предоставляя ей требуемые ресурсы.

1) NFV Управление и Оркестрация – NFV Management and Orchestration (MANO). Целью MANO является создание инфраструктуры, необходимой для гибкого развертывания и управления сетевыми функциями. MANO стандартизирует процессы взаимодействия между компонентами.

Основными составляющими блока MANO являются:

- Оркестратор.
- Менеджер виртуализированных сетевых функций VNFM (VNF Manager).
- Менеджер виртуализированной инфраструктуры VIM (Virtualized Infrastructure Manager).

На данный момент при виртуализации сетевых функций в качестве менеджера виртуализированной инфраструктуры (VIM) часто используется такая платформа, как OpenStack [3].

Такое решение дает пользователям достаточную гибкость для использования виртуализированных и физических сетевых функций, поддерживающих несколько гипервизиров различных поставщиков, и интеграцию с рабочими фреймворками OpenStack.

OpenStack является комплексом проектов свободного программного обеспечения по созданию средств управления вычислительными и сетевыми ресурсами для организации облачных вычислений, с открытым исходным кодом.

Основными задачами OpenStack являются создание и управление виртуальными ресурсами (ресурсами хранения, вычисления и сетевыми ресурсами), а также обеспечение их безопасности.

Технология OpenStack имеет модульную архитектуру и включает в себя несколько компонентов, которые могут меняться и дополняться в зависимости от релиза. В работе рассматривается релиз OpenStack Kilo.

Ниже представлены основные его компоненты [2]:

- **OpenStack Compute (Nova)** – контроллер, управляющий работой вычислительных ресурсов.
- **OpenStack Object Storage (Swift)** – распределенное отказоустойчивое хранилище данных.
- **OpenStack Image Service (Glance)** – сервис хранения изображений и образов виртуальных машин.
- **OpenStack Dashboard (Horizon)** – инструмент пользовательского интерфейса для общения с более высокопроизводительными сервисами, такими как Nova, Swift и др.
- **OpenStack Network Service (Neutron)** – компонент, предоставляющий сервис «подключение к сети, как услуга» между интерфейсами устройств, которые управляются другими сервисами OpenStack.
- **OpenStack Block Storage (Cinder)** – это сервис блочного хранения данных, служба работы с блочными устройствами хранения данных.

- **OpenStack Identity (Keystone)** – сервис идентификации.
- **OpenStack Telemetry (Ceilometer)** – инструмент измерений и телеметрии.

Технология OpenStack обеспечивает виртуализацию сетевой инфраструктуры и доступ к ней пользователей.

Реализация сетевых функций осуществляется за счет возможностей компонента OpenStack Networking, представляющего собой отдельный сервис, который может быть установлен независимо от других проектов OpenStack. Компонент Neutron может быть как распределен между несколькими хостами в целях обеспечения необходимых устойчивости и избыточности, так и может быть сконфигурирован для работы на одном узле.

Работа компонента Neutron обеспечивается при помощи программных и аппаратных компонентов [2].

К внутренним составляющим Neutron относятся три основных процесса – Neutron-server, плагины и агенты.

Аппаратными компонентами являются узлы, которые поддерживают один или несколько программных компонентов. Иными словами, под «узлами» понимается аппаратная платформа: узел контроллера (Controller Node), узел вычислений (Compute Node), сетевой узел (Networking Node).

Neutron позволяет реализовывать основные функции, которые применяются в ЦОДах. К ним относятся функции коммутации, маршрутизации, балансировки нагрузки и обеспечения межсетевой безопасности.

На рисунке представлена простейшая топология сети, созданная в OpenStack.

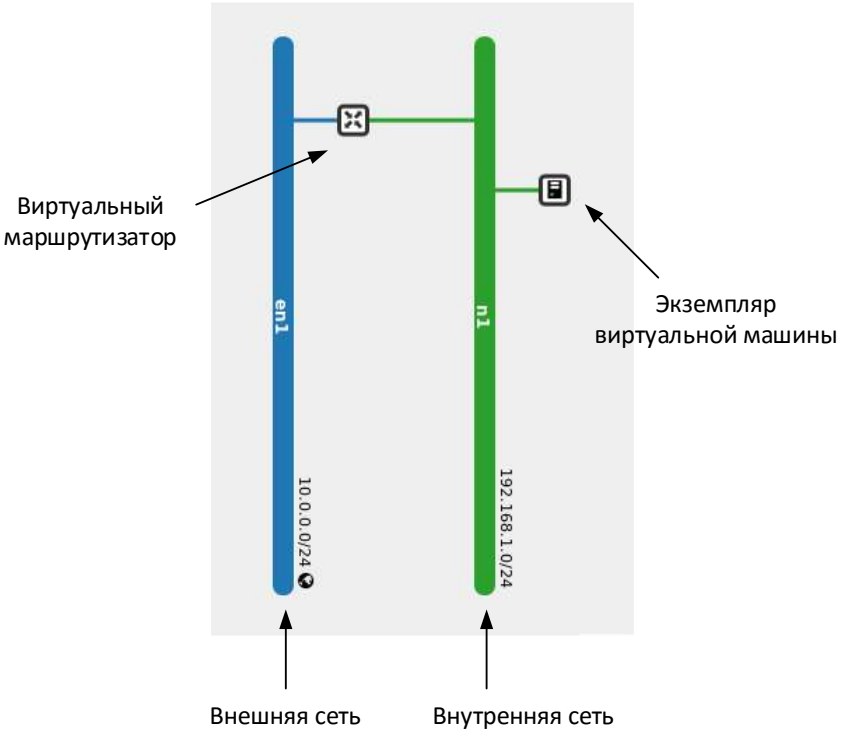


Рис. 2. Простейшая сетевая топология, реализованная в OpenStack Neutron

К функциям коммутации в Neutron можно отнести: обеспечение соединения с экземплярами на втором уровне, предоставление интерфейсов виртуальной сети, соединение мостами [2].

Маршрутизацию и возможности NAT OpenStack Networking обеспечивает за счет использования IP – пересылки, iptables и пространства сетевых имен. Каждое пространство имен имеет собственную таблицу маршрутизации и процессы iptables, которые обеспечивают фильтрацию и трансляцию сетевых адресов (NAT). Настройка маршрутизатора на основе Neutron позволяет экземплярам взаимодействовать с внешними сетями. Также в эту функциональную категорию входят возможности DHCP.

Балансировка нагрузки в Neutron, как расширенный сервис (LBaaS), обеспечивает возможность равномерного распределения входящего трафика между виртуальными машинами в облаке.

В результате проделанной работы был сделан вывод, что на данный момент виртуализация сетевых функций очень актуальна и для её внедрения применяются облачные платформы различных вендоров, среди которых большой популярностью пользуется OpenStack. Эта платформа состоит из нескольких проектов, каждый из которых отвечает за выполнение определенных функций. Возможность виртуализации базовых сетевых функций предоставляет компонент OpenStack Neutron.

Список используемых источников

1. ETSI GS NFV 002 V1.2.1 (2014-12) / ETSI Group Specification – Network Functions Virtualisation (NFV); Architectural Framework
2. Learning OpenStack Networking (Neutron) [Электронный ресурс] / James Denton. URL: www.it-ebooks.info
3. Accelerating NFV Delivery with OpenStack [Электронный ресурс]. URL: https://www.openstack.org/

Статья представлена научным руководителем ассистентом Селивановым А. Е.

УДК 004.932

Д. А. Метелев (студент группы ИКПИ-41, СПбГУТ)

ОРГАНИЗАЦИЯ ДИНАМИЧЕСКОЙ ЗАГРУЗКИ ПАРАМЕТРОВ ПРИ РАБОТЕ С ИЗОБРАЖЕНИЯМИ В ВИДЕ СКАЛЯРНЫХ ПОЛЕЙ

В статье рассматривается способ динамического изменения параметров сжатия изображения, в частности при работе с изображениями в виде скалярных полей.

скалярное поле, изображение, сжатие изображения.

Введение

Данная программа для сжатия изображений является не только рабочей, но и исследовательской, она должна поддерживать изменение настроек работы с изображениями, поэтому для удобства пользователя в настройке программы под свои нужды необходимо предусмотреть возможность динамического изменения опций обработки изображений.

Постановка задачи

Данная работа имеет перед собой цель расширения функционала приложения для операционной системы Windows, которое обеспечивает редактирование и сжатие изображения пользователем, а также построение сглаженных полей и полей особых точек. Необходимо реализовать возможность динамического изменения опций обработки изображений, таких как: размер окна, сглаживание, порог и четвертая опция, которую можно использовать для своих нужд, в частности – для отладки.

Доступ к изменению опций должен осуществляться через меню.

Решение задачи

Сложность работы заключается в том, что данная программа состоит из пяти связанных между собой проектов, содержит огромное количество файлов, в том числе и системных, редактировать которые нужно максимально аккуратно, что требует уметь разбираться в программном коде каждого из проектов.

Для начала необходимо определить файл, в котором происходит разметка элементов на форме.

Нужным нам файлом является файл ресурсов одного из проектов – **CompressBMP.rc.**

```
265  IDD_OPTIONS_DLG DIALOGEX 0, 0, 205, 131
266  STYLE DS_SETFONT | DS_MODALFRAME | DS_FIXEDSYS | WS_POPUP | WS_CAPTION | WS_SYSMENU
267  CAPTION "PCB Options"
268  FONT 8, "MS Shell Dlg", 400, 0, 0x1
269  BEGIN
270      DEFPUSHBUTTON   "OK",IDOK,37,110,50,14
271      PUSHBUTTON      "Cancel",IDCANCEL,113,110,50,14
272
273      EDITTEXT        IDC_EDIT_WIN,81,30,79,14,ES_AUTOHSCROLL
274      LTEXT           "Размер окна:",IDC_STATIC,19,32,45,8
275
276      EDITTEXT        IDC_EDIT_AV,81,45,79,14,ES_AUTOHSCROLL
277      LTEXT           "Порог:",IDC_STATIC,19,47,24,8
278
279      EDITTEXT        IDC_EDIT_SM_WINSIZE,81,60,79,14,ES_AUTOHSCROLL
280      LTEXT           "Smooth Win size",IDC_STATIC,19,62,53,8
281
282      EDITTEXT        IDC_EDIT_4TH_OPT, 81, 75, 79, 14, ES_AUTOHSCROLL//8/
283      LTEXT           "Коррекция:", IDC_STATIC, 19, 77, 60, 14
284  END
```

Рис. 1. Файл ресурсов одного из проектов – CompressBMP.rc

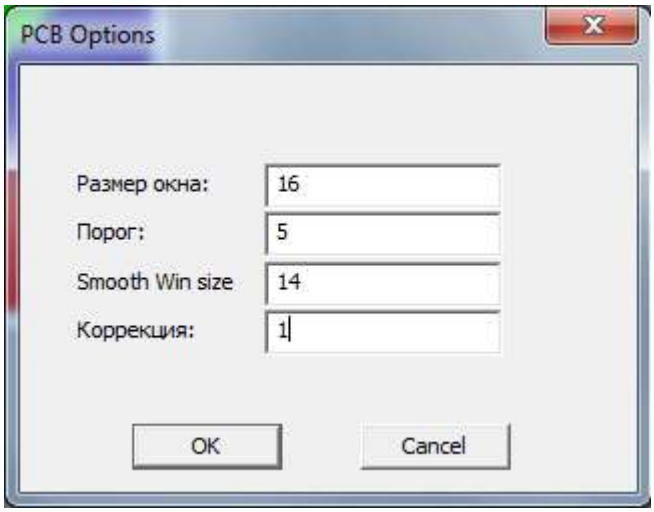


Рис. 2. Форма редактирования

Теперь нужна переменная, которая будет хранить введенное в окно значение, а так же методы доступа к ней – они объявляются в header-файле OptFile.h в проекте, отвечающем за опции:

```
int m_nFourthOption;

int GetFourth();
 void SetFourthOption(int nFourthOption);
```

Для возможности сохранения параметров и загрузки их при запуске программы, нужно организовать запись в файл:

```
void CPCBOptFile::WriteOptionsEx() const
{
    FILE * cfg_file;
     fopen_s(&cfg_file, m_sFileName.data(),"w");
    if  (cfg_file  == 0 )
        return;
    fprintf(cfg_file, "[threashold=%d,window=%d,smoothWinSize=%d,FourthOption=%d]", m_nAv, m_nWin, m_nSmoothWinSize, m_nFourthOption);
    fclose(cfg_file);

}
```

После создания элементов взаимодействия нужно привязать свежий элемент ввода к переменной, используя метод DoDataExchange():

```
DDX_Text(pDX, IDC_EDIT_4TH_OPT, m_nFourthOption);
 DDV_MinMaxLong(pDX, m_nFourthOption, 0, 2147483647);
```

С помощью данного метода нужно проводить отладку, подключая к нему предназначенную для отладки переменную.

Вывод

Таким образом, была организована возможность динамического изменения и хранения настроек обработки изображений, которые можно комбинировать необходимым образом.

Для улучшения решения задачи стоит разработать возможность добавления новых параметров без вмешательства в код.

Список используемых источников:

1. Козин С. В. Курс лекций по предмету «Объектно-ориентированное программирование».

2. Болтов Ю. Ф., Чечель А. О. Интерпретатор графической информации в полевой модели. Построение и возможности. Часть 1. // Телекоммуникации. М. : Наука и технологии, 2012. № 8. С. 88–95.

3. Болтов Ю. Ф. Научно- исследовательский комплекс для обработки визуальной информации на основе полевой модели: структура и возможности // Материалы 64-й МНТК профессорско-преподавательского состава, научных сотрудников и аспирантов, 20–24 февраля 2012 г. СПб. : СПбГУТ, 2012. С. 209–210.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Болтовым Ю. Ф.

УДК 004.312.43

Я. Д. Мещеряков (студент группы ИКТ-406, СПбГУТ)

ПОВЕДЕНЧЕСКАЯ МОДЕЛЬ КОНЕЧНОГО АВТОМАТА В MODELSIM С ДАЛЬНЕЙШИЙ ПРОГРАММИРОВАНИЕМ УСТРОЙСТВА В ПЛИС CYCLONE V

В настоящее время весьма актуально программирование различных устройств в программируемые логические интегральные схемы (ПЛИС). Для того, чтобы избежать ошибок в дальнейшей работе такого устройства, необходимо предварительное моделирование его поведения.

счетчик, Verilog, ModelSim, Testbench, CycloneV.

В качестве примера синтеза конечного автомата рассмотрим синтез двоичного реверсивного счётчика. Так как синтез производится под программирование в FPGA, необходимо полностью описать все возможности функционирования счетчика с учетом сигналов на его входах.

За основные входы всегда принимаются асинхронный сброс (*reset*) и вход синхронизации, как правило, фронт импульса. Однако, на момент поступления фронта синхроимпульса, необходимо учитывать состояния дополнительных управляющих входов. Так, в счетчике всегда возможны: синхронный сброс (*sync_clr*), синхронная загрузка начального состояния (*load*), разрешение продолжения счета (*en*) и, для реверсивного счетчика, указание направления счета (*up*).

Рассмотрим таблицу установок возможных уровней на перечисленных входах к моменту подачи синхроимпульса и получаемые результаты:

sync_clr	***load***	***En***	***Up***	**Состояние выходов *q***	**Операция**
1	-	-	-	00…00	Синхронный сброс
0	1	-	-	*data*	Параллельная загрузка
0	0	1	1	*q*+1	Счет вверх
0	0	1	0	*q*-1	Счет вниз
0	0	0	-	*q*	Пауза

Запишем программу восьмиразрядного счётчика на языке Verilog.

В языке Verilog есть два типа переменных: *wire* (линия), *reg* (регистр).

Входы и выходы будут проводами по принципу языка *Verilog*, а для изменения входных значений будем использовать регистры.

Конструкция *always* позволяет учитывать список чувствительности.

```
module schetchik_program  // название программы
#(parameter N=8) // объявление константы
(
input wire clk,sync_clr,load,en,up,reset,// объявление входных одноразрядных линий
input wire [N-1:0] d,// объявление 8-ми разрядной загрузочной линии
output wire [N-1:0] q// объявление выходной линии счётчика
);
reg[N-1:0] q_reg;// удержание входного значения
wire [N-1:0] q_next;// удержание следующего значения
wire [N-1:0] q_previous;// удержание предыдущего значения

always@(posedge clk,posedge reset)
if(reset)
q_reg<=0;
else if(sync_clr)
q_reg<=0;
else if(load)
q_reg<=d;
else if(en)
begin
  if(up) q_reg<=q_next;
  else q_reg<=q_previous;
end
else q_reg<=q_reg;

assign q_next=q_reg+1;
assign q_previous=q_reg-1;
assign q=q_reg;
```

```
endmodule
```

Следующим шагом нужно проверить работоспособность программы, для этого нужно написать Testbench (временное тестирование).

```
`timescale 1ns/10ps //шаг 1 нс, точность 10 пс
module testbench();

reg reset1,syn_clr,load,en,up,clk;
reg [7:0] d;
wire [7:0] q;

schetchik_program
sch(.reset(reset1),.sync_clr(syn_clr),.load(load),.en(en),.up(up),.clk(clk),
.d(d),.q(q));// подключаем входы к program_schetchik
initial
begin:CLOCK_GENERATOR
  clk=0;
  forever
        begin
        #20 clk = ~clk;
// генерация clc каждые 20 нс значение clc изменяется на противоположное
        end
end
initial// далее следует текст инициализации тестируемого модуля;
……
Endmodule
```

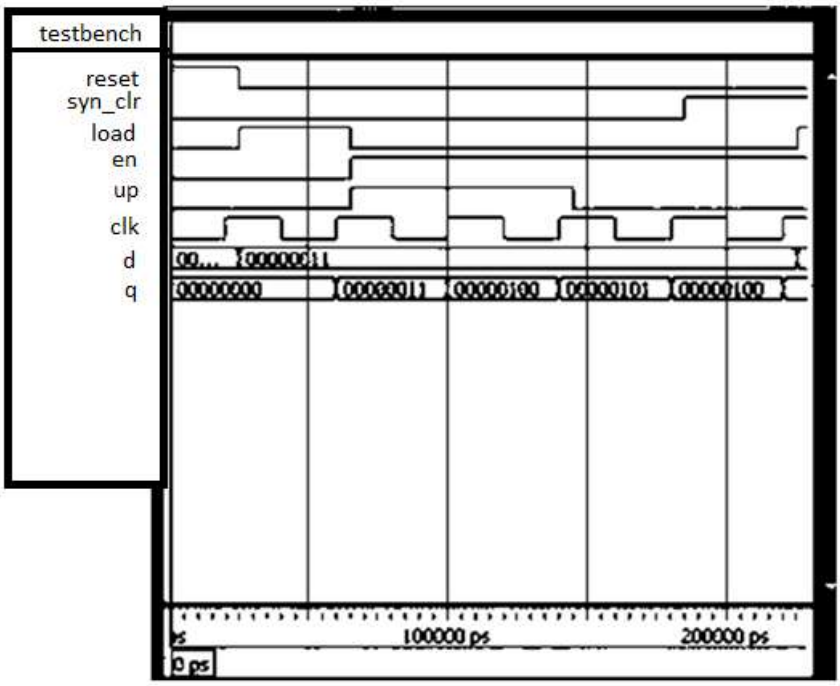


Рис. 1. Результат выполнения программы в Testbench

После отладки программы в ModelSim производим программирование ПЛИС.

Так как тактовая частота Cyclone V 50 мГц, то, с помощью программы делителя понижаем частоту до 2 Гц для визуального наблюдения за работой счетчика на макете.

Счётчик-делитель будет считать до 12 500 000, и значению медленного тактового сигнала будет присваиваться значение «1», а при счете от 12 500 000 до 25 000 000 – значение «0».

```
module reg_cnt
#(parameter N=24)//N=24 так как 2^24 =16777216
(
input wire clk,
output reg[N:0] chastota2,
output reg chetchik
);
reg [N:0] gen2;
wire[N:0] gen2_next;
wire chetchik_next;
always@(posedge clk)
gen2<=gen2_next;
if (gen2=24'd12500000)
  begin
gen2<=0;
chetchik<=chetchik_next;
  end
assign gen2_next=gen2+1'b1;
assign chetchik_next=chetchik+1'b1;
endmodule
```

Для отображения цифр на макете, необходимо написать программу декодера, преобразующего состояние счетчика в шестнадцатеричный символ на семисегментном индикаторе. Сегменты зажигаются нулями.

Реализуемый в макете модуль выглядит следующим образом:

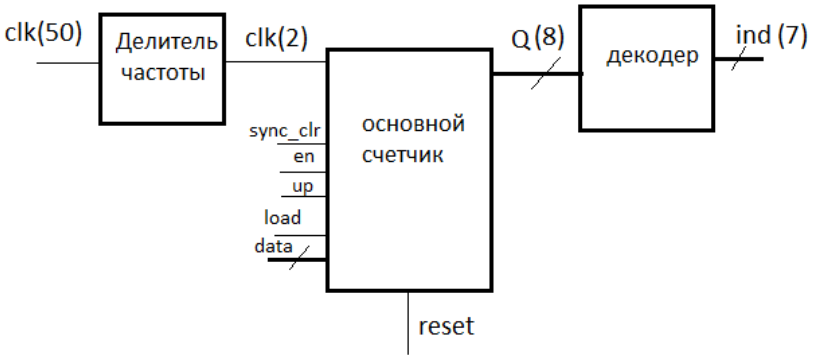


Рис. 2. Реализуемый в макете модуль

Проект был реализован на FPGA Cyclone V фирмы Altera и представлен на Дне факультета ИКСС.

Список используемых источников

1. Грушвицкий Р. И., Мурсаев А. Х., Угрюмов Е. П. Проектирование систем на микросхемах программируемой логики. СПб. : БХВ-Санкт-Петербург, 2002. 230 с.

2. Pong P. Chu. FPGA prototyping by Verilog examples. : Wiley, 2008. 488 p. ISBN 978-0-470-18532-2.

Статья представлена научным руководителем,
старшим преподавателем Нееловой О. Л.

УДК 316.353

А. С. Мишин (студент группы ИКТЗ-24, СПбГУТ)
И. И. Перепелица (студент группы ИКТЗ-24, СПбГУТ)
Н. Л. Пиховкин (студент группы ИКТЗ-24, СПбГУТ)

ИССЛЕДОВАНИЕ РАСПРОСТРАНЕННОСТИ ПИРАТСТВА В РОССИИ СРЕДИ МОЛОДЫХ ЛЮДЕЙ

В настоящее время большинство интернет-пользователей использует пиратский контент, уклоняясь от оплаты лицензионных продуктов. Из-за этого правообладатели теряют значительную долю прибыли, а порой и вовсе вынуждены прекращать производство своих продуктов. В работе исследуются причины, по которым молодые люди предпочитают использовать нелицензионные копии, тем самым нарушая законные права правообладателей, а также анализируется эффективность блокировки ресурсов с пиратским контентом.

пиратство, авторское право, блокировка интернет-сайтов.

По данным исследований, только треть россиян платит за скачиваемый контент [1]. Результаты опроса, проведенного Всероссийским центром изучения общественного мнения (ВЦИОМ) показали, что лишь 11 % интернет-пользователей готовы начать платить за скачивание контента в том случае, даже если все пиратские ресурсы будут заблокированы [2].

Цель исследовательской работы – выяснить, какой процент лиц в возрасте от восемнадцати до двадцати трех лет использует пиратский контент. А также, понять, по какой причине люди отказываются от приобретения лицензионных продуктов.

В качестве инструмента опроса был использован сервис создания анонимных опросов GoogleForms. Встроенные в структуру опроса ветвления предлагали респондентам отвечать на определенные вопросы в зави-

симости от их ответов на предыдущие. С целью повышения качества результатов были соблюдены условия полной анонимности. Созданный опрос был разослан молодым людям, входящим в исследуемую возрастную категорию, посредствам социальных сетей.

По достижении отметки в 100 ответов был проведен анализ. Наибольшей популярностью среди молодых людей пользуются три категории контента: фильмы, музыка и мобильные приложения. При этом оплачивают лицензионные продукты лишь 54,5 % опрошенных. То есть каждый второй интернет-пользователь не платит за скачиваемый контент. Более того, 35,6 % респондентов ответили, что платят не более трехсот рублей в месяц. Это свидетельствует о том, что оплачивается лишь меньшая часть используемого контента.

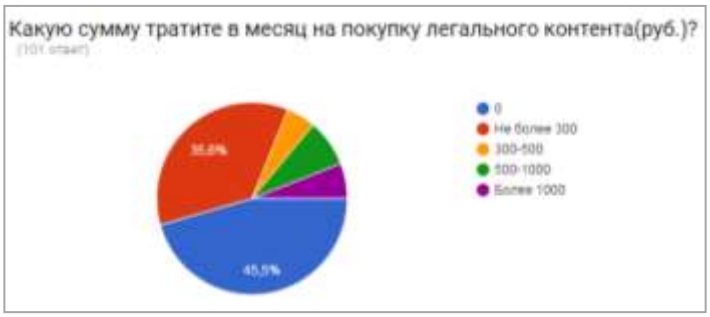


Рис. 1. Статистика расходов на легальный контент

Высокая стоимость легального контента стала основной причиной (рис. 2) использования пиратских ресурсов для подавляющего большинства опрошенных (69 %). Так как опрос проводился в возрастной категории от восемнадцати до двадцати трех лет, вопрос цен действительно актуален. Возможно компаниям, выпускающим продукты, которые пользуются популярностью у студентов, имеет смысл построить систему лояльности, ориентированную на молодых покупателей. Ведь если взрослый человек может позволить себе приобретать исключительно лицензионные продукты, то молодым людям это может оказаться не по карману.

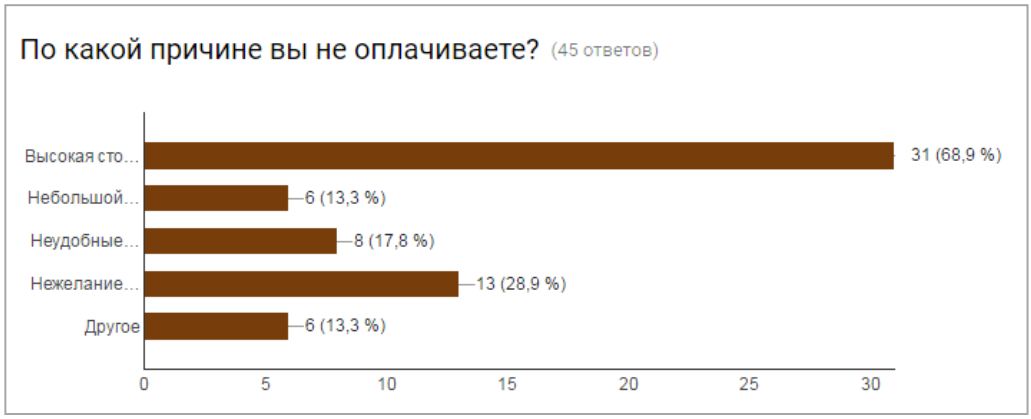


Рис. 2. Основные причины уклонения от оплаты скачиваемого контента

Почти половина (48,5 %) молодых людей знает, на каких ресурсах можно найти информацию о технических средствах обхода блокировок. Из них 76,5 % активно ими пользуется.

На вопрос «Если бы большинство сайтов с пиратским контентом были заблокированы, а способы обхода блокировок тщательно скрыты, вы бы задумались о приобретении лицензионных продуктов?» ответы разделились поровну. Первая половина ответила положительно, вторая половина опрошенных ответила, что продолжила бы искать способы обхода блокировок не жалея на это своего времени. Таким образом, блокировки сайтов в том виде, в котором они существуют сейчас, не обеспечивают должной защиты от пиратства. Хотя такая защита была бы востребована. Если бы блокировки интернет ресурсов с пиратским контентом повысили свою защищенность, а информация об их обходе тщательно скрывалась – компании, выпускающие легальный контент увеличили бы число своих покупателей на 50 %.

Список используемых источников

1. Synovate Comcon: исследование пиратского ПО в России [Электронный ресурс]. URL: http://www.comcon-2.ru/default.asp?trID=47 (дата обращения 15.05.2016).

2. Пресс-выпуск ВЦИОМ №2401 [Электронный ресурс]. URL: http://wciom.ru/index.php?id=236&uid=114467 (дата обращения 15.05.2016).

Статья представлена научным руководителем,
ассистентом Диптаном В. А.

УДК 681.3.066

А. С. Мишин (студент группы ИКТЗ-24, СПбГУТ)

ПОСТРОЕНИЕ ЭКРАНИРУЮЩЕГО МАРШРУТИЗАТОРА СООТВЕТСТВУЮЩЕГО ТРЕБОВАНИЯМ РУКОВОДЯЩЕГО ДОКУМЕНТА ФСТЭК РОСИИ

В топологии любой крупной сети присутствует такой элемент, как маршрутизатор. Данное сетевое устройство выполняет такие задачи, как маршрутизация, фильтрация и фрагментация сетевых пакетов. Функциональные возможности современных маршрутизаторов очень высоки.

экранирующий маршрутизатор, UNIX, Netfilter, iptables,

ФСТЭК России – Федеральная Служба по Техническому и Экспортному Контролю. В её функции включен специальный контроль в некото-

рых областях. К сфере деятельности ФСТЭК относятся средства защиты информации без использования средств криптографии и не составляющих государственную тайну. То есть обеспечение защиты информационной безопасности некриптографическими методами. В своем руководящем документе, ФСТЭК классифицирует экранирующие маршрутизаторы по пяти классам стойкости [1].

Устройства, соответствующие требованиям ФСТЭК имеют высокую стоимость и потребитель не всегда может себе их позволить. Однако, построение экранирующего маршрутизатора, удовлетворяющего требованиям как минимум четвертого класса защищенности возможно и без значительных финансовых затрат.

Все, что требуется для создания данного устройства – персональный компьютер с установленной операционной системой (ОС) семейства UNIX. При этом для реализации не требуется дополнительное программное обеспечение. Вся настройка может быть выполнена исключительно штатными средствами UNIX.

Для маршрутизации пакетов в ОС UNIX используется набор утилит IPRoute2. Для фильтрации пакетов служит механизм Netfilter. Он включает в себя ряд модулей, каждый из которых отвечает за определенный параметр фильтрации. Для удобства настройки, Netfilter имеет набор утилит. Так, за настройку модуля ip_tables отвечает утилита iptables, а за настройку модуля nf_conntrack утилита conntrack [2]. Полная схема механизма Netfilter представлена на (рис. 1).

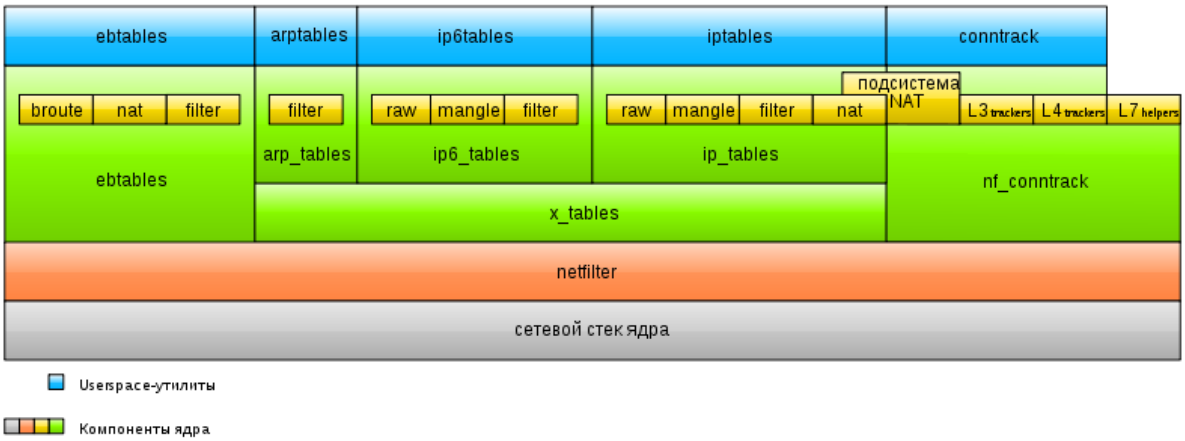


Рис. 1. Компоненты Netfilter

Требования ФСТЭК России к маршрутизаторам различных классов защищенности представлены в (табл. 1).

ТАБЛИЦА 1. Требования ФСТЭК к межсетевым экранам

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Для построения экранирующего маршрутизатора 4 класса защищенности необходимо обеспечить фильтрацию на сетевом уровне. Это возможно реализовать инструментами iptables и conntrack. Созданный набор правил представлен на рисунке 2. По умолчанию, все входящие и проходящие транзитом пакеты отбрасываются. Разрешены лишь исходящие сетевые пакеты и те пакеты, которые соответствуют хотя бы одному из описанных правил. Если, пройдя по всей цепочке правил, сетевой пакет не был принят – он отбрасывается маршрутизатором. Таким образом, производится фильтрация сетевых пакетов по портам, по состоянию сетевого соединения, а также по входным интерфейсам.

Требования идентификации и аутентификации выполняются межсетевым экраном за счет системы доступа, позволяющей просматривать/редактировать настройки межсетевого экрана только администратору.

Регистрация действий осуществляется логированием. То есть автоматической записью любого действия системы в документ. Тонкая настройка механизма логирования доступна через утилиту iptables. Для соответствия требованиям ФСТЭК для четвертого класса защищенности достаточно включить логирование отброшенных пакетов командой: -A INPUT -i eth0 -j LOG --log-level debug --log-prefix «INPUT DROP:». Эта команда включает логирование событий в цепочке INPUT на интерфейсе eth0. Каждая запись будет начинаться с префикса «INPUT DROP:» и содержать полную информацию об отброшенном пакете, включая адрес и время. Для цепочек правил FORWARD и OUTPUT необходимо включить логирование анало-

гичными командами, заменив название цепочки и префикс на FORWARD и OUTPUT соответственно.

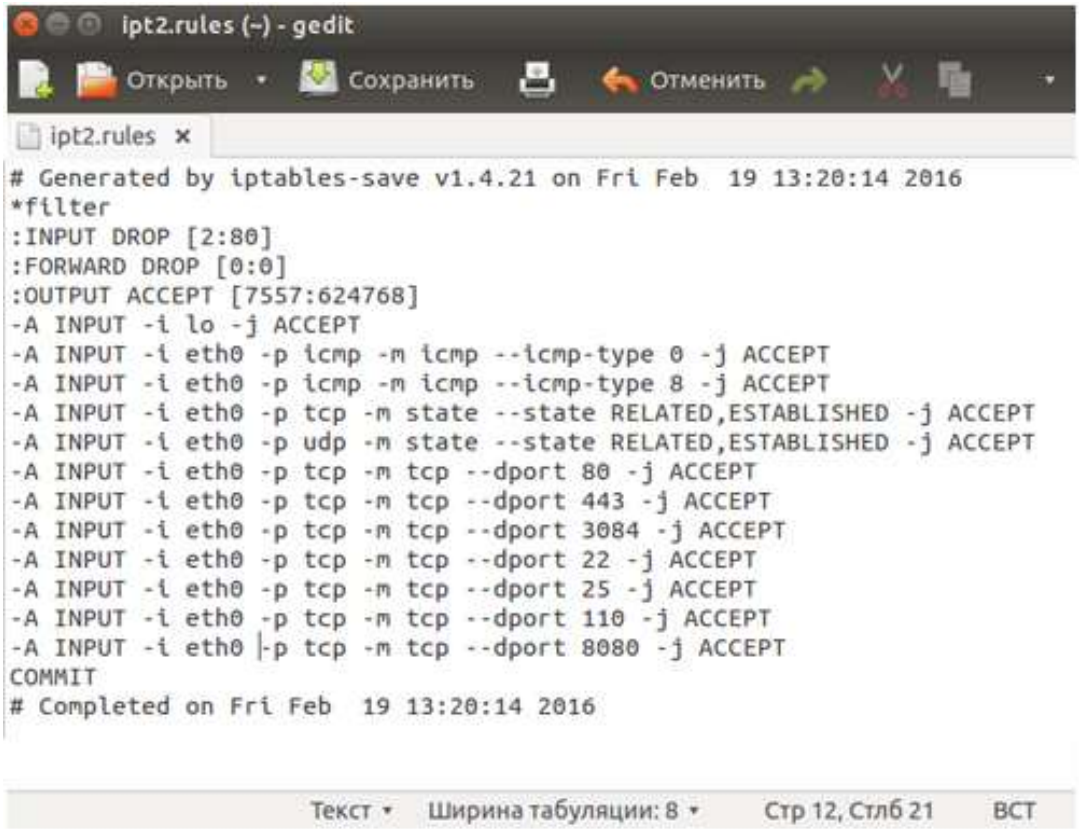


Рис. 2. Набор правил Iptables

Контроль целостности настроек экранирующего маршрутизатора возможен методом сравнения хэш-сумм системных файлов. Любое изменение в файле приведет к изменению его хэш-суммы. Таким образом, записанные значения хэш-сумм дают возможность в любой момент убедиться в целостности файлов. Команды «md5sum /etc/sysconfig/iptables» и «md5sum /etc/network/interfaces» выводят на экран контрольные суммы файлов iptables.rules и interfaces, которые, в свою очередь, хранят основные настройки маршрутизатора.

В случае несовпадения контрольных сумм системных файлов, восстановление свойств экранирующего маршрутизатора возможно благодаря команде «iptables-restore < /etc/sysconfig/iptables». Команда загружает настройки iptables из указанного файла. Сохранить все настройки в файл можно командой «iptables-save > /etc/sysconfig/iptables» (настройки будут сохранены в файл «iptables.rules», который будет располагаться в /etc/sysconfig/iptables).

Составление тестовой и конструкторской документации по построенному экранирующему маршрутизатору должно производится разработчи-

ком программного обеспечения. Так как многие механизмы могут быть сконфигурированы под индивидуальные требования заказчика.

Тестирование построенного экранирующего маршрутизатора выполняется согласно предоставленной эксплуатационной документации по межсетевому экрану, которую разработали производители ОС. Состояние портов позволяет контролировать утилита NMap. Информация обо всех отброшенных пакетах будет отображаться в лог файле «Syslog», находящемся в каталоге /var/log после настойки syslogd. Процесс аутентификации администратора может быть протестирован при выполнении в терминале любой команды связанной с конфигурированием операционной системы. После соответствующей настройки правил журналирования интерпретатора команд, все действия администратора записываются в файл «auth.log» находящийся в каталоге /var/log. Контролировать целостность позволяют хэш-суммы, получаемые командой «md5sum», а проследить за процедурой восстановления (при использовании «iptables-restore») можно при помощи команды просмотра правил iptables – «sudo iptables -L».

Таким образом, построение экранирующего маршрутизатора, соответствующего требованиям руководящего документа ФСТЭК России, возможно штатными средствами операционной системы семейства UNIX. Для построения не требуется дополнительное программное обеспечение. Построенный маршрутизатор удовлетворяет требованиям 4 класса защищенности ФСТЭК России.

Список используемых источников

1. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ. ФСТЭК России. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

2. Andreasson O. Iptables Tutorial 1.1.19 / пер. с англ. Андрей Киселев. 2001–2003 [Электронный ресурс]. URL: http://www.opennet.ru/docs/RUS/ iptables/ # STATEMA CHINE

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Юркиным Д. В.

УДК 004.312.24

В. Е. Николаев (студент группы ИКТ-408, СПбГУТ)

МОДЕЛИРОВАНИЕ ДВУХУРОВНЕВОГО МУЛЬТИПЛЕКСОРА ПОД ПРОГРАММИРОВАНИЕ В ПЛИС

В работе рассматривается моделирование двухуровневого мультиплексора, предназначенного для считывания данных из регистров, и состоящего из: 4 мультиплексоров первого уровня и одного мультиплексора 2 уровня в программе Modelsim на языке программирования Verilog, получение файла testbench для проверки работоспособности устройства и временной диаграммы устройства.

Производится программирование устройства в ПЛИС Cyclone V для дальнейшей демонстрации.

микропроцессор, мультиплексор, ПЛИС, TimeQuest,

Цель работы

Разработать устройство, которое позволяет считывать данные с четырехразрядного регистра с глубиной в 4 бита, в котором данные представлены по принципу FIFO *(First In, First Out)* (рис. 1).

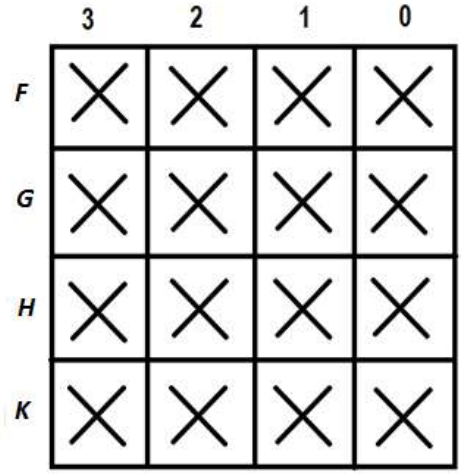


Рис. 1. Принципиальная схема регистра

Для подачи корректных адресов на проектируемое устройство нам также необходим понижающий счетчик.

Таким образом, проектируемое устройство будет иметь 2 адресных входа, 1 вход данных и один выход, который будет выводить данные с регистра. Полная схема подключения устройства приведена на рисунке 2.

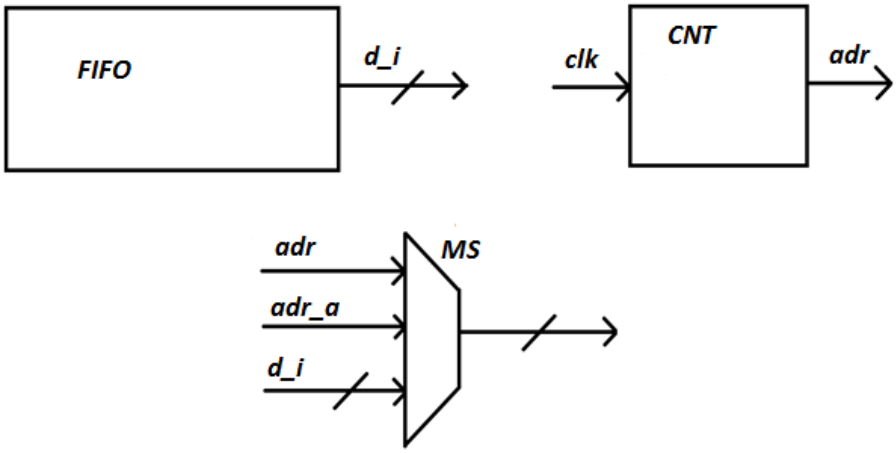


Рис. 2. Полная схема подключения устройства

Этапы проектирования

В данной работе подробно рассматривается создание именно мультиплексора.

Проектируемое устройство можно условно разбить на 2 уровня:

- На нижнем уровне располагаются 4 мультиплексора на 4 входа данных, которые подключены к ячейкам регистра, один адресный вход, который подключен к понижающему счетчику, и один выход.
- Верхний уровень будет представлен аналогичным мультиплексором, но на адресный вход подаются адреса с той же частотой что и тактовая частота.

Первый этап

Построение нижнего уровня

Для упрощения поставленной задачи был написан модуль «mult_w», который представляет собой простейшее коммутационное устройство. Его код на языке Verilog представлен ниже:

```
module mult_w
(
input wire [3:0] d_i, [1:0] adr,
output reg dat
);
always @*
case (adr)
2'b00:dat<=d_i[0];
2'b01:dat<=d_i[1];
2'b10:dat<=d_i[2];
2'b11:dat<=d_i[3];
endcase
endmodule
```

Для завершения построения нижнего уровня необходимо объединить 4 модуля, которые описаны выше (рис. 3).

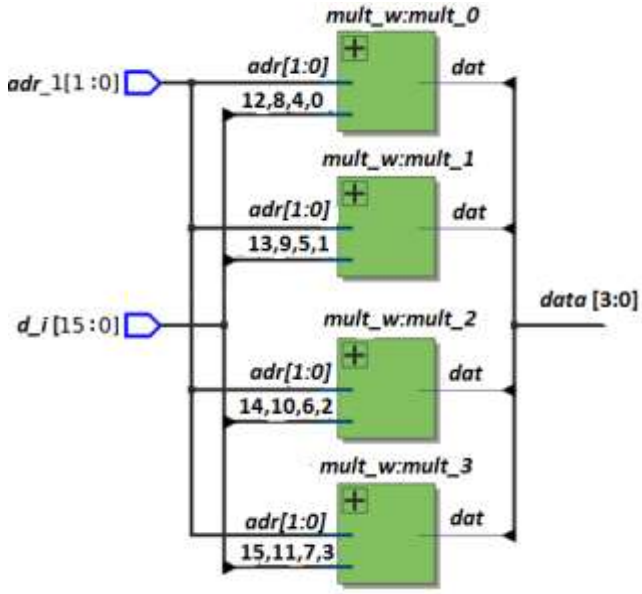


Рис. 3. Схема построенного нижнего уровня

Второй этап

Построение верхнего уровня и завершение проектирования устройства.

Верхний уровень устройства также представлен мультиплексором, но в данной работе я использовал один из модулей, встроенных в среду разработки, и он называется «*Mux*0». Его структура и свойства аналогичны тому модулю, что описан выше.

Конечная структура устройства приведена на рисунке 4.

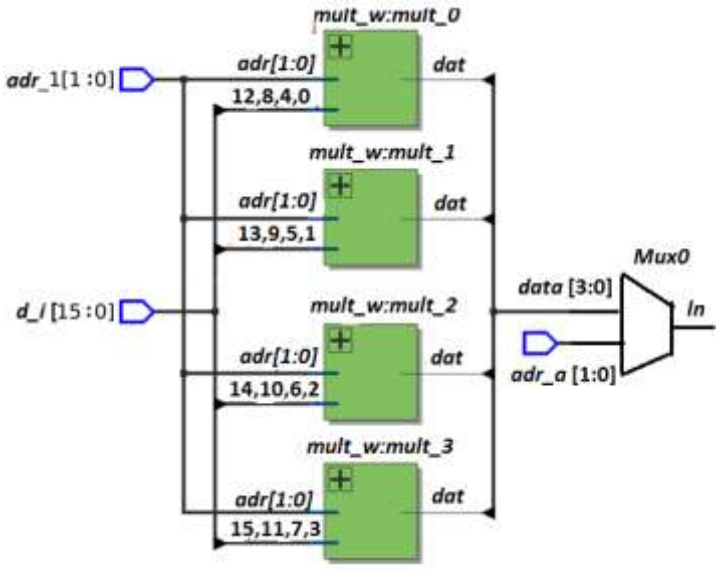


Рис. 4. Конечная структура устройства

Выводы

На рисунке 5 приведена временная диаграмма работы устройства, которая демонстрирует корректность работы полученного модуля.

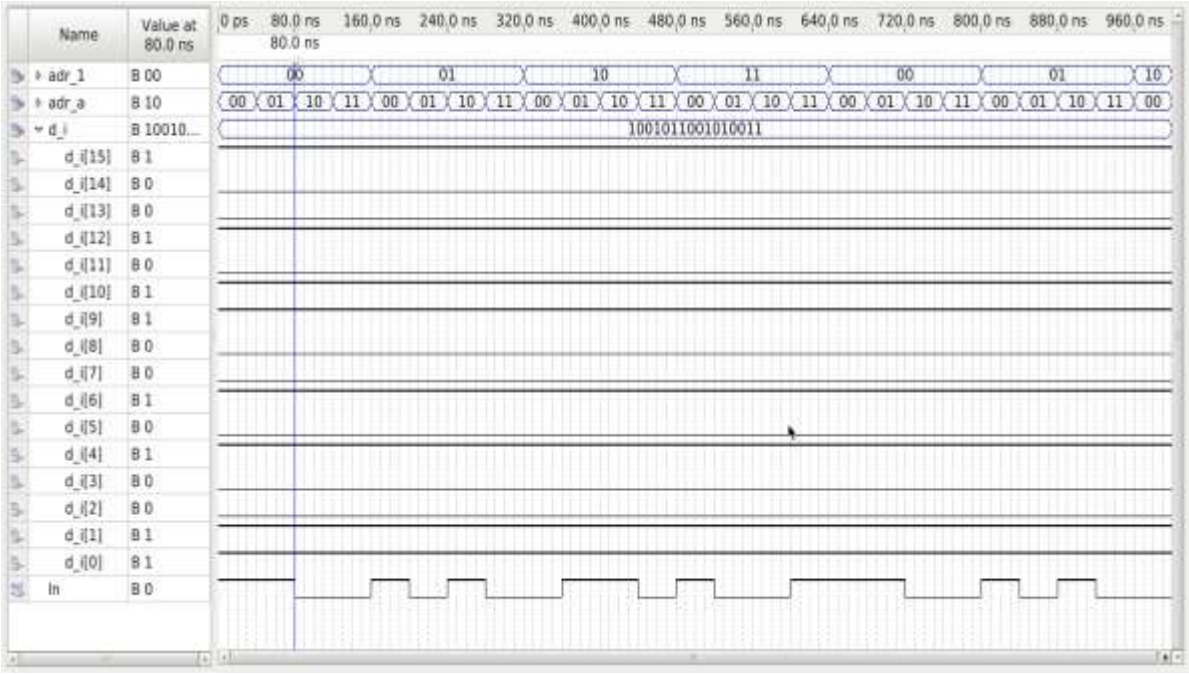


Рис. 5. Временная диаграмма работы устройства

В результате этой работы был получен модуль, позволяющий выполнять задачи, описанные в целях работы, сократить задержки работы устройств, в которые будет включен проектируемый модуль, и облегчить создание TimeQuest.

Список используемых источников

1. Pong P. Chu. FPGA prototyping by Verilog examples. : Wiley, 2008. 488 p. ISBN 978-0-470-18532-2.

Статья представлена научным руководителем,
старшим преподавателем Нееловой О. Л.

УДК 004.056.53

Н. Л. Пиховкин (студент группы ИКТЗ-24 СПБГУТ)
Д. В. Сахаров (кандидат технических наук, доцент СПбГУТ)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ С УЧЕТОМ УПРАВЛЕНИЯ РИСКАМИ

Информационно-вычислительные сети, объединяющие в единую систему все подразделения и филиалы, позволяют одновременно работать с распределенными или централизованными приложениями, базами данных и другими сервисами. Одной из главных задач обеспечения необходимого уровня защищенности таких сетей является процесс управления рисками, который позволяет направить все усилия на защиту от наиболее вероятных угроз. В докладе анализируется важность управления рисками в процессе обеспечения информационной безопасности, а также описывается риск-ориентированная методика построения защищенной распределенной сети, разработанная на основе ведущих мировых стандартов и рекомендаций.

информационная безопасность, управление рисками, угроза, информационная система, распределенная сеть.

Построение защищенной территориально распределенной сети - это сложная комплексная задача. При ее решении приходится учитывать множество факторов и рисков, которые могут оказать негативное влияние на деятельность компании, а также поставить под угрозу конфиденциальность, целостность, доступность информации, качество и скорость ее обработки и передачи. Ограниченные ресурсы и постоянно меняющейся ландшафт угроз и уязвимостей делают невозможным полное снижение всех рисков. Специалисты по безопасности должны иметь набор средств, который поможет оценить воздействие рисков на деятельность организации и, если необходимо, снизить их до приемлемого уровня. Для формирования понимания приоритетности мероприятий, направленных на повышение уровня ИБ, разрабатывается механизм управления рисками. В этом случае все усилия направляются на защиту от наиболее вероятных угроз, позволяя снизить возможные потери и минимизировать затраты. Это делается потому, что бессистемное и выборочное внедрение защитных мер не может обеспечить необходимого уровня защищенности. Кроме того, необходимость проведения управления рисками определена в российских и международных стандартах по информационной безопасности (ГОСТ Р ИСО/МЭК 17799:2005, CRAMM, ISO 27001:2013) и нормативных документах государственных органов РФ (например, документах ФСТЭК России по защите персональных данных и ключевых систем информационной инфраструктуры).

Специалист, отвечающий за построение безопасной информационно-вычислительной сети, должен найти баланс как минимум в трех показателях – производительности, безопасности и стоимости. При снижении рисков и повышении уровня безопасности сети, как правило, увеличивается стоимость и снижается производительность. Также конфликтующими свойствами являются надежность и защищенность, с одной стороны, удобство и открытость – с другой. Отсюда следует, что построение безопасной сетевой инфраструктуры – это управление рисками, возникающими вследствие определенных компромиссов.

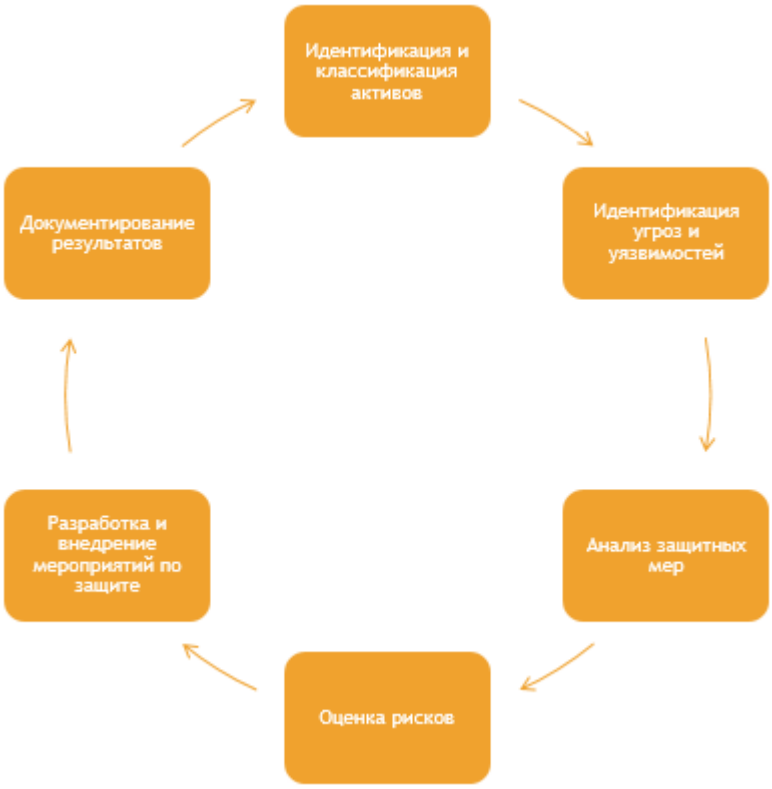


Рис. 1. Процесс управления рисками

Процесс управления рисками информационной безопасности, подробно описанный на рисунке 1, сводится к получению следующих данных [1, 3]:

1) какие риски существуют в организации;
2) какова вероятность их реализации и масштаб возможных последствий;
3) какие риски руководство организации готово принять;
4) какие средства защиты являются наиболее эффективными (в том числе с экономической точки зрения) для борьбы с той или иной уязвимостью;
5) какой объем средств должен находиться в резерве в случае возникновения инцидента ИБ.

В случае информационно-вычислительных сетей риск-ориентированная методика обеспечения безопасности будет состоять из следующих последовательных шагов:

1) сбор информации о сетевой инфраструктуре;
2) классификация и определение ценности сетевых активов;
3) идентификация и классификация актуальных угроз;
4) анализ существующих защитных мер;
5) анализ рисков сетевой безопасности;
6) проектирование и внедрение системы обеспечения безопасности;
7) документирование результатов;
8) мониторинг эффективности.

На первых этапах проводится анализ документации, интервьюирование работников, отвечающих за функционирование и безопасность сетевой инфраструктуры. Специалисты проводят опрос персонала каждого подразделения с целью выявления используемых активов. Не все активы имеют одинаковую ценность для организации, поэтому после идентификации всех ценных активов они должны быть классифицированы в соответствии с уровнем потенциального ущерба в случае возникновения инцидента. Классификация позволит определить, какие защитные меры и в каком приоритете должны применяться к каждому классу, а также сделать это наиболее экономически эффективным способом.

Далее проводится проверка объектов на наличие уязвимостей и, при необходимости, проведение тестирования на проникновение с использованием выявленных уязвимостей. Как правило, при проведении инструментального сканирования используется программное обеспечение, позволяющее автоматизировать процесс, однако могут быть задействованы и ручные проверки. По завершении всех работ составляется отчетная документация, в которую входит информация об обнаруженных уязвимостях, а также рекомендации по их устранению.

После всестороннего изучения сетевой инфраструктуры проводится анализ рисков, связанных с нарушением безопасности сетевых активов. В настоящее время существует множество инструментов и программных инструментов, позволяющих автоматизировать этот процесс – ГРИФ, RiskWatch, Risk Advisor, FRAP, CRAMM, Microsoft Security Assessment Tool, Symantec Lifecycle Security (основные сравнительные характеристики приведены в табл. 1). Несмотря на большое разнообразие, все они так или иначе основаны на двух фундаментальных к оценке рисков – на количественном или на качественном [2].

Для определения очередности обработки рисков выполняется операция их ранжирования. Один из самых простых способов – это ранжирование по вероятности реализации угрозы и по степени критичности информации, исходя из которого составляется многоуровневая шкала или матри-

ца рисков, показывающая степень воздействия выявленных угроз на сетевую инфраструктуру. Пример матрицы рисков приведен на рисунке 2.

ТАБЛИЦА 1. Основные сравнительные характеристики инструментов анализа рисков

	ГРИФ	RiskWatch	Risk Advisor	FRAP	CRAMM	MSAT	Symantec LS
Способы измерения величины риска							
Качественный метод	+	+	+	+	+	+	+
Количественный метод	+	+	-	-	+	+	-
Подход к анализу и оценке риска							
Модель анализа угроз и уязвимостей	+	+	-	+	+	-	+
Метод информационных потоков	+	+	+	-	+	+	+
Элементы риска							
Материальные активы	+	+	+	+	+	+	+
Нематериальные активы	+	+	+	+	+	+	+
Ценность активов	+	+	+	+	+	+	+
Угрозы	+	+	+	+	+	+	+
Уязвимости	+	+	+	+	+	+	+
Средства защиты	+	+	+	+	+	+	-
Потенциальный ущерб	+	+	+	+	+	+	+
Вероятность реализации угрозы	+	+	+	+	+	+	+
Финансовые показатели							
Расчет возврата инвестиций (ROI)	+	+	-	-	-	-	-
Расчет ожидаемых годовых потерь (ALE)	-	+	-	-	-	-	-

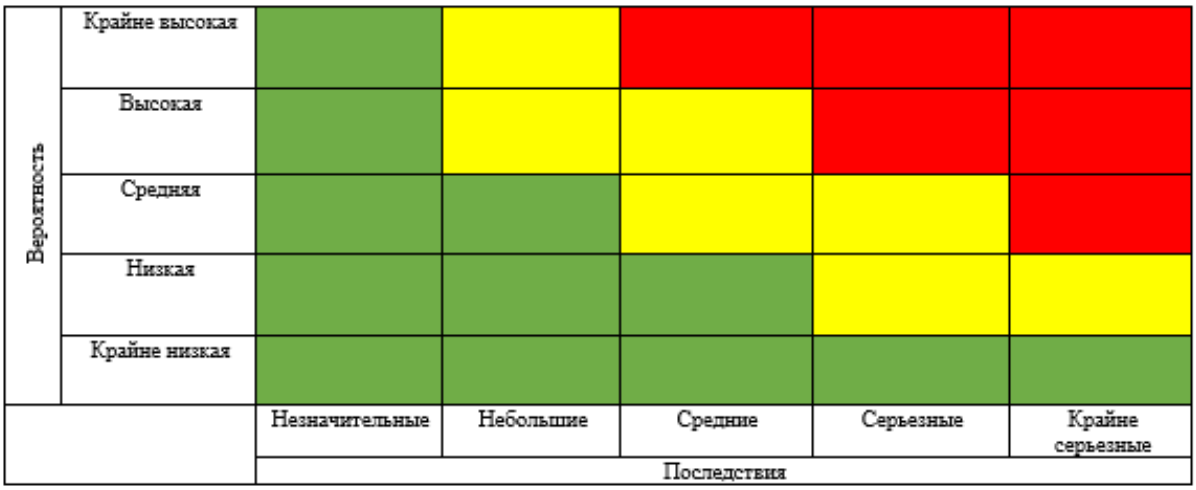


Рис. 2. Процесс управления рисками

На основе данных, полученных на предыдущих этапах, проектируется подходящий дизайн сетевой инфраструктуры и разрабатываются политики информационной безопасности. Написание и строгое соблюдение политик определяет работу всей системы защиты. После этого начинается непосредственное внедрение средств защиты.

Еще одной важной составляющей обеспечения безопасности и непрерывной работы сетевых сервисов является осуществление мониторинга сети, который позволяет своевременно реагировать на возникающие угрозы и значительно упрощает работу сетевых администраторов.

Таким образом, можно сказать, что применение риск-ориентированного подхода позволяет выбрать состав системы защиты сети, который полностью отвечает заданным условиям и требованиям. Это максимально повышает эффективность внедренных мер защиты, а также позволяет снизить затраты на обеспечение и поддерживание необходимого уровня информационной безопасности. Управление рисками в сфере информационной безопасности информационно-вычислительных сетей играет такую же важную роль, как и во всех других областях человеческой деятельности.

Список используемых источников

1. Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н. Организационно-правовое и методическое обеспечение информационной безопасности. СПб. : Университет ИТМО, 2016. 168 с.

2. Steven Hernandez. Official (ISC)^2 Guide to the CISSP CBK, Third Edition. ISC2 Press, 2012. 968 с.

3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М. : Издательство стандартов, 2010. 51 с.

УДК 65.011.56

Н. С. Плетнева (студентка группы ИКТК-27, СПбГУТ)

АНАЛИЗ ОСОБЕННОСТЕЙ ЖИЗНЕННОГО ЦИКЛА ЗИП В СИСТЕМАХ КЛАССА RMS

Современная система автоматизированного учёта движения материальных ресурсов (Resource Management System, RMS), разрабатываемая для операторов связи, должна уметь управлять логистикой запасных частей, инструментов и принадлежностей (ЗИП). Такая функциональность системы крайне востребована телекоммуникационными компаниями.

OSS/BSS, RMS, RLM, TMForum, ЗИП, жизненный цикл, рюкзак монтажника.

Информационно-телекоммуникационная сеть – технологическая система, включающая различные методы и технологии, с помощью которых фирмы и пользователи получают доступ к необходимой информации.

При интенсивном использовании сети могут возникать перебои в работе телекоммуникационного оборудования. От того, как быстро эксплуатационный персонал реагирует на возникающие ошибки, зависит состояние и работа сети в целом. Бывают случаи, когда полностью заменить неисправное оборудование невозможно. Альтернативой полной замене оборудования является использование комплектов запасных частей, инструментов и принадлежностей (ЗИП), когда восстановление работоспособности оборудования сводится к локальной замене отказавших элементов исправной запасной частью (ЗЧ). Такую замену может выполнять эксплуатационный персонал, но она требует специального управления, и поэтому возникает необходимость дополнения существующей OSS инфраструктуры функциональностью учета ЗИП в системах RMS (*Resource Management System*).

Система RMS, входящая в состав OSS/BSS, при соответствующей доработке поможет вести учет и управлять передвижениями ЗИП, а также грамотно и своевременно планировать закупки и поставки оборудования ЗИП.

Система автоматизированного учёта движения материальных ресурсов (*RMS*) оператора связи построена на основе стандартов и методологии *TM Forum*, согласно которым *RMS* входит в функционал RLM (*Resource Lifecycle Management*, Управление жизненным циклом ресурса) карты приложений *Telecom Application Map (TAM)* и отвечает за следующие бизнес-процессы:

- управление сквозным жизненным циклом ресурсов,
- стратегическое и тактическое планирование,
- планирование внедрения,
- ввод в эксплуатацию,
- управление спецификациями возможностей ресурсов и ведение их каталога.

RMS предназначена для поддержки и частичной автоматизации процессов учета, управления активами ресурсов и контроля актуального состояния остатков по складской структуре предприятия оператора связи, поддерживает выполнение операций в рамках пред- и постэксплуатационной обработки, а также обеспечивает поддержку операций в рамках взаимодействия этапов жизненных циклов складского и технического (эксплуатационного) учета.

Жизненный цикл в системах RMS рассматривается с точки зрения правил и методов ведения бухгалтерского и складского учета, адаптированных под бизнес-процессы, используемые операторами связи.

При описании жизненного цикла в системе RMS предполагается использовать три параметра:

1) область хранения,
2) статус,
3) требуемое действие.

Комбинация из этих трех параметров точно описывает местонахождение комплекта, его состояние и действие, которое необходимо совершить над комплектом. Данная информация будет использоваться системой для создания отчетности, автоматизации заполнения актов и подбора оборудования.

Статус комплекта ЗИП в системе при перемещении из одного места хранения в другое будет принимать любое из четырех значений: готово к использованию, не готово к использованию, используется или списано. Все возможные перемещения и соответствующие им изменения параметров оборудования (области хранения, статуса и требуемого действия) указаны на рисунке 1:

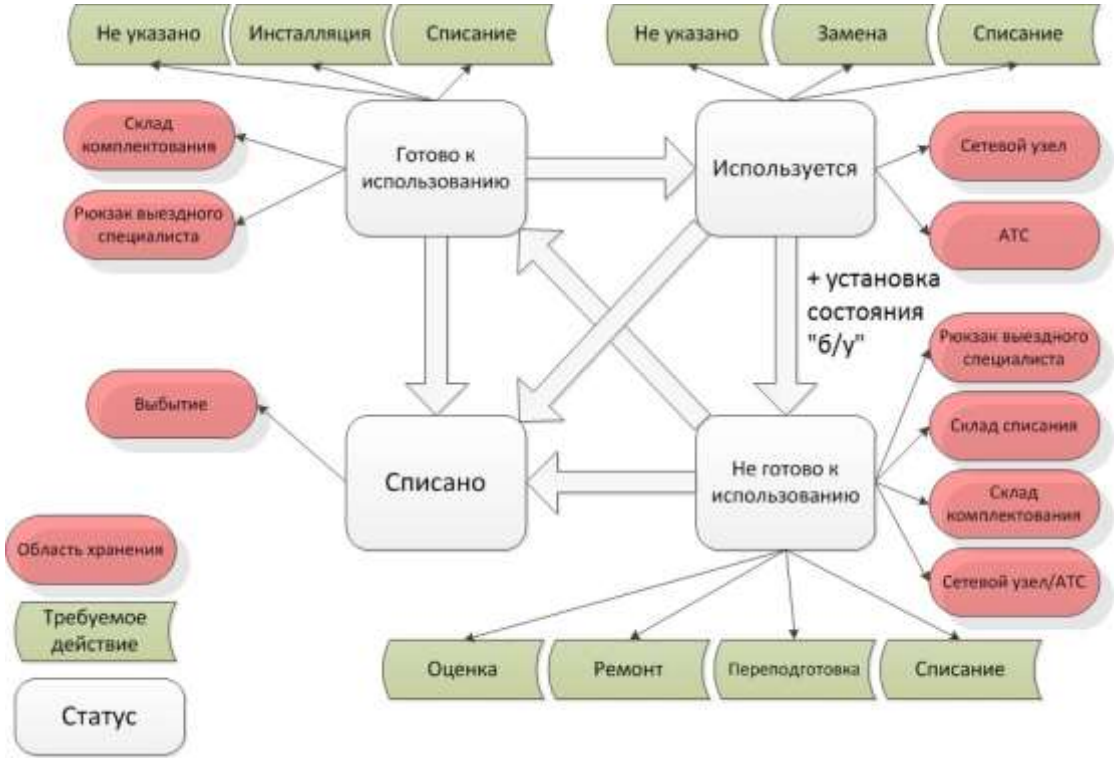


Рис. 1. Диаграмма жизненного цикла комплектов ЗИП

В качестве примера рассмотрим более подробно один из сценариев перехода комплектов ЗИП по этапам жизненного цикла в системе RMS до установки на сеть, представленный на рисунке 2:

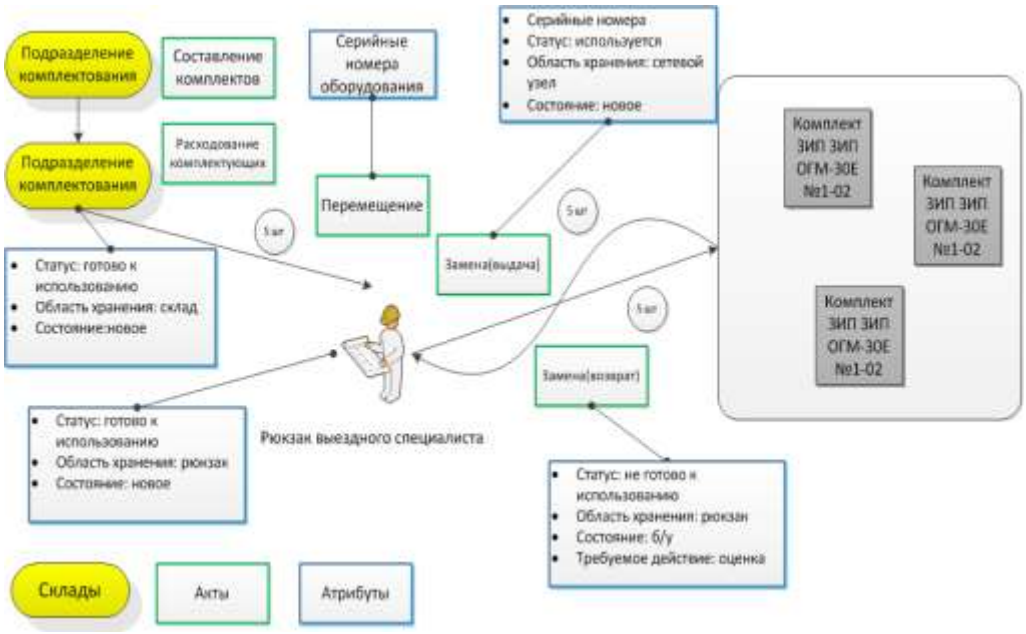


Рис. 2. Диаграмма перехода комплектов ЗИП по этапам жизненного цикла до установки на сети

Комплекты не поступают от поставщика, поэтому прежде чем они будут задействованы в работе у оператора, они формируются на складе. Система поддерживает создание комплекта, в который могут входить ресурсы любого типа и в любом количестве.

Переход по этапам ЖЦ начинается с составления комплектов, происходящее на складе комплектования, на котором уже заранее находятся ресурсы из состава комплекта в состоянии «Новое», статус – «Готов к использованию», Требуемое действие – «Составление комплектов».

Сформированные комплекты перемещаются к рабочему персоналу, который отвечает за подключение оборудования. Перемещение комплектов фиксируется в акте – внутреннем документе системы, описывающем производимые над ресурсами хозяйственные операции – с обязательным указанием серийных номеров перемещаемого оборудования. После перемещения эксплуатационный персонал производит замену вышедшего из строя оборудования и устанавливает новый комплект ЗИП в необходимом сетевом узле или на станции.

После установки ЗИП, сеть может продолжить функционировать, но на этом жизненный цикл комплекта ЗИП не заканчивается.

Комплект ЗИП может быть возвращен или списан по причине неисправности, непригодности для использования на конкретном участке сети или по другим причинам.

Также комплект ЗИП может быть возвращен, после чего экспертная комиссия должна вынести решение о возможности дальнейшего использования ресурса. В результате проведения оценки комплекта могут быть вынесены следующие решения:

- ресурс готов к использованию и дальнейшей установке на сети,
- ресурс неисправен и подлежит ремонту.
- ресурс не полностью укомплектован и подлежит переподготовке,
- ресурс подлежит списанию.

Опыт эксплуатации сложных систем подсказывает, что время восстановления работоспособности оборудования после отказа в основном зависит от наличия запасных элементов. Так, при эксплуатации телекоммуникационных систем отсутствие ЗИП может привести к увеличению времени восстановления в 10 раз.

Применение комплектов запасного имущества и принадлежностей в эксплуатационной деятельности телекоммуникационных операторов поможет существенно снизить затраты и расходы на восстановление работоспособности оборудования при его неполадках и быстро возобновить работу всей сети. А возможность управлять и учитывать ЗИП в системах RMS позволит оператору управлять логистикой ЗИП, контролировать сроки поставок и закупок ЗИП, а также риски и расходы на комплекты ЗИП в течение его жизненного цикла.

Список используемых источников

1. Джон Райли, Мартин Кринер NGOSS: построение эффективной системы поддержки и эксплуатации сетей для операторов связи. М. : Альпина Бизнес Букс, 2007. 192 с. ISBN: 978-5-9614-0632-0, 978-0-9551087-0-9.

2. Самуйлов К. Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Системы следующего поколения для поддержки операционной деятельности инфокоммуникационной компании: учебное пособие. М.: РУДН, 2008. 123 с.

3. Атцик А., Гольдштейн А., Сизюхин К. SID: абстракция на службе практики// CONNECT № 10. 2012. С. 54–58.

4. TM Forum. [Электронный ресурс]. URL: https://www.tmforum.org (дата обращения 15.06.2016).

5. Петровский Н., Никуллин В., Бакин С7, Еще несколько слов о ресурсах оператора, или «что такое RMS»? // Мобильные телекоммуникации. Апрель 2014. № 3. С. 26–27.

6. Гребешков А. Ю. Управление и технический учет ресурсов в телекоммуникациях. М. : ИРИАС, 2008. 326 с.

7. Черкесов Г.Н., Оценка надежности систем с учетом ЗИП: учебное пособие. СПб. : БХВ-Петербург, .2012. 480 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Гольдштейном А. Б.

УДК 621.395

В. А. Поздняков (студент группы ИКТК-26, СПбГУТ)

РАЗРАБОТКА СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА УСЛУГ И ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ СЕТЕЙ ЭЛЕКТРОСВЯЗИ

На основе проведенного анализа нормативной базы в области качества услуг электросвязи и в области показателей эффективности эксплуатации разработана система взаимодействия показателей качества услуг и показателей эффективности эксплуатации сетей электросвязи. Также разработана техническая реализация упомянутой системы, которая реализована путем построения структуры взаимодействия системы управления качеством (Service Quality Management, SQM) и системы управления качеством со стороны потребителя (Customer Experience Management, CEM).

показатели качества услуг (Quality of Service, QoS и Quality of Experience, QoE), показатели эффективности эксплуатации (Key Performance Indicator, KPI и Key Quality Indicator, KQI), SQM, CEM, Service Level Agreement (SLA).

В современном обществе телекоммуникации занимают особое место. Данная сфера деятельности стремительно развивается. Одним из важнейших направлений развития отрасли связи является обеспечение удовлетворенности потребителей качеством услуг связи и возможности осознанного выбора поставщика услуг. На рынке появляется большое число компаний, которые хотят предоставлять телекоммуникационные услуги, то есть наблюдается высокий уровень конкуренции. Безусловно многие люди стремятся получить современные услуги связи, то есть растет число потребителей. Наконец, растет число и самих услуг связи.

В соответствии с вышесказанным можно выделить основные потребности участников рынка:

− потребитель: хочет получить определенный продукт/услугу надлежащего качества;

− оператор связи: хочет предоставить востребованную услугу требуемого качества с минимальными затратами.

Оператору связи необходимо максимально удовлетворить потребности клиента, чтобы быть успешным в сложившейся высоко конкурентной отрасли телекоммуникаций. Поэтому он массово внедряет различные системы OSS/BSS (*Operation Support System/Business Support System*) для повышения эффективности деятельности.

На основе получаемых данных из сети и систем OSS/BSS можно рассчитать показатели качества обслуживания и показатели эффективности эксплуатации сетей электросвязи. Необходимость разработки системы взаимодействия упомянутых показателей обусловлена тем, что оператор свя-

зи сможет определить сколько будет стоить услуга/продукт и какую прибыль она сможет принести. Данные показатели можно рассчитать с помощью системы управления качеством (*Service Quality Management*, SQM). Теперь необходимо определить какая именно услуга нужна клиенту и какого качество. Для решения этой задачи необходимо использовать показатели восприятия качества услуги потребителем, которые можно получить из систем CEM (*Customer Experience Management*). Данные показатели дополняют информацию, имеющуюся в распоряжении оператора связи, и позволяют ему эффективно взаимодействовать с клиентами. В связи с вышесказанным, целесообразно разработать систему взаимодействия SQM и CEM.

Качество услуги (QoS) – совокупность характеристик услуги электросвязи, которые имеют отношение к ее возможности удовлетворять установленные и предполагаемые потребности пользователя услуги [1].

Качество восприятия услуги пользователем (QoE) – общая приемлемость приложения или услуги, субъективно воспринимаемая конечным пользователем. Включает восприятие всех составляющих услуги (сети, терминала, инфраструктуры услуги и т. п.) [2].

Качество можно измерить с помощь KPI (*Key Performance Indicator*) и KQI (*Key Quality Indicator*).

Ключевой показатель функционирования (KPI) – мера определенного аспекта функционирования ресурса услуги или группы ресурсов одного вида. KPI всегда относится к определенному виду ресурсов [3].

Ключевой показатель качества услуги (KQI) – мера определенного аспекта функционирования продукта, его компонента (услуги) или элементов услуги и выводится с помощью математических формул из множества источников, включающих KPI или KQI [3].

Каждый оператор связи стремится, чтобы его деятельность была эффективной. Эффективность деятельности оператора связи можно оценивать по трем направлениям: финансы, взаимодействие с пользователем, операционная деятельность [4].

Показатели эффективности эксплуатации тесно связаны с картой бизнес-процессов eTOM. Поэтому можно выделить четыре группы показателей эффективности эксплуатации [5]:

- стоимостные показатели,
- временные показатели,
- показатели качества выполнения процесса,
- показатели производительности системы эксплуатации.

На рисунке 1 представлена система взаимодействия показателей качества услуг и показателей эффективности эксплуатации сетей электросвязи.

Рис. 1. Система взаимодействия показателей качества услуг
и показателей эффективности эксплуатации

Для технической реализации взаимодействия, указанного на рисунке 1, необходимо реализовать взаимодействие систем SQM и CEM. Система SQM предназначена для сбора и обработки статистики, анализ которой позволит оператору связи оценить показатели качества услуг и показатели эффективности эксплуатации. Также указанная система позволяет сократить эксплуатационные затраты (OpEx) за счет автоматизированного процесса поддержания гарантированного качества услуг в реальном времени и повысить удельную выручку от абонента (ARPU).

Система CEM позволяет операторам связи разрабатывать стратегию управления пользовательским восприятием качества услуг связи, которая улучшает лояльность клиентов, увеличивает доходы, сокращает затраты и уменьшает отток клиентов по всему ассортименту предлагаемых продуктов и услуг.

На рисунке 2 представлена структура системы взаимодействия SQM и CEM.

На уровень сбора данных и их обработки, уровень 1, поступают разнородные данные, они собираются через адаптеры и помещаются в модуль хранения. Данный модуль взаимодействует с модулем ETL (*extract/transformation/loading*), с помощью которого производится предварительная обработка данных.

На втором уровне данные попадают в модуль работы с *Big Data*, именно в котором и производится аналитика данных и их хранение по средствам HDFS (*Hadoop Distribution File System*) и SQL-решений. За аналитику поступающих данных отвечает модуль алгоритмов, который может иметь разнообразную программную реализацию в зависимости от поставщика. Далее производится обработка данных в соответствии с задачами:

- расчет KPI/KQI;
- расчет CEI (*Customer Experience Index*);
- мониторинг SLA (*Service Level Agreement*) – данный модуль нужен для отслеживания соответствия KPI/KQI, указанных в SLA, KPI/KQI, получаемых из сети;
- статистическое моделирование – данный модуль используется совместно с модулем создания правил и нужен для моделирования ситуаций, которые могут вызывать ухудшение качества обслуживания и отток клиентов;
- корреляция показателей качества услуг и показателей эффективности эксплуатации сетей электросвязи.

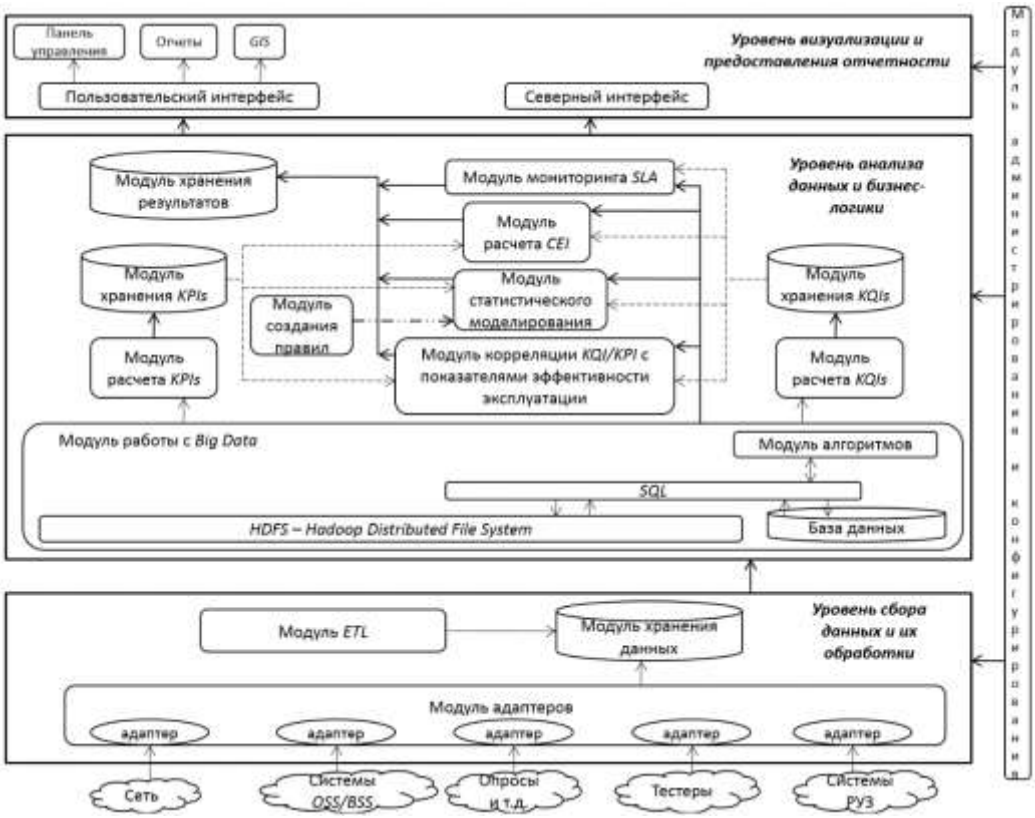


Рис. 2. Структура системы взаимодействия SQM и CEM

Все промежуточные и итоговые результаты находятся в раздельных модулях хранения.

На 3 уровне имеется пользовательский и северный интерфейс. Первый нужен для взаимодействия конечного пользователя с системами CEM и SQM, поддерживающий различные инструменты визуализации и представления отчетности, а второй нужен для взаимодействия с другими информационными системами оператора связи.

Модуль администрирования и конфигурирования является сквозным, так как он осуществляет взаимодействие со всеми уровнями. Он имеет доступ к каждому элементу на любом уровне архитектуры.

Разработанная система взаимодействия SQM и CEM позволит операторам связи понять какие услуги важны для клиентов, какого качества и по какой стоимости.

Список используемых источников

1. Качество услуг электросвязи: концепции, модели, связанные с качеством услуг электросвязи. Определение терминов, относящихся к качеству обслуживания: Рекомендация E.800. ITU-T, 09/2008.
2. Словарь по рабочим характеристикам и качеству обслуживания: Рекомендация P.10/G.100. ITU-T, 07/2006.
3. Wireless Service Measurements Solution Suite: Рекомендация GB923. TM Forum, 2004.
4. Костин А. А., Ревелова З. Б., Николаева Е. В., Качество услуг связи глазами пользователей: ожидание и реальность // Первая Всероссийская конференция «Обеспечение качества телекоммуникационных услуг». Москва, 4–5 июля 2012 г. С. 23–24.
5. Business Performance Metrics Development Guide: Рекомендация BM1001. TM Forum, 2012.

Статья представлена научным руководителем,
доктором технических наук, профессором Костиным А. А.

УДК 004.4

А. В. Помогалова (студент группы ИКТ-405 СПбГУТ)

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

Многие студенты, только что поступившие в университет сталкиваются с такой проблемой, как учебное расписание академических групп. Проблему составляет его понимание, а также некоторое неудобство в ежедневном использовании, так как excel-файл в большей степени подходит для просмотра на стационарном компьютере или ноутбуке, в связи с чем просмотр расписания на телефоне может стать проблематичным из-за сравнительно небольшого размера экрана и мелкого шрифта, что приводит к необходимости создания картинок или других приспособлений для большего удобства. Учитывая все вышесказанное, напрашивается вывод, что мобильное приложение с возможностью представления его в виде виджета и выводом расписания на каждый день может решить проблему расписания у студентов.

расписание университета, мобильное приложение, Android, excel.

Для разработки такого программного продукта мы определили следующие задачи:

1) создать мобильное приложение на платформе Android, способное считывать и обрабатывать excel-файлы с расписанием академических групп для создания индивидуального расписания с перечнем занятий на каждый день;

2) разработать возможность представления приложения в виде виджета на одном из экранов смартфона;

3) учесть возможности редактирования предметов по индивидуальному желанию, такие как переименование, удаление/перенос учебного занятия на другой день/неделю.

На данный момент в Play Маркете содержится довольно большое количество приложений, специализированных на отображении расписания. При запросе в Play Маркете появляются приложения для адаптации расписания определенных университетов, таких как ГрГУ, МГТУ и т. д. Приложений адаптированных не для конкретного ВУЗа, меньше, но в топе находится приложение «Универ», предлагающее расписания всех университетов.

«Универ» предлагает найти свой университет, а также факультет, затем выбрать группу и загрузить расписание. Проблемы возникли уже при поиске нашего СПбГУТ – на выбор представлено два варианта нашего университета.

При выборе первого варианта не был найден факультет ИКСС, при выборе второго варианта был найден факультет ИКСС и группа ИКВТ-52, но выбрать группу было крайне проблематично – при нажатии на экран строка пропадала, а потом вновь появлялась. В итоге создать, отобразить расписание приложение так и не смогло. Также «минусом» является наличие или необходимость приобретения полной платной версии, чтобы иметь доступ ко всем функциям приложения.

Приложение «Расписашка» также предлагает загрузить расписание из сети, но в списке доступных университетов нет СПбГУТ.

Остальные приложения предлагают ввод расписания вручную, но на это тратится много времени и усилий.

Также в Play Маркете было найдено приложение SUT. В нем отражены основные события университета, правда, прошедшие, а также некоторая информация о жизни университета для иностранных студентов. Вся информация представлена на английском языке и отношения к расписанию для русскоязычных студентов не имеет.

Поэтому особенностью нашего приложения является то, что оно будет считывать расписание из excel-файла с сайта СПбГУТ, то есть специализировано именно под формат нашего университета, что должно помочь избежать трудностей и учесть все критерии и «подводные камни» расписания в нашем ВУЗе, а также минимизировать «ручные» действия над расписанием.

Проанализировав продукцию Play Маркета и выявив недостатки представленных приложений, мы пришли к выводу, что наше приложение должно включать в себя следующие функции:

- чтение excel-файлов;
- пользователю предлагается считать расписание из excel-файла, который он скачивает с сайта СПбГУТ, и указывает к нему путь в приложении;
- ввиду небольших ресурсов телефона для экономии памяти предлагаем пользователю самостоятельно выбрать файл, который он хочет преобразовать в нашем приложении.
- считывание названий предметов, времени, недель и аудиторий;
- уведомление на 16–17 неделях о приближении экзаменов, напоминание скачать расписание экзаменов (будут использоваться push-уведомления для большего привлечения внимания);
- составление и вывод расписания на каждый день, неделю, месяц, семестр;
- редактирование названий предметов и аудиторий пользователем;
- возможность переноса учебной дисциплины на другой день;
- возможность добавления дополнительной учебной дисциплины (факультатив, дополнительные занятия);
- графическое выделение цветом дисциплин (по желанию пользователя);
- отображение приложения в виде виджета;

Также нами был проведен опрос среди учащихся студентов СПбГУТ, который помог выявить наиболее популярную операционную систему мобильных телефонов студентов. В результате опроса была выбрана операционная система Android. После успешного тестирования и запуска продукта, приложение будет продублировано для системы IOS и Windows Phone.

Рис. 1. Используемая операционная система

Опрос показал, что наибольший процент студентов использует мобильные устройства на операционной системе Android (рис. 1), также большинство студентов просмотр расписания осуществляют с помощью телефонов (рис. 2), что в очередной раз показывает необходимость создания такого приложения.

Рис. 2. Устройство для просмотра расписания

Список используемых источников

1. Дейтел П., Дейтел Х., Дейтел Э., Моргано М. Android для программистов. Создаем приложения. СПб. : Питер, 2013. 560 с. ISBN: 978-5-459-01646-8.

2. Томас М., Пател П., Хадсон А., Болл Д. Секреты программирования для Internet на Java / пер. с англ. СПб. : Питер, 1997. 640 с. ISBN 5-887882-119-1.

Статья представлена научным руководителем,
старшим преподавателем Ермаковой Т. В.

УДК 535.92

С. С. Попова (студентка группы ИКТФ-51м СПБГУТ)

МЕТОДИКА РАСЧЕТА ДЛИНЫ РЕГЕНЕРАЦИОННОГО УЧАСТКА ВОЛС С КОМПЕНСАТОРАМИ ДИСПЕРСИИ

Хроматическая дисперсия является одним из основных факторов, ограничивающих длину регенерационного участка. В докладе рассмотрены методы компенсации хроматической дисперсии и предложены методики расчета длины регенерационного участка ВОЛС с компенсаторами дисперсии на основе специального волокна DCF и волоконной брэгговской решетки с переменным периодом.

длина регенерационного участка, хроматическая дисперсия, компенсация дисперсии, волокно для компенсации дисперсии, волоконная брэгговская решетка.

Известно, что длина регенерационного участка (РУ) волоконно-оптической линии связи (ВОЛС) может ограничиваться одним из двух факторов – затуханием и хроматической дисперсией. В [1] предлагаются выражения для расчета длин РУ l_{pe} и l_{pd}, ограниченных затуханием и хроматической дисперсией соответственно:

$$l_{pe}(\lambda) = \left(p_{out} - p_n - 2 \cdot a_p - a_d - a_{df} - a_{ez}\right) / \left(\alpha(\lambda) + a_n / l_{sd}\right), \quad (1)$$

$$l_{pd}(\lambda) = \frac{\pi \cdot c \cdot K^2 \cdot t_T^2}{2 \cdot \lambda^2 \cdot D(\lambda)} \cdot \sqrt{\frac{2 \cdot \left(K_1^2 - 1\right)}{2 + \left(\pi \cdot \Delta\nu \cdot K \cdot t_T\right)^2}}, \quad (2)$$

где p_{out} – уровень сигнала на выходе передатчика, p_n – уровень чувствительности приемника, a_p и a_n – средние потери в разъемном и неразъемном (сварном) соединении оптических волокон (ОВ) соответственно, a_d и a_{df} – дополнительные затухания, вызванные уширением импульса из-за хроматической дисперсии и АЧХ фотоприемного устройства, a_{ez} – энергетический запас, α и D – коэффициент затухания и хроматическая дисперсия стандартного ОВ, l_{sd} – строительная длина оптического кабеля, λ – длина волны, K – коэффициент, равный отношению ширины гауссовского импульса на выходе регенератора к ширине тактового интервала t_T, $\Delta\nu$ – ширина гауссовского спектра излучения источника на уровне $1/e$, c – скорость света в вакууме, K_1 – коэффициент, учитывающий допустимое дисперсионное расширение импульса и равный отношению ширины импульса на входе регенератора к ширине импульса на выходе регенератора.

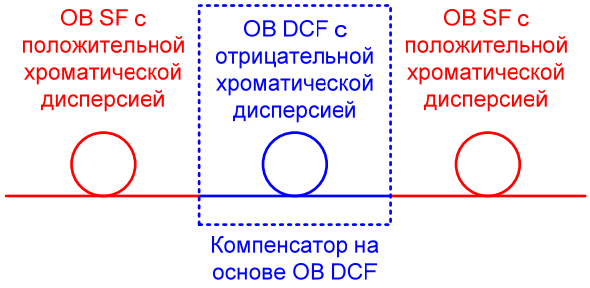
Результирующая длина РУ определяется по выражению:

$$l_p(\lambda) = \min\left[l_{pe}(\lambda), l_{pd}(\lambda)\right]. \quad (3)$$

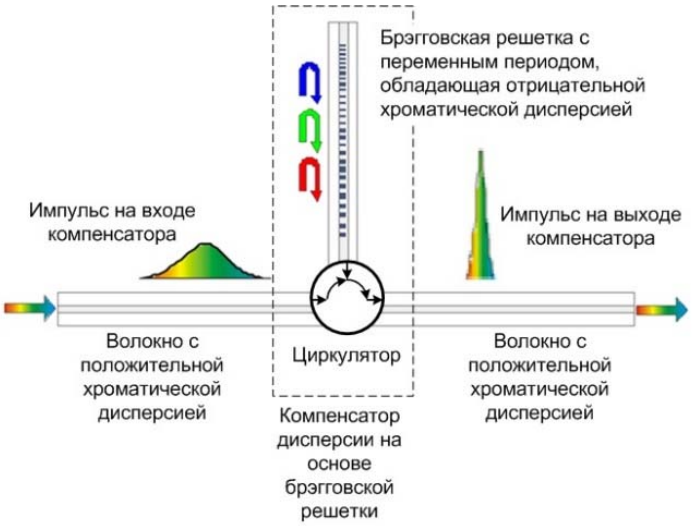
Если $l_{pd}(\lambda) < l_{pe}(\lambda)$, длина РУ ограничена хроматической дисперсией и ее можно увеличить путем компенсации дисперсии.

Компенсация хроматической дисперсии может осуществляться как оптическими, так и электронными методами. Наиболее часто применяется линейный оптический метод компенсации хроматической дисперсии, который заключается в том, что в ВОЛС между участками телекоммуникационного оптического волокна (ОВ) устанавливаются устройства, хроматическая дисперсия которых равна по величине и противоположна по знаку дисперсии предшествующего им участка телекоммуникационного ОВ. В большинстве случаев суммарная дисперсия ВОЛС в рабочем диапазоне длин волн положительна, поэтому для ее компенсации используются устройства с отрицательной дисперсией. В докладе рассмотрены два вида таких устройств – на основе специального ОВ для компенсации дисперсии (Dispersion Compensation Fiber, DCF) и на основе волоконной брэгговской дифракционной решетки (Fiber Bragg Grating, FBG) с переменным периодом.

Рассмотренные компенсаторы являются пассивными устройствами, могут включаться в ВОЛС как на оконечных пунктах, так и между ними, и осуществляют сосредоточенную компенсацию хроматической дисперсии. Схемы включения компенсаторов в ВОЛС представлены на рисунке 1.



а



б

Рис. 1. Схемы включения компенсаторов дисперсии на основе ОВ DCF (*а*) и FBG (*б*)

На рисунке 2 представлены зависимости коэффициента затухания α_{DCF} и хроматической дисперсии D_{DCF} ОВ DCF, предназначенного для компенсации хроматической дисперсии в стандартном ОВ, от длины волны λ [2]. Для проведения дальнейших расчетов была проведена аппроксимация $\alpha_{DCF}(\lambda)$ и $D_{DCF}(\lambda)$ следующими выражениями:

$$\alpha_{DCF}(\lambda) = \chi/\lambda^4 + g_{inf} \cdot \Delta\lambda_{inf} \Big/ \left(2 \cdot \pi \cdot \left[(\lambda - \lambda_{inf})^2 + (\Delta\lambda_{inf}/2)^2\right]\right), \quad (4)$$

$$D_{DCF}(\lambda) = S_0 \left(\lambda - \lambda_0^4/\lambda^3\right)/4. \quad (5)$$

Значения входящих в (1) и (2) параметров, полученных в результате аппроксимации, представлены в таблице 1.

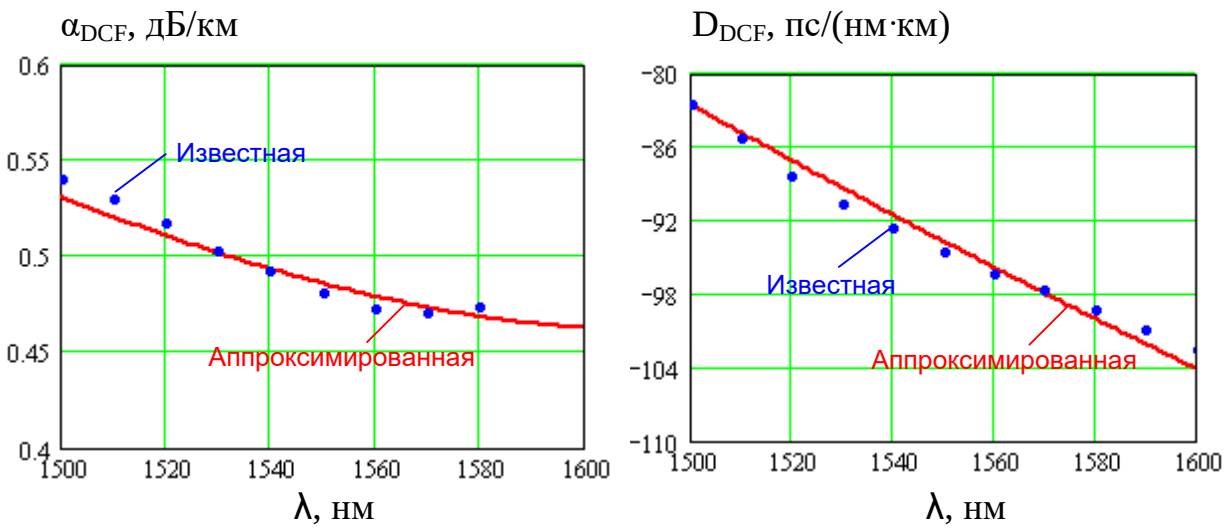


Рис. 2. Спектральные зависимости коэффициента затухания и хроматической дисперсии волокна DCF

ТАБЛИЦА 1. Параметры для расчета $\alpha_{DCF}(\lambda)$ и $D_{DCF}(\lambda)$

Параметр	Значение
Коэффициент релеевского рассеяния χ, дБ·мкм^4/км	2,469
Резонансная длина волны пика поглощения λ_{inf}, мкм	1,800
Ширина пика поглощения $\Delta\lambda_{inf}$, нм	1,0
Амплитуда пика поглощения g_{inf}, дБ·мкм/км	20
Длина волны нулевой хроматической дисперсии λ_0, мкм	1,100
Наклон дисперсионной характеристики S_0 на длине волны нулевой дисперсии, пс·нм^2/км	−0,39

FBG с переменным периодом также обладает отрицательной хроматической дисперсией. Период решетки должен меняться от Λ_{min} до Λ_{max}, которые определяются выражениями:

$$\Lambda_{min} = \frac{\lambda - \Delta\lambda/2}{2n_{eff}}, \quad \Lambda_{max} = \frac{\lambda + \Delta\lambda/2}{2n_{eff}}, \tag{6}$$

где n_{eff} – эффективный показатель преломления, $\Delta\lambda$ – ширина спектра оптического сигнала. Отрицательную хроматическую дисперсию D_G решетки можно рассчитать по выражению:

$$D_G = 2n_{eff} / \left(c \cdot \Delta\lambda_{chirp}\right), \tag{7}$$

где $\Delta\lambda_{chirp}$ – ширина диапазона, в котором работает решетка.

В ВОЛС без оптических усилителей полная компенсация хроматической дисперсии, при которой уширение импульса на выходе РУ равно ну-

лю, нецелесообразна, так как вносимые компенсатором потери приводят к уменьшению длины РУ по затуханию. В [3] предлагается считать оптимальным такой компенсатор, при установке которого длины регенерационных участков по дисперсии и затуханию будут одинаковыми.

При использовании оптимального компенсатора на основе ОВ DCF длину РУ и соответствующую длину компенсирующего ОВ можно рассчитать по выражениям:

$$l_p(\lambda)=\frac{A\cdot\alpha_{DCF}(\lambda)-B\cdot D_{DCF}(\lambda)}{D_{SF}(\lambda)\cdot\alpha_{DCF}(\lambda)-\left(\alpha_{SF}(\lambda)+\frac{a_n}{l_{sd}}\right)\cdot D_{DCF}(\lambda)}, \quad (8)$$

$$l_{DCF}=\frac{D_{SF}(\lambda)\cdot B-A\cdot\left(\alpha_{SF}(\lambda)+\frac{a_n}{l_{sd}}\right)}{D_{SF}(\lambda)\cdot\alpha_{DCF}(\lambda)-\left(\alpha_{SF}(\lambda)+\frac{a_{nc}}{l_{sd}}\right)\cdot D_{DCF}(\lambda)}, \quad (9)$$

где $A=\frac{\pi c K^2 t_T^2}{2\lambda^2}\sqrt{\frac{2\cdot\left(K_1^2-1\right)}{2+\left(\pi\Delta\nu K t_T\right)^2}}$, $B=p_{out}-p_n-2a_p-a_d-a_{df}-a_{ez}-2a_{nk}$,

α_{SF} и D_{SF} – коэффициент затухания и хроматическая дисперсия стандартного ОВ, a_{nk} – потери в соединении стандартного ОВ и ОВ DCF.

При использовании оптимального компенсатора на основе FBG длину РУ и соответствующую длину FBG можно рассчитать по выражению:

$$l_p(\lambda)=\frac{A\cdot\alpha_{SF}(\lambda)-B_1\cdot D_G(\lambda)}{D_{SF}(\lambda)\cdot\alpha_{SF}(\lambda)-\left(\alpha_{SF}(\lambda)+\frac{a_{nc}}{l_{sd}}\right)\cdot D_G(\lambda)}, \quad (10)$$

$$l_G=\frac{Lsf\cdot Dsf(\lambda)}{Dg(\lambda)}, \quad (11)$$

где $B_1=p_{out}-p_n-2a_p-a_d-a_{df}-a_{ez}-4a_{pk}-a_c$, a_{pk} – потери в соединениях между циркулятором и ОВ, a_c – потери в циркуляторе.

По выражениям (1)–(11) были проведены расчеты длин РУ без использования компенсации дисперсии и с использованием оптимальной компенсации и параметров компенсаторов дисперсии. Расчеты проведены при следующих параметрах: λ = 1550 нм, p_{out} = 10 дБм, l_{sd} = 6 км, a_p = 0,2 дБ, a_n = 0,05 дБ, a_{nk} = 0,8 дБ, a_{ez} = 3 дБ, a_d = 0,67 дБ, a_{df} = 0,67 дБ, K = 0,55, K_1 = 1,17, a_{pk} = 0,2 дБ, a_c =1 дБ, n_{eff} = 1,44. Значения p_n для различных систем передачи приведены в таблице 2. Результаты расчетов представлены в таблице 3.

ТАБЛИЦА 2. Значения чувствительности фотоприемных устройств

Система передачи	**STM-1**	**STM-4**	**STM-16**	**STM-64**
Скорость передачи, Гбит/с	0,155	0,622	2,5	10
p_n, дБм	−34	−28	−24,5	−21

ТАБЛИЦА 3. Результаты расчета длины регенерационного участка при использовании DCF волокна

Ширина спектра источника Δν, ГГц	Система передачи	Параметры компенсаторов		Длина регенерационного участка, км		
		на основе DCF	на основе FBG			
		Длина ОВ DCF, км	Длина FBG, мм	Без компенсации	С компенсатором на основе DCF	С компенсатором на основе FBG
100	STM-1	9,2	244,79	88,1	135,6	164,06
	STM-4	16,1	205,58	22,0	105,0	137,78
	STM-16	16,6	182,76	5,5	89,5	122,45
	STM-64	15,1	160,63	1,4	77,0	107,12
10	STM-1	0	0	179,5	Компенсация не нужна	
	STM-4	0	0	152,1	Компенсация не нужна	
	STM-16	8,8	18,83	53,5	99,1	122,45
	STM-64	13,6	22,6	10,6	80,5	107,12
1	STM-1	0	0	179,5	Компенсация не нужна	
	STM-4	0	0	152,1	Компенсация не нужна	
	STM-16	0	0	136,1	Компенсация не нужна	
	STM-64	12,6	16,06	16,6	81,5	107,12

По результатам расчетов можно сделать следующие выводы: 1) с увеличением ширины спектра излучения источника и скорости передачи длина РУ уменьшается; 2) использование компенсаторов дисперсии позволяет существенно увеличить длину регенерационного участка; 3) при компенсации дисперсии в узком диапазоне длин волн эффективность компенсаторов на основе FBG выше, чем компенсаторов на основе ОВ DCF.

Список используемых источников

1. Глаголев С. Ф. Особенности проектирования современных высокоскоростных волоконно-оптических линий передачи // Фотон-экспресс. 2006. № 6.

2. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М. : ЛЕСА*арт*, 2003. 288 с.

3. Былина М. С., Глаголев С. Ф., Кузнецова Н. С., Рык О. Н. Компенсация дисперсии в оптических линейных трактах с использованием DWDM // Фотон-Экспресс. 2009. № 7.

Статья представлена научным руководителем кандидатом технических наук, доцентом Былиной М. С.

УДК 004.315.5

Д. И. Похлупнёв (студент группы ИКТО-31, СПбГУТ)
М. Н. Халилов (студент группы ИКТО-31, СПбГУТ)

СИНТЕЗ УМНОЖИТЕЛЯ НА БАЗЕ ПЛИС CYCLONE V ALTERA

В представляемой работе произведена разработка схемы 4-разрядного умножителя, с использованием языка VHDL. Все операнды сохраняются в двухбуферных регистрах, управление считыванием и записью осуществляется изменением состояний конечного автомата, частота работы которого согласована с задержками распространения сигнала в КЦУ. Реализация осуществляется на базе ПЛИС Cyclone V фирмы Altera.

синтез умножителя, ПЛИС Cyclone V.

Комплект разработчика DE1-SoC представляет собой надежную платформу разработки аппаратных средств, построенную на системе Altera на кристалле (SoC) FPGA, который сочетает в себе последний двухъядерный Cortex-A9. Плата разработки DE1-SoC включает в себя аппаратные средства, такие как, например, высокоскоростная память DDR3, видео и аудио возможности, создание сетей Ethernet, и многое другое [1, с. 3].

Представляемая работа предназначена для лабораторных занятий студентов по изучению синтеза вычислительных схем. В проекте произведена разработка схемы 4-разрядного умножителя, с использованием языка VHDL. Все операнды сохраняются в двухбуферных регистрах, управление считыванием и записью осуществляется изменением состояний конечного автомата, частота работы которого согласована с задержками распространения сигнала в КЦУ. Реализация осуществляется на базе ПЛИС Cyclone V фирмы Altera. Результат вычислений выводится на светодиоды в виде шестнадцатеричного числа.

Алгоритм разработки проекта.

Структурная схема реализуемого проекта представлена на рисунке 1.

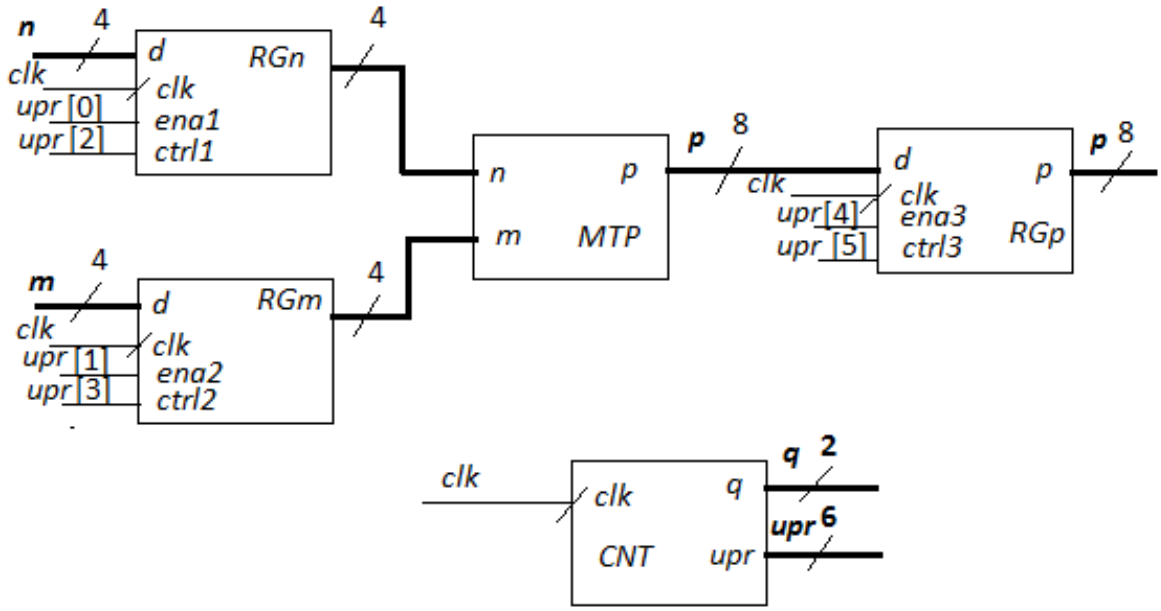


Рис. 1. Структурная схема проекта

1. Записываем два 4-разрядных двоичных числа «*n*» и «*m*» в соответствующие регистры.

```
if(rising_edge(clk_i)) then
if(ena ='1') then
regist <= data_i;
end if;
end if;
end process;
data_out <= regist when ctrl = '1' else "ZZZZ";
```

2. Перемножаем два введённых числа. Реализация происходит путём поразрядного логического перемножения первого числа на второе, и поэтапного сложения результатов этого умножения. Сначала получаем сумму результатов умножения множимого на 0-й и 1-й разряды множителя, затем эту сумму складываем с результатом умножения на 2-й разряд множителя, т. о. для 4-разрядных чисел имеем 16 символов результата умножения и три сложения.

3. Управление записью и считыванием осуществляется с помощью изменений состояний конечного автомата (в данном случае, двухразрядный счётчик). Формирование сигналов управления представлено в таблице 1.

ТАБЛИЦА 1. Сигналы управления записью и считыванием

upr[5..0]	*ctrl*3	*ena*3	*ctrl*2	*ena*2	*ctrl*1	*ena*1
	5	4	3	2	1	0
0 0	1	0	0	0	0	1
0 1	0	0	0	1	0	0
1 0	0	1	1	0	1	0
1 1	1	0	0	0	0	0

```
if (res = '0') then cnt<=(others=>'0');
elsif(rising_edge(clk)) then
if(ena ='1') then
cnt <=cnt + "01";
...
case cnt is
when "00"=>upr<="100001";
when "01"=>upr<="000100";
when "10"=>upr<="011010";
when "11"=>upr<="100000";
end case;
```

4. В программе *Quartus* 15 реализован модуль симуляции распространения задержки (*TimeQuest*). Этот компонент помогает оценить работу устройства в реальных условиях, т. е. задержки распространения сигнала в КЦУ.

Использованы две модели – *slow* и *fast*. Исследована их работа при максимальной температуре – 85 °*C*.

Максимальная задержка между портами при использовании *slow* модели составляет 6,283 нс. Соответственно, частота работы конечного автомата в данном случае составляет 159 МГц. При использовании *fast* модели максимальная задержка между портами составляет 10,056 нс. Частота работы конечного автомата в данном случае составляет 99 МГц.

5. Далее информация поступает в буферный регистр, который так же как и рассматриваемые до этого регистры имеет дополнительные входы для разрешения подключения входов или выходов к шине данных. Управление всеми процессами осуществляется изменением состояний конечного автомата.

6. После сохранения в регистре вычисленное произведение двух чисел в двоичном виде поступает на декодеры. Всего декодеров два: первый работает с разрядами с 0 по 3, второй – с 4 по 7. Каждый из декодеров двоичное число представляет в виде 7-разрядной двоичной последовательности, которая представляет собой фактически команды – зажигать соответствующий сегмент светодиода или нет (рис. 2).

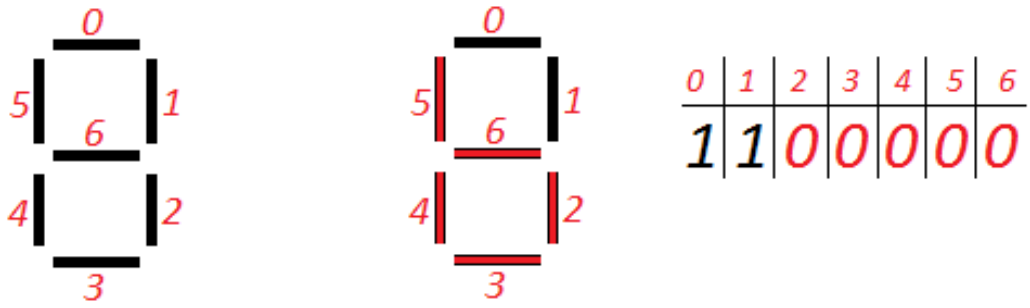


Рис. 2. Отображение чисел на светодиодах

7. Результат работы проекта проверяем с помощью редактора временных диаграмм [2, с. 3–12]. Как видно из результатов симуляции на рисунке 3 управление процессом умножения происходит в соответствии с описанными выше шагами.

Полученный в результате работы проекта результат является верным: перемножение чисел 1101 и 1111 даёт 11000011.

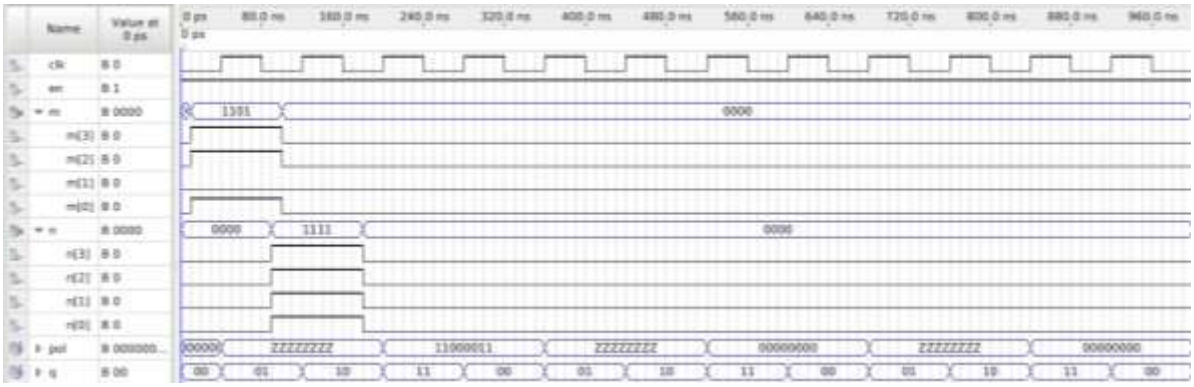


Рис. 3. Результат работы редактора временных диаграмм

Для того, чтобы представить вычисленное произведение на светодиодах требуется также выполнить дополнительные шаги, помимо сборки непосредственно проекта.

1) Необходимо выполнить распиновку входов и выходов (каждого сегмента задействованного светодиода).

2) Конфигурирование ПЛИС в режиме JTAG. В цепи JTAG есть два устройства: HPS и FPGA. В FPGA загружается наша конфигурация. При запуске данной конфигурации выбранное устройство готово к работе.

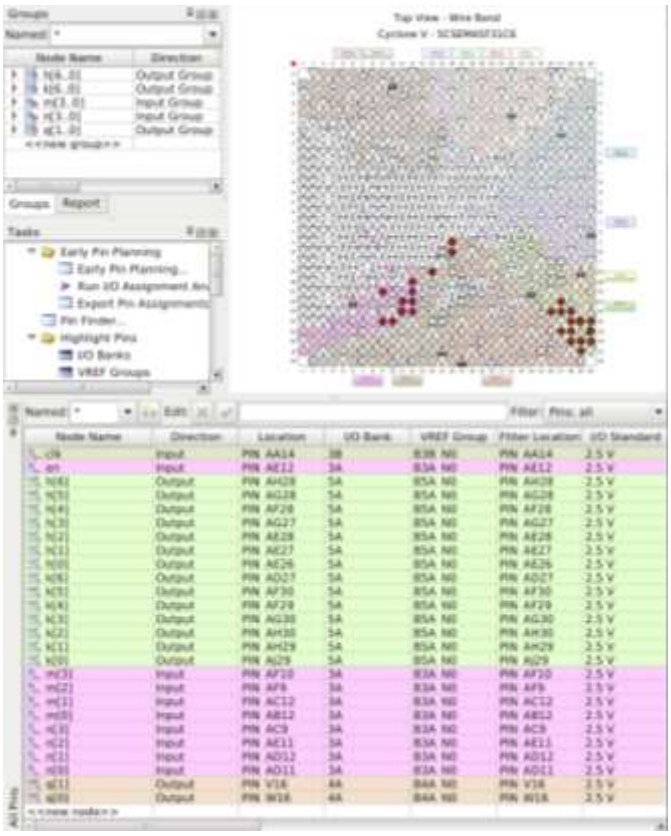


Рис. 4. Окно вкладки Pin Planner

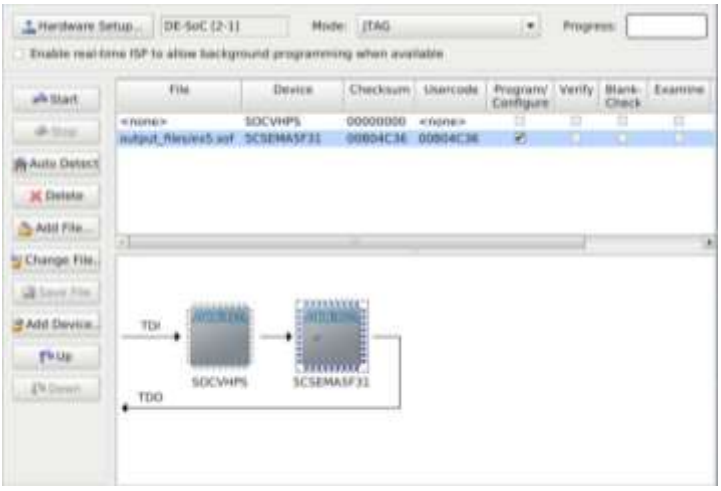


Рис. 5. Окно вкладки Programmer

Таким образом, поставленная цель работы – разработка двоичного умножителя 4-разрядных чисел – выполнена. При реализации данного проекта была рассмотрена работа на базе ПЛИС Cyclone V фирмы Altera в среде VHDL. Были освоены и проанализированы возможности нового ПО – Quartus 15.0, такие как обновлённый модуль анализа временных диаграмм работы устройства, модуль, симулирующий работу устройства в реальных условиях (наличие временных задержек).

Список используемых источников

1. Terasic DE1-SoC User Manual, 2013. p. 109.
2. Introduction to Simulation of VHDL Designs, 2015. p. 26.

Статья представлена научным руководителем,
старшим преподавателем Нееловой О. Л.

УДК 654.739

Э. О. Самсонов (студент группы МФО-21, СПбГУТ)

РАЗРАБОТКА УЧЕБНО-ЛАБОРАТОРНОГО МОДУЛЯ ДЛЯ ИССЛЕДОВАНИЯ СПЕКТРОВ ПОЛУПРОВОДНИКОВЫХ ИСТОЧНИКОВ ИЗЛУЧЕНИЯ

Полупроводниковые источники излучения используются для волоконно-оптических систем передачи (ВОСП) в составе передающих устройств, а также в качестве элементов приборов для измерения параметров оптических волокон (ОВ), пассивных и активных компонентов линейных трактов волоконно-оптических линий связи (ВОЛС). Спектральные свойства излучателя существенно влияют на характеристики оптических систем. Имея учебно-исследовательское оборудование для анализа оптического спектра, можно проводить измерения спектров излучателей, изучать эволюцию спектра, а также демонстрировать студентам принципы работы и возможные конструкции спектральных приборов.

спектрометрия, волоконно-оптические системы передачи, полупроводниковые источники излучения, оптическое волокно.

В оптической связи наиболее распространены лазерные и светоизлучающие диоды; практический интерес представляет изучение спектральных характеристик данных излучателей, а также эволюции их спектра от тока накачки. Известно, что с увеличением тока накачки изменяется ширина спектра и смещается центральная длина волны. Лазерные диоды при работе ниже порога генерируют спонтанное излучение и ведут себя как светоизлучающие диоды. Когда ток накачки достигает порогового значения, ЛД переходит в режим генерации, испускаемое излучение сильно сужается по ширине спектра, и по пространственной расходимости. С увеличением тока спектр уширяется и сдвигается центральная длина волны из-за повышения температуры *p-n* перехода. Эволюцию ширины спектра лазерного диода можно наблюдать на рисунке 1.

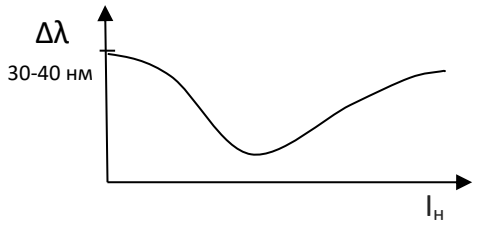


Рис. 1. Эволюция ширины спектра лазерного диода
с увеличением тока накачки

Для практического изучения спектров необходимо иметь специализированное оборудование, которое позволит наглядно демонстрировать принцип работы спектрального прибора. Серийные приборы не позволяют наблюдать процесс измерения и имеют высокую стоимость, поэтому целесообразно разработать и собрать специализированный спектроскоп, удовлетворяющий учебно-демонстрационным целям.

Так как разрабатываемая установка предназначена для учебно-демонстрационных целей, к установке и ее узлам предъявляются некоторые специфические требования, одно из которых – наглядность принципов работы; физические процессы, протекающие при измерении, также должны быть наглядными. Схемы, узлы и компоненты спектроскопа должны быть простыми и доступными.

При выборе схемы установки предпочтительнее спектроскоп, а не монохроматор, он позволяет визуально наблюдать весь спектр и его эволюцию.

Анализ показал, что для типичных полупроводниковых излучателей целесообразно использовать дифракционный решеточный спектроскоп. Призменный спектроскоп имеет недостаточное разрешение, а интерферометр Фабри – Перо малую область сканирования. Решёточный спектроскоп с решёткой 600 штрихов на миллиметр, при размере засвеченной пучком области 1,122 мм, в первом порядке обеспечивает разрешающую способность решетки $Rrr = 762$, для $\lambda = 850$ нм. Спектральный интервал $\Delta\lambda$, который можно разрешить с помощью данного спектроскопа:

$$\Delta\lambda = \frac{\lambda}{R_{rr}} = 1{,}115 \text{ нм}.$$

Оптическая схема модуля показана на рисунке 2. Здесь *1* – источник излучения; *2* – оптическое волокно; *3* – торец оптического волокна; *4* – линза-коллиматор f_1 = 10 мм; 5 – дифракционная решетка; 6 – фокусирующая линза f_2 = 150 мм; *7* – ФПУ (WEB-камера); *8* – ПК.

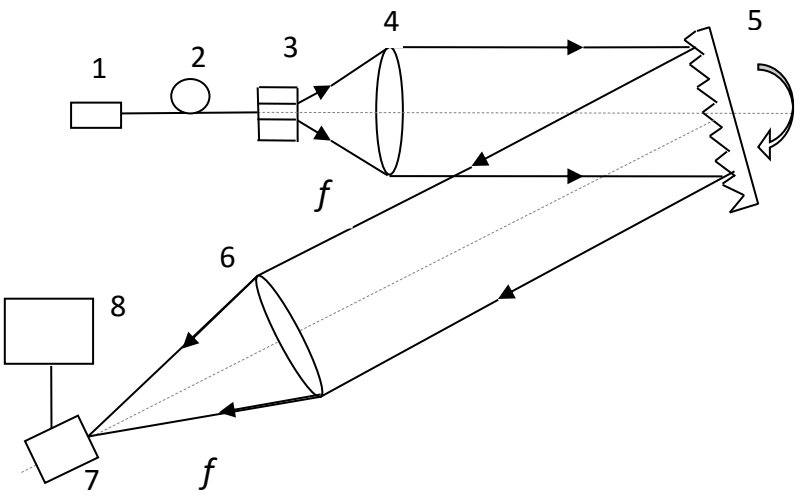


Рис. 2. Схема учебно-лабораторного модуля

Эксперименты показали, что при использовании многомодового волокна, вследствие интерференции мод, появляется спекл-картина. Наличие спекл-картины вызывает искажение измеренной формы спектральной линии и затрудняет интерпретацию результатов измерения спектра. Кроме того, из-за большего диаметра сердцевины волокна, т. е. большего диаметра входной щели D_1, ширина аппаратной функции прибора будет больше, что уменьшит разрешающую способность.

Если же в качестве входной щели использовать торец одномодового оптического волокна, типичный размер изображения $D_1 \geq 2a \approx 10$ мкм, что соизмеримо с длиной волны излучения. В этом случае использование геометрической оптики некорректно. Необходимо рассматривать поток излучения от торца оптического волокна как гауссов пучок.

Необходимо определить диаметр перетяжки пучка на выходе схемы, изображенной на рисунке 3, в том месте, где должна быть установлена WEB-камера.

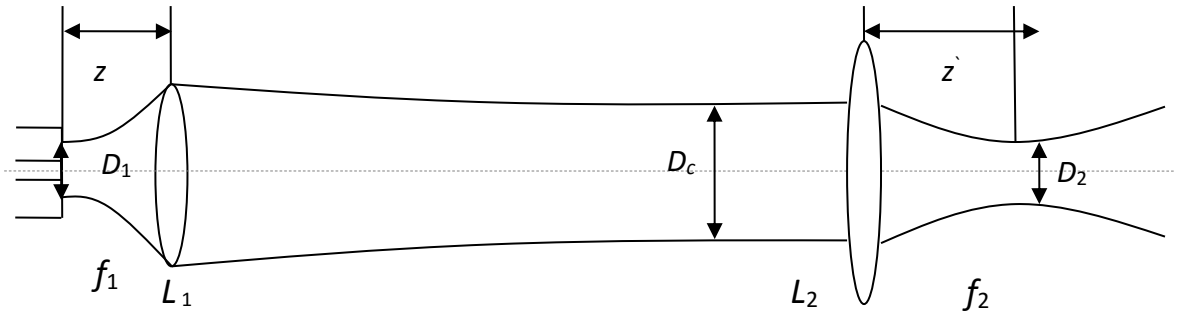


Рис. 3. Прохождение Гауссового пучка через систему линз

Источник излучения ЛД, $\lambda_0 = 659$ нм; фокусное расстояние линзы-коллиматора $f_1 = 10$ мм; фокусное расстояние фокусирующей линзы

f_2 = 150 мм; z – расстояния от перетяжки пучка (торца ОВ) до линзы L_1; z – расстояния от линзы L_2 до перетяжки выходящего пучка.

Диаметр перетяжки пучка D_1 равен диаметру модового поля $2w_0$ входного волокна (1), который рассчитывается по формуле Маркузе [1].

$$2w_0 = 2\alpha\left[0{,}65 + 0{,}434\left(\frac{\lambda}{\lambda_c}\right)^{\frac{3}{2}} + 0{,}0149\left(\frac{\lambda}{\lambda_c}\right)^{6}\right] = 7{,}283 \text{ мкм}, \qquad (1)$$

где $2a$ – диаметр сердцевины одномодового волокна, 9 мкм; λ – длина волны излучения, 659 нм; λ_c – длина волны отсечки, 1270 нм.

Для λ = 659 нм диаметр перетяжки (2) коллимированного пучка D_c рассчитывается по формулам, описывающим прохождение Гауссового пучка через линзу [2].

$$2w_0^{`} = D_c = M2w_0 = 1{,}123 \text{ мм}, \qquad (2)$$

где M – увеличение линзы.

Диаметр перетяжки на выходе оптической схемы:

$$D_2 = M_2 2w_0^{`} = 0{,}110 \text{ мм}.$$

На рисунках 4*а* и 4*б* фотографии нулевого и первого порядка, полученные с помощью данного спектроскопа, в котором излучение вводится в одномодовое волокно. Источник излучения ЛД, λ_0 = 659 нм.

а *б*

Рис. 4. *а* – нулевой порядок;
б – первый порядок, источник излучения ЛД, λ_0 = 659 нм

$D_t = D_2$ = 0,110 мм диаметр пятна нулевого порядка в фокусе линзы L_2, теоретически рассчитанный. На матрице камеры размер пятна равен D_p = 0,105 мм, что хорошо совпадает с теоретическим расчетом.

Проведенные расчеты и эксперименты показали, что использование решеточной схемы и выбор параметров оптических элементов в соответствии с расчетом позволяют наблюдать и регистрировать изображения

спектров реальных излучателей, и наблюдаемые характеристики полученных изображений хорошо совпадают с предсказанными по расчетам.

При сборке и настройке макета спектроскопа были проведены измерения и исследования спектров нескольких полупроводниковых излучателей различных типов, отобранных для использования в лабораторной установке. Нулевой и первый порядок спектра лазерного диода, работающего на длине волны λ_0 = 659 нм изображены на рисунках 4*а* и 4*б*. На рисунках 5*а* и 5*б* изображены нулевой и первый порядок спектра лазерного диода *LDI H-V*, работающего на длине волны λ_0 = 857,5 нм.

а б

Рис. 5. *а* – нулевой порядок,
б – первый порядок, источник излучения *LDI H-V*

Развитие вынужденного излучения в используемом лазерном диоде по мере повышения тока накачки можно наблюдать на рисунках 6*а*, 6*б*, 6*в*.

а *б* *в*

Рис. 6. Первый порядок, излучатель – лазерный диод *LDI H-V*:
а – I_n = 2 мА, *б* – I_n = 4 мА, *в* – I_n = 10 мА

Когда ток накачки I_n = 2 мА меньше порогового I_p = 3,9 мА, наблюдается самый широкий спектр (рис. 6*а*), при токе немного больше порогового I_n = 4 мА спектр максимально узкий (рис. 6*б*), когда ток намного выше порогового I_n = 10 мА, спектр снова уширяется, что заметно на рисунке 6*в*.

Таким образом, с помощью разработанной лабораторной установки получены изображения спектров полупроводниковых лазеров и светоизлучающего диода. При использовании специализированного ПО, может быть практически измерена ширина спектра исследуемых излучателей.

Учебно-исследовательская установка демонстрирует конструкцию действующей модели решеточного спектроскопа, наглядно показывает физические процессы, протекающие при измерении спектра, позволяет визуально наблюдать спектры полупроводникового и лазерного диода, дает

возможность измерять ширину спектра лазерного диода и наблюдать его эволюцию.

Установка будет полезна для изучающих волоконно-оптические системы передачи, методы контроля волоконно-оптических компонентов, оптические измерительные системы. Она позволяет ознакомить студентов со спектральными характеристиками полупроводниковых излучателей, дает возможность самостоятельно измерить ширину спектра, наглядно демонстрирует работу спектрального прибора.

Список используемых источников

1. Кауфман М., Сидман А. Практическое руководство по расчетам схем в электронике : справочник. В 2-х т. Т. 1. : пер. с англ. / под ред. Ф. Н. Покровского. М. : Энергоатомиздат, 1993. 368 с.

2. Салех Б., Тейх М. Оптика и фотоника. Принципы и применения: учебное пособие. В 2 т. Т. 1 / пер. с англ. Долгопрудный : Издательский Дом «Интеллект», 2012. 760 с. ISBN 978-5-91559-038-9.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Астаховым А. В.

УДК 004.457

С. Д. Смаль (студент группы ИКТЗ-23, СПбГУТ)

АНАЛИЗ И ОБНАРУЖЕНИЕ УЯЗВИМОСТИ ВЫПОЛНЕНИЯ ПРОИЗВОЛЬНОГО КОДА SHELLSHOCK

В данной статье рассматривается уязвимость в командном интерпретаторе bash, который используется по умолчанию в большинстве UNIX-систем. В статье описываются технические детали уязвимости, векторы, используя которые злоумышленники могут осуществить атаку на целевую систему, а также приведены результаты сканирование хоста в локальной сети на наличие уязвимости. Также приводятся меры по устранению уязвимости и приведены результат повторного сканирование хоста для проверки эффективности предпринятых мер безопасности.

уязвимости, Shellshock, bash, обнаружение уязвимостей, анализ защищённости, информационная безопасность.

Проблема поиска и устранения уязвимостей берёт начало с момента появления программно-аппаратного обеспечения. За всё время их существования уязвимости были найдены во всех основных операционных системах и многих приложениях. С каждым годом специалисты по информационной безопасности непрерывно обнаруживают всё новые уязвимости.

24 сентября 2014 г. в командной оболочке bash специалистом по Unix и Linux Стэфаном Чазеласом была найдена критическая уязвимость, получившая впоследствии название Shellshock. Впервые информацию об уязвимости опубликовали 25 сентября 2014 г. Уязвимости был присвоен самый высокий уровень опасности 10 из 10. Такую высокую оценку данной уязвимости присвоили за счёт лёгкой эксплуатации уязвимости и за отсутствие необходимости аутентификации для использования bash с помощью скриптов.

Приложения и сетевые устройства, которые используют bash в качестве командного интерпретатора, включают в себя маршрутизаторы, ip-камеры, домашние роутеры, серверы печати и даже смартфоны. Широкая распространённость командной оболочки bash позволяет говорить об огромном количестве потенциально уязвимых систем. Угрозе подвержены все версии bash включительно до версии bash-4.3. Уязвимость позволяет удаленному пользователю выполнить произвольный код на целевой системе.

Данная статья ставит перед собой цель описать уязвимость Shellshock, рассмотреть технические детали этой уязвимости, указать основные векторы атаки, которые могут использовать злоумышленники, обнаружить на практике данную уязвимость, указать меры по устранению данной уязвимости с последующим повторным сканированием для проверки эффективности предпринятых мер безопасности.

Рассмотрим причину, по которой возникает уязвимость Shellshock. Как упоминалось ранее, bash является командной оболочкой в Unix-подобных операционных системах. В Unix-системах, каждый процесс имеет своё информационное пространство. В этом пространстве можно задавать переменные окружения. В них хранится: информация о текущем пользователе, положение конфигурационных файлов, требуемые параметры интерфейса и другие параметры. Согласно [1] в Unix дочерний процесс создаётся как точная копия родительского, поэтому его окружение – также точная копия родительского. При запуске новых экземпляров bash из существующего bash происходит передача значений существующих переменных окружения и определений функций в порождаемый процесс. Уязвимость Shellshock связана с некорректной обработкой переменных окружения и определений функций. Уязвимость возникает по причине того, что после обработки определения функции оболочка не останавливается, а продолжает обрабатывать команды после определения функции, что позволяет осуществить атаку с внедрением кода. Как указано в [2] в качестве примера можно привести код, позволяющий проверить наличие этой уязвимости: *“env x='() { :;}; echo vulnerable' bash -c 'echo this is a test' “*. Если система подвержена уязвимости, то bash возвращает в консоли “ *vulnerable this is a test* “ как показано на рисунке 1.

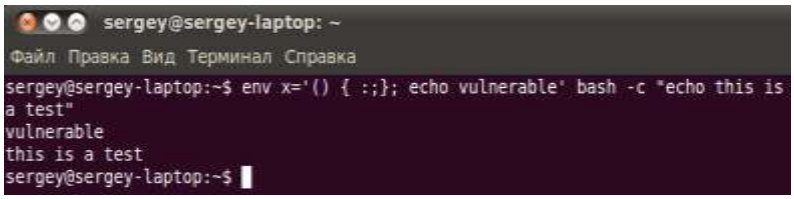


Рис. 1. Демонстрация наличия уязвимости Shellshock

Таким образом, уязвимость Shellshock позволяет организовать выполнение кода в контексте другого сеанса bash.

Как уже упоминалось, уязвимость позволяет удалённому пользователю выполнить произвольный код на целевой системе, тем самым компрометирую систему. Потенциально в качестве цели для атаки может быть выбрано любое приложение, которое запускает bash. Основные векторы атаки, которыми могу воспользоваться злоумышленники для эксплуатации этой уязвимости, изображены на рисунке 2.

Рис. 2. Векторы атаки, использующиеся злоумышленниками

Как описано в [3] веб-сервера, исполняющие CGI-скрипты передают подробности о пользовательском запросе через переменные окружения, например *HTTP_USER_AGENT*. Если запрос обрабатывается программой bash, либо другой программой, которая внутри себя вызывает bash, то атакующий может подменить передаваемую по http строку User-Agent добавив свои собственные команды. Например, злоумышленник может отправить вместе с запросом на веб-сервер следующую строку: () {:; }; */bin/cat /etc/passwd*. Это приведёт к тому, что содержимое файла */etc/passwd*, хранящегося на сервере и содержащего имена пользователей системы, будет отображено на экране злоумышленника как часть запрашиваемой им веб-страницы сервера

Популярным вектором атаки является атака на клиента DHCP-сервера. При обычном взаимодействии клиента и сервера DHCP-клиент запрашивает у DHCP-сервера сетевые настройки, такие как ip-адрес, маску подсети, шлюз по умолчанию и другие. Однако DHCP-сервер вместе с основными сетевыми настройками может отправить дополнительные параметры, которые клиент сохранит в переменных окружения. Злоумышленник может настроить на своей локальной машине DHCP-сервер, и перехватывать запросы клиентов к настоящему DHCP-серверу. Как указано

в [4] необходимо установить в качестве значения дополнительной опции DHCP-сервера строку вида: () {:;} *echo 'test'*. В итоге DHCP-клиент при запросе сетевых параметров DHCP-сервера получит вместе с необходимыми полями ещё и вредоносный код и выполнит его с правами суперпользователя, так как DHCP-клиент в большинстве систем работает с правами *root*.

Ещё одним вектором для атаки является атака на SSH-сервер. SSH-сервер позволяет ограничивать пользователя ограниченным набором доступных команд. Так называемая опция «ForceCommand». Фиксированная команда исполняется даже если пользователь запросил исполнение иной команды. Как описано в [5] запрошенная команда в этом случае сохраняется в переменной среды «*SSH_ORIGINAL_COMMAND*». Если фиксированная команда исполняется в интерпретаторе bash, то bash обнаружит заложенные в среду значения *SSH_ORIGINAL_COMMAND* при запуске, и, исполнит встроенные туда команды. Таким образом атакующий с доступом лишь к ограниченной оболочке получает неограниченный доступ.

Для анализа защищённости компьютеров в сети и установленных на них программного обеспечения, используют сканеры уязвимостей. Сканеры уязвимости представляют собой специальные программные или аппаратные средства, осуществляющие сканирование сети, компьютеров или программ, установленных на них, на предмет выявления возможных проблем в системе безопасности. Одним из популярных сканеров уязвимостей является OpenVAS. Он используется ФСТЭК в качестве средства для анализа защищённости систем. В статье приводится результаты сканирования системы с помощью сканера безопасности OpenVAS на наличие уязвимости Shellshock. При проведении сканирования использовался хост с операционной системой Ubuntu 14.04 LTS с предварительно установленным сканером уязвимостей OpenVAS, объектом сканирования является хост с операционной системой Ubuntu 10.04 LTS, подверженный уязвимости Shellshock.

В результате сканирования хоста были выявлены многочисленные проблемы в безопасности системы. На рисунке 3 изображен отчёт обо всех найденных уязвимостях с классификацией уязвимостей в соответствии с их уровнем опасности.

Рис. 3. Отчёт о найденных уязвимостях

В результате сканирования было обнаружено 102 критических уязвимостей. Среди обнаруженных критических уязвимостей наибольшую опасность представляет уязвимость Shellshock. Уязвимости Shellshock присвоен наивысший уровень опасности 10 из 10. Найденные уязвимости командной оболочки *bash* изображены на рисунке 4.

Vulnerability	Severity	QoD	Host	Location	Actions
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 02	10.0 (High)	75%	192.168.3.30 (sergey-laptop.linux.lan)	general/tcp	
GNU Bash Stacked Redirects aka 'redir_stack' Memory Corruption Vulnerability (LSC)	10.0 (High)	75%	192.168.3.30 (sergey-laptop.linux.lan)	general/tcp	
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 03	10.0 (High)	75%	192.168.3.30 (sergey-laptop.linux.lan)	general/tcp	
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC) - 04	10.0 (High)	75%	192.168.3.30 (sergey-laptop.linux.lan)	general/tcp	
GNU Bash Environment Variable Handling Shell RCE Vulnerability (LSC)	10.0 (High)	75%	192.168.3.30 (sergey-laptop.linux.lan)	general/tcp	

Рис. 4. Найденные критические уязвимости

Самый простой способ устранить уязвимость Shellshock – с помощью менеджера пакетов обновить версию bash.

В результате повторного сканирования системы после обновления версии командной оболочки bash уязвимость Shellshock не обнаружена, что подтверждает эффективность предпринятых мер по обеспечению безопасности. Результаты повторного сканирования системы отображены на рисунке 6.

Рис. 6. Результаты сканирования хоста после обновления версии *bash*

Уязвимость Shellshock затронула огромное количество устройств, использующих командную оболочку bash. Для данной уязвимости не существует более быстрого и надёжного способа её устранения, кроме установки обновления от производителя. Ещё многие годы специалисты будут находить системы подверженные этой уязвимости. Особо уязвимыми остаются оффлайн системы, не имеющие возможности обновления, и встраиваемые системы, для некоторых из которых вообще не будет никаких новых прошивок.

Список используемых источников

1. Введение в администрирование UNIX [Электронный ресурс]. URL: http://heap.altlinux.org/modules/unix_base_admin.dralex/ch01s02.html (дата обращения 29.06.2016).
2. Компрометация системы в bash [Электронный ресурс]. URL: http://www.securitylab.ru/vulnerability/458762.php (дата обращения 29.06.2016).
3. Bashdoor [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Bashdoor (дата обращения 29.06.2016).
4. Shellshock DHCP RCE Proof of Concept [Электронный ресурс]. URL: https://www.trustedsec.com/september-2014/shellshock-dhcp-rce-proof-concept/ (дата обращения 29.06.2016).
5. How can shellshock be exploited over SSH? [Электронный ресурс]. URL: http://unix.stackexchange.com/questions/157477/how-can-shellshock-be-exploited-over-ssh (дата обращения 29.06.2016).

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Юркиным Д. В.

УДК 004.057.4

А. Н. Фадеев (аспирант, МТУСИ)

ОРГАНИЗАЦИЯ РЕТРАНСЛЯЦИИ ДАННЫХ В ОВЧ ЛПД РЕЖИМА 4

Статья посвящена актуальной на сегодняшний день проблеме организации управления воздушного движения (УВД), вызванной бурным ростом количества летательных аппаратов (ЛА), включая легкие и беспилотные ЛА и несовершенством существующих систем УВД. Как один из вариантов решения данной проблемы рассмотрена предлагаемая Минтрансом РФ система АЗН-В ОВЧ линия передачи данных (ОВЧ ЛПД) режима 4 (VDL mode 4) и её основные характеристики и уровни. Подробно описаны подуровни VDL mode 4, в рамках которых будет работать данный протокол. Описаны типы сообщений протокола согласования частот, которые будут использоваться протоколом, и показано, что для передачи этих сообщений достаточно коротких процедуры передачи на подуровне DLS. Перечислены плюсы и минусы применения данного протокола.

АЗН-В, VDL mode 4, ретрансляция.

В последние годы в авиации наблюдается интенсивный рост летательных аппаратов (ЛА) во всем мире, вызванный массовым распространением легких, сверхлегких и беспилотных ЛА. Согласно прогнозу Федерального управления гражданской авиации США продажи БПЛА только на территории США к 2020 г. возрастут до 7 миллионов в год [1]. Учиты-

вая то, что разработкой этих ЛА занимаются в основном частные компании, а использование легких и сверхлегких ЛА в части авиации общего назначения не требует получения сертификата, тенденция к росту будет сохраняться.

Исторически сложилось так, что речевая коммуникация для управления воздушным движением является устойчивым видом связи и используется до сих пор, несмотря на то, что ещё в 1980-х гг. стали очевидны ограничения существующих систем связи, навигации и наблюдения (*communications, navigation and surveillance* (CNS)) связанные с распространением радиосигналов, вызванные трудностями с внедрением и обеспечением эксплуатации систем CNS, обусловленные использованием речевой связи «воздух-земля» и отсутствием обмена цифровыми данными которые обеспечивали бы применение автоматизированных систем. В 1991 г. была разработана концепция развития систем управления воздушным движением (*air-traffic management* (ATM)), которая подразумевала использование цифровых систем передачи данных для обеспечения требуемого уровня эффективности, пропускной способности и гибкости аэронавигационной системы. В данной концепции для организации связи «воздух-земля» и «воздух-воздух» предполагалось использовать мобильные подсети: ОВЧ-линии передачи данных, линии передачи данных режима *S*, ВЧ-линии передачи данных и другие.

ОВЧ ЛПД режима 4 (VDL mode 4) является системой, входящей в реализацию систем вещательного автоматического зависимого наблюдения АЗН-В (ADS-B) в Российской федерации, осуществляемой в соответствии с программой «Внедрение средств вещательного автоматического зависимого наблюдения (2011–2020 гг.)», утвержденной Минтрансом России 19 мая 2011 г. [2]. VDL mode 4 объединила в себе основные преимущества предыдущих версий. Для доступа к среде используется самоорганизующийся доступ с временным разделением каналов, работает в диапазоне 117,975–137 МГц, на физическом уровне применяется GFSK, а ширина канала 25 КГц. Особенность ОВЧ ЛПД заключается в том, что большинство приложений, такие как ADS-B, ADS-C, TIS-B и другие реализуются на основе подуровней, а сама система предлагает широкие возможности для реализации этих приложений. К примеру, на основе уровней VSS, DLS и LME поддерживается, адресация, синхронизация, передача пользовательских данных, подтверждение приема и передачи. Это позволяет использовать VDL mode 4 как основу для протокола согласования частот для передачи речи, включая возможную ретрансляцию, так как стандартно в данную систему не заложена возможность голосовой связи. Предполагается, что для передачи информации и её ретрансляции будет использоваться один из каналов ОВЧ диапазона.

VDL mode 4 описывает первые три уровня модели OSI [3] представленные на рисунке 1, остальные уровни реализуется согласно стеку систем CNS/ATN:

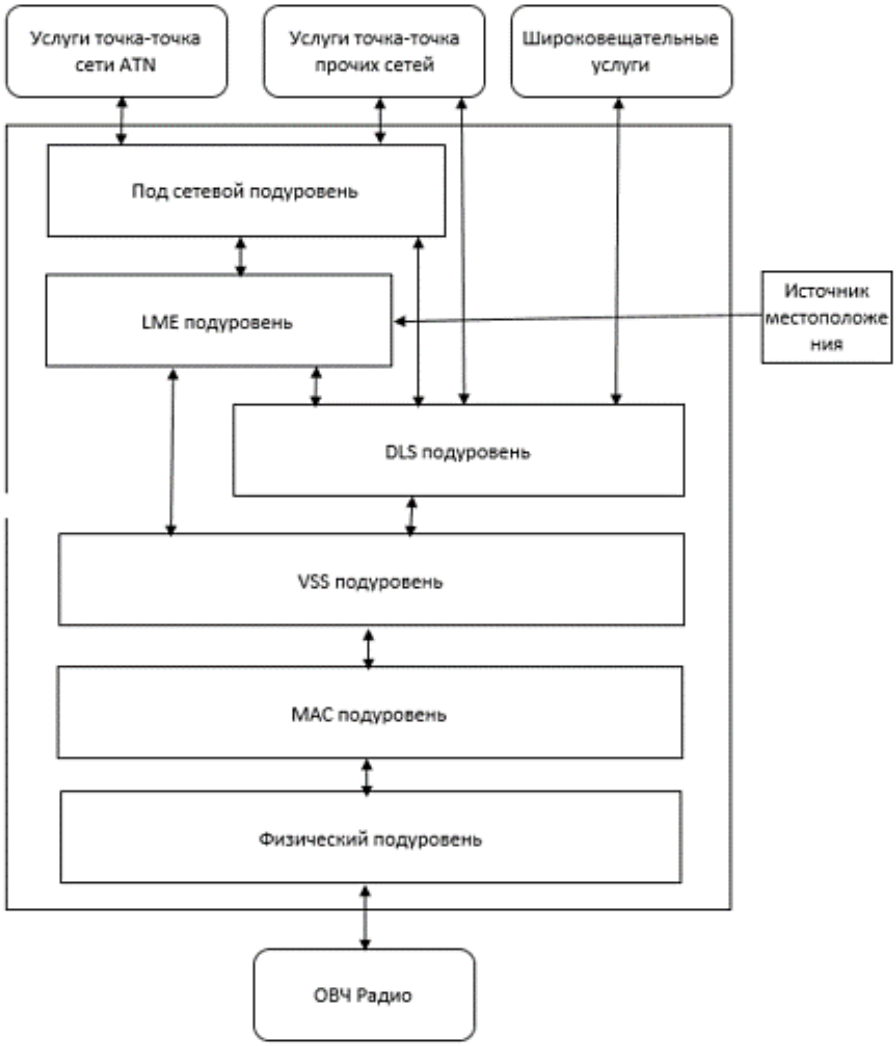


Рис. 1. Подуровни ОВЧ ЛПД режима 4

Физический уровень предоставляет функции управление частотой передатчика, модуляция/демодуляция данных, оценку уровня сигнала, измерение времени прихода сообщения.

Канальный уровень в свою очередь разделяется на три подуровня среди которых:

Управления доступом к среде (MAC) предоставляющий доступ к физическому уровню посредством временного разделения каналов, управляемого подуровнем VSS, синхронизацию времени, обнаружение ошибок.

Подуровень VSS (*VDL mode 4 Specific Services*) производит контроль доступа к каналу посредством самоорганизующегося процесса резервирования и обновления таблицы резервирования. А также ограниченно под-

держивает приложения, использующие широковещательные соединения или соединения типа точка-точка.

Подуровень DLS (*Data Link Services*) предоставляет возможность обмена данными для организации соединений. В зависимости от того, какой тип связи будет применяться использует протокол NSCOP (*negotiated setup connection orientated protocol*) или ZOCOP (*zero overhead connection orientated protocol).* NSCOP применяется для организации связи «земля-воздух», тогда как ZOCOP для «воздух-воздух».

Подуровень LME (*Link Management Entity*) обеспечивает установление соединения между приложениями подуровня DLS и поддержку широковещательных соединений. Так же на подуровне LME хранится таблица соседей, содержание которой обновляется по информации из пакетов, периодически рассылаемых всеми участниками сети.

Подсетевой уровень является частью подуровня SNAcP (*Subnetwork Access Protocol*) и обеспечивает передачу по виртуальной сети, восстановление ошибок, управление потоками данных и управление соединениями на подсетевом уровне.

Для организации канала голосовой связи между двумя ЛА необходима информация о маршрутизации в случае, если участники сеанса связи удалены друг от друга более чем на два интервала ретрансляции. VDL mode 4 не предоставляет подобной информации и стандартными средствами реализовать связь между двумя ЛА на расстоянии более одной ретрансляции не представляется возможном. Для организации подобной связи необходимо приложение или подуровень, который будет отвечать за обработку информации о маршрутизации. При этом, попытка организовать связь не более чем на два интервал ретрансляции стандартными средствами, не встречает особых проблем, так как каждый узел на подуровне LME хранит информацию о соседних узлах. В случае если устанавливается связь между наземной станцией и ЛА, процесс установления соединения тоже не встречает особых сложностей, так как сообщения наземной станции ретранслируются участниками воздушного движения [4], и у ЛА есть информация, от кого пришло сообщение. Таким образом, если ЛА хочет установить соединение с наземной станцией, оно отправляет сообщение в обратном направлении с пометкой «ретранслировать к наземной станции», а если наземная станция хочет вызвать ЛА, то в своем сообщении она указывает о том, что хочет вызвать его и вызываемый ЛА начинает процесс установления соединения. Все эти сообщения будут передаваться в рамках подуровня DLS.

Для передачи информация об установлении соединения необходимо: 4 бита для передачи информации о типе передаваемого сообщения в протоколе, 1 бит для индикации установления соединения, 12 бит для кодирования используемой частоты и ещё 10 бит для сопутствующей информации. Таким образом, сообщение данного приложения будут использовать

короткую процедуру установления соединения и в зависимости от того, какое соединение устанавливается соответствующий протокол либо NSCOP, либо ZOCOP. Всего предполагается использовать 3 базовых типа сообщений: «запрос на соединение», «подтверждение соединения», и «отмена». Запрос на соединение выполняется одновременно с DATA пакетом, а подтверждение соединения отправляется с пакетом ACK. При уже установленном соединении сообщение «подтверждение соединения» будет использоваться для поддержки соединения, и в случае, если необходимо сменить маршрут, будет отправляться сообщение «запрос на соединение».

Плюсы использования подобной системы:

- Так как VDL mode 4 предлагает инструменты для реализации приложений на канальном уровне, это позволит избежать издержек, которые могли бы возникнуть, если используется стек модели OSI.
- Так как, каждый узел VDL хранит таблицу своих соседей, то реализация передачи через один ретранслятор будет очень проста. Передающий узел рассылает широковещательный пакет, в котором указывает адресата, все узлы принимают этот пакет и обрабатывают. На каждом узле рассчитывается успешность этого узла как ретранслятора в соответствии с информацией, хранящейся в таблице на узле. Узел, выбравший себя самым успешным для организации передачи данных, устанавливает соединение между соответствующими узлами, и по нему сообщает информацию, по которой он готов принимать и передавать сигнал.
- Для организации подобных каналов связи не важен тип информации, для которой необходимо установить соединение, т. е. по каналу ВДЛ можно сообщить необходимую информацию, к примеру, для ретрансляции сигналов 1090ES.

Возможные проблемы:

- Для организации ретрансляции необходима информация о состоянии канала, на котором будет происходить ретрансляция, отсюда следует что необходимы дополнительные виды приемников передатчиков.
- Можно перехватить эти сообщения и устроить в этих каналах помеху, отсюда следует, что необходимо наблюдать за ними, все время.
- Из-за того, что протокол реализуется на подуровнях системы VDL mode 4, появляется фактор привязанность к конкретной системе.

Таким образом, протокол организации ретрансляций в ОВЧ ЛПД режима 4 можно использовать для организации двух интервальной связи между двумя ЛА и много интервальной связи между наземной станцией и ЛА, не прибегая к помощи дополнительных средств. А для организации много интервальной связи придется дополнительно разрабатывать протокол или подуровень маршрутизации.

Список используемых источников

1. FAA Aerospace Forecasts [Электронный ресурс] // Federal Aviation Administration, 2016. URL: http://www.faa.gov/ data_research/ aviation/ aerospace_forecasts/ (дата обращения: 01.04.2016).
2. Программа «Внедрение средств вещательного автоматического зависимого наблюдения в Российской Федерации (2011–2020 годы)», утверждена Минтрансом РФ в 2011 году. М., 2011. 179 с.
3. Документ ETSI EN 301 842-2 V1.7.1 (2015-04), VHF air-ground Digital Link (VDL) Mode 4 radio equipment; Technical characteristics and methods of measurement for ground-based equipment; Part 2: General description and data link layer.
4. Manual on VHF Digital Link (VDL) Mode 4 – ICAO Doc 9816 AN/448, First Edition – 2004.

Статья представлена научным руководителем,
доктором технических наук, профессором Шавриным С. С.

УДК 654.9, 681.5

В. В. Фицов (старший преподаватель, СПбГУТ)

ПОВЕДЕНИЕ ИМИТАЦИОННОЙ МОДЕЛИ СИСТЕМЫ DPI ПРИ РАЗЛИЧНЫХ ЗАКОНАХ РАСПРЕДЕЛЕНИЯ ВХОДНОГО ПОТОКА ЗАЯВОК

В данной статье рассмотрены вопросы исследования работы имитационной модели системы DPI. В качестве среды моделирования применяется ПО GPSS World. Входной поток заявок в сеть массового обслуживания (СеМО) представляется различными законами распределения.

DPI, GPSS, система массового обслуживания (СМО), сеть массового обслуживания (СеМО), закон распределения.

Введение

Система DPI (*Deep Packet Inspection*, глубокого анализа пакетов) распознает приложения по потоку пакетов, проводит мониторинг трафика, собирает статистику, ограничивает скорость трафика по приложениям и число сессий, перенаправляет трафик на сервера услуг, предупреждает пользователей об опасностях [1].

В статье рассмотрено поведение системы DPI, при поступлении на нее потоков пакетов, с межпакетными интервалами в соответствии с различными законами распределения. Для этого применена имитационная модель DPI, построенная в ПО GPSS World. Показано возможное влияние на каче-

ство обслуживания (QoS, *Quality of Service*) различного распределения потока заявок.

Имитационная модель DPI в GPSS World

Модель DPI содержит основные ,элементы изображенные на рисунке 1.

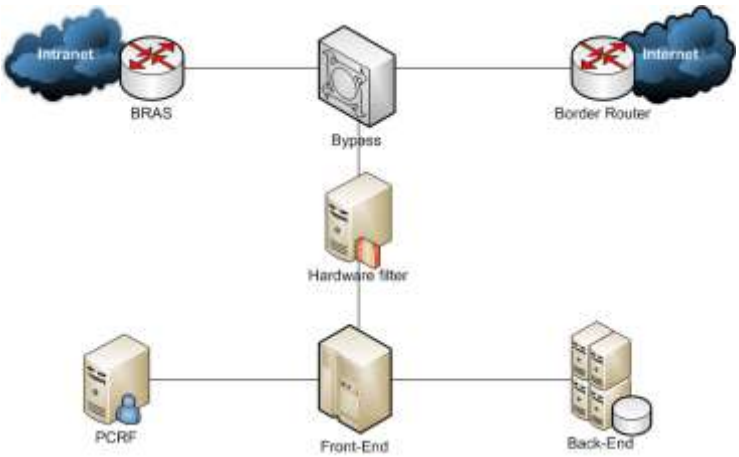


Рис. 1. Обобщенная архитектура системы DPI

Система DPI представлена как сеть массового обслуживания (СеМО), состоящая из Bypass, аппаратного фильтра, Front-End, PCRF и Back-End. В функциональной модели в качестве СМО1 выступает аппаратный фильтр совместно с Bypass. СМО2-4 соответствуют Front-End, PCRF и Back-End.

Для построения имитационной модели на основе СеМО был выбран классический симулятор GPSS (*General Purpose Systems Simulator*, Универсальная система моделирования) систем массового обслуживания. В основе алгоритмов GPSS лежит дискретно-событийный подход и имеется большой набор законов распределения для законов поступления и обработки трафика [2]. В [3] указано определение в GPSS World 25 распределений: Равномерное, Дискретное равномерное, Бета (I)*, Гамма (III)*, Эрланга, Пирсона V и VI, Экспоненциальное (X)*, Пуассоновское, Нормальное (Гаусса (XI)*), обратное Гаусса, Логнормальное, Парето, Вейбулловское и обратное, Биномиальное и отрицательное, Геометрическое, Треугольное, Лапласово, Логлапласово, Логистическое, Логлогистическое, Extreme Value A и Value B.

В результате симуляции GPSS World выдает информацию о работе устройства (СМО), очередей и значения отслеживаемых переменных. Отчет о работе устройства включает количество заявок, прошедших через устройство (entries), среднее время обработки одной заявки устройством (ave. time). Отчет по статистике в очередях содержит: максимальную дли-

ну очереди (max), общее число заявок (entry), среднюю длину очереди (ave. cont.), среднее время пребывания заявки в очереди (ave. time).

При определении влияния закона распределения входящих заявок на задержку распознавания потоков пакетов следует учитывать заданную скорость обработки заявок системой DPI представленную в таблице 1.

ТАБЛИЦА 1 Заданное среднее время обработки заявки на устройстве

Устройство	Действие	Ср. время, мс	Дисперсия, мс
Network	do instruct	0,2	0,05
Hardware Filter	toNetwork, toNetworkUnk, toFront-End	0,1	0,01
	NewInstruct	0,05	0,005
Front-End	Analyze	2,5	0,25
	toPCRF, roBack-End	0,01	0,001
	toFilter	0,001	0,0001
PCRF	Finding	0,1	0,01
Back-End	Finding	0,1	0,01

Влияние законов распределения на работу имитационной модели

Код GPSS взят из [3] (табл. 2).

ТАБЛИЦА 2. Описание законов распределения в GPSS World

№	Название	Команда в GPSS
1	Равномерное	GENERATE (UNIFORM(100,0,1000))
2	Бета (I)	GENERATE (BETA(1, 0, 1000, 0.5, 0.5))
3	Гамма (III)	GENERATE (GAMMA(1, 0, 1, 5))
4	Эрланга (2)	GENERATE (GAMMA(1, 0, 1, 2))
5	Пирсона VI и V	GENERATE (PEARSON6(1,0, 1, 5, 5)) GENERATE (PEARSON5(1, 0, 1, 5))
6	Экспоненциальное (X)	GENERATE (Exponential(1,50,500))
7	Пуассоновское	GENERATE (POISSON(1, 5))
8	Нормальное (Гаусса (XI))	GENERATE (Normal(1,50,500))
9	Логнормальное	GENERATE (LOGNORMAL(1,0,1,5))
10	Парето	GENERATE (PARETO(1, 1, 1))
11	Вейбулловское	GENERATE (WEIBULL(1, 0, 1, 1))
12	Логлапласово	GENERATE (LOGLAPLACE(1,0,1,5))

Величина входящего потока пакетов была выбрана как 1 000 заявок. В первую очередь отслеживалось количество заявок, поступившее на каждое из устройств, в том числе для повторной обработки (распределение числа заявок по СМО) (табл. 3), средняя очередь и время необходимое для их обработки системой (табл. 4), и результаты по обработке потока пакетов системой DPI в зависимости от закона распределения (табл. 5). Для упрощения сравнения полученных результатов, они были нормированы по величине результатов для равномерного распределения.

На фильтр поступают заявки на обработку и правила применения политик, что составляет 120 % от изначального числа заявок. Front-End обычно загружен 35 % от первичных заявок, PCRF – 12 %, а Back-End – 3 %. Числовой коэффициент в таблице 3 равен отношению заявок Back-End к поступающим на Filter.

ТАБЛИЦА 3. Нормированное количество заявок на устройствах системы DPI

Распределение	**Filter, ед., норм**	**Front-End, ед., норм**	**PCRF, ед., норм**	**Back-End, ед., норм**	**Коэфф.**
Равномерное	1217	393	136	40	0,032
Бета (I)	0,967	0,839	0,897	0,775	0,026
Гамма (III)	0,984	0,834	0,801	0,525	0,017
Эрланга (2)	0,980	0,895	0,963	0,7	0,023
Пирсона V	0,984	0,834	0,801	0,525	0,017
Пирсона VI	0,976	0,806	0,779	0,55	0,018
Экспоненциальное	0,985	0,885	0,889	0,7	0,023
Пуассоновское	0,996	0,936	0,941	0,675	0,022
Нормальное	0,987	0,933	0,985	0,775	0,025
Логнормальное	0,986	0,941	1	0,825	0,027
Парето	0,985	0,885	0,889	0,7	0,023
Вейбулловское	0,986	0,885	0,889	0,675	0,022
Логлапласово	0,985	0,885	0,889	0,7	0,023

Принято считать, что трафик пакетных сетей лучше других описывают распределения: Логнормальное, Парето, Вейбулловское, Гамма, Гиперэкспоненциальное 2-го порядка и пр. [4]. Парето, Вейбулла и логнормальное, относятся к распределениям с “тяжелым хвостом” и обладают бесконечной дисперсией в диапазоне $1 < a < 2$, где a характеризует «тяжесть» хвостов и пачечную структуру процесса. Такие процессы считаются самоподобными [5].

Наименьшую загруженность СМО имитационной модели дают распределения Гамма и Пирсона. Эрланга 2-го порядка, Экспоненциальное, Парето, Вейбуловское и Логлаплассово, меньше равномерного распределения. Пуассоновское, Нормальное и Логнормальное наиболее близкую к равномерному.

ТАБЛИЦА 4. Нормированная величина очередей Filter и Front-End (ед. и время)

Распределение	**Filter, ед., норм**	**Filter, ч., норм**	**Front-End, ед, норм**	**Front-End, м., норм**	**Числ коэфф.**
Равномерное	105,566	12,3	0,608	13,1	0,0057
Бета (I)	0,847	0,818	0,389	0,433	0,0026
Гамма (III)	0,927	0,009	0,379	0,004	0,0023
Эрланга (2)	0,953	0,003	2,960	0,012	0,0178
Пирсона V	0,940	0,002	0,402	0,002	0,0024
Пирсона VI	0,874	0,0004	0,976	0,0002	0,0064
Экспоненциальное	0,980	1,099	1,125	1,404	0,0066
Пуассоновское	1,034	1,017	1,001	1,048	0,0055
Нормальное	0,947	0,941	3,113	3,270	0,0189
Логнормальное	0,513	551,021	3,947	4437,630	0,0442
Парето	1,481	0,111	1,473	0,123	0,0057
Вейбулловское	0,983	0,002	1,126	0,002	0,0065
Логлапласово	0,979	0,002	1,120	0,002	0,0065

В таблице 4 показано среднее число заявок в очереди и среднее время обработки. Значения показывают существенную загрузку числом заявок фильтра и Front-End, и низкую загрузку PCRF. Шанс появления очереди на Back-End в ходе имитации возникает только после 1 млн заявок. Числовой коэффициент в таблице 4 показывает отношение среднего числа заявок в очереди Front-End к их числу в аппаратном фильтре.

Распределение Парето отличается средней длинной очереди фильтра, которая в 1,5 раза больше, чем при равномерном распределении. А логнормальное распределение имеет в 2 раза меньшую длину очереди фильтра, что вызвало увеличение длины очереди на Front-End в 4 раза, и нетипичное время нахождения в очереди обоих устройств. При нормальном распределении и Эрланга 2-го порядка, длина очереди на Front-End в несколько раз выше, чем при равномерном распределении. При распределениях Пирсона 5-го порядка, Бета и Гамма очереди имеют наименьшие значения. А остальные показали значения очереди близкие к равномерному распределению.

ТАБЛИЦА 5. Нормированное распределение результатов обработки заявок

Распределение	Извест.	Усп. анализ.	Неизв. PCRF	Нерасп.	Потер PCRF	Неизв. Back-End	Потер. Back-End
Равномерное	783	210	21	7	1	2	0
Бета (I)	1,051	0,828	0,809	0,428	1	0,5	0
Гамма (III)	1,024	0,919	1,190	0,714	1	0,5	0
Эрланга (2)	1,030	0,885	1,285	1	2	1	0
Пирсона V	1,024	0,919	1,190	0,714	1	0,5	0
Пирсона VI	1,035	0,857	1	1,285	1	0	0
Экспоненциальное	1,022	0,923	0,904	0,714	1	1	0
Пуассоновское	0,266	3,747	1,238	0,571	2	2	1
Нормальное	1,019	0,919	1,380	1,285	3	0,5	0
Логнормальное	1,020	0,923	1,476	1	4	0	0
Парето	1,022	0,923	0,904	0,714	1	1	0
Вейбулловское	1,021	0,928	0,904	0,714	1	1	0
Логлапласово	1,022	0,923	0,904	0,714	1	1	0

По числу заранее известных и успешно проанализированных заявок большинство распределений близки к равномерному. Исключением является Пуассоновское распределение, с низким числом заранее известных заявок и высоким числом успешно проанализированных. Нормальное и логнормальное распределения отличаются более высоким числом неизвестных PCRF и требующих запроса к Back-End заявок. В Пуассоновском и Бета распределении нераспознанных заявок приблизительно вдвое меньше, чем при равномерном, несмотря на разное число известных и успешно распознанных заявок.

Таким образом, Гамма распределение меньше загружает СМО по числу заявок, чем равномерное. Негативное влияние на величину очереди оказывают Логнормальное распределение и Парето. Увеличивает число нераспознанных потоков пакетов логнормальное распределение. Были представлены первичные результаты работы имитационной модели с различными распределениями потока заявок. Требуется дальнейшее изучение. Модель системы DPI в GPSS World позволяет задать параметры системы, и получить данные о загрузке СеМО. Результаты могут использоваться для эффективного распределения ресурсов системы DPI.

Список используемых источников

Якимович С. Управление трафиком и услугами в сетях ШПД с помощью решений DPI // Вестник связи. 2010. № 12. С. 27–29, С. 27.

Бронов С. А. Имитационное моделирование: учебное пособие. Красноярск: ФГОУ ВПО «Сибирский федеральный университет», 2007. 82 с., С. 16.

GPSS World Reference Manual. Copyright Minuteman Software. Holly Springs, NC, U.S.A. Fifth Edition, 2009. 468 p., pp. 354–379.

Ложковский А. Г., Каптур В. А., Вербанов О. В. Математическая модель пакетного трафика // Вестник национального политехнического университета «ХПИ». Харьков, 2011. № 9. С. 113–119, С. 116.

Савицкий О. К., Сорокина Е. А. Обоснование метода для расчета показателей качества обслуживания мультисервисной сети [Электронный ресурс] // Вопросы радиоэлектроники. 2012. Т. 3. № 3. С. 64–69, С. 65.

Статья представлена кандидатом технических наук,
доцентом кафедры Гойхманом В. Ю.

УДК 004.056.53

П. И. Шариков (студент группы ИКТЗ-23, СПбГУТ)

МЕТОДИКА ЭФФЕКТИВНОЙ ЗАЩИТЫ БАЙТ-КОДА JAVA-ПРИЛОЖЕНИЯ

Защита программного обеспечения является актуальной задачей. В статье объясняется необходимость защиты байт-код java-приложения, также проводится анализ существующих способов защиты байт-кода Java. Рассматриваются преимущества и недостатки каждого метода. На основе анализа существующих методов производится вывод о использовании конкретных методов в методике.

Java, bytecode, байт-код, методы защиты байт-кода.

Файлы Java и C++ компилируются по-разному. В таблице 1 представлена сравнительная характеристика Java и C++ на предмет защищенности готового скомпилированного файла от действий злоумышленника.

ТАБЛИЦА 1. Сравнение скомпилированных файлов Java и C++

Набор целевых инструкций	
C++	Java
Набор команд низкого уровня специфичных для целевого оборудования, например, x86, ARM или Power PC.	Компилирует на высоком уровне портативный байт-код, который работает с типизированными значениями: объекты, примитивные типы и массивы.
Оптимизация компилятора	
Многочисленные оптимизации кода выполняются во время компиляции.	Just-In-Time для повышения производительности. Стандартный javac компилятор не делает никаких оптимизаций.

Связка	
Программы статически связанны между собой. Имена классов, членов и переменных не должны присутствовать в скомпилированной программе.	Зависимости во время выполнения, когда классы загружаются. Имя класса, имена его методов и полей, импортируемых классов должны присутствовать в class-файле.
Формат поставки	
Приложение поставляется в виде монолитного исполняемого файла.	Поставляется в виде файлов .jar, которые не зашифрованы и архивируют содержащиеся внутри отдельные .class файлы.

Декомпилировать программу на Java проще по сравнению с программой, написанной на C++. Чтобы получить исходный код программы на C++, злоумышленнику придется приложить в разы больше усилий.

Существует несколько основных способов защиты байт-кода. Ниже представлены способы в порядке используемости:

1) обфускация имен,
2) потоковое преобразование данных (data flow obfuscation),
3) использование функций метапрограммирования (reflection),
4) AOT компиляторы,
5) вставка лишних инструкций,
6) шифрование последовательности,
7) шифрование байт-кода.

Обфускация имен

Обфускация имен или запутывание (obfuscation). На данный момент самый популярный способ защиты байт-кода. Замена названий имен – процесс замены идентификаторов. Производится выбор кодирующего стандарта и обрабатывается исходный код всего приложения.

Недостатки:

1) Нельзя скрыть имена стандартных классов API Java.
2) Невозможность получить динамический доступ к классу или методу сторонней библиотеки.
3) Большая часть обфускаторов автоматически исключают классы, которые реализуют java.io.serializable интерфейс.
4) Обфускатор не меняет саму структуру, классы, методы, вызовы. На основе этих сведений можно легко восстановить исходный код.

Потоковое преобразование данных

Модифицирует программу таким образом, что она дает тот же результат при запуске, но при этом ее невозможно декомпилировать в структурированный java-файл. Преобразование данных может включать в себя:

1) Изменение местоположения обычного или естественного на нехарактерное, необычное местоположение.

2) Кодирующие преобразования над данными (data encoding obfuscation).

3) Перегруппировка данных. Увеличение массива размерности массива. Объединение нескольких переменных в одну.

4) Изменение порядка данных в массиве.

Ограничения: классы, прошедшие обфускацию, могут не пройти более строгую проверку bytecode верификатора в будущих реализациях JVM. Потоковое преобразование данных сказывается на производительности.

Использование средств метапрограммирования

Reflection – скрытие информации о методе, который будет вызываться. Используя рефлексию, мы скрываем доступ к полю. Получаем через reflection поле, далее скрываем доступ к методу. Данными действиями мы удаляем из констант пула (constant pool) ссылку на метод.

Недостатки:

1) Страдает скорость выполнения программы.

2) Увеличивается размер байт-кода, так как увеличивается количество инструкций.

3) Boxing/unboxing примитивных типов.

4) Нельзя вызвать метод super.superMethod().

Ahead-of-time (AOT) компиляторы

Данный инструмент опережает по времени родной java-компилятор. Компилирует файл в оптимизированный машинный код и на выходе дает обычный исполняемый файл. Таким образом, AOT компилятор, получая на вход .jar и .class файлы, создает обычный исполняемый файл, который является «родным» для целевой платформы.

Преимущества:

1) Компилятор AOT выполняется на системе разработчика без временных ограничений компиляции или ресурсов.

2) «Родной» код, созданный с помощью оптимизации AOT компилятора будет также сложно декомпилировать, как и оригинальную программу на C++.

Недостатки:

1) JIT-компилятор имеет потенциальное преимущество над AOT компиляторами в том, что он может выбрать шаблон генерации кода в соответствии с реальным оборудованием, на котором выполняется приложение, что значительно ускоряет загрузку приложения.

Вставка лишних инструкций

Если в байт-коде найти инструкции определенного метода класса возвращающего переменную инструкцией return, то можно вставить инструк-

цию pop, после инструкции return. В этом случае многие декомпиляторы воспримут это как ошибку и не смогут корректно декомпилировать код, а JVM выполнит его без ошибок.

Шифрование последовательности

Замена строковых литералов с вызывами метода, который расшифровывает его параметр, делает задачу расшифровки кода более трудоемкой.

Недостаток шифрования последовательности заключается в том, что строки должны быть расшифрованы во время выполнения, так чтобы соответствующий код мог быть включен в приложение. Кроме того, большинство алгоритмов в инструментах шифрования настолько просты, что можно легко расшифровать код, написав программу, которая будет вызывать методы дешифровки для всех строк.

Шифрование байт-кода

Данный подход не логичен. На рисунке 1, ниже, показано, как происходит class encryption.

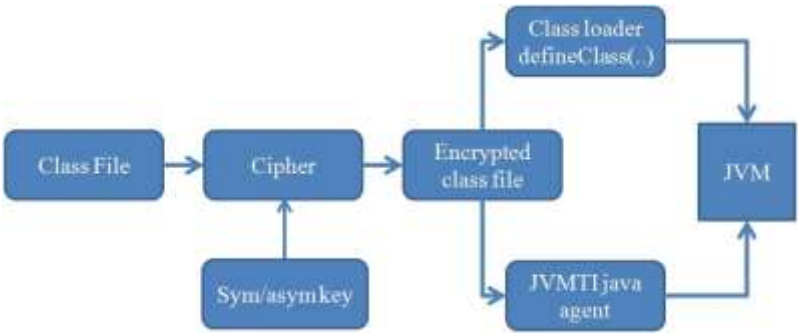


Рис. 1. Шифрование файла и его запуск в JVM

Как видно из рисунка 1, каким бы образом не был зашифрован файл, в итоге он все равно пройдет либо через Class Loader, либо через java agent, а потом в JVM. Недостаток данного метода в том, что JVM не может загрузить и выполнить зашифрованные классы.

Каждый метод по отдельности имеет наименьшую вероятность защиты байт-кода java. Исходя из этого, необходимо использовать комплекс мер из представленных выше методов. Проанализировав все критические моменты, была выработана методика целью, которой является максимально эффективная защита байт-кода java-приложения от декомпиляции.

1) Использование средств метапрограммирования в разных классах.
2) Реализовать проверку целостности java кода.
3) Выполнить компиляцию основного java кода.
4) Применить метод потокового преобразования данных.
5) Применить метод обфускации имен.

6) Применить метод вставки лишних инструкций в байт-код.

7) Далее зашифровать .class файлы любым алгоритмом шифрования, например RSA.

8) Запаковать .class файлы в .jar.

9) Создать лицензию.

Вывод

Данная методика не является панацеей, так как в информационном мире при наличии достаточно мощных вычислительных ресурсов можно взломать практически все. Данная методика увеличивает количество времени необходимое для декомпиляции программы или ее файлов. Таким образом, затраченные средства и время на расшифровку программы защищенной данной методикой, очень вероятно могут сильно перекрывать важность самой программы, а по истечении некоторого времени и актуальность. Если приложение создается под конкретную платформу, возможно, после 9 шага использовать AOT компилятор.

Было проверено порядка 100 файлов для защиты которых использовалась данная методика. Результатом было практически втрое большее время работы декомпиляторов с файлами, использующими для защиты данную методику, по сравнению с файлами без предлагаемой защиты. Декомпилятор «Fernflower» считающийся одним из лучших, правильно декомпилировал лишь 57 файлов. Файлы были с неточностями в функциях и лишними goto операциями в байт-коде. В 35 % случаев, даже после декомпиляции файлов чтение кода и разбор функций программы был затруднительным и требовал дополнительного времени.

На основании этих данных можно сделать вывод, что даже сильные декомпиляторы не могут с 100 % гарантией правильно декомпилирвоать защищенные файлы.

Список используемых источников

1. Intel 64 and IA-32 Architectures Software Developer’s Manual. Volume 2A: Instruction Set Reference, A-M: Intel Corp. 2008. 764 p.

2. Intel 64 and IA-32 Architectures Software Developer’s Manual. Volume 2B: Instruction Set Reference, N-Z: Intel Corp. 2008. 524 p.

3. Красов А. В., Штеренберг С. И., Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполняемые и библиотечные файлы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2013. С. 847–852.

4. Шариков П.И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 58–62.

Статья представлена научным руководителем,
кандидатом технических наук, профессором Красовым А. В.

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 517.958:004.42 (076)

А. С. Аверкова (курсант группы ПМ-37, СПб УГПС МЧС РФ)

МОДЕЛИРОВАНИЕ ТЕМПЕРАТУРНОГО ПОЛЯ ПЛАТЫ КОМПЬЮТЕРА С ТРЕМЯ МИКРОСХЕМАМИ

Статья посвящена процессу моделирования температурного поля платы компьютера с тремя микросхемами. В качестве моделирующей среды выбрана компьютерная система MathCad.

математическая модель, компьютерная система Mathcad, плата компьютера, уравнения эллиптического типа, уравнение Пуассона.

Современные интегрированные пакеты прикладных программ (ППП) позволяют получать оптимальные решения по математическим моделям ситуационных задач [1, 2, 3]. Например, моделирование различных тепловых нагрузок, процессов турбулентной диффузии, волновых процессов в твердых телах после ударного воздействия, дифракции сфокусированного светового пучка и др. Как правило, математические модели таких ситуаций связаны с краевыми задачами математической физики.

Фокус внимания сместим на тепловое моделирование температурного поля платы компьютера.

Не исключено, что вследствие температурного расширения области платы с повышенной температурой будут претерпевать различные деформации, вспучиваться и коробиться. При многократном нагревании и охлаждении это может привести к выходу из строя, как самой платы, так и расположенных на ней элементов, отслаиванию печатных проводников и нарушению контактов. Своевременная идентификация таких областей позволит избежать разрушительных последствий в ходе испытаний и эксплуатации готовых изделий.

В процессе анализа выполняется трехмерное моделирование суммарного поля течения и отдельных тепловых областей с учетом теплопроводности, конвекции и теплового излучения.

Цель модели состоит в определении степени нагрева отдельных элементов платы компьютера.

Обеспечение необходимого температурного режима является важной задачей для надежного функционирования компьютера. Во всех современных компьютерах предусматривается установка вентиляторов для охлаждения микросхем, а также датчиков температуры, показания которых можно контролировать.

Показания датчиков температуры дают важную, но все же очень ограниченную информацию о температурном режиме компьютера, поскольку измерения производятся только в нескольких точках. Поэтому рассмотрение вопроса о тепловом моделировании компьютера является актуальным и своевременным. Решения по математической модели температурного поля платы компьютера проведем в компьютерной системе MathCad.

Рассчитаем в MathCad и сделаем видимым температурное поле компьютерной платы, т. е. распределение температуры по всей поверхности, включая различные микросхемы и сильно греющийся микропроцессор.

Будем рассматривать упрощенное представление компьютерной платы с тремя микросхемами (рис. 1).

Рис. 1. Упрощенное представление компьютерной платы

В микросхемах выделяется теплота, которая распространяется вдоль платы посредством теплопроводности. С верхней и нижней поверхностей происходит теплоотдача в окружающую среду.

При включении питания компьютерная плата будет разогреваться, но затем температура установится на некотором уровне, а внутреннее тепловыделение будет полностью компенсироваться теплоотводом в окружающую среду. Такой режим называется стационарным, не меняющимся во времени.

Стационарное поле температуры можно описать дифференциальным уравнением в частных производных второго порядка эллиптического типа. Поэтому математическая модель температурного поля платы компьютера будет представлена уравнением Пуассона.

Для решения уравнения Пуассона в MathCad с произвольными граничными условиями следует использовать функцию relax. Использование данной функции подразумевает следующую последовательность действий:

1) Задаем пять квадратных матриц a, b, c, d, e. Эти матрицы будут содержать коэффициенты в формуле приближенного вычисления оператора Лапласа:

$$(\Delta u)_{ij} = a_{ij} \cdot u_{i+1j} + b_{ij} \cdot u_{i-1j} + c_{ij} \cdot u_{i+1j} + d_{ij} \cdot u_{i-1j} + e_{ij} \cdot u_{ij}.$$

Стандартные значения для элементов этих матриц:

$$a_{ij} = b_{ij} = c_{ij} = d_{ij} = 1, \; e_{ij} = 4a_{ij}.$$

Размер этих матриц может быть выбран любой. Главное, чтобы все матрицы, задаваемые для функции relax, были одинакового размера.

2) Задаем матрицу F, задающую интенсивность источника в каждой точке квадратной области. Если все элементы этой матрицы имеют нулевые значения, то полученный результат будет решением уравнения Лапласа.

3) Задаем матрицу v. Первый и последний столбцы и первая и последняя строки этой матрицы задают граничные условия для решения уравнения. Значения внутренних элементов матрицы не играют особой роли, а используются лишь как начальное приближение при поиске решения.

4) Теперь можно использовать функцию relax. Это делается следующим образом:

U := relax(a,b,c,d,e,F,v,r).

Здесь r – так называемый спектральный радиус Якоби. Это число в диапазоне от 0 до 1. Если функция relax не может решить уравнение, то надо попробовать уменьшить значение спектрального радиуса.

Для функции relax, как и для multigrid, единственным параметром, контролирующим точность, является размер используемых матриц. Также при использовании функции relax не следует забывать о том, что все матрицы должны быть квадратными и их размеры должны совпадать.

Моделирование температурного поля платы компьютера с использованием функции relax представлено на рисунке 2 в виде листинга.

Графические модели температурного поля в виде линий уровня и поверхности представлены на рисунке 3.

Цвет изображений на графиках воспроизводит различные значения температуры. Области с высокой температурой – это три микросхемы.

Процессор компьютера (самая большая микросхема) нагрет наиболее сильно.

Причин перегрева может быть достаточно много. Большую часть из них пользователь может устранить самостоятельно.

Основные причины перегрева:

- запыленность и загрязненность внутренних деталей,
- высохшая термопаста,
- неисправность охлаждающей системы,
- выход из строя элементов материнской платы.

Причиной перегрева является и, накапливаемая со временем внутри корпуса компьютера, пыль.

Эта проблема не возникнет, если периодически проводить профилактическую чистку, используя баллон со сжатым воздухом, который можно приобрести в любом компьютерном магазине.

Действия по удалению пыли это первое, что необходимо сделать.

$n := 32$ сетка $n * n$ для разбиения квадратной платы

$S_0 := 50$ параметр тепловыделения

$\beta := 0.5$ коэффициент теплоотдачи на поверхности платы

Формирование матрицы коэффициентов:

$i := 0..n \quad j := 0..n$ обход по всей расчетной области платы

$a_{i,j} := 1 \quad b := a \quad c := a$

$d := a \quad e_{i,j} := -(4 + \beta)$ матрицы с коэффициентами

$Tinit_{i,j} := 0$ начальное приближение на краях платы

$Source_{i,j} := 0$ обнуление массива, в котором будут рассчитаны значения внутреннего тепловыделения в микросхемах

$i := 18..26 \quad j := 6..n - 6$

$Source_{i,j} := -S_0$ тепловыделение в большой микросхеме (процессоре)

$i := 6..14 \quad j := 2..\frac{n}{2} \quad Source_{i,j} := -\frac{S_0}{2}$

$i := 6..14 \quad j := 22..26 \quad Source_{i,j} := -\frac{S_0}{1.2}$

тепловыделение в двух маленьких микросхемах

$r := 0.95$ спектральный радиус Якоби

$T := relax(a, b, c, d, e, Source, Tinit, r)$

Рис. 2. Листинг модели температурного поля платы компьютера

Перегрев может сочетаться с выходом из строя некоторых элементов платы. Например, южного или северного моста. В этом случае при полной неисправности микросхемы мобильный ПК перестанет включаться, а при частичной могут появиться разнообразные глюки.

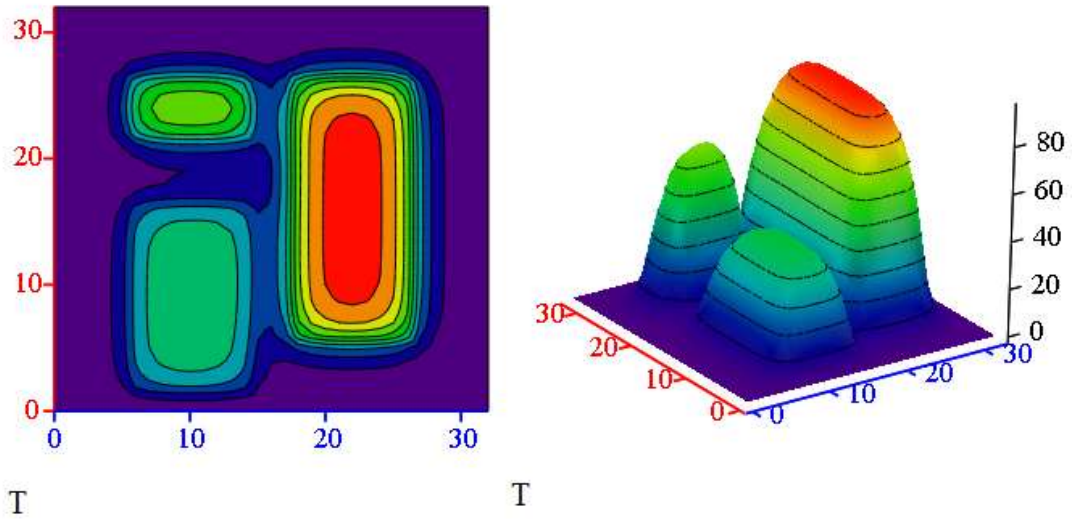


Рис. 3. Графические модели температурного поля

Решение по математической модели температурного поля компьютерной платы в Mathcad достигается с помощью применения функции relax.

Используя компьютерную систему Mathcad по тепловому моделированию компьютерной платы можно своевременно избежать поломок ПК.

Список используемых источников

1. Трофимец Е. Н. Информационные технологии математического моделирования в экономических вузах / Образовательные технологии и общество. 2012. Т. 15. № 1. С. 414–423.

2. Трофимец Е. Н. Информационно-аналитические технологии обучения менеджеров в образовательных учреждениях России и за рубежом // Вестник РУДН. Серия: Информатизация образования. 2010. № 1. С. 86–95.

3. Трофимец Е. Н. Интегральный подход в обучении математике студентов-экономистов: монография. Ярославль: Ярославский гос. технический ун-т, 2009. 170 с.

Статья представлена научным руководителем,
кандидатом педагогических наук, доцентом Трофимец Е. Н.

УДК 004.02

С. Т. Аль-Мехди (студент группы М091401(70), МТУСИ)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ИДЕНТИФИКАЦИИ ШАБЛОНА НА ИЗОБРАЖЕНИИ

Имеется набор изображений, представляющих из себя некоторые документы, заверенные печатью какой либо организации, требуется произвести сравнение с уже ранее известным шаблоном для локализации печати и/или других признаков подлинности заверения. Для решения этой задачи, были рассмотрены алгоритмы и методы сопоставления и сравнения, такие как «сумма квадратов разности», «кросс-корреляция» и «быстрое преобразование Фурье», и возможности применения этих методов для выделения и локализации печати и/или других признаков подлинности заверения. Алгоритмы реализованы в программной среде MATLAB. Исследованы исковые характеристики указанных алгоритмов и найдены оптимальные решения.

быстрое преобразование Фурье, сумма квадратов разности, кросс-корреляция.

1. Определение проблемы и Среда разработки

В нашей работе мы хотим показать необходимость применения обработки изображений при работе в области юриспруденции для определения подлинности документов путем распознавания подписей, печатей и/или других специфических характеристик документов. Необходимо усовершенствовать процесс обработки изображений [1] в этих важных государственных органах с целью сокращения сроков получения необходимых документов, ускоряя процесс идентификации подлинности печатей и подписей. Другая немаловажная особенность – это избегание ошибок, что ведет к нарушению законодательства, если подписи и печати будут идентифицированы неверно. Вся работа, была провидена, методами обработки изображений используя математические алгоритмы в среде MATLAB.

2. Постановка задачи

На рисунке 1 заданы: *1)* изображение документа (доверенности) содержащее печать содержащую герб РФ, которую нужно будет обнаружить; *2)* изображение документа, содержащего несколько печатей, в том числе гербовую; *3)* шаблон печати с гербом РФ.

Задача состоит в реализации обнаружения печати содержащую герб РФ, и не выделять другие печати, а так же сравнить скорость исполнения задачи, между методами учитывая при этом размер входного изображения и шаблона.

1) 2) 3)

Рис. 1. Входящие изображения

3. Обработка изображения с помощью «Кросс-корреляции»

Среда MATLAB содержит функцию, отвечающую за вычисления Корреляции между двумя матрицами – *corr*2 Синтаксис:

$$r = corr2(A, B). \tag{1}$$

Функция (1) считает корреляцию между двумя одинаковыми матрицами *A* и *B*, но поскольку нам нужно сравнить маленькое изображение с большим (т. е. найти одно в другом) [2] мы помещаем шаблон в матрицу, заполненную нулями такого же размера, как и входное изображение, и повторяем операцию передвигая значения шаблона по всей нулевой матрице до нахождения совпадения. Результат применения «кросс-корреляции»

а) б)

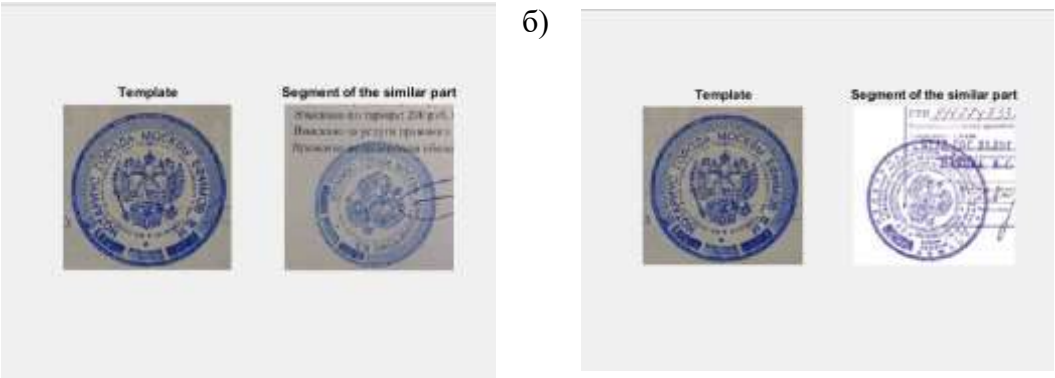


Рис. 2. Результаты сопоставления с помощью «кросс-корреляции»

Как видно на рисунке 2 результаты очень хорошие, нужные печати были обнаружены и выделены, не смотря на то, что на оригинальных документах они были нанесены в наклонном виде. Операция заняла около 3 мин для результата *а)*, и около 1 мин. для результата *б)*. Учитывая, что размер изображения 1 составлял 83,7 КБ, размер изображения 2 составлял 174 КБ, а размер шаблона – 46,8 КБ.

4. Обработка изображения с помощью «БПФ» и «обратного БПФ»

Синтаксис:

$$Y = fft2(X) \quad (2)$$
$$Y = fft2(X, m, n) \quad (3)$$
$$Y = ifft2(X) \quad (4)$$
$$Y = ifft2(X, m, n) \quad (5)$$

Функция (2) вычисляет двумерное ДПФ, возвращая результат в матрице комплексных чисел *Y*, имеющей тот же размер, что и матрица *X* [3]*;* *X* может быть вектором, в этом случае возвращается вектор *Y*, имеющий такую же ориентацию, что и вектор *X*. Функция (3) вычисляет двумерное преобразование Фурье матрицы *mxn*, при необходимости дополняя нулями или усекая исходную матрицу *X*, возвращая результат в матрице *Y* размера *mxn*. Массив *Y* имеет формат представления данных *double*. Функция (4) вычисляет обратное двумерное ДПФ, возвращая результат в матрице *Y*, имеющей тот же размер, что и матрица *X; X* может быть вектором, в этом случае возвращается вектор *Y*, имеющий такую же ориентацию, что и вектор *X*. Функция (5) вычисляет двумерное преобразование Фурье матрицы *mxn*, при необходимости дополняя нулями или усекая исходную матрицу *X*. Возвращается матрица *Y* размера *mxn.* С точностью, определяющейся ошибками округления, $ifft2(fft2(X)) = X$, однако, если *X* содержит только действительные элементы, $ifft2(fft2(X))$ может содержать комплексные элементы с малыми по величине комплексными частями. Массив *Y* имеет формат представления данных *double*. Двумерное преобразование Фурье вычисляется выполнением двух одномерных преобразований $fft(fft(x).')$*;* сначала вычисляется ДПФ каждого столбца, а затем каждой строки результата [4]. Обратное двумерное преобразование Фурье вычисляется по тому же принципу, который реализован в функции *fft2*, т. е. двумерное преобразование выполняется с помощью двух последовательных одномерных обратных преобразований Фурье для строк и столбцов. Время расчетов минимально, если *m* и *n* являются степенями числа 2. Если *m* и *n*, простые числа – время расчетов максимально. Результат применения «БПФ» и «обратного «БПФ»».

Как видно на рисунке 3 результаты довольно точны, нужная печать была обнаружена и выделена. Сравнивая предыдущий метод, примененный к изображению 1 и шаблону 3, результат был достигнут за несколько секунд, что позволяет сделать вывод, что методы быстрых преобразований являются лучшим средством для обработки изображений [5] и могут быть эффективно использованы, не только для сжатия, реставрации, реконструкции и пере-дискретизации изображений, но и для эффективного сравнения спектра и выявления схожести, между изображениями, превосходя своей скоростью обработки, медленные методы сопоставления, тем

самым, улучшая качество работы, сокращая его время выполнения, сохраняя эффект точности.

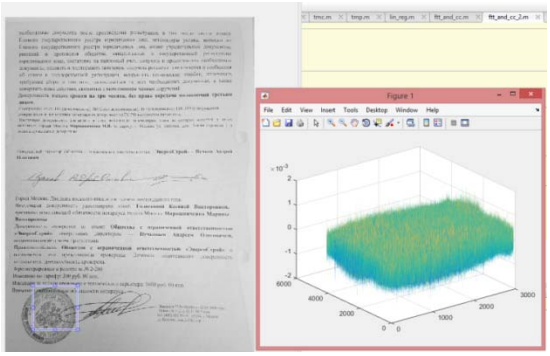


Рис. 3. Результаты сопоставления с помощью «БПФ»

Список используемых источников

1. Yaroslavsky L. P., Digital Picture Processing: An Introduction, Springer, Berlin, Germany, 1985.
2. MathWorks: [сайт]. URL: www.mathworks.com
3. Прэтт У. Цифровая обработка изображений: В 2 т. / пер. С англ. М. : Мир, 1982. 480 с.
4. Korman S., Reichman D., Tsur G. and Avidan S., "FAsT-Match: Fast Affine Template Matching", CVPR2013.
5. Ярославский Л. П. Введение в цифровую обработку изображений. М. : Советское радио, 1979. 312 с.

Статья представлена научным руководителем,
доктором технических наук, профессором Яшиной М. В.

УДК 004.056.5 + 004.382.7

К. В. Белоус (кандидат технических наук, СПбГУТ)
Д. А. Берин (студент группы ТСС-25, СПбГУТ)
Е. В. Давыдова (старший преподаватель, СПбГУТ)

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА НА БАЗЕ ARDUINO

Показана возможность построения системы контроля и управления доступом на базе микроконтроллерной платы Arduino. Контроллеры объединены в сеть с помощью Ethernet-shield. В качестве средства идентификации используется карта радиочастотной идентификации стандарта 125 кГц. Информация о правах доступа хранится в реляционной базе данных.

контроль доступа, сервер, радиочастотная идентификация, учёт посещаемости, безопасность.

В настоящий момент в связи с необходимостью обеспечения безопасности предприятий различных форм собственности, а так же учёта и контроля их посещаемости возрастает роль различных систем контроля и управления доступом, интегрированных в Единое информационное пространство предприятий. Особую важность и значимость системы данного класса приобретают в учебных заведениях, где необходимо контроль как посещаемости лекций студентами, с целью использования данной информации при выставлении итоговых отметок, так и с целью контроля преподавателей.

Внедрение системы контроля и управления доступом в высших и средних учебных заведениях позволит кроме разграничения прав доступа и учёта посещаемости позволит регулировать учебную и трудовую дисциплину со стороны, как студентов, так и преподавателей, будет способствовать обеспечению сохранности материальных ценностей внутри аудиторного фонда, а также позволит контролировать соблюдение внутреннего расписания. Кроме того, облегчится процесс проведения внутренних расследований по инцидентам.

Новизна разрабатываемой системы, в части идентификации студентов, позволит упростить ведение журналов посещаемости лекционных и практических занятий, ускорить процесс внесения данных об учебном процессе в автоматизированные системы учебных заведений, сократить количество бумажных носителей, сэкономить время занятий, исключая опросы присутствующих, а также частично нивелировать человеческий фактор. В общем виде СКУД может быть представлена совокупностью элементов (рис. 1).

Архитектурно-технологическая схема системы контроля и управления доступом представлена на рисунке 1 Основными компонентами системы являются: модули радиочастотной идентификации стандарта 125 kHz, микроконтроллерные платы Arduino с установленными расширения Ethernet shield, структурированная кабельная система, обеспечивающая связь микроконтроллерных плат с сервером, обрабатывающим запросы от плат. Запирающим устройством, представляющим собой электромагнитный замок (рис. 2), и блок реле (рис. 3), обрабатывающего сигналы от микроконтроллерной платы и вырабатывающим сигнал на открытие/закрытие дверей. Для повышения надёжности микроконтроллерные платы, а так же коммутационное оборудование и электромагнитные замки могут быть снабжены автономными источниками питания. Фрагмент системы СКУД, обеспечивающей защиту одного помещения представлен на рисунке 4. Пины подключения микроконтроллерной платы и дополнительного оборудования показаны условно. Для настройки взаимодействия

с MySQL и исполнения запросов использовались материалы блога http://drcharlesbell.blogspot.ru/. Карты доступа стандарта 125 кГц могут обеспечить достаточное количество комбинаций для идентификации пользователей. В случае утери карты происходит её блокировка администратором системы. Для рассылки sms-уведомлений о происходящих событиях использовалось API https://www.clickatell.com/.

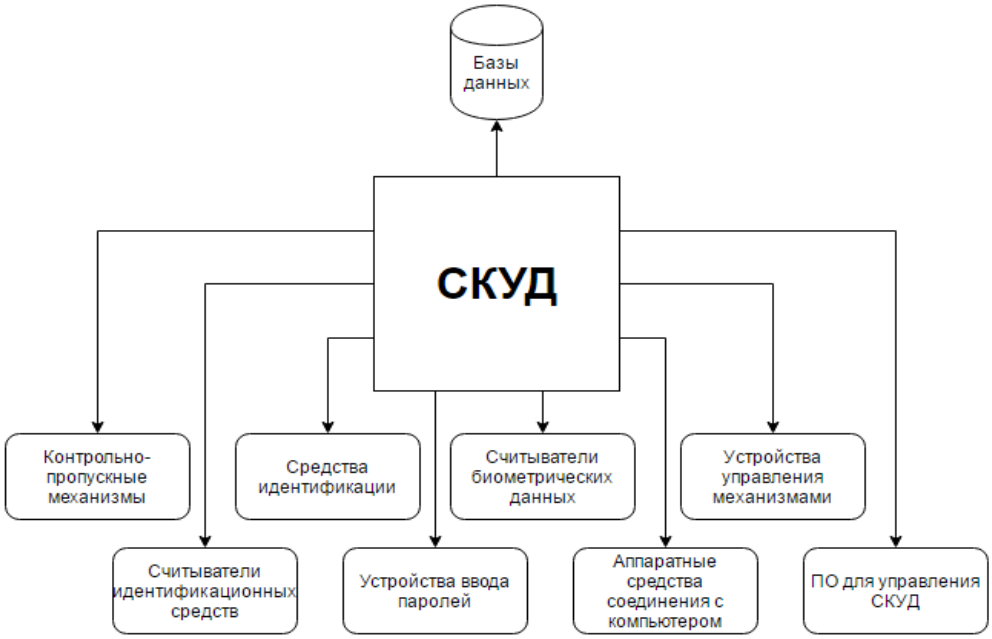


Рис. 1. Составные компоненты СКУД

Рис. 2. Электромагнитный замок

Рис. 3. Малогабаритное реле

При необходимости ограничения доступа в помещение на дверь необходимо установить электромагнитный замок и произвести коммутационные соединения. При включении микроконтроллерной платы в сеть происходит автоматическое получение IP-адреса по протоколу DHCP, после чего организуется передача MAC-адреса в базу данных. Предварительно через интерфейс администрирования необходимо добавить mac-адрес для исключения возможности несанкционированного подключения (рис. 5, рис. 6).

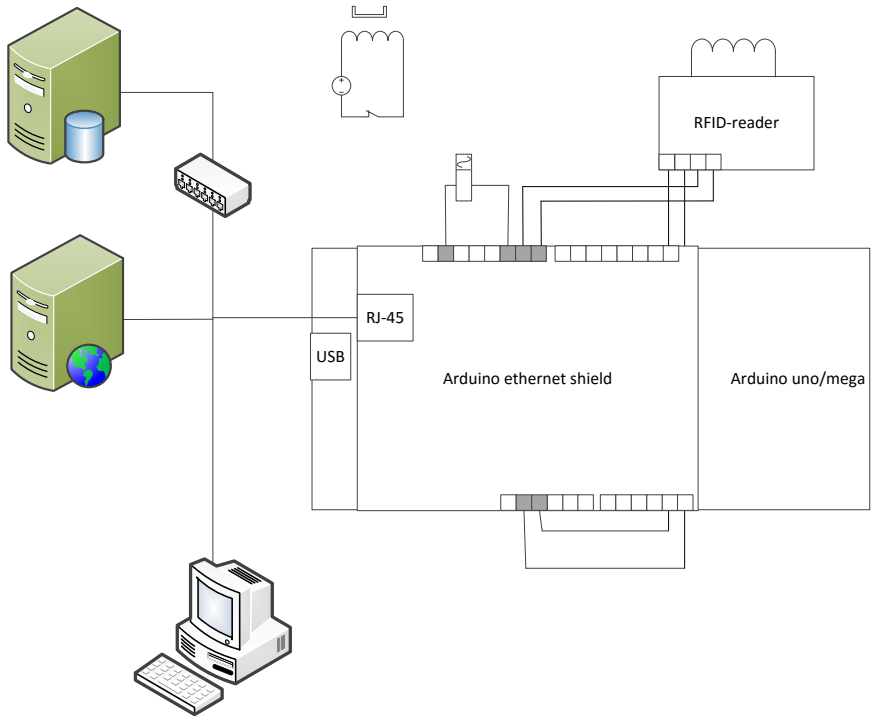


Рис. 4. Фрагмент СКУД

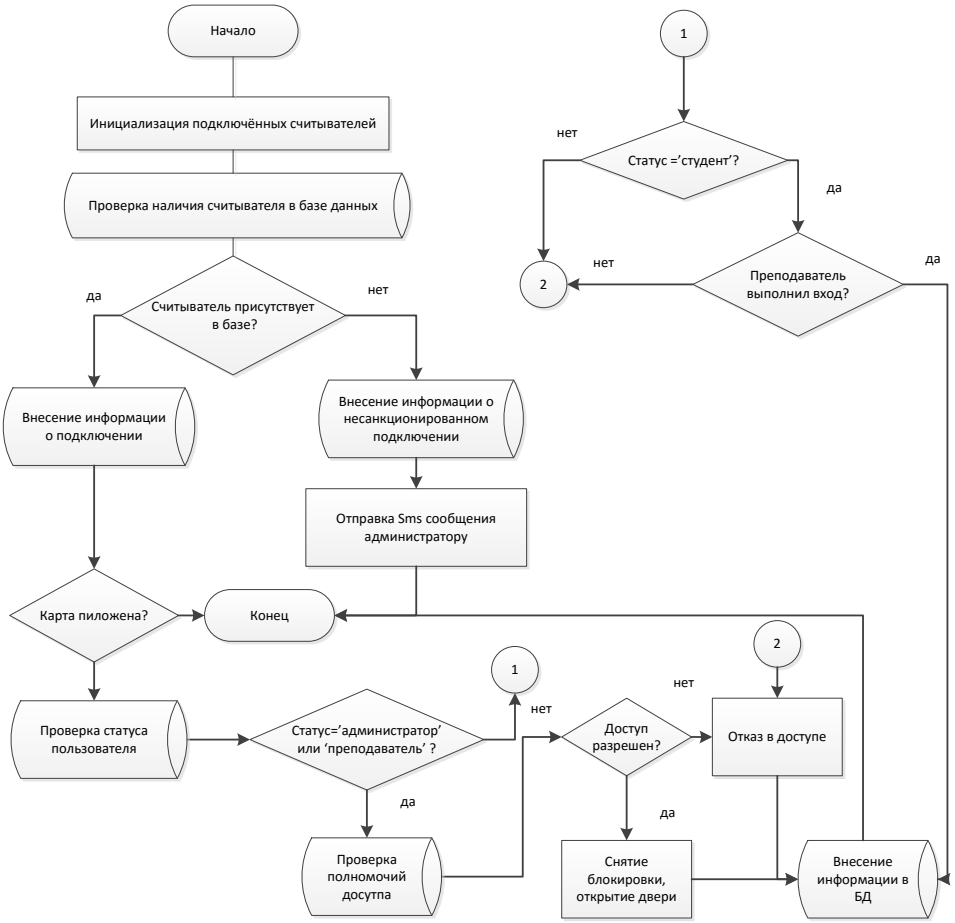


Рис. 5. Обобщённый алгоритм работы СКУД

Интерфейс системы, представленный на рисунке 7, позволяет выполнять следующие операции.

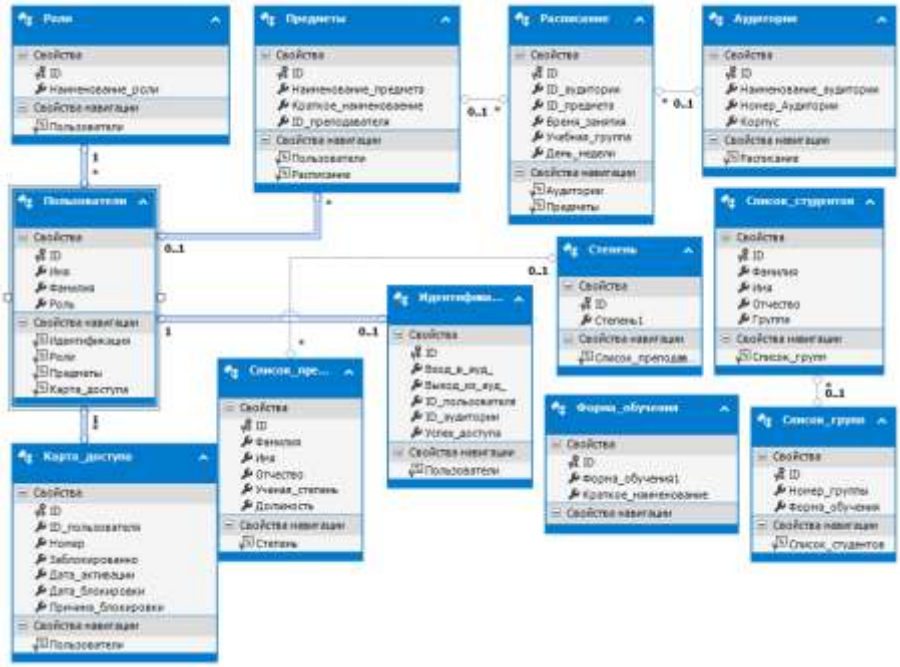


Рис. 6. Объектная модель предметной области

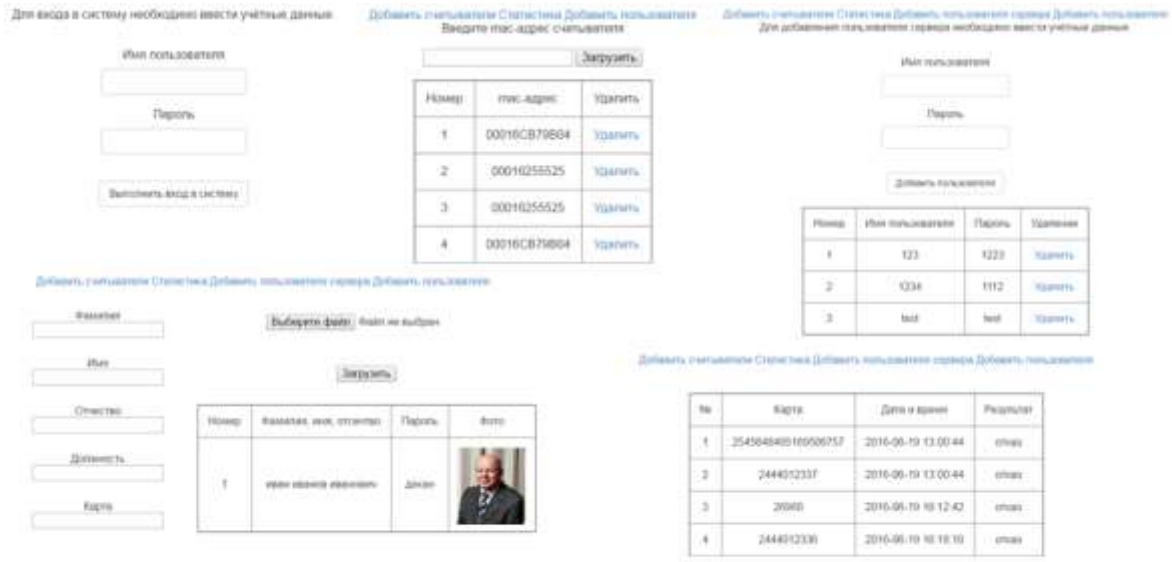


Рис. 7. Экранные формы

Список используемых источников

1. Сёмкин С. Н., Беляков Э. В., Гребенёв С. В. Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие. М. : Гелиос АРВ, 2005. 192 с.

2. Петин В. А. Проекты с использованием контроллера Arduino. 2-е изд., перераб. и доп. СПб. : БХВ-Петербург, 2016. 464 с.
3. Кузнецов С. Д. Базы данных: языки и модели: учебник. М. : ООО «Бином-Пресс», 2008. 720 с.
4. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М. : Горячая линия-Телеком, 2013. 272 с.
5. Финкенцеллер Клаус RFID-технологии. Справочное пособие / пер. с нем. Н. М. Сойунхароваэ. М. : Додэка-XXI, 2010. 496 с.

УДК 004.946

В. В. Березин (курсант 3 курса, ВКА им. А.Ф. Можайского)
А. Б. Менисов (адъюнкт, ВКА им. А.Ф. Можайского)

СИСТЕМА АВТОМАТИЗИРОВАННОЙ ИДЕНТИФИКАЦИИ ИНФОРМАЦИОННЫХ ДЕЙСТВИЙ НА YANDEX MARKET, ВЛИЯЮЩИХ НА РЕЙТИНГ ТОВАРА

Статья посвящена проблеме информационных действий конкурентов на Yandex Market.

Автор не только анализирует современные подходы к идентификации информационных действий, влияющих на рейтинг товара, но и современные способы автоматизации данного процесса через API веб-ресурса.

В статье содержатся примеры информационных действий конкурентов и их идентификация.

информационное воздействие, маркетинг, yandex market.

Информационное воздействие является эффективным инструментом во множестве сфер, где ведется борьба за внимание публики. Простые обыватели редко задумываются, какой смысл заключен в той или иной статье, отзыве, рекламном ролике, баннере, принимая лишь то, что представлено на поверхности. На самом деле, это процесс формирования определенного, нужного конкретному человеку, мнения. Все данные элементы в комплексе или по отдельности формируют устоявшуюся мысль, которую на самом деле несли эти элементы информационного процесса. Следует более подробно рассмотреть влияние отзывов и комментариев о товаре на мнения покупателей.

Не многие покупатели подвергают сомнению отзывы, тем более если их несколько. Люди склонны доверять таким же простым пользователям, не задумываясь, что это может быть специально подстроенная акция, нацеленная на подрыв продаж товаров конкурента.

Отзывы и благодарные письма могут влиять по-разному, это зависит от качества самих отзывов: некоторые владельцы сайтов и интернет магазинов заказывают положительные отзывы на форумах. Такие некачественные искусственные отзывы, пользователи легко распознают и эти поддельные «впечатления» о товаре наоборот влияют весьма негативно на решение о покупке. Отсюда можно сделать вывод: не только негативные отзывы могут отвернуть покупателя от того или иного товара, но и положительные.

Можно выделить два вида отзывов:

- Отрицательные «искренние» отзывы.
- Позитивные излишне навязчивые отзывы.

Наиболее традиционным является первый тип отзывов, но умелое использование отзывов второго типа может не хуже, а иногда даже лучше помочь достичь необходимой цели.

Можно выделить три подхода к идентификации информационный действий по задействованию оператора:

1) Экспертный подход – основан на полном задействовании оператора, использующего свои знания и опыт для выявления информационных действий, осуществляется качественный поиск, но низкая оперативность.

2) Автоматизированный подход – наиболее оптимальный подход, оператор с помощью программы выявляет информационные действия, программа ускоряет работу эксперта, упрощает некоторые элементы его работы, за счет чего растет оперативность без потерь качества.

3) Автоматический подход – программа самостоятельно выявляет информационные действия, представляя оператору готовый результат, является наиболее сложным для реализации подходом, требующего учета большого количества факторов.

Подходы идентификации информационных действий по аспектам информации:

1) семантический подход – рассматривает смысловую нагрузку информационных сообщений;

2) прагматический подход – рассматривает прагматику информационных сообщений;

3) синтаксический подход – рассматривает качественный и количественный анализ составных элементов информационного сообщения.

Не исключается использование смешанных подходов. Ниже мы рассмотрим способы автоматизации идентификации информационных действий на основе автоматизированного синтаксического подхода.

Автоматизация идентификации информационных действий подразумевает под собой создание программы, которая будет упрощать работу эксперта по выявлению информационных действий. Поскольку предстоит работа с сайтом, в нашем случае это Yandex.Market, нам понадобится API (application program interface) Yandex.Market.

API Yandex.Market – представляет собой набор процедур, протоколов и инструментов для построения программных приложений связанных с Yandex Market. **API** определяет, как программные компоненты должны взаимодействовать с сайтом.

В перспективе программа должна с точностью до 0.7 выделять предумышленные отзывы от настоящих отзывов пользователей.

Оператору необходимо только выбрать товар или производителя, запустить программу, получить обработанные данные и принять решение. Система существенно сократит время работы эксперта-аналитика при определении

Методика идентификации информационных действий:

1) Авторизация на Yandex.Market.

API Яндекс.Маркета доступно только авторизованным пользователям. Идентификация происходит с помощью ключей авторизации, выдаваемых системой Яндекс.Маркета. Для получения данного ключа отправляется запрос.

2) Обращение к Yandex.Market, вывод ресурсов.

На этом этапе осуществляется запрос на вывод отзывов. Запросы к API Яндекс.Маркета передаются по протоколу HTTPS, XML.

3) Получение результатов.

Получение ответа от сервера, вывод результатов для дальнейшей обработки.

4) Обработка результатов.

На четвертом этапе происходит непосредственно обработка данных. Обработка данных происходит в несколько этапов:

a. Выделения отзывов из массива информации.

b. Сортировка отзывов по тональности.

c. количественный анализ.

Количественный анализ основывается на таких показателях как: количество отзывов по тональностям, количеству просмотров данного товара, количеству сделанных покупок данного товара.

d. Качественный анализ.

Качественный анализ основывается на соотношении с эталонными словарями термов сообщений.

e. Заключительная обработка.

5) Вывод полученных данных.

Вывод всех показателей анализа данных в удобном для работы эксперта виде.

6) Принятие решения операторомю

В результате работы методики оператор должен сделать вывод о наличии информационных действий в отношении данного товара. При наличия подобных действий оператор предлагает руководству варианты решения проблемы и проведение возможных контрмер.

Таким образом, рассмотренная проблема информационного воздействия на потенциальных покупателей путем подтасовки отзывов приводит к изменению рейтингов товаров. Представлен алгоритм автоматизации процесса выявления информационных действий.

Данная система позволит выявить негативное воздействие на рейтинг товара, что позволит своевременно принять контрмеры, которые в свою очередь позволят сохранить покупателей и репутацию производителя, уменьшить потери продаж.

Список используемых источников

1. Сегаран Тоби. Программируемый коллективный разум: учебное пособие. СПб. : Символ-Плюс, 2008. 360 с.
2. Крысько В. Г. Секреты психологической войны. Минск: Харвест, 2000. 448 с.
3. Менисов А.Б., Усков А.С. Информационная система автоматизированного сбора данных в социальных сетях / Материалы конференции военно-научного общества ВКА имени А.Ф. Можайского / под общ. ред. Ю.В. Кулешова. СПб.: ВКА имени А.Ф. Можайского, 2015. 377 с.
4. Менисов А. Б. Система комплексного сбора графических данных в социальных сетях / III Открытая выставка научно-технического творчества ВКА имени А.Ф. Можайского – 2015.
5. Менисов А.Б. Информационно-аналитическая система выявления информационного повода в англоязычных средствах массовой коммуникации / III Открытая выставка научно-технического творчества ВКА имени А.Ф. Можайского – 2015.
6. Руководство к разработчикам. API Яндекс.Маркет.
7. Все технологии API Marketa: [сайт]. URL: https://tech.yandex.ru/market/

УДК 004.42

Е. А. Бовыкин (студент группы ИСТ-541, СПбГУТ)
Н. С. Фёдоров (студент группы ИСТ-541, СПбГУТ)

ОПТИМИЗАЦИЯ ПЕРЕМЕЩЕНИЯ ЛАЗЕРНОЙ ГОЛОВКИ С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

Оптимизация перемещения головки станка лазерной резки является важной задачей производства, так как позволяет экономить время и механический ресурс станка. Нахождение оптимального пути можно свести к решению «задачи коммивояжёра», которая является NP-полной, и для более эффективного её решения можно применить биоинспирированные методы.

генетические алгоритмы, задача коммивояжёра, оптимизация.

Описание проблемы и постановка задачи

Станки для лазерной резки металлов отличаются высокой точностью и скоростью работы, однако имеют несколько недостатков. При лазерной резке станком потребляется большое количество электроэнергии, что сказывается на себестоимости продукции. Ещё один недостаток такого метода производства заключается в том, что запасные части к оборудованию имеют высокую цену и производятся за границей. Для устранения недостатков такого рода и повышения общей эффективности производства важна оптимизация всех его аспектов.

Наиболее подвержены износу движущиеся механические части станков. В лазерной резке механические части используются в основном для перемещения режущего элемента или системы зеркал.

Чтобы снизить нагрузку на механические системы станка необходимо провести оптимизацию программы управления, которая осуществляет расчёт траектории движения режущей головки по сегментам контура обрабатываемой детали.

Математическая формализация задачи

Схема формализации задачи оптимизации траектории движения при обработке излучением представлена на рисунке 1. Все дорожки, определяющие суммарную траекторию движения, подвергаются сегментации и нумеруются. Каждый сегмент $S_{(i)}$ может быть представлен следующим образом:

$$S_{(i)} \stackrel{\text{def}}{=} \langle x_a, y_a, x_b, \mathrm{y}_b, l, v, t, d, i \rangle, \tag{1}$$

где x_a, x_b, y_a, y_b – координаты начала и конца сегмента (точки a и b сегмента на рисеуrt 1), соответственно, l – длина сегмента, v – скорость прохождения сегмента, t – время, затрачиваемое на прохождение сегмента, d – направление прохождения сегмента, i – номер сегмента в очереди обработки. Список сегментов полностью определяет траекторию обработки:

$$List \stackrel{\text{def}}{=} \langle S_{(i,j)} \rangle, i, j \in \overline{1, n}, \tag{2}$$

где n – число сегментов, i – номер (идентификатор) сегмента, j – номер сегмента в списке, определяющий очередь обработки. Тогда время, затрачиваемое на обработку, будет:

$$T = T_{\text{р}} + T_{\text{хх}}, \tag{3}$$

где $T_{\text{р}}$ – время, затрачиваемое на обработку, $T_{\text{хх}}$ – общее время, затрачиваемое на прохождение кареткой от одного сегмента к другому, плюс время, необходимое для подхода к первому сегменту, и от первого к базе. Отсюда

задачу оптимизации можно сформулировать, как нахождение последовательности обработки сегментов и их ориентацию (начало и конец обработки), при которой время T, будет минимальным. Так как время, затрачиваемое на лазерную обработку сегментов не зависит от последовательности обработки сегментов, то интерес представляет минимизация только времени $T_{\text{хх}}$.

Описание генетического алгоритма

Исходя из условия задачи видно, что кодирование и оператор кроссинговера аналогичны задаче коммивояжёра [1], решаемой с помощью генетических алгоритмов [2, 3], за исключением добавления направленности прохождения сегмента d. Так как генетические алгоритмы показали свою эффективность при решении задачи коммивояжёра, то имеются все основания полагать, что они окажутся эффективными и для решения задачи оптимизации траектории движения обработке излучением.

1. Ген

В качестве гена будем использовать непосредственно список всех сегментов.

$$gene \stackrel{\text{def}}{=} List. \tag{4}$$

2. Фитнесс-функция

Определим фитнесс-функцию, как функцию, обратную расстоянию $T_{\text{хх}}$ холостого хода каретки.

$$f(gene) = \frac{1}{T_{\text{хх}}}. \tag{5}$$

3. Кроссовер

В качестве кроссовера будем использовать циклический кроссовер, или CX-crossover. Алгоритм, порождающий одного потомка, можно определить так:

1) Из двух потомков выбрать общий цикл C, начинающийся с первого элемента.
2) Из первого родителя выбираем все значения, которые попали C.
3) Из второго родителя выбрать все остальные значения, не попавшие в цикл C.

Пример.

Представим родителя в виде перестановки $(S_{(1,)}, S_{(2)} \dots S_{(n)})$ где $S_{(x)}$ – сегмент, стоящий на месте x.

Пусть первый родитель будет (1, 2, 4, 3), а второй – (2, 1, 3, 4). Общим циклов, начинающимся с первого элемента, будет (1, 2). Тогда порожденный потомок будет выглядеть (1, 2, 3, 4).

4. Мутация

Мутация будет проходить в два этапа. На первом выберем два случайных сегмента и поменяем их местами. На втором выберем случайный сегмент и перевернем его, то есть поменяем его направление. Формально второе изменение можно описать так

$$S_{(i,d)} = S_{(i,1-d)}, \tag{6}$$

где $S_{(i,d)}$ – случайно выбранный сегмент, а d – его направление прохода.

5. Отбор

Отбирать будем лучшую половину всей популяции сегментов, основываясь на определенную ранее фитнесс-функцию. Оставшуюся половину будем порождать при помощи определенного ранее кроссовера. Мутацию будем проводить каждый десятый цикл, мутируя 2 % популяции, но не меньше одной особи.

Заключение

Задача о минимизации движения режущего элемента в станке похожа на задачу коммивояжера, следовательно, для ее решения можно применять похожие методы. Являясь NP-полной, эту задачу, тем не менее, можно приближенно решать при помощи полиномиальных оптимизационных алгоритмов. Одним из них является генетический алгоритм, который даже на больших объемах данных дает хорошие приближенные результаты.

Программа, реализующая вышеописанный алгоритм, написана на языке C# с использованием технологии объектно-ориентированного программирования.

Список используемых источников

1. Моров В. А., Применение генетического алгоритма к задачам оптимизации. Реализация генетического алгоритма для задачи коммивояжера / Вестник АмГУ. 2012. № 57. С. 18–22.
2. Емельянов В. В., Курейчик В. В., Курейчик В. М. Теория и практика эволюционного моделирования. М. : Физматлит, 2003. С. 432.
3. Гладков Л. А., Курейчик В. В, Курейчик В. М. Биоинспирированные методы в оптимизации: монография. М. : Физматлит, 2009. С. 384.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Акимовым С. В.

УДК 004.946

И. М. Быжко (курсант 3 курса, ВКА им. А. Ф. Можайского)
А. Б. Менисов (адъюнкт, ВКА им. А. Ф. Можайского)

ВЫЯВЛЕНИЯ ВЗАИМОСВЯЗЕЙ ИСТОЧНИКОВ ПРОПАГАНДЫ ИГИЛ (ЗАПРЕЩЕННОЙ В РФ)

Статья посвящена проблеме пропаганды терроризма в сети Интернет. Автор приводит особенности современной пропаганды ИГИЛ (запрещенной в РФ), а также способы ее идентификации.

социальные сети, ИГИЛ, Maltego.

Исламское государство Ирака и Леванта – международная исламистская суннитская террористическая организация, действующая преимущественно на территории Сирии (частично контролируя её северо-восточные территории) и Ирака (провозглашённое как всемирный халифат 29 июня 2014 г.), непризнанное государство с шариатской формой правления [1].

У ИГИЛ (организация запрещена на территории РФ решением Верховного суда) существует мощная пропагандистская структура, нацеленная на иностранную аудиторию, в частности, на «европейских» мусульман. Под «европейскими» понимаются как этнические, так и новообращенные мусульмане, проживающие в Западной Европе, Северной Америке, Австралии.

Главным медиа-центром, ведущим пропаганду среди иноязычной аудитории, является агентство «*Alhayat*». Данный медиа-центр выпускает короткие видеоролики, которые стали популярным способом привлечения новобранцев.

Вся продукция, выпускаемая агентством «*Alhayat*» для привлечения новых сторонников, концентрируется вокруг нескольких сюжетов и тем.

ИГИЛ присутствует в Интернет-пространстве повсеместно. О своих победах и различных акциях формирование тут же объявляет, выкладывая очередной ролик или пост в социальной сети. Группировка часто фигурирует в новостных лентах Европы и США, что усиливает присутствие ИГ в мировом информационном пространстве. Конечно, главной площадкой для пропаганды и информационной экспансии идей «Исламского Государства» являются социальные сети, такие как *Facebook* и *Twitter*, где несмотря на противодействие администрации сайтов группировка оперирует тысячами аккаунтов [2].

В настоящее время деятельность террористической группировки ИГИЛ (запрещенной в РФ) представляет собой угрозу национальной безопасности. Это угроза распространяется не только в материальном мире

(в виде терактов, убийств и захвате мирных людей), но и виртуальном. Данная группировка проводит полномасштабные акции пропаганды и вербовки не только в социальных сетях и на отдельных сайтах, но и имеет свои периодические издания.

Основным изданием ИГИЛ является журнал «*Dabiq*», целью которого является распространение радикальных взглядов, объединение последователей джихада. Начало издания «*Dabiq*» – 2014 год. Является не первым профессиональным изданием террористическим журналом.

Одним из родоначальников был «*Inspire*». Журнал начал издаваться под редакцией Аль-Каиды в 2010 г. В отличии от «*Dabiq*» здесь есть разделы «сделай сам», а также адреса для обратной связи с редакцией журнала.

Собирая информацию в сети Интернет, связанную с этими адресами, посредством программы «*Maltego*», была определена взаимосвязь между ними, а также валентность источников информации и пропаганды ИГИЛ. «*Maltego*» – это инструмент для построения и анализа связей между различными субъектами и объектами [3]. Особенностями данной программы является визуализация полученных данных, добытых из открытых источников, комбинирование для глубокого анализа данных полученных из закрытых и открытых источников, автоматический анализ открытых источников и автоматическое построение взаимосвязей между обнаруженными объектами.

Данная программа может быть использована для выявления отношений и реальных связей между: людьми, группами людей (социальные сети), компаниями, организациями, веб-сайтами, интернет инфраструктурами, факторами, документами и файлами (рис. 1).

Введя перечень адресов, которые опубликованы для обратной связи с редакцией журнала, программа проанализировала и выявила связи между данными электронными адресами.

Рис. 1. Выявленные связи между электронными адресами

На графике можно увидеть входящие и исходящие связи электронного адреса (рис. 2). Входящих связей всего две, а исходящих 13. Следовательно, что превосходящее количество входящих связей на объект подразуме-

вает под собой объект вербовки и пропаганды. А превосходящее количество исходящих связей на объект – означает источник пропаганды и вербовки. Можно сделать вывод, что данный электронный адрес используется для пропаганды Исламского государства и также для вербовки людей.

Рис. 2. Результат выявления взаимосвязей источников пропаганды

В настоящее время деятельность террористической группировки ИГИЛ (запрещенной в РФ) представляет собой угрозу национальной безопасности. Это угроза распространяется не только в материальном мире (в виде терактов, убийств и захвате мирных людей), но и виртуальном. Существующая необходимость выявления данного распространения возможно решить не только в ручном режиме, но и в автоматизированном. Одним из примеров, является расширение «Maltego» ОС «Kali Linux».

Список используемых источников

1. Менисов А. Б., Быжко И. М. Идентификация процесса вербовки и пропаганды радикального исламизма в российском секторе социальных сетей, проводимый международной террористической организацией ИГИЛ // Информационное обеспечение: материалы конференции военно-научного общества Военно-космической академии им. А.Ф. Можайского. СПб., 2015. С. 196–199.

2. По ту сторону халифата: как происходит вербовка в ИГИЛ / Империя – информационно-аналитический портал. URL: http://www.imperiyanews.ru/details/10162a15-eef0-4743-a190-38c93aac092a

3. *Maltego* для помощи социальным инженерам / HPC: [сайт] – URL: http://hpc.name/thread/36977/p1.html

УДК 004.42

Д. О. Вахрушев (студент группы ИСТ-22, СПбГУТ)

ИССЛЕДОВАНИЕ СРЕДСТВ ИНФОРМАЦИОННОЙ УДАЛЕННОЙ ПОДДЕРЖКИ РЕСУРСОВ ИНФРАСТРУКТУРЫ КОМПАНИИ

В повседневной работе офиса важную роль играет бесперебойная работа техники. Менеджеры, работающие с документами и клиентами, зачастую плохо владеют техникой, и не могут решить даже незначительные проблемы.

В каждой компании есть системный администратор или IT отдел. Поскольку у компании может быть несколько филиалов по городу или по стране, то большую роль играет удаленная IT поддержка, которая помогает оперативно решить проблемы с техникой, прикладывая минимум усилий и финансы компании.

IT поддержка, удаленная поддержка, IT отдел, технологии.

Технологии автономной информационной поддержки рассчитаны на решение проблем без подключения к интернету. К таким технологиям можно отнести справочники, компонент «устранения неполадок» Windows, базы знаний. Данная технология информационной поддержки малоэффективна и может решать исключительно типовые проблемы малой сложности.

Во многих программах имеется встроенный справочник, в котором можно найти нужную информацию о функционале программы и найти методы исправления типовых ошибок программы. Использование справочников позволяет найти информацию намного быстрее, чем с помощью других источников. Огромным плюсом данного вида информационной автономной поддержки является простота использования и отсутствие каких-либо дополнительных установок [1].

Раздел «Устранение неполадок» содержит программы, которые способны автоматически исправлять распространенные проблемы, например, проблемы, возникающие при работе с сетью или проблему совместимости программ.

В базе знаний компании хранится информация о всех неисправностях, которые были замечены и работах, которые проводились на компьютерах компании. Это совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью компьютеров, представленная в объективной форме [2].

Стандартная запись в базе знаний хранит в себе следующие сведения:

– дата обращения;
– номер компьютера, на котором возникла не исправность;
– данные специалиста, который устранял неисправность;

– описание неисправности;
– описание метода решения неисправности.

Ведение базы знаний неисправностей позволяет:

– быстро исправлять неисправности, которые уже возникали на компьютерах компании;

– отслеживать проблемные места в сети компании;

– проводить инструктаж сотрудников по проблемам которые наиболее часто встречаются;

– проводить обучение сотрудников, которые неуверенно пользуются ПК.

При совместной работе или обучении персонала новым программным компонентам системы, используется управление удаленным рабочим столом, компьютера, посредством передачи данных через сеть интернет. Данные процессы стали возможны, благодаря способности современных программ передавать данные на удаленный компьютер [3].

В настоящее время можно выделить два средства, которые обеспечивают данную технологию.

Программное обеспечение Radmin (*RemoteAdministrator*) для платформы Microsoft Windows позволяет сотруднику IT-отдела одновременно работать сразу на нескольких удалённых компьютерах посредством графического интерфейса. В программе реализована возможность передачи файлов и использование текстового или голосового общения с пользователем удаленного компьютера.

Удалённый компьютер может располагаться как в локальной сети, так и в сети Интернет. Программа имеет возможность настройки качества картинки, что позволяет использовать её даже при низкой скорости соединения.

Вторым средством, позволяющим удаленно подключаться к компьютеру, является TeamViewer. В программе реализованы функции обмена файлами, голосовыми и текстовыми сообщениями, а также вести сеансы видеосвязи и веб-конференции. TeamViewer работает на большинстве известных операционных системах, таких как: Windows, Mac OS X, iOS, Linux, Android. Помимо прямого соединения, доступ возможен через веб-браузер. По официальной информации данная программа установлена более чем на 15 миллионах компьютеров по всему миру.

В таблице 1 представлено сравнение средств удаленной поддержки.

ТАБЛИЦА 1. Сравнение средств удаленной поддержки

Продукт	**TeamViewer**	**Radmin**
Протокол	Собственный	Собственный
Лицензирование	Собственный	Собственный

Продукт	TeamViewer	Radmin
Режим работы	Клиент&Сервер	Клиент&Сервер
Встроенное шифрование	Aes-256	Aes-256
Передача файлов	+	+
Передача звука	+	+
Многоклиентный режим	+	+
Бесшовные окна	+	+
Удаленный помощник	+	+
Запрос права доступа	+	+
Обход NAT	+	-
FreeBSD клиент	-	-
Linux клиент	+	+
Mac OS клиент	+	-
Microsoft windows клиент	+	+
Java клиент	+	-
IOS клиент	+	-
Android клиент	+	-
Фиксированный ID	+	-

Таким образом, программа TeamViewer является лучшей программой для работы с удаленным компьютером.

Наличие клиентских приложений способствует упрощению работы конечного пользователя базы данных. От него скрыты объекты базы данных, содержащие реальную информацию, программный код, а также происходящие внутри нее события. Современные технологии делают работу с прикладными программами для конечного пользователя более интуитивной: они дают ему возможность сосредоточится на выполнении своих прямых обязанностей и, тем самым, способствуют повышению производительности его труда.

Компания Актуальный дизайн, существующая с 2002г. ежедневно сталкивается с проблемами, связанными с отсутствием интернета. Создание специализированного программного решения позволит оперативно исправлять возникшие проблемы с подключением и экономить финансы компании. Интерфейс проектируемого средства представлен на рисунке 1.

Предлагаемая программа требуется при отсутствии подключения к интернету и невозможностью решения проблемы программой автономной поддержки. Смысл работы программы заключается в возобновлении работы интернета. Она не предусмотрена для работы с модемами, так как у

них имеются собственные средства для проверки корректности соединения, а так же программа не исправляет ошибки со стороны провайдера.

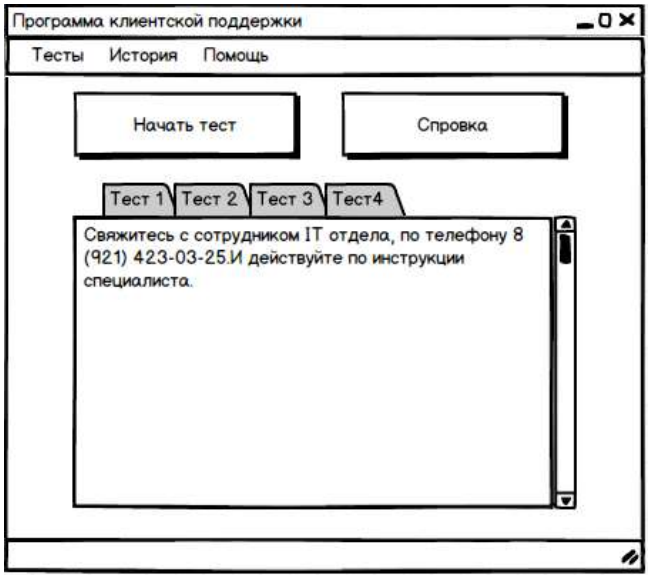


Рис. 1. Интерфейс программы

Суть программы заключается в пошаговой проверке интернет соединения посредством стандартных программ ping, tracer, nslookup и ipconfig. По окончанию проверки, программа выдает отчет о правильности настройки ip адреса, маски подсети, основного шлюза и DNS сервера. В случае обнаружения ошибки, команда выводит инструкцию по ее исправлению, а также показывает место сети, где обрывается сигнал. Данная информации поможет системному администратору в кратчайшие строки наладить работу сети.

Список используемых источников

1. Граничин О. Н., Кияев В. И. Информационные технологии в управлении: учебное пособие. М. : ИНТУИТ, 2008. 336 с.

2. Грекул В. И., Денищенко Г. Н., Коровкина Н. Л. Управление внедрением информационных систем: учебник. М. : Интернет-Университет Информационных Технологий, 2008. 224 с.

3. Рой Аалдерс ИТ аутсорсинг. Практическое руководство / пер. с англ. С. Зинюк.М. : Альпина Бизнес Букс, 2004. 300 с.

Статья представлена научным руководителем,
старшим преподавателем Гвоздковым И. Д.

УДК 629.7.05

А. В. Гаврилова (курсант 923 уч. группы, ВКА им. А. Ф. Можайского)

ВЫБОР ТЕЛЕМЕТРИРУЕМЫХ ПАРАМЕТРОВ С УЧЕТОМ ИХ ЦЕННОСТИ ДЛЯ РАСПОЗНАВАНИЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ КОСМИЧЕСКИХ СРЕДСТВ

В статье рассматриваются вопросы формализованного представления семантических свойств диагностической информации, используемой для анализа состояния сложных технических объектов. Предлагается алгоритм выбора дискретных диагностических признаков с учетом их ценности для распознавания технического состояния космических средств. Процедура распознавания технического состояния представляется в виде ориентированного графа.

космические средства, техническое состояние, ценность информации, процедура анализа технического состояния.

Достоверность результатов анализа технического состояния (ТС) бортовых систем (БС) космических средств (КСр) зависит от различных свойств информации, используемой лицом, принимающим решения, для выработки и реализации соответствующих действий, эффективность которых может быть в какой-то мере оценена. К настоящему времени разработаны алгоритмы оценивания синтаксических свойств информации. Попытки же формализованного представления семантических свойств информации сопряжены с определенными трудностями, связанными с субъективизмом при оценивании смысла и ценности информации.

Одним из первых, кто ввел понятие ценности (полезности) информации, был академик А. А. Харкевич [1]. Он определил ее как свойство информации изменять эффективность (результативность) инициированного ею целенаправленного процесса, в частности, процесса функционирования системы, в которой используется данная информация.

Обстоятельный анализ подходов к определению и вычислению ценности информации сделан в работе Г. П. Шанкина [2], который предложил аксиоматическое определение понятия «ценности информации» и разработал ряд математических моделей, позволяющих вычислять ценность информации, необходимой пользователю для достижения некоторой цели. Развиваемый в этой работе подход базируется на трудах Р. Л. Стратоновича и М. М. Бонгарда.

В работе [3] В. И. Корогодин предложил другой способ исчисления ценности информации, при котором ее величина изменяется от 0 до 1. Для некоторых приложений теории анализа технического состояния такой подход может представлять практический интерес.

Для постановки и решения задачи воспользуемся моделями, состоящими из упорядоченных множеств [4]:

$$\mathrm{M}_{\text{о}} = \langle S, \Pi, \Sigma, P, \Phi \rangle; \quad (1)$$

$$\mathrm{M}_{\text{п}} = \langle S, \Omega, \mathrm{P}, \hat{\Pi} \rangle. \quad (2)$$

Первое из этих множеств является моделью объекта анализа, а второе – моделью процесса анализа ТС КСр.

Здесь $S = \{S_i \mid i = \overline{1,m}\}$ – множество ТС, в одном из которых находится анализируемый объект; $\Pi = \{\pi_j \mid j = \overline{1,n}\}$ – множество диагностических признаков, на котором все состояния $S_i \in S$ попарно различимы; $\hat{\Pi} = \{\hat{\pi}_j \mid j = \overline{1,n}\}$ – множество проверок заданных (или выбранных) диагностических признаков; $\Sigma = \{\sigma_{ij} \mid i = \overline{1,m}; j = \overline{1,n}\}$ – множество значений модельных признаков, каждый из которых означает наиболее вероятный исход проверки $\hat{\pi}_j \in \hat{\Pi}$ в ТС $S_i \in S$; $P = \left\{ P(S_i) \mid \sum_{i=1}^{m} P(S_i) = 1 \right\}$ – множество вероятностей ТС $S_i \in S$; $\Phi : S \times \Pi \to \Sigma$ – отображение, при котором $\sigma_{ij} = \Phi(S_i, \hat{\pi}_j)$; $\Omega = \{R \mid R \subseteq S\}$ – алгебра (или σ-алгебра) подмножеств множества S в которой элементы R имеют смысл информационных состояний (ИС) моделируемого процесса, а каждый из них представляет собой подмножество «подозреваемых» ТС, в одном из которых может находиться объект в момент анализа его состояния; $\mathrm{P} = \left\{ P(R) \mid P(R) = \sum_{S_i \in R} P(S_i), R \in \Omega \right\}$ – вероятностная мера, заданная на множестве Ω. Вероятности $P(R) \in \mathrm{P}$ информационных состояний $R \in \Omega$ как элементов алгебры случайных событий определяются вероятностями входящих в них «подозреваемых» ТС.

В рамках моделей (1) и (2) реализуется последовательная процедура анализа (ПА) ТС. Основными ее элементами являются ИС $R \in \Omega$. Под действием проверок $\hat{\pi}_j \in \hat{\Pi}$ производится последовательный переход от одного ИС к другому, пока не будет определено ТС, в котором находится объект.

Каждая проверка $\hat{\pi}_j \in \hat{\Pi}$ может иметь некоторое (конечное) число исходов. Общее число исходов проверки $\hat{\pi}_j$ в ИС R_k обозначим через ω_{kj}, а порядковый номер исхода – через $v = \overline{1, \omega_{kj}}$. Отдельная проверка $\hat{\pi}_j$ при

ее v-м исходе ($v=\overline{1,\omega_{kj}}$) переводит процесс анализа из некоторого ИС $R_k \subseteq S$ в состояние $R_{kj}^v \subset R_k$, реализуя отображение

$$\hat{\pi}_j : R_k \to R_{kj}^v \ (v=\overline{1,\omega_{kj}}),\ R_{kj}^v = \{S_i \mid S_i \in R_k\}. \qquad (3)$$

Вероятность $P_k\left(\hat{\pi}_j^v\right)$ перехода из ИС R_k в ИС R_{kj}^v при выполнении проверки $\hat{\pi}_j \in \hat{\Pi}$ определяется по формуле

$$P_k\left(\hat{\pi}_j^v\right) = \frac{\sum\limits_{S_i \in R_{kj}^v} P(S_i)}{\sum\limits_{S_i \in R_k} P(S_i)},\ v=\overline{1,\omega_{kj}}. \qquad (4)$$

Для достижения конечного ИС R_i в общем случае требуется несколько раз выполнить отображение (3), используя при этом проверки различных признаков $\pi_j \in \Pi$. Они выбираются при составлении ПА ТС объекта. В совокупности эти признаки составляют подмножество $\Pi_i \subseteq \Pi$, проверка которых необходима для определения i-го ТС объекта.

Рассмотрим меру ценности информации, предложенную В. И. Корогодиным в работе [3], и модифицируем ее для использования в рассматриваемой предметной области.

Эта мера имеет следующий вид:

$$C = \frac{P-p}{1-p}, \qquad (5)$$

где P и p представляют собой вероятности достижения цели при использовании получаемой информации и без ее использования соответственно.

Целью функционирования ПА является распознавание конкретного ТС $S_i \in S$, в котором находится анализируемый объект. Следовательно, в качестве вероятности p в формуле (5) можно использовать вероятность $P(S_i)$.

Рассмотрим теперь ИС $R_{kj}^v \subset R_k$, полученное в результате проверки $\hat{\pi}_j \in \hat{\Pi}$, выполненной в ИС R_k. Это ИС включает в свой состав в общем случае несколько предполагаемых ТС $S_i \in S$, в одном из которых может находиться объект анализа.

Для распознавания этих состояний необходима дополнительная информация, которая обладает некоторой ценностью. Эта информация может быть получена в результате выполнения последующих проверок.

Тогда в качестве вероятности P в формуле (5) можно использовать уточненную вероятность P_i ТС $S_i \in R_{kj}^{v}$, определяемую по формуле

$$P_i = \frac{P(S_i)}{\sum\limits_{S_i \in R_{kj}^{v}} P(S_i)}. \tag{6}$$

Обозначим через $V_{kj}^{v}(S_i)$ ценность информации, которую необходимо получить для распознавания конкретного ТС $S_i \in R_{kj}^{v}$ и будем определять ее по формуле

$$V_{kj}^{v}(S_i) = \frac{P_i - P(S_i)}{1 - P(S_i)}. \tag{7}$$

Если ИС R_{kj}^{v} состоит только из одного ТС $S_i \in S$, то в соответствии с (6) вероятность P_i становится равной единице.

Ценность информации, которая необходима для распознавания всех ТС $S_i \in R_{kj}^{v}$, определяется по формуле

$$V_{kj}^{v} = \sum_{S_i \in R_{kj}^{v}} P_i \cdot V_{kj}^{v}(S_i). \tag{8}$$

Для вычисления ценности информации $V_k(\hat{\pi}_j)$, получаемой при выполнении проверки $\hat{\pi}_j \in \hat{\Pi}$ в ИС R_k, необходимо усреднить результаты, полученные при вычислениях по формуле (8), по вероятностям реализации исходов этой проверки, используя формулу

$$V_k(\hat{\pi}_j) = \sum_{v=1}^{\omega_{kj}} P_k(\hat{\pi}_j^{v}) \cdot V_{kj}^{v}, \tag{9}$$

Выражение (9) можно записать в развернутом виде:

$$V_k\left(\hat{\pi}_j\right)=\sum_{v=1}^{\omega_{kj}}\frac{\sum\limits_{S_i\in R_{kj}^v}P\left(S_i\right)}{\sum\limits_{S_i\in R_k}P\left(S_i\right)}\left[\sum_{S_i\in R_{kj}^v}\frac{P\left(S_i\right)}{\sum\limits_{S_i\in R_{kj}^v}P\left(S_i\right)}\cdot\frac{\dfrac{P\left(S_i\right)}{\sum\limits_{S_i\in R_{kj}^v}P\left(S_i\right)}-P\left(S_i\right)}{1-P\left(S_i\right)}\right]. \quad (10)$$

Формулы (9) и (10) будем использовать для вычисления ценности информации, получаемой в процессе анализа ТС объекта.

В работе [3] отмечается, что к ценности информации принцип аддитивности неприложим. В связи с этим предложенную формулу (9) можно использовать только для определения ценности информации, получаемой в процессе функционирования ПА, реализуемой последовательным методом, т. е. «прямым ходом», начиная от ИС $R_k=S$ и заканчивая конечными состояниями $R_i=\{S_i\}(i=\overline{1,m})$. На каждом шаге функционирования ПА выбирается наилучший для проверки признак согласно условию

$$\pi_j=\arg\max_{\pi_s\in\Pi_k}\left\{V_k\left(\hat{\pi}_s\right)\right\},$$

где Π_k – подмножество допустимых для проверки признаков $\pi_j\in\Pi$, определяемое из условия

$$\pi_j\in\Pi_k,\ \text{если}\ \exists\left(S_i,S_f\in R_k\right):\left(s_{ij}\neq s_{fj}\right).$$

В результате найдем все упорядоченные подмножества, задающие состав и очередность проверки признаков $\pi_j\in\Pi$ для определения конкретного ТС $S_i\in S$ БС. Вместе с тем найдем все ветви ПА, задающие условия перехода от одного проверяемого признака к другому в зависимости от исходов проверки первого. Эти условия позволяют при распознавании ТС привлекать именно то подмножество наиболее ценных телеметрируемых параметров, которое объективно необходимо для идентификации состояния БС.

С помощью разработанного алгоритма и реализующего его программного обеспечения может быть синтезирована процедура определения как работоспособных ТС БС КСр в различные моменты времени, так и неработоспособных состояний, обусловленных различными дефектами бортовой аппаратуры. При этом выбор минимально необходимого числа диагностических признаков (минимального необходимого числа проверок), обладающих наибольшей ценностью, позволяет значительно сократить

объем обрабатываемой телеметрической информации, уменьшить число измерительно-преобразовательных устройств (датчиков), упростить и удешевить процедуру распознавания ТС БС, в том числе и отказов.

Список используемых источников

1. Харкевич А. А. О ценности информации. Проблемы кибернетики. Вып. 4. М. : Физматгиз, 1960. С. 53–72.

2. Шанкин Г. П. Ценность информации. Вопросы теории и приложений. М.: Филоматис, 2004. 128 с.

3. Корогодин В. И., Корогодина В. Л. Информация как основа жизни. Дубна: Издательский центр «Феникс», 2000. 205 с.

4. Мышко В. В., Кравцов А. Н., Копкин Е. В., Чикуров В. А. Теоретические основы и методы оптимизации анализа технического состояния сложных систем: монография. СПб. : ВКА им. А. Ф. Можайского, 2013. 303 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Кравцовым А. Н.

УДК 004.021

Д. С. Давыдова (курсант 923 уч. группы, ВКА им. А. Ф. Можайского)

ОПЕРАТИВНЫЙ АЛГОРИТМ СПЕКТРАЛЬНО-КОРРЕЛЯЦИОННОЙ ОБРАБОТКИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ РАКЕТ КОСМИЧЕСКОГО НАЗНАЧЕНИЯ

Комплексный анализ позволил выявить нерациональность использования «классического» подхода к оцениванию спектрально-корреляционных свойств телеметрической информации ракет космического назначения ввиду больших временных затрат. Разработан оперативный алгоритм на основе теории выбросов, позволяющего вычислять все значимые спектрально-корреляционные характеристики на этапе экспресс-обработки с требуемой степенью точности.

Приведено описание программного модуля, осуществляющего оценивание спектрально-корреляционных свойств двумя способами: применяемым на современном этапе и разработанным в данной работе с помощью характеристик превышения уровней.

телеметрическая информация, спектрально-корреляционные характеристики, форма спектра.

В общем случае процесс обработки телеизмерений состоит из оперативной и полной обработки [1]. Структуры и режимы работы подсистем, а также методы, алгоритмы обработки и используемые в этих системах средства существенно различны.

Под оперативной обработкой понимают обработку информации, полученной от наиболее важных источников, с целью оценки функционирования испытуемых РН и КА и установленных на них систем, а также хода проведения испытаний в целом

Полная обработка является значительно более трудоемким и длительным процессом: производится обработка всех собираемых при испытании РН данных по достаточно сложным алгоритмам и производится учет всех прямо или косвенно влияющих на полет факторов.

В качестве исходных данных выступают измерения функциональных ТМП РКН, которые являются аналоговыми, однако передаются дискретными наблюдениями $y(t_i)$ в моменты времени t_i, i=0, 1 ..., N, отсчитанные с фиксированным шагом $T_0 = t_i - t_{i-1}$ дискретизации по времени.

Для этих исходных данных необходимо синтезировать и реализовать алгоритмы, определяющие последовательность операций по оцениванию следующих характеристик [1, 2]:

1) Корреляционной функции $R_{xx}(\tau)$.

2) Амплитудно-частотного спектра (спектральной плотности мощности) $S(\omega)$.

3) Коэффициент формы спектра $\aleph$.

По полученным характеристикам провести классификацию ТМП $y(t_i)$ (временных отрезков ТМП) по типам соответствующего им случайного процесса.

Для данной постановки установим следующие допущения и ограничения:

- все измерения $y(t_i)$ поступают последовательно, нет пропусков измерений и соответствующих им моментов времени;
- отбраковка аномальных измерений уже произведена;
- каждый из множества анализируемых ТМП можно отнести к одному из трёх наиболее распространённых классов случайных процессов.

В настоящее время для решения указанных задач применяются следующие основные подходы [3]:

- БПФ с прореживанием по времени;
- непараметрические методы (периодограмм, Уэлча, Бартлетта, Томсона);
- параметрические (авторегрессионный, Берга, ковариационный, Юла-Уолкера);
- применение соотношений Винера-Хинчина.

Для классификации ТМП по виду корреляционной зависимости в алгоритмах обработки в качестве метрики используется показатель ν^2, учитывающий корреляционную зависимость между значениями процесса и его второй производной в одинаковые моменты времени [4, 5]:

$$\nu^2 = 1 - \left(\frac{N^+(0,1)}{N_{\max}(1)} \right)^2, \quad \nu^2 \in [0,1] \tag{1}$$

где $N^+(0,1)$ – среднее число положительных пересечений траекторией информационного процесса нулевого уровня; $N_{\max}(1)$ – среднее количество локальных максимумов.

Характеристика ν^2 содержит полную информацию о законе распределения высот локальных максимумов.

Данная характеристика может принимать значения в диапазоне от нуля (гармонический процесс) до единицы (широкополосный шум). Исследования зависимости функции плотности вероятности высоты локальных экстремумов от характеристики ν^2 привели к выводу о том, что три модели информационных процессов наиболее равномерно перекрывают диапазон от узкополосного гармонического до широкополосного процессов.

Разобьём область определения ν^2 на три интервала, каждый из которых будет соответствовать определенному типу спектра:

$$\nu^2 \in [0;\ 0.556] \rightarrow \text{тип №1},$$

$$\nu^2 \in [0.556;\ 0.775] \rightarrow \text{тип №2},$$

$$\nu^2 \in [0.775;\ 1] \rightarrow \text{тип №3}.$$

Попадание ν^2 в один из этих интервалов определит тип спектральной плотности исследуемого процесса.

В результате статистических исследований наиболее часто используемых в задачах обработки информации моделей информационных процессов с различными видами корреляционных функций были выделены три модели (табл. 1), которые, являясь достаточно простыми, позволяют с высокой достоверностью оценивать корреляционные свойства ТМП.

Использование характеристики ν^2 дает возможность получать информацию о поведении того или иного параметра уже на этапе получения или экспресс обработки ТМИ, при этом корректирую и выбирая оптимальные алгоритмы сжатия и отбраковки аномальных измерений.

ТАБЛИЦА 1. Характеристики «превышений уровней» и спектрально-корреляционные характеристики информационных процессов с различными формами спектра

№	χ	ν^2	$S(\omega)$	$r(\tau)$	$-r''(0)$	$N_1^+(0,1)$	$N_{\max}(1)$
1	0,289	0,445	$\begin{cases} 2\pi/\Delta\omega, \lvert\omega\rvert \le \Delta\omega/2 \\ 0, \lvert\omega\rvert > \Delta\omega/2 \end{cases}$	$\frac{\sin(\Delta\omega\tau/2)}{\Delta\omega\tau/2}$	$\frac{\Delta\omega^2}{12}$	$\Delta\omega\left(1+\frac{\gamma_2}{8}\right)$	$0{,}25\Delta\omega\left(1+\frac{\gamma_2}{8}\right)$
2	0,399	0,667	$\sqrt{\frac{\pi}{\alpha}}\exp\left(-\frac{\omega^2}{4\alpha}\right)$	$\exp(-\alpha\tau^2)$	2α	$0{,}225\sqrt{\alpha}\left(1+\frac{\gamma_2}{8}\right)$	$0{,}39\sqrt{\alpha}\left(1+\frac{\gamma_2}{8}\right)$
3	0,490	0,888	$\frac{16\alpha^5}{3\left(\alpha^2+\omega^2\right)^3}$	$\left(1+\alpha\lvert\tau\rvert+\frac{1}{3}(\alpha\tau)^2\right)\times \exp(-\alpha\lvert\tau\rvert)$	$\frac{\alpha^2}{3}$	$0{,}092\alpha\left(1+\frac{\gamma_2}{8}\right)$	$0{,}276\alpha\left(1+\frac{\gamma_2}{8}\right)$

Таким образом, предложен следующий алгоритм оценивания формы спектральной плотности по статистикам превышения уровней, представляющий собой последовательность 5 основных шагов.

Шаг 1. Вычисление среднего числа положительных пересечений траекторией информационного процесса нулевого уровня

В том случае, если анализируемый процесс пересекает значение нуля с «минуса» на «плюс», то счетчик $N^+(0,1)$ прибавляет одно значение.

Шаг 2. Вычисление среднего количества локальных максимумов.

Шаг 3. Расчет характеристики ν^2: после анализа крайнего значения телеметрируемого процесса и завершения подсчетов пересечений и максимумов, вычисляется численное значение ν^2 по формуле (1).

Шаг 4. Формирование решающего правила: область определения ν^2 [0,1] разбивается на подмножества в соответствии с приближением к модельным значениям ν^2 основных учитываемых при анализе форм спектра.

Шаг 5. Определение типа спектра определяется принадлежность полученного на шаге 3 значения ν^2 к одному из интервалов разбиения, и в соответствии с этим приближенно определяется наиболее близкая к анализируемому процессу форма спектральной плотности.

Алгоритм оперативного оценивания типа спектра посредством вычисления метрики реализован на языке высокого уровня C++ в среде разработки Borland C++ Builder 6.

Основные функции, реализованные в программе:

- загрузка в программу принятых значений ТМП;
- отображение полученных дискретных значений процесса на график;
- оценивание спектральной плотности классическим способом с помощью дискретного преобразования Фурье;
- оценивание типа спектра по статистикам превышения уровней по коэффициенту;
- построение графиков фазового и амплитудного спектра сигнала;

- построение графиков корреляционной функции и модельной спектральной плотности в соответствии с решающим правилом;
- сохранение полученных результатов.

Для исследования достоверности работы разработанного алгоритма были смоделированы значения случайного процесса с заданными свойствами, а именно ТМП с корреляционными функциями, соответствующими основным трем формам спектра (см. табл. 1).

Для исследования достоверности работы разработанного алгоритма были смоделированы значения случайного процесса с заданными свойствами, а именно ТМП с корреляционными функциями, соответствующими основным трем формам спектра 1–3 из табл.1.

Для них были получены оценки корреляционных функций $R(\tau)$ смоделированных случайных процессов, а затем путём применения преобразования Фурье к корреляционной функции была получена спектральная плотность $S(\omega)$ анализируемых измерений.

На выходе программы разработанного алгоритма оперативного анализа формы спектральной плотности было получено числовое значение характеристики ν^2, в соответствии с которым проанализирована наиболее близкая к смоделированному процессу модельная форма спектральной плотности.

Телеизмерения были смоделированы с третьим типом спектральной плотности. В результате выполнения алгоритма на выходе программы получена оценка $\aleph$, в соответствии с которым был правильно определен тип спектра анализируемого процесса. Таким образом, можно говорить о достаточно высокой достоверности работы алгоритма.

В качестве исходных данных алгоритма были использованы измерения телеметрируемого процесса на борту РКН «Союз-2».

После применения разработанного алгоритма было выявлено, что на данном временном промежутке форма спектральной плотности совпадает с формой спектра на любом интервале анализа, причём оценка характеристики ν^2 и соответствующее ей значение $\aleph$ соответсвовало модели случайных процессов 1–3 (см. табл.1).

Таким образом, в данной работе была решена научно-практическая задача разработки алгоритмов оценивания спектрально-корреляционных характеристик ТМП при оперативной обработке телеметрической информации РКН. При этом были получены следующие основные результаты:

1) Результаты анализа современных подходов к оцениванию спектрально-корреляционных характеристик ТМП.

2) Алгоритм оперативного анализа типа спектральной плотности ТМП с использованием статистик превышения уровней.

3) Сегмент программного комплекса обработки ТМИ, реализующего разработанный алгоритм в виде программы на языке высокого уровня.

4) Результаты экспериментальных исследований как для моделированных, так и для реальных ТМП для оценивания качества работы алгоритма, а также предложения по практическому его использованию разработанного алгоритмов.

Новизна работы состоит в формировании, реализации и исследовании нового алгоритма оценивания спектрально-корреляционных характеристик ТМП РКН, основанного на элементах теории выбросов. При этом данный алгоритм может быть использован в программных комплексах обработки ТМИ РКН, эксплуатируемых в частях запуска и управления космических войск Воздушно-космических сил, а также в учебном процессе Военно-космической академии имени А. Ф. Можайского.

Список используемых источников

1. Чикуров В. А., Шмелев В. В., Зиновьев В. Г. Автоматизированная обработка телеметрической информации: учеб. СПб. : ВКА им. А. Ф. Можайского, 2014. 476 с.
2. Бендат Дж., Пирсол А. Прикладной анализ случайных данных. М. : Мир, 1989 540 с.
3. Сергиенко А. Б. Цифровая обработка сигналов. СПб. : Питер, 2002. 60 с.
4. Каргин В. А., Нездоровин Н. В., Николаев Д. А., Самойлов Е. Б. Особенности обработки ТМИ РН в реальном масштабе времени // Информация и космос. 2009. № 4. С. 77–82.
5. Тихонов В. И., Хименко В. И. Выбросы траекторий случайных процессов. М. : Наука, 1987. 304 с.

Статья представлена научным руководителем,
кандидатом технических наук Самойловым Е. Б.

УДК 654.739

В. О. Долгун (студент группы ИСТ-27, СПбГУТ)

РАЗРАБОТКА ИФНОРМАЦИОННОЙ УПРАВЛЯЮЩЕЙ СИСТЕМЫ ТИПА «УМНЫЙ ДОМ»

Комфорт является одним из важнейших стимулов прогресса, мотивируя человека изобретать всевозможные новшества в сфере информационных технологий для улучшения и облегчения собственной жизни. Данная статья посвящена рассмотрению разработки информационной управляющей системы типа «Умный дом».

умный дом, локальная сеть, сенсоры, контроллер домена, файловый сервер, коммутация, интернет, персональный компьютер, автоматизация.

Умный дом или здание – это, строение, которое оснащено специально разработанным планом проводки электроники для данного объекта, что позволяет пользователям дистанционно управлять или программировать массив автоматизированных домашних устройств путем ввода одной команды [1]. Особенностью Умного дома является то, что одна система может управлять другой, то есть системы объединены в целый управляемый комплекс.

Если рассматривать определение более детально, то под Умным домом следует понимать некую совокупность автоматизированных процессов, способную распознавать разные ситуации в различных режимах работы самого здания, будь то пожар или любое другое событие. Важным фактором, который отличает Умный дом от других систем, является то, что человек, используя смартфон, может одним нажатием задать нужное состояние подконтрольного помещения. В данном случае отпадает необходимость использования нескольких пультов и выключателей, потому как, нам достаточно иметь сенсорную панель или любое дистанционное управление для запуска одного из сценариев нужной подсистемы. Так, проходя по коридору, путь будет освещен, специальная система безопасности будет полностью выполнять все поставленные пользователем задачи, к которым могут относиться плановые проверки в течение дня, измерение температуры на улице и в доме, проверки утечки газа, копирование важных данных в установленных разделах и многое другое.

Главное и самое важное преимущество – это возможность контролировать всю систему дома из единого центра, который может находиться как в пределах строения, так и на сколь угодно удаленном расстоянии.

Умный дом – это не фантастика, как считали раньше, а новый уровень интеллектуальных систем управления, помогающий обеспечить согласованность и автоматику всех инженерных приборов и сетей дома в единое целое. Основной идеей Умного дома является управление всей бытовой техникой, климатом, освещением, охраной, сервером. Принципом системы является заданный и заранее прописанный алгоритм, который управляется автоматикой дома. Такая система помогает правильно распределить нагрузку на дом, обеспечить простоту и интуитивно понятный интерфейс контроля и управления домом.

Одновременно с управлением система предоставляет возможность пользователю получать информацию о состоянии различных параметров системы и событий, которые происходят в строение, а так же посылать на сервер команды для управления системой и ее отдельными компонентами.

Если рассматривать с точки зрения глубины реализации данной возможности, то выделяют три формы:

1) Автономная. Объект автономный, самоуправляемый и регулируемый. В его систему входит различная автоматика. Данная модель Умного

дома самая примитивная и распространенная в средствах массовой информации, где Умный дом выступает чудом техники, созданным человеком, предоставляющим ему массу возможностей.

2) Интеллектуальный дом. Дом имеет доступ к локальной сети и помогает связать все подсистемы в единое целое, а также осуществляет мониторинг различных подсистем: безопасности, сбережения энергоресурсов и других.

3) Высшая форма интеллектуального жилища. Дом, используя стандартные цифровые протоколы, способен обмениваться информацией как внутри, так и за его пределами. Все элементы системы включены в единую коммутационную сеть.

Любой Умный дом характеризуется наличием системы автоматизации и управления. Это комплекс разработанного программного обеспечения для взаимодействия подсистем и управления оборудованием, администрированием, автоматизацией, сбором данных с сенсоров в виде графиков. Главная цель, которую преследует автоматизация – бесперебойное и безопасное обслуживание всей инженерной и бытовой техники жилого или не жилого помещения, а так же различных сооружений. Управление происходит при помощи системы в которую уже заложен сценарий выполнения того или иного хода действий.

Модернизация становится доступной благодаря новым и современным устройствам управления, модулям, реле, которые в свою очередь замыкают или размыкают цепь, блокируют ее или же оптимизируют. При появлении процесса оптимизации человеку становится на много проще жить, так как он в любом месте, в любое время может посмотреть, как протекает тот или иной процесс. Например, к таким особенностям можно отнести возможность проведения незамедлительного просмотра и правильного учета всех данных с использованием контроллеров и датчиков [2].

В свою очередь датчик является объектом, целью которого становится обнаружение событий или изменений в окружающей среде, а затем обеспечение соответствующего вывода на контроллер.

В настоящий момент различные датчики широко применяются во время построения систем автоматического управления.

Расход электроэнергии с целью освещения может быть заметно снижен достижением оптимальной работы освещения в любой момент времени.

Добиться контроля освещения и учета присутствия людей в помещении можно применяя автоматическое включение света при движении. Управление освещением осуществляется с помощью инфракрасного датчика движения, который посылает на реле команду, указывающую, что нужно разомкнуть или замкнуть цепь электропитания.

На данный момент «Умный дом» является одним из передовых достижений в развитии домашних технологий. К основным достоинствам та-

кой автоматизации можно отнести комфорт и сохранение энергии, поскольку осуществляется контроль над температурой внутри строения и вне его, включения или выключения света, поддержания нужной температуры в котле дома для его обогрева и многое другое, на это требуется время и внимание. Исходя из всего этого «Умный дом» является эффективным и комфортным в управлении, помогая сэкономить время и деньги на его содержание.

Список используемых источников

1. Тесля Е. В. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире. СПб. : Питер, 2008. 224 с.
2. Arduino: [сайт]. URL: https://www.arduino.cc/ (дата обращения: 14.05.2016).

Статья представлена научным руководителем,
старшим преподавателем Козловой О. А.

УДК 004.925.83

Л. С. Дудаков (студент группы ИКПИ-41, СПбГУТ)
А. В. Тарлыков (начальник НОЦ «Лаборатория программирования», СПбГУТ)

РЕШЕНИЕ ЗАДАЧИ ВИЗУАЛИЗАЦИИ ПРОЦЕДУРНО ГЕНЕРИРУЕМОГО ЛАНДШАФТА ПРИ ПОМОЩИ АЛГОРИТМА НА ОСНОВЕ СТРУКТУРЫ «ДЕРЕВО КВАДРАНТОВ»

В статье описан алгоритм визуализации процедурно генерируемого ландшафта, который слабо занимает процессор и практически полностью оставляет его под нужны приложения. Кратко затронута тема процедурной генерации ландшафта.

компьютерная графика, ландшафт, визуализация, генерация, дерево квадрантов.

Введение

Визуализация ландшафта является важной задачей в области компьютерной графики. В играх и других приложениях часто присутствует необходимость отрисовки больших открытых территорий. Создание этих территорий является трудоемкой задачей для человека, поэтому часто её выполнением частично или полностью занимается компьютер. Таким образом, для использования ландшафта в компьютерной графике необходимо решить две задачи: его генерацию и визуализацию.

1. Обзор задач

Задача генерации ландшафта не является основной для этой статьи, поэтому будут рассмотрены лишь некоторые аспекты в области взаимодействия с задачей визуализации. Для генерации будут использованы комбинации многомерных функций, а именно: симплекс шум и диаграмма Вороного. Правильно подобранная сумма результатов работы таких функций неплохо справляется с задачей генерации, при этом вычисление такой суммы вполне возможно в реальном времени.

Сложность задачи визуализации состоит в том, что наблюдатель должен видеть все детали ландшафта на значительном расстоянии: как крошечные детали вблизи, так и крупные элементы вдалеке. В этом же состоит и основной путь оптимизации: вблизи ландшафт должен отображаться детализированно (высокий уровень детализации), а вдалеке можно обойтись гораздо меньшей детализацией (низкий уровень детализации), снижая тем самым количество данных для отрисовки.

Ландшафт может быть задан трехмерной моделью, или функцией от координат точки. В предлагаемой реализации ландшафт не моделируется заранее, а генерируется, поэтому представляться он будет функцией от координат. Можно выделить два вида таких функций: функция плотности и функция высоты. Функция плотности – это функция от координат точки (x, y, z), которая возвращает значение: если оно положительно, точка находится внутри ландшафта, если отрицательно – снаружи (в воздухе), если равно нулю, точка находится на поверхности ландшафта. Функция высоты – это функция от координат точки, которая возвращает расстояние, на которое эту точку необходимо сместить вверх (или вниз, если значение отрицательное). Использование функции высоты имеет ограничение в строгой горизонтальной направленности ландшафта. С ее помощью нельзя задать ландшафт с пещерами или навесами. Но это ограничение, будучи минусом, значительно упрощает и ускоряет работу с таким ландшафтом за счет устранения одного измерения. Поэтому алгоритм, описанный в этой статье, работает именно с ландшафтом, заданным такой функцией.

Далее будет описан алгоритм визуализации, который практически не задействует процессор при работе и хорошо подходит для отображения ландшафта, генерируемого в реальном времени. Он основывается на простейшем алгоритме визуализации ландшафта с помощью дерева квадрантов, но имеет и свои особенности. Освобождение процессора является важным моментом, поскольку именно процессор обычно занят логикой самого приложения или компьютерной игры.

2. Описание базового алгоритма на основе дерева квадрантов

Дерево квадрантов находится в основе многих алгоритмов визуализации с уровнями детализации. Описать базовый алгоритм его использования можно следующим образом:

a) В основании дерева находится квадрат (четыре трехмерные точки).

b) При необходимости повышения детализации (приближение камеры) он делится на четыре квадрата. Подобное деление применимо и к созданным дочерним квадратам.

c) При необходимости понижения детализации (отдаление камеры) четыре дочерних квадрата удаляются, вместо них остается один родительский. Удаления возможны пока не останется один квадрат – корень дерева.

При рисовании дерева происходит отбрасывание ветвей, которые находятся вне области видимости. Эта операция называется отсечением по пирамиде вида и подробнее про нее можно прочесть в статье [1].

3. Недостатки базовой версии

Базовая версия алгоритма предполагает, что каждый квадрат представляет из себя четыре трехмерные точки. И если вызывать процедуру рисования для каждого квадрата, то происходит обработка всего лишь этих четырех точек. Загружать все точки в буфер не представляется возможным, поскольку структура динамична и все время перестраивается при движении камеры. При приближении сильно возрастает количество квадратов-листьев в дереве, вместе с тем возрастает количество вызовов процедуры рисования. Это неэффективно: много раз вызывать рисование малого числа элементов. К тому же приходится хранить все точки, не смотря на то, что в соседних квадратах они дублируются.

4. Расширение алгоритма

Сетка вместо четырех точек в элементе дерева

Загрузка всех точек в единый буфер не представляется возможным, поэтому необходимо вызывать процедуру рисования для каждого листа дерева отдельно. Очевидно, что для повышения эффективности вызовов квадрат придется заменить на структуру, содержащую больше данных о ландшафте, чем четыре точки. Самым простым вариантом является квадратная регулярная сетка точек (рис. 1*a*). Регулярной называется сетка, все точки которой равномерно расположены. Вместо одного квадрата элемент дерева теперь представляет из себя сетку $N \times N$ квадратов. Вызовы процедуры рисования становятся намного более эффективными, и кроме того снижается число этих вызовов. Действительно, раз один элемент становится эквивалентен $N \times N$ элементам старого дерева, то и для поддержания тре-

буемого уровня детализации при приближении камеры придется производить гораздо меньше делений. Меньше делений – меньше листьев у дерева, а значит и меньше вызовов процедуры рисования.

На рисунке 1 можно наглядно наблюдать использование дерева квадрантов с регулярной сеткой в качестве элемента дерева: а) дерево состоит из одного элемента-основания; б) появляются четыре дочерних элемента (выделены красным), с аналогичными сетками 4×4; в) один из красных элементов делится, образуя четыре дочерних (выделены зеленым), с теми же сетками. Размер 4×4 используется только для демонстрации и не слишком повысит эффективность рисования по сравнению с алгоритмом без сетки. При решении реальных задач нужно использовать больший размер сетки, например, 64×64.

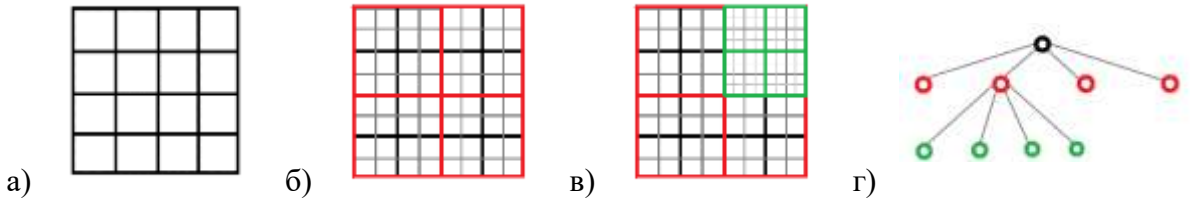


Рис. 2. Дерево квадрантов с использованием сетки 4×4

Одна единственная сетка на все элементы дерева

Решение одной проблемы найдено. И общее число точек снизилось за счет того, что в сетке дублирующиеся точки квадратов представляются в единичном экземпляре. Но возможно ли еще снизить количество точек?

Из рисунка 2 видно, что сетки разных элементов различаются лишь масштабом и высотой точек. Каждая точка в сетке обладает уникальным значением высоты. В данной реализации высота точки – это результат функции высоты от координат точки. Иными словами, высоту не обязательно хранить. Ее можно вычислить в любой момент, зная лишь координаты точки. А если не хранить высóты, то все сетки становятся абсолютно одинаковыми за исключением координат центра и масштаба.

Главная особенность, предлагаемого в данной статье алгоритма, заключается в использовании для отрисовки всех элементов одной единственной квадратной регулярной сетки двумерных (без значений высоты) точек. Левый верхний ее угол имеет координаты (−1; −1), а правый нижний (1; 1). В элементе дерева (квадратной области) находится информация о центре и о масштабе.

При отрисовке ландшафта на графический конвеер один раз передается сетка точек. Далее выполняется обход дерева и для конечных элементов дерева (листьев), которые находятся внутри пирамиды вида, выполняется следующее:

- В видеокарту посылаются данные о трансформации квадратной области (центр, масштаб).

- На этапе вершинного шейдера к каждой точке сетки применяются трансформации (сдвиг, масштабирование). Расчитывается и применяется к точке значение функции высоты от полученных координат. Так сетка принимает облик той части ландшафта, которая относится к текущей квадратной области.
- На этапе фрагментного шейдера через градиент функции высоты вычисляется нормаль. По значениям высоты и нормали генерируется цвет фрагмента. Применяется освещение.

Таким образом, значительно сокращается количество данных, передаваемых видеокарте для отрисовки.

Использование карт высот, нормалей, цветов

Если функция высоты является простой, то на данном этапе можно остановиться. Но получение сложного и интересного ландшафта возможно только с использованием сложной функции. А ее вычисление при каждом рисовании является слишком затратной операцией. Хорошо было бы по-прежнему не хранить значения высот и использовать одну единственную сетку для отрисовки, но при этом производить генерацию только по мере необходимости (при разделении квадрата на четыре дочерних). Решением этой задачи будет использование карт высот, нормалей и цветов. Карты представляют из себя текстуры с данными о куске ландшафта, который соответствует данной квадратной области. Для заполнения карты высот необходимо расчитать значения функции высоты в квадратной области точек. Такие массовые и независимые расчеты хорошо подходят для вычисления на видеокарте, тем более можно сразу производить запись результатов в текстуру, и не произойдет дополнительной нагрузки процессора. В используемом для этого фрагментном шейдере описаны функции генерации (шумы, ячеечные шумы и др.) и итоговая функция высоты. Затем по карте высот создается карта нормалей. Создание карты нормалей в отдельной операции экономит на расчетах градиентов (значения функции высоты берутся из карты высот). Во время этой операции можно также вычислять значения цветов и записывать их в карту цветов.

Заключение

В данной статье был описан эффективный алгоритм визуализации процедурно генерируемого в реальном времени ландшафта. Он прост в реализации и практически не занимает времени процессора, что является немаловажным фактором при разработке требовательных к процессору приложений и компьютерных игр. Также этот алгоритм обеспечивает высокую производительность на видеокартах средней мощности.

Список используемых источников

1. Бессмельцев М. Отсечение по пирамиде видимости в OpenGL [Электронный ресурс] // Работа с OpenGL. [2004]. URL: http://pmg.org.ru/nehe/nehex2.htm (дата обращения 11.06.2016).
2. Noise [Электронный ресурс] // Shadertoy Wikia: [сайт]. URL: http://shadertoy.wikia.com/wiki/Noise (дата обращения 27.05.2016).
3. Framebuffer Object [Электронный ресурс] // OpenGL Wiki: [сайт]. [2015]. URL: https://www.opengl.org/wiki/Framebuffer_Object (дата обращения 03.06.2016).
4. Framebuffer Object Examples [Электронный ресурс] // OpenGL Wiki: [сайт]. Электрон. текстовые дан. [2013]. URL: https://www.opengl.org/wiki/Framebuffer_Object (дата обращения 28.05.2016).

Статья представлена научным руководителем,
доктором технических наук, доцентом Ю. Ф. Болтовым.

УДК 004.91

О. А. Заварина (студент группы ТСС-25, СПбГУТ)

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ СОЗДАНИЯ И ОБРАБОТКИ ДАННЫХ УЧЕБНО-МЕТОДИЧЕСКОГО КОМПЛЕКСА

Рассматривается вопрос реализации программного обеспечения для создания и обработки данных учебно-методического комплекса, которое приведёт к повышению эффективности обучения, а также к экономии времени и ресурсов. Использование данной системы будет доступна пользователю в более легкой форме эксплуатации.

программа, данные учебно-методического комплекса, дисциплина, база данных, средства автоматизации, варианты использования (use case), объектная модель.

В настоящий момент в Российской образовательной системе происходят масштабные изменения, связанные с присоединением Российской Федерации к болонской декларации, а также принятые за последние годы различные указы, законы, постановления, направленные на реформирование всего образования. Высшего образования в особенности. Одной из важнейших частей учебного процесса является учебно-методический комплекс (УМК) дисциплины, представляющий собой совокупность учебно-методической документации, средств обучения и контроля, разрабатываемых в высшей школе Российской Федерации для каждого предмета, и обеспечивающий преподавание учебных дисциплин в соответствии с требованиями Федеральных государственных образовательных стандар-

тов [1]. Одной из важнейших проблем является создание комплекса, содержащий в себе:

- создание нового УМК,
- редактирование информационного профиля УМК,
- добавление новых дисциплин,
- редактирование информационного профиля дисциплин,
- добавление информации о лабораторных рабах,
- добавление практических работ в дисциплину,
- добавление курсовых работ в дисциплину,
- управление трудоемкостью,
- распределение дисциплин по блокам базовой и вариативной частей.

Исходя из этого приходим к выводу, что создание комплекса учебно-методического обеспечения образовательного процесса является очень сложной и трудоемко задачей, и такую сложную систему нужно поддерживать актуальной, что непросто, поэтому требуются средства автоматизации создания и обработки данных учебно-методического комплекса.

Разрабатываемая система должна обеспечить поддержку жизненного цикла УМК, начиная от формирования списка дисциплин, состава лабораторных работы и практических занятий, заканчивая согласованным внесением изменений в информационные профили элементов учебно-методического комплекса.

Для представления взаимодействия пользователей с разрабатываемой системой создания и обработки данных учебно-методического комплекса используются прецеденты (use cases), определяющие варианты использования системы. На рисунке 1 представлена диаграмма вариантов использования описывающая взаимодействие разработчика УМК и сотрудника УМУ с системой.

Структура объектов системы создания и обработки данных учебно-методического комплекса описывается с помощью объектной модели, в которой представлены атрибуты и операции системы, а также взаимосвязи с другими объектами. Для сохранения состояния объекта объектной модели, в данной системе используется база данных, в которой данные УМК хранятся в организованном порядке [2]. Автоматизированная система создается в виде веб-приложения ASP.NET, и реализует концепцию SaaS – доставка программного обеспечения по требованию [3].

Далее представлен интерфейс пользователя, в котором реализована программа в виде графических изображений понятных для посетителя данной веб-страницы. При входе в систему пользователь попадает на страницу заполнения данных УМК. После введения данных в поле «название» и «код» направления они сохраняются в базе данных при нажатии кнопки «добавить план» и отображаются на странице в таблице. При нажатии на ссылку «редактирование» пользователь переходит на вкладку с более подробным

описанием учебного плана. После введения значений в поля и нажатия кнопки «сохранить», данные записываются в базу данных. В последующем открытии данной веб-страницы загружаются данные, которые уже сохранены в базу данных, но при повторном редактировании информации и нажатии кнопки «сохранить», данные в базе данных обновляются. Графическое представление заполнения данных УМК и их редактирование представлено на рисунке 2.

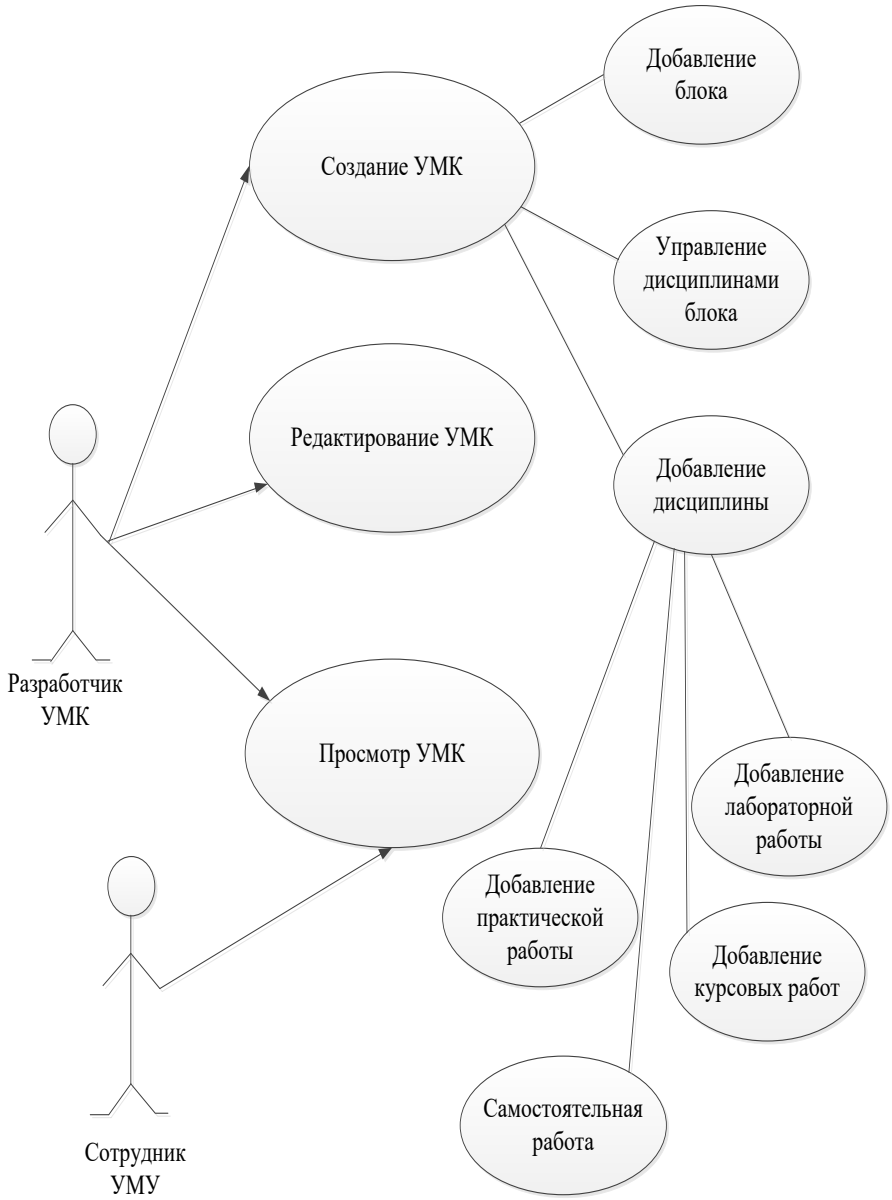


Рис. 1. Диаграмма вариантов использования

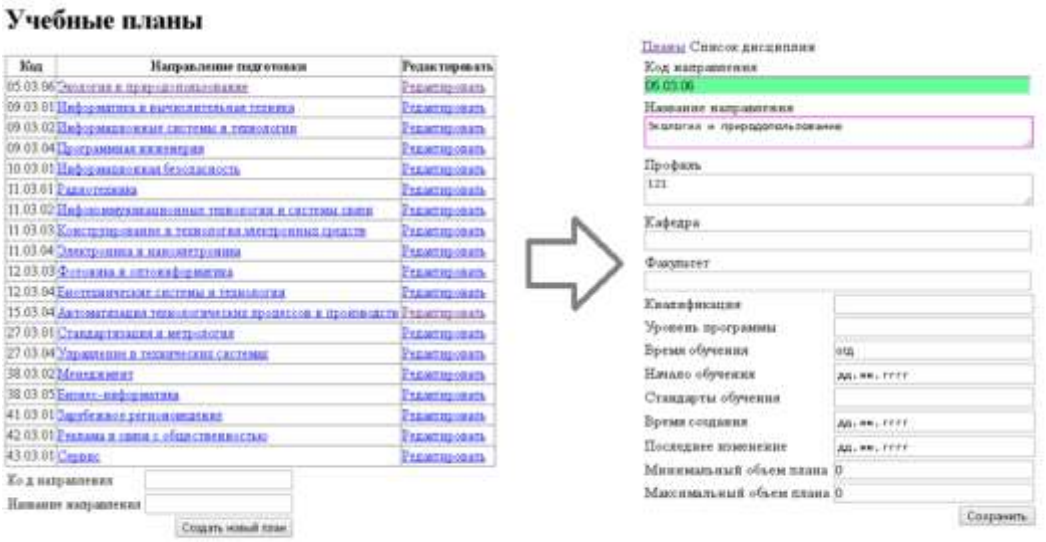


Рис. 2. Начальная страница заполнения данных УМК и их редактирование

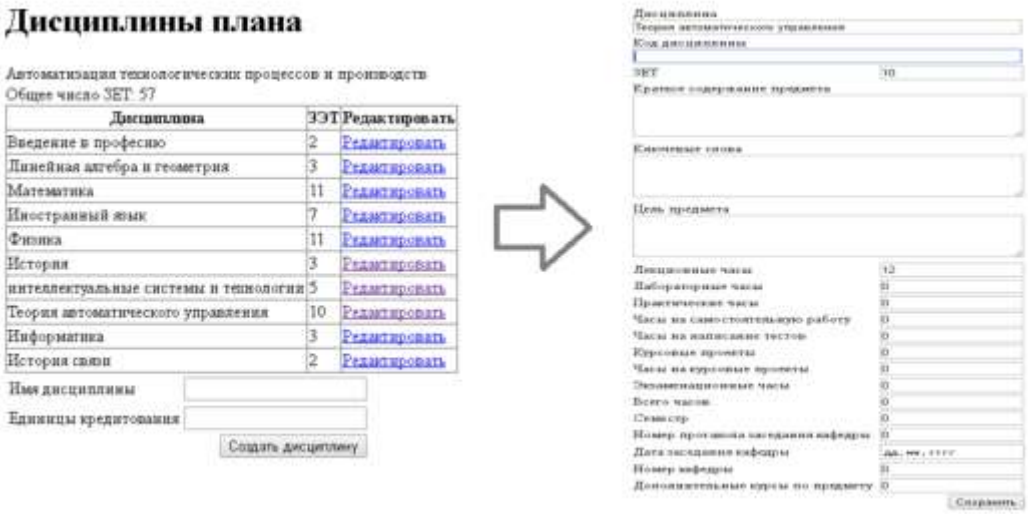


Рис. 3. Страница заполнения дисциплин и их редактирование

При нажатии на название направления, пользователь переходит на веб-страницу с добавлением дисциплин. После введения данных в поле «название» и «ЗЕТ» дисциплины они сохраняются в базе данных при нажатии кнопки «добавить дисциплину» и отображаются на странице в таблице. Также на данной странице осуществляется суммирование количества зачетных единиц всех дисциплин данного направления. На данной странице также имеется кнопка «редактирование», которая переходит на веб-страницу с подробным описанием дисциплины. После введения значений в поля и нажатия кнопки «сохранить», данные записываются в базу данных. В последующем открытии данной веб-страницы загружаются данные, которые уже сохранены в базу данных, но при повторном редактировании информации и нажатии кнопки «сохранить», данные в базе

данных обновляются. На рисунке 3 представлено заполнение и редактирование дисциплин учебно-методического комплекса.

В результате создания данной системы, пользователям данные УМК будет доступны в более легкой форме эксплуатации, что приведет к повышению эффективности, к экономии времени и ресурсов, а также повысит эффективность обучения.

Список используемых источников

1. Лебедева М. М. Введение / Болонский процесс: проблемы и перспективы. М. : Оргсервис, 2006. С. 6–10

2. Хомоненко А. Д., Цыганков В. М., Мальцев М. Г. Базы данных: учебник для высших учебных заведений / под ред. проф. А.Д. Хомоненко. СПб. : КОРОНА принт, 2000. 416 с.

3. Джеф Просиз. Программирование для Microsoft .NET = Programming Microsoft .NET. М. : Русская редакция, 2003. С. 704. ISBN 5-7502-0217-8.

Статья представлена научным руководителем,
доктором технических наук, профессором Верховой Г. В.

УДК 623.746

В. В. Звонарев (начальник лаборатории, ВКА им. А. Ф. Можайского)
И. Ю. Парамонов (докторант, ВКА им. А. Ф. Можайского)
И. С. Петрова (научный сотрудник, ВКА им. А. Ф. Можайского)

ПРОБЛЕМНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ СИСТЕМ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ

Увеличение возможностей систем и комплексов на основе беспилотных воздушных судов привело к использованию их для решения широкого круга задач пользователями, имеющими самые различные цели. Для эффективного противодействия злоумышленникам требуется создание системы противодействия беспилотным воздушным судам.

информационное обеспечение, воздушное судно, эффективность, обнаружение.

Введение

В соответствии с [1] беспилотное воздушное судно (БВС) – воздушное судно, которое предназначено выполнять полет без пилота на борту [1]. К БВС относятся самолеты, планеры, вертолеты, свободные аэростаты и т. д. Сфера применения БАС постоянно расширяется. Они выполняют задачи патрулирования,

аэрофотосъемки, видеосъемки, поиска и спасания, наблюдение за распределенными объектами, ретрансляция данных и пр.

Высокая потенциальная опасность и возможный ущерб от применения малоразмерных БВС и низкая эффективность современных средств обнаружения и подавления (поражения) малоразмерных БВС обуславливают необходимость проведения комплексных исследований по вопросам противодействия БВС. Одним из важных является вопрос повышения эффективности информационного обеспечения систем противодействия БВС. Качество информации (своевременность, безопасность, достоверность, полнота, достаточность и т. д.) определяет качество решения задач и эффективности функционирования системы противодействия БВС.

1. Системы противодействия БВС

При малой дальности действия средств обнаружения малоразмерных БВС, малых высотах полета и высоких относительных скоростях БВС существует проблемная ситуация, которая обостряется в связи с широким распространением и применением малоразмерных нано-, микро- и мини-БВС. Малые значения эффективной площади рассеяния БВС значительно затрудняют решение задачи их своевременного обнаружения и сопровождения «традиционными» радиолокационными средствами. Наибольшую трудность вызывает решение задачи обнаружения малоразмерных БВС с малыми значениями эффективной площади рассеяния, функционирующих без вмешательства пилота в управление полетом. Отсутствие информационного обмена БВС с пунктом управления и пунктами приёма специальной информации приводит к тому, что бортовое радиоэлектронное оборудование таких БВС не излучают радиосигналы, что не позволяет использовать пассивные средства, включая средства радио и радиотехнической разведки. Задача поиска и обнаружения малоразмерных БВС должна решаться комплексно средствами, которые построены на основе различных физических принципов.

Средства, комплексы и системы борьбы с малоразмерными БВС должны обеспечивать:

- своевременное обнаружение БВС,
- определение и выдачу координат БВС потребителям,
- эффективное управление силами и средствами поражения (подавления) БВС,
- поражение (подавление) БВС,
- подавление каналов управления и передачи данных.

Для решения проблемы борьбы с малоразмерными БВС необходима разработка новых способов, создание сил и средств борьбы с БВС, основанных на применении различных видов оружия различного базирования.

Для повышения дальностей обнаружения малоразмерных БВС могут использоваться системы на базе БВС (аэростатов, дирижаблей, вертолетов и т. д.), в состав бортового оборудования которых входят активные и пассивные радиолокационные средства, акустические средства, оптические средства и т. д. Необходимо применять соответствующие методы обработки разнородных данных, полученных на основе различных физических принципов.

Для поражения БВС и подавления (поражения) бортовых информационных систем БВС применяются кинетическое оружие, лазеры, средства радиоэлектронного подавления [4]. Ведутся работы по созданию оружия, основанного на применении мощных электромагнитных импульсов, способных выводить из строя радиоэлектронное оборудование БВС, что потенциально позволит повысить эффективность подавления (поражения)малоразмерные БВС.

Компания Northrop Grumman разработала и испытала высокоадаптивный многоцелевой радар HAMMR (*Highly Adaptable Multi-Mission Radar*) на основе активной антенной решетки с электронным сканированием, который предназначен для установки на истребителе.

Компания Thales Nederland использует в тактическом радаре Squire многолучевые методики с двухосными накопленными пучками и активными сканирующими решетками с целью достижения необходимого высокого доплеровского разрешения и времени необходимого для подсветки цели.

Компания Thales Air Defence производит зенитный комплекс RAPIDFire, который включает обзорную РЛС Thales CONTROL Master 60 и модуль управления CONTROLView, который может контролировать до шести зенитных установок RAPIDFire. Пушки в этом случае могут наводиться при помощи РЛС или прицельной оптико-электронной системы, установленной на крыше башни RAPIDFire. По данным Thales Air Defence 40-мм комплекс RAPIDFire приводится к бою за 60 секунд и обладает потенциалом ведения огня в движении. Последнее особенно важно для систем противодействия тактическим и малым БВС.

Во время испытаний в 2009 г. лазерной системы Laser Avenger, установленной на Boeing, проверялось смешанное применение боевых лазеров помогающих традиционным системам вооружения уничтожать БВС. Во время испытаний инфракрасный твердотельный лазер Laser Avenger был использован для подогрева небольшого БВС имеющего очень низкую тепловую сигнатуру до такого уровня, когда его смогла захватить на сопровождение и уничтожить ракета FIM-92 Stinger.

Швейцарская компания Rheinmetall Air Defence и немецкая Rheinmetall Defence разработали лазерную установку высокой мощности HPLW (high-power laser weapon), предназначенную первоначально для перехвата неуправляемых ракет, артснарядов и мин, но которая в перспективе может найти применение для борьбы с БВС. В 2010 г. были успешно проведены испытания HPLW по наземным целям. Киловаттный лазер HPLW уничтожил минометный выстрел. В 2011 г. в Швейцарии прошли демонстрационные стрельбы системы мощностью 5 кВт по БВС. Планируется провести испытания системы мощностью 20 кВт с большей дальностью действия.

В середине 2010 г. компания Raytheon испытала лазеры, добавив их к комплексу Phalanx CIWS. Во время испытаний было успешно подожжено небольшое БВС.

Израильская компания ARTsys 360 разработала радар для обнаружения малоразмерных БВС. Радар RS360-400 функционирует в диапазоне 4,8–5,8 ГГц, обеспечивает обзор пространства на 360° и предназначен для установки на земле, зданиях и т. д. и позволяет обнаруживать и сопровождать до 3-х БВС на дальностях до 400 м. На дальностях менее 300 м точность определения коор-

динат БВС составляет ±3 м [3]. Такие радары могут выдавать информацию предупреждения о приближении БВС на другие информационные средства или на средства подавления (поражения).

2. Информационное обеспечение систем противодействия БВС

Под информационным обеспечением будет понимать организованный непрерывный технологический процесс подготовки и выдачи информации потребителям в соответствии с их нуждами для поддержания эффективной деятельности [5].

Наличие сложного радиоэлектронного оборудования на борту современных БВС обусловливает наличие большого числа уязвимостей к внешним деструктивным воздействиям, а наличие уязвимостей позволяет эффективно реализовывать различные угрозы.

Для решения задач по предназначению и по управлению БВС в состав бортового оборудования входят следующие устройства и системы:

- приемник сигналов спутниковой радионавигационной системы,
- устройства получения специальной информации,
- радиолинии приема-передачи информации.
- командные радиолинии,
- бортовая цифровая вычислительная машина (БЦВМ),
- устройство хранения (накопления) информации и т. д.

При решении многих задач необходимо поддерживать постоянный информационный обмен между БВС и наземными пунктами управления и приема информации, что значительно снижает скрытность их функционирования. При использовании современных средств радио и радиотехнической разведки, а также средств постановки помех, обеспечение требуемых скрытности и устойчивости функционирования радиоканалов становится трудной задачей. Используя современные системы и комплексы РЭБ для подавления систем навигации, управления и связи можно значительно снизить эффективность боевого применения БВС.

Наличие на борту БВС радиоэлектронной аппаратуры позволяет использовать для их подавления (поражения) не только преднамеренные помехи, но и мощные электромагнитные импульсы, лазерное воздействие и т. п.

Определенную сложность применения средств поражения (подавления) БВС представляет наличие большого количества БВС как своих, так и противника, и как следствие необходимость обеспечения их разделение и избирательное поражения (подавления), особенно на больших дальностях.

Информационные средства должны обеспечивать своевременное обнаружение, идентификацию, определение координат БВС и выдачу данной информации на средства поражения (подавления).

Одним из направлений повышения эффективности систем противодействия БВС является сокращение длительности цикла управления, которое возможно реализовать по нескольким направлениям:

- увеличение дальности обнаружения БВС,
- увеличение скорости протекания информационных процессов,

- увеличение скорости реакции средств подавления (поражения).

Ни одно из перечисленных направлений самостоятельно не может обеспечить требуемую эффективность функционирования систем противодействия БВС. Для эффективного противодействия малоразмерным БВС необходимо создавать комплексную специализированную систему.

Скорость реакции средств поражения (подавления) на современном уровне развития технологий практически достигла своего максимального уровня.

Наибольший интерес представляют первые два направления. Необходимо в перспективные средства внедрять технологии, основанные на более полном учете качества обрабатываемой информации. Увеличение количества данных, сведений не всегда приводит к повышению качества решения задач, а в ряде случаев наблюдается обратный эффект. Необходимо собирать, обрабатывать, передавать, хранить и т. д. только те сведения, которые являются ценными и несут полезную информацию именно для системы управления или лица, принимающего решения. Информационные средства должны удовлетворять информационные потребности потребителей, не перегружая лишними данными и сведениями, не несущими полезной информации.

Если необходимость дальнейшего развития и применения БВС для решения «мирных» задач вызывает меньше вопросов, то их использование в военных целях может столкнуться с рядом серьезных проблем [2, 3, 4, 7].

Общие проблемы развития и применения «мирных» и военных БВС:

1) определение правил, порядка и условий использования воздушного пространства;

2) определение правил, порядка и условий использования радиочастотного спектра БВС и т. д.

Специфические проблемы военных БВС:

1) «разделение» БВС на «свои» и «чужие»;

2) повышение устойчивости функционирования автономных БВС в условиях деструктивных воздействий;

3) повышение устойчивости функционирования каналов и линий связи и управления БВС в условиях воздействия помех;

4) избирательное подавление (поражение) БВС и т. д.

Кроме того, применение БВС против технологически развитого противника, имеющего современные средства РЭБ и другие средства противодействия БВС, может оказаться малоперспективным [6], а, следовательно, вкладывание ресурсов в создание систем противодействия БВС может оказаться неэффективным. Использование же БВС террористами, партизанами и т. д. может привести к большому ущербу, поэтому для защиты особо важных объектов – потенциальных террористических целей необходимо использовать соответствующие средства, системы и комплексы, в которых реализованы самые современные достижения науки и техники.

Заключение. Имеющиеся системы обнаружения и поражения (подавления) малоразмерных БВС не обеспечивают выполнение требований по противодействию БВС. Необходимо разрабатывать комплексные системы противодействия БВС, в которых должны быть реализованы как современные достижения в обла-

сти противодействия БВС, так исследоваться и апробироваться перспективные направления.

Одновременно с увеличением пропускной способности каналов и линий связи систем противодействия БВС, а также производительности информационных средств, необходимо систему информационное обеспечение развивать в направлении более полного и глубокого учета качества информации (семантики и прагматики).

Список используемых источников

1. ГОСТ Р 56122 – 2014 Воздушный транспорт. Беспилотные авиационные системы. Общие требования. М. : Стандартинформ, 2015. 11 с.

2. Организация системы борьбы с малоразмерными БВС [Электронный ресурс] / Арсенал Отечества – информационно-аналитический журнал : [сайт]. URL: http://arsenal-otechestva.ru/article/389-antidrone.

3. Новый радар для обнаружения самых малых объектов [Электронный ресурс]. URL: http://popmech.ru/technologies/231275-bespilotniki-pod-kolpakom-novaya-stantsiya-zametit-lyubye-drony.

4. Старые и новые способы борьбы с беспилотными аппаратами [Электронный ресурс]. URL: http://topwar.ru/37629-starye-...apparatami.html.

5. Урсул А. Д. Информация и мышление. М. : Знание, 1970. 50 с.

6. Беспилотник Predator является бесполезным вооружением при выполнении большинства боевых задач – генерал ВВС США [Электронный ресурс]. URL: http://vpk.name/news/2013-09-25.

7. Сычев В. Армии США разрешили выводить БПЛА в общее пространство [Электронный ресурс]. URL: http://lenta.ru/articles/2010/09/22/uavs.

УДК 004.622

А. Л. Иофик (студентка группы ТСС-25, СПбГУТ)

РАЗРАБОТКА МУЛЬТИМЕДИЙНОГО АГРЕГАТОРА НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ

Рассматривается вопрос реализации системы по созданию агрегатора научно-технической информации, который может быть использован в качестве вспомогательного элемента для обучения. Он повышает работоспособность студентов в связи с тем, что позволяет минимизировать время, затрачиваемое на поиск информации.

веб-технологии, семантический веб, интернет, медиаконтент, база данных, класс.

Повышение качества современного образования предполагает внедрение и активное использование в учебном процессе современных инфокоммуникационных технологий, а также различных средств комплексного представления информации. С каждым годом количество информации, которое необходимо обрабатывать и усваивать, возрастает, в связи с этим

возникает ряд проблем, связанных с ее поиском. Важнейшим этапом, на наш взгляд, является этап поиска достоверного источника. Сложность данного этапа связана с существованием множества мошеннических сайтов, требующих оплату за скачивание материалов, или сайтов, содержащих вредоносное программное обеспечение в виде скриптов и java-апплетов. Проблему поиска также затрудняет существование массы web-страниц, которые имеют своей целью распространение рекламы, в качестве наживки используя научную литературу или ложно представляя себя научным источником. В сети существует масса сайтов, информационную ценность которых можно позиционировать как спорную по причинам приуроченности к зависимому исследованию или расположенности вне научного дискурса. Кроме того, информация, содержащаяся в скачанном файле, не всегда будет релевантна запрашиваемой. Таким образом, возникает необходимость применения/использования/создания систем комплексного анализа информационных источников по нескольким критериям с целью построения ранжированного списка в порядке возрастания/убывания научной ценности/значимости.

Одним из аналогов системы, обеспечивающей комплексное представление информации, являются статьи, но они имеют ряд недостатков, таких как отсутствие гиперссылок, т. е. возникают сложности организации переходов между статьями, невозможность использования информации в различном представлении (текст, аудио, видео), также отсутствие закладок и возможности пометок. В связи с этим необходима служба, обеспечивающая концентрацию информации определенного содержания, хранящейся в интернете. Службой, лишённой вышеназванных недостатков является агрегатор. Основным преимуществом данной службы является полная интеграция различного представления информации, в отличие от некоторых известных ресурсов, например, википедии.

Рассмотрим функциональные возможности системы более подробно. В системе существует несколько категорий пользователей, наделенных разными правами (рис. 1). Редактор агрегатора, который может создавать новую запись, производить ее редактирование, добавлять видеоресурсы и различные ссылки, а также просматривать записи. Системный администратор может регистрировать пользователей, управлять правами доступа и просматривать записи. Также это может быть простой посетитель, который может только просматривать имеющиеся записи.

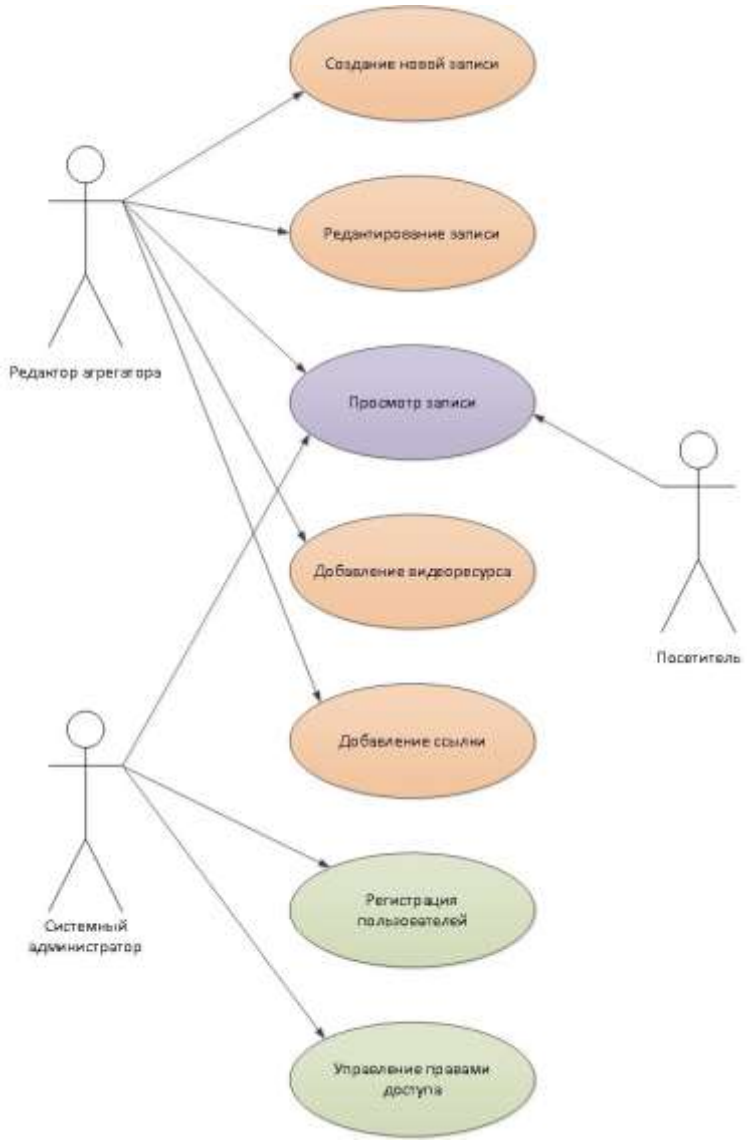


Рис. 1. Диаграмма вариантов использования

Система реализует следующие функциональные возможности: создание базы данных, добавление статей и их редактирование, а также переходы по ссылкам на различные дополнительные источники и медиа ресурсы. Данная система была создана на основе интегрированной среды разработки MS VisualStudio 2015, языка программирования C#, технологии ASP.NET, технологии доступа к данным Entity framework и системы управления базами данных MS SQL Server. Поскольку используется технология Entity Framework, то основу приложения составляет объектная модель (рис. 2) [1]. Основной сущностью данной модели является сущность статьи, которая взаимодействует с видео, аудио и различными ссылками.

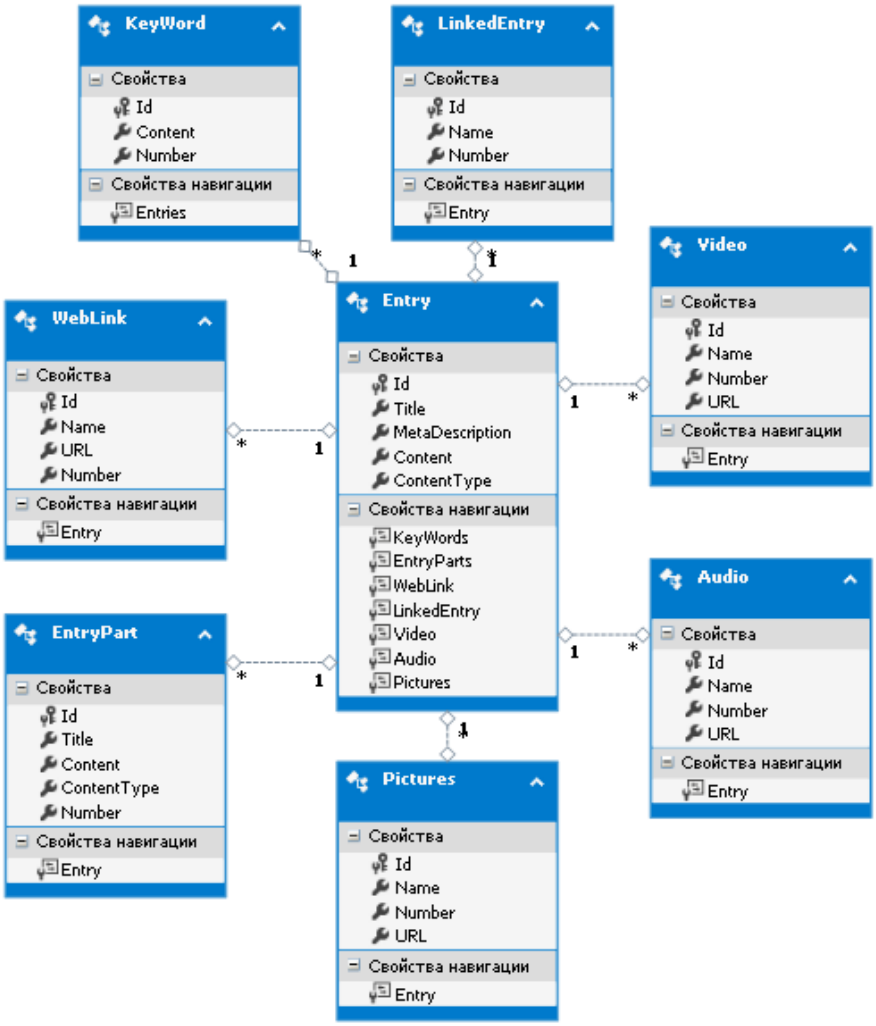


Рис. 2. Диаграмма объектной модели

В разработанной системе используется большой объем информации, для хранения которой используется база данных. База данных представляет собой информационную модель, позволяющую упорядоченно хранить данные о группе объектов, обладающих одинаковым набором свойств. В данной работе использовалась реляционная база данных [2]. При создании сущностей, в базе данных создаются таблицы, в которые записывается определенная информация.

В зависимости от роли пользователя в системе, ему предоставляется различный пользовательский интерфейс, зависящий от уровня полномочий. Один предназначен для редактора агрегатора (рис. 3), а второй для простого посетителя (рис. 4). Обычный посетитель, при входе на страницу, видит список словарных статей. При нажатии на название определенной статьи, благодаря идентификатору, пользователь автоматически переходит на веб-страницу с необходимой статьей, где видит всю необходимую информацию.

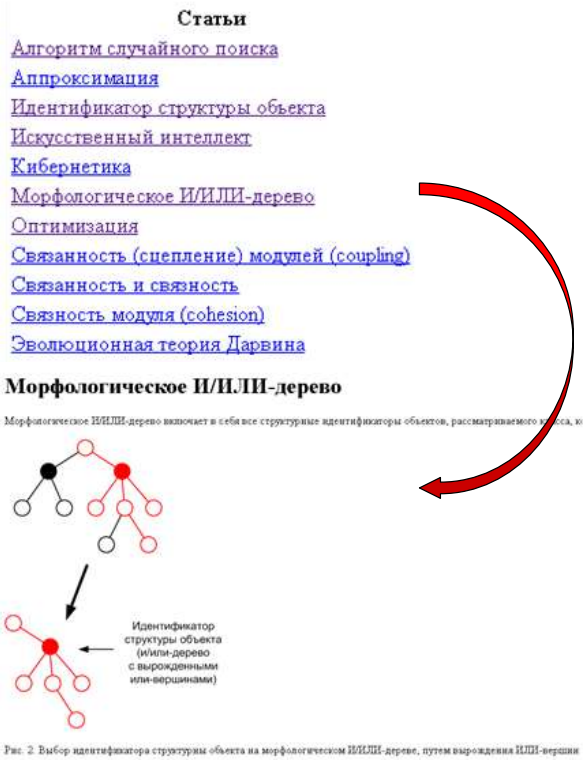


Рис. 3. Интерфейс гостя

При входе реактора агрегатора на веб-страницу, он попадает на веб-страницу создания словарной статьи, где необходимо заполнить поля названия, краткой аннотации, ключевых слов, содержания статьи и выбрать необходимый тип содержимого. Далее необходимо нажать на кнопку «добавить», после чего созданная статья автоматически добавляется в расположенную ниже таблицу со всеми добавленными ранее статьями. При нажатии на активную ссылку «редактирование», которая существует для каждой словарной статьи, редактор агегатора переходит на веб-страницу, содержащую введенные ранее данные о статье. При необходимости, пользователь может внести нужные изменения в существующие поля. После того, ка редактор внес все необходимые изменения, он нажимает кнопку «сохранить», после чего база данных обновляется в соответствии с изменениями, и пользователя возвращает на страницу создания словарных статей.

Разработанная система может быть использована в качестве вспомогательного элемента для обучения. Она повышает работоспособность студентов в связи с тем, что позволяет минимизировать время, затрачиваемое на поиск информации. Данная система позволяет упростить поиск научно-технической информации в интернете. Возможно дальнейшее усовершенствование агрегатора с помощью создания базы данных большего объема, добавления большего количества медиа контента, с видео- и аудио-информацией, добавления системы поиска.

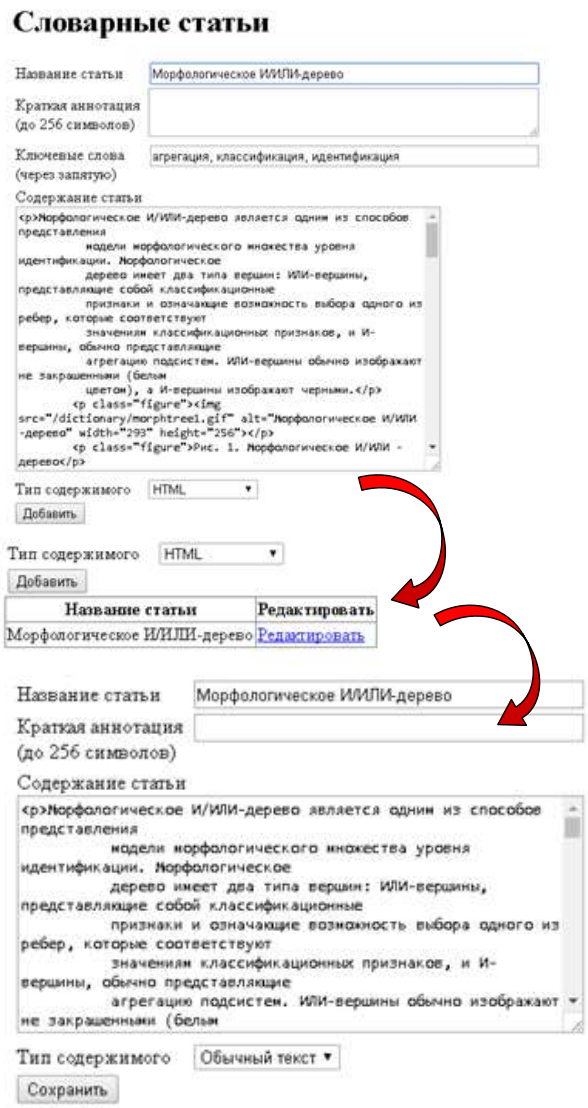


Рис. 4. Интерфейс редактора

Список используемых источников

1. Сайт проекта MSDN, компании Microsoft. URL: http://msdn.microsoft.com
2. Дейт К. Руководство по реляционной СУБД DB2 / пер. с англ. и предисл. М. Р. Когаловского. М. : Финансы и статистика, 1988. 320 с.

Статья представлена научным руководителем,
доктором технических наук, профессором Верховой Г. В.

УДК 004.031.42 : 069.1

В. С. Казачкова (студент группы ИСТ-22, СПбГУТ)
М. В. Котлова (старший преподаватель, СПбГУТ)

ЭЛЕКТРОННЫЙ КАТАЛОГ КАК ЕДИНЫЙ ИНФОРМАЦИОННЫЙ ПОРТАЛ МУЗЕЙНОГО ФОНДА РОССИЙСКОЙ ФЕДЕРАЦИИ

На данный момент существуют проекты, объединяющие множество музеев в интерактивном информационном пространстве. Одним из таких проектов является электронный каталог Музейного фонда Российской Федерации, представляющий собой базу данных с основными сведениями о каждом музейном предмете в составе Музейного фонда. При изучении каталога обнаружен ряд факторов, затрудняющих процесс корректного представления информации. В данной работе выполнен анализ электронного каталога на соответствие требованиям размещения информации на электронном портале, а также сформированы основные критерии по оптимизации работы государственного электронного каталога Российской Федерации.

электронный каталог, портальные технологии, оптимизация, музейный фонд, логическая структура.

На современном этапе развития информационных технологий музеи и другие учреждения культурного наследия начинают оцифровывать и представлять на своих сайтах коллекции для расширения целевой аудитории и привлечения посетителей [1]. Помимо этого, на данный момент существуют проекты, представляющие наследие множества музеев на единой информационной площадке [2]. Одним из таких проектов является государственный электронный каталог Музейного фонда Российской Федерации. Он функционирует как единый информационный ресурс с общедоступными данными обо всех музейных предметах и коллекциях, включённых в Музейный фонд Российской Федерации (рис. 1).

Электронный каталог Музейного фонда Российской Федерации предназначен для информационного обеспечения пользователей сети Интернет, заинтересованных в деятельности музеев, потенциальных посетителей, а также работников музейных предприятий и представителей коммерческих музейных организаций [3]. На ресурсе располагаются сведения о предметах и коллекциях всех музеев, включенных в состав Музейного фонда Российской Федерации, что свидетельствует о большой ресурсоемкости и обширной базы данных проекта.

Рис. 1. Государственный электронный каталог
Музейного фонда Российской Федерации

В ходе исследования изучена структура и функционирование данного ресурса, что привело к выявлению существенных недостатков. По ряду запросов выходные данные не соответствуют условиям и параметрам поиска, а большое количество ответов выводится без изображения и описания, что затрудняет идентификацию предметов. Обнаружено дублирование информации и невозможность регистрации пользователей, не являющихся сотрудниками музейных учреждений. В связи с выявленными факторами, целью исследования является комплексный анализ процесса виртуализации музеев [4] и средств функционирования портальных технологий спосследующим формированием перечня критериев, способствующих оптимизации структуры государственного электронного каталога.

На основании изучения функционирования портальных технологий [5] была спроектирована сравнительная таблица для выявления критериев по оптимизации информационного ресурса (табл. 1).

ТАБЛИЦА 1.Сравнительная характеристика портальной технологии
и предмета исследования

Характеристика	Портал	Электронный каталог
Контент	Большой объем разнообразной информации, всевозможные интерактивные сервисы и ссылки на другие веб-сайты.	Ограниченное количество информации, ссылок на сторонние ресурсы нет.
Навигация	Удобная, понятная и простая навигация.	Доступ затруднителен к некоторым структурным подразделениям сайта.

Характеристика	Портал	Электронный каталог
Целевая аудитория	Охват широкого круга аудитории.	Информация для сотрудников музеев и узкого круга пользователей ресурса.
Информативность	Предоставление максимально полной информации заданной тематики.	Информации о предметах выбранной коллекции недостаточно.
Обновление	Наличие регулярно обновляемого контента: новостей, статей, информационных сводок	Каталог не обновляется, обновление новостной ленты происходит редко.
Авторизация	Единый авторизованный персонифицированный доступ к внутренним и внешним информационным ресурсам.	Доступ предоставляется только сотрудникам музейных организаций, имеющих логин и пароль, возможность регистрации недоступна.
Типы поддерживаемой информации	• Документы (текстовые ресурсы). • Медиа-ресурсы. • Ссылки на другие документы (web-ресурсы). • Таблицы, отчеты. • Структурированные (базы данных) и неструктурированные данные.	• Документы. • Изображения низкого качества. • Отсутствие ссылок.
Поиск	Службы поиска с помощью классификаций и ключевых слов; параметризация (фильтрация и сортировка выходных данных).	Поиск по параметрам затруднен; неточный вывод интересующей информации; невозможность фильтрации.

На основании полученных результатов сформулированы технические требования к структуре и содержанию электронного каталога Музейного Фонда Российской Федерации.

Со стороны контента, наполнение информацией должно проводиться с использованием шаблонов страниц сайта. Также важно предусмотреть возможность модификации шаблонов, размещения на страницах сайта ссылок и прикрепления файлов любого формата, размещения и форматирования текста, графической, табличной и мультимедийной информации.

Навигационные элементы должны обеспечивать однозначное понимание пользователем их смысла: ссылки на страницы должны быть снабжены заголовками и комментариями, условные обозначения соответствовать общепринятым. Для обеспечения быстрого поиска должно предусматриваться создание автоматически генерируемой страницы, содержащий полный иерархический список всех разделов - карты сайта.

Для изучения целевой аудитории ресурса необходим анализ посещаемости портала Музейного фонда Российской Федерации, который должен производиться с использованием независимой системы сбора статистики.

Пользовательский интерфейс портала музейного фонда Российской Федерации должен обеспечивать наглядное и интуитивно понятное представление размещенной на нем информации, быстрый и логичный переход к разделам и страницам. Интерфейс должен обеспечивать возможность оптимального по скорости выполнения функций, в том числе возможность эффективного ввода при помощи клавиатуры, использование справочников и подсказок, возможность сортировок.

Все типовые способы взаимодействия с пользователем должны происходить единообразно во всех модулях, работающих в составе информационного портала. Группа разработчиков интерфейса должна обеспечить обратную связь с пользователями для приёма предложений и замечаний по функционированию ресурса и регулярно обновлять контент ресурса.

Каждый сотрудник, посетитель либо другой авторизованный пользователь (коллекционер, владелец негосударственного музейного предприятия) должен иметь постоянный идентификатор. Для входа в систему пользователь пользуется двумя строками – логин и пароль. Первоначально все логины создаются из идентификаторов пользователей, затем отдельным категориям пользователей предоставляется возможность сменить логин, при этом дублирование имён исключается. Система включает резервирование специальных логинов для администраторов ресурса.

Необходимо предусмотреть возможность восстановления забытого пароля через e-mail при помощи контрольного слова, введённого пользователем или активации ссылки, направленной на почту. Система должна обеспечивать эффективные способы защиты от подбора пароля и в первую очередь устранить угрозу безопасности в случае возникновения стандартных типов хакерских атак.

В процессе работы портал должен предоставлять пользователю возможность перехода на другие материалы. Например, при просмотре какого-либо предмета музейной коллекции и желании получить наиболее полную информацию о данном предмете, пользователь должен иметь возможность перехода на связанный ресурс, раскрывающий интересующий материал. При переходе из просмотра на сторонний сайт должна оставаться возможность возврата на портал.

Поиск информации в документах должен осуществляться средствами базы данных, используемой при разработке. Система должна позволять производить поиск с использованием полнотекстового индекса сайта, обеспечивающая морфологический анализ вводимых пользователем слов русского языка и поиск всех их словоформ.

В результате анализа структуры информационного портала выявлено следующее: электронный каталог Музейного фонда Российской Федера-

ции включает в себя сложную иерархию разделов и большой объем информации, при этом структурирование данных нарушено, что затрудняет пребывание на ресурсе для большинства пользователей. Для всех вышеуказанных проблем предложены критерии, оптимизирующие представление данных на веб-ресурсе (табл. 2).

ТАБЛИЦА 2. Предложения по оптимизации

Выявленная проблема	Предложение по оптимизации
Избыточность переходов на главной странице к подразделу о музеях и регистрации в электронном каталоге	Сокращение количества ссылок, ведущих к подразделу «Музеи» и «Регистрация» до одной
Сортировка раздела «Новости» по годам и месяцам	Обобщение всех подразделов в единый с названием «Архив» и добавление подраздела «Календарь событий» с актуальным новостным блоком
Объемная классификация предметов коллекций всех музеев; избыточность некоторых названий подразделов	Уменьшение количества подразделов пункта «Каталог» с добавлением упрощенных названий
Невозможность фильтрации информации при поиске интересующего предмета на главной странице ресурса и при переходе из раздела «Каталог»	Добавление фильтров и характеристик для уменьшения количества выходных результатов и наиболее точного вывода информации
Наличие ссылок на несуществующие страницы	Удаление неактивных ссылок с переносом информации
Расширенное разделение пункта «Документы»	Перенос раздела «Документы» в личный кабинет сотрудника музея
Невозможность регистрации для пользователей ресурса, не являющимися сотрудниками музейных организаций	Добавление регистрации для пользователей и личного кабинета как для сотрудников, так и для заинтересованных лиц
Частичное преобразование ресурса при переходе на английскую версию	Доступность всех страниц ресурса на двух языках (русский и английский)

В ходе исследования выполнен анализа электронного каталога Музейного фонда Российской Федерации на предмет соответствия требованиям портальной технологии и механизмов представления данных и доступа к ресурсу. На основании полученных результатов сформированы основные критерии по оптимизации работы государственного электронного каталога Российской Федерации и возможности его функционирования в качестве полноценного информационного портала.

Список используемых источников

1. Борисова Н. А. Инфокоммуникационные технологии в музейной деятельности [Электронный ресурс] // Почтовые музеи: взгляд из прошлого в будущее. [2006]. URL:

http://www. rustelecom-museum.ru/objects/?ContainerID=7069&ContainerType= 73 &object ID = 8982&langID=57 (дата обращения 05.05.2016).

2. Бернштейн Б. М. Визуальный образ и мир искусства: исторические очерки. СПб. : Петрополис, 2006. 565 с.

3. Ноль Л.Я. Компьютерные технологии в музее: учеб. пособие / Рос. ин-т переподготовки работников культуры, искусства и туризма, каф. музееведения. М.: [б. и.], 1999. 115 с.

4. Гурьева М.М. Автоматизация учета музейных коллекций: электронные базы данных // Рекомендации по работе с фотодокументами, входящими в составы государственных фондов Российской Федерации, 2012 г, С.57-60.

5. Интернет-порталы: содержание и технологии: сб. науч. ст. / под ред. А. Н. Тихонова; ГНИИ ИТТ «Информика». М. : Просвещение, 2004. Вып. 2. 499 с.

УДК 004.5

Е. С. Казначеева (студент группы ИСТ-23, СПбГУТ)

РАЗРАБОТКА ИНФОРМАЦИОННОЙ МОДЕЛИ НАВИГАЦИИ В ПРОСТРАНСТВЕ ЗДАНИЙ СО СЛОЖНОЙ АРХИТЕКТУРОЙ

В настоящее время инновации и технологии внедряются во все сферы жизнедеятельности. Идет активная постройка различных сооружений и торговых центров, и чтобы облегчить людям поиск в здании, создается многой решений для организации навигации и позиционирования со сложной архитектурой. Навигация помогает людям сориентироваться в незнакомом месте, не затрачивая на это длительное время для поиска.

системы позиционирования, геолокация, технология Beacon, маячки IBeacon, университет, интерфейс.

Проблема навигации внутри помещений, а также предоставления посетителям услуг, основанных на их местоположении LBS (*Location-based service*) становится все более популярной. Методы и решения, используемые в навигации внутри помещений, помогают также ориентироваться вне зданий. Например, на улице, где есть плотная застройка и отсутствуют системы спутниковой навигации, так как нет спутников в прямой видимости, а присутствуют только отраженные. Данная проблема актуальна для Японии, как для страны с густой плотностью городских построек.

Таким образом, сервисы позиционирования местоположения внутри помещений имеют широкий спектр охвата: парковка, склады торговых центров, аэропорты, музеи, бизнес-центры, локационные игры. И все они нуждаются в indoor-навигации.

В современном мире существует различные методы, с помощью которых можно осуществить навигацию и позиционирование. Все технологии имеют свои плюсы и минусы, ниже будут приведены основные методы, отвечающие за геопозиционирование [1]:

Фемтосоты – миниатюрная базовая станция сотовой связи малой мощности, подключение которой осуществляется к сети оператора связи через широкополосный интернет-канал. Фемтосота представляет собой беспроводной роутер, работающий в лицензированном частотном диапазоне для операторов сотовой связи. Зона покрытия одной фемтосоты составляет до 1 000 кв. м, при наличии стенок и перегородок – сигнал, поступающий от фемтосоты затухает.

Геомагнитное позиционирование – Данная технология основана на ориентировании по магнитному полю Земли и осуществляется за счет геомагнитных аномалий, которые возникают из-за неоднородности геомагнитного поля. Процесс происходит следующим образом: зафиксированные геомагнитные аномалии наносятся на карту территории, на которой будет происходить ориентирование. Далее навигация осуществляется по карте, с помощью устройства, содержащего магнитометр. Точность геомагнитного позиционирования составляет 2 м. С помощью данной технологии можно ориентироваться в зданиях, имеющих большую высоту, а также под землей, где отсутствует GPS.

Wi-Fi – Способ определения координат по Wi-Fi точкам следующий: пользовательское устройство сканирует доступные Wi-Fi-точки доступа, полученную информацию отправляет на сервер, где эти данные сверяют по базе данных и сопоставляют с координатами этих точек доступа, далее происходит вычисление координат пользователя. Точность при таком подходе составляет 3–5 м. Стоит учесть, что не всегда координаты всех точек точно известны, поскольку их могут переносить из одного места в другое, или координаты точки заменили, следовательно, результат будет неточный. Погрешность составляет до 25 м.

Beacon-маячки – это маячки, работающие на технологии BLE (*Bluetooth Low Energy*). Маячки соотносимы с размером спичечной коробки, работают от батарейки и распространяют по протоколу Bluetooth информацию о своем расположении. Если у человека на мобильном устройстве стоит приложение компании, которое предоставляют информацию о последних скидках и новинках, то в зоне действия маячка, происходит активация и пользователь мгновенно получит оповещение. Технология маячков Beacon является последней и самой перспективной, даже затрагивая финансовые стороны этого метода.

Анализ таблицы 1 отображает сравнение систем позиционирования по основным параметрам.

ТАБЛИЦА 1. Сравнительная таблица аналогичных систем

Критерий	Фемтосоты	Wi-Fi	Геомагнитное позиционирование	Ibeacon-маячки
Устойчивость к помехам	-	-	-	+
Точность определения, м	100	2–4	2	10
Скорость передачи данных	-	-	-	+
Радиус действия, м	100–150	10–50	10	20–50
Стоимость решения, $	50 000	23	200	7

После проведения анализа видно, что лидирует технология – Ibeacon. Достоинства системы в том, что маячки небольшие по размеру, легки в установке, могут проработать без замены батарейки до 2 лет.

Рассмотрим, из чего же состоит маячок (рис. 1). Под корпусом маячка находится ARM-компьютер, соединенный с Bluetooth-модулем – они питаются от батареи. На микросхеме содержится прошивка, которая отслеживает точность работы маячков и в принципе гарантирует их работу. На сужающейся части маячка расположен короткий провод, идущий напрямую от процессора – это антенна. Широковещательная антенна излучает волны определенной частоты и длины: радиоволны частотой 2,4 ГГц. Антенна имеет изогнутую форму.

Рис. 1. Состав Beacon-маячка

Маячки Ibeacon в количестве 4 штук были использованы для проведения эксперимента по навигации. Для этого маяки были размещены в холле 1-го этажа, далее с помощью приложения «Beacon-map» были записаны положения маячков и их работа в течении 3 мин. Определение местоположения осуществляется за счет математического метода – трилатерация. Трилатерация – это метод определения положения объектов в пространстве с известным местоположением нескольких объектов и измеренным расстоянием между каждым из опорных объектов (Beacon-маячки), и устройством для которого определяется позиционирование.

Благодаря определению системы геопозиционирования, были созданы дизайн-макеты для приложения по навигации внутри Санкт-

Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича [2]. Перед началом создания дизайн-макетов, была определена целевая аудитория, после этого прототипирование страниц и создание дизайн-макетов в программе Justinmind Prototyper. На рисунках 2–3 представлены варианты дизайн-макетов.

Рис. 2. Главный экран приложения

Рис. 3. Выбор аудитории для поиска

Современный ритм жизни не дает стоять человеку на месте. Каждый день во всех сферах жизнедеятельности, в том числе и науке, появляются все новые и новые открытия, проекты, разработки. Не стоят на месте и технологии в области позиционирования и навигации. Имеющиеся на сегодняшний день технологии в этой области помогают решать человечеству множество задач не только индивидуального плана, но и государственного масштаба. Таким образом, отражены технологии, с помощью которых можно осуществлять позиционирование в зданиях со сложной архитектурой и показаны дизайн-макеты для приложения по навигации в СПбГУТ.

Список использованных источников

1. Indoor навигация и позиционирование [Электронный ресурс] / Habrahabr.ru: [сайт]. URL: https://habrahabr.ru/ company/sap/blog/267433/

2. Джеф Раскин «Интерфейс: новые направления в проектировании компьютерных систем». СПб. : Символ-Плюс, 2005. 272 с.

Статья представлена научным руководителем,
старшим преподователем Кисленко Л. С.

УДК 004.7:004.422.8

Д. А. Кондратьев (аспирант, СПбГУТ)
Н. Эльсабаяр Шевченко (студент группы ИСТ-511м, СПбГУТ)

ИНТЕЛЛЕКТУАЛЬНЫЕ ПРОФИЛИ СЕРВИС-ОРИЕНТИРОВАННЫХ АРХИТЕКТУР

Актуализировано динамическое конфигурирование интеллектуальных сервис-ориентированных систем, обоснованы возможные различия в целях динамического конфигурирования, выделены перспективные подходы к обеспечению динамического конфигурирования, представлены новые функциональные задачи динамического конфигурирования интеллектуальных сервис-ориентированных систем, предложена система сервисов для решения функциональных задач динамического конфигурирования, определены контексты формирования системы новых сервисов в зависимости от целей динамического конфигурирования.

сервис-ориентированная система, интеллектуальная информационная система, динамическое конфигурирование, сервис диспетчеризации, сервис планирования.

Концепция сервис-ориентированных архитектур является открытой для формирования функциональных спецификаций соответствующих систем [1]. Благодаря указанной особенности, предоставляются широкие возможности по обеспечению гибкости в интеграции объединяемых сервис-ориентированных средств в единую систему. Интеграция сервис-ориентированных средств выполняется, как правило, с помощью многоцелевого диспетчера. В многоцелевом диспетчере различаются диспетчер сервисов обслуживания и диспетчер сервис-ориентированной деятельности. Диспетчер сервисов обслуживания предназначается для реализации различных востребованных профилей интерфейсных функциональных задач, а диспетчер сервис-ориентированной деятельности – для решения задач конфигурирования. Профили интерфейсных функциональных задач группируются по принципам однородности заказов клиентов и их требований. Концептуальная модель интеграции сервис-ориентированных средств, присущая традиционной архитектуре, раскрывается на рисунке 1.

Перспективное направление развития функциональных спецификаций базируется на интеллектуализации сервис-ориентированных систем, осуществляемой на основе различных подходов к воспроизведению мыслительных процессов субъекта; воспроизведению рациональных рассуждений; реализации функций, требующих интеллектуальности при их выполнении людьми; реализации рациональных действий. Различия в подходах отображаются на многообразия сервис-ориентированных средств, нацеленных на достижение свойств систем, необходимых для профессиональной или досуговой деятельности.

Ввиду представительности многообразия создаются объективные основания для динамического конфигурирования сервис-ориентированных средств. Кроме того, множество объективных оснований расширяется по мере учёта динамического характера ситуаций в профессиональной деятельности и поведении клиентов, а также учёта особенностей процессов изменения состояний инфокоммуникационных сред, в окружении которых реализуется функционирование сервис-ориентированных систем. При подобном обилии изменяющихся факторов в окружении сервис-ориентированных систем результаты их функционирования становятся трудно прогнозируемыми и, тем более, негарантированными. Преодоление указанного недостатка может выполняться с помощью модельно-аналитического интеллекта, генерируемого согласно методике из [1]. Построенная концептуальная модель интеллектуальных сервис-ориентированных систем с мониторингом их качества приводится на рисунке 2.

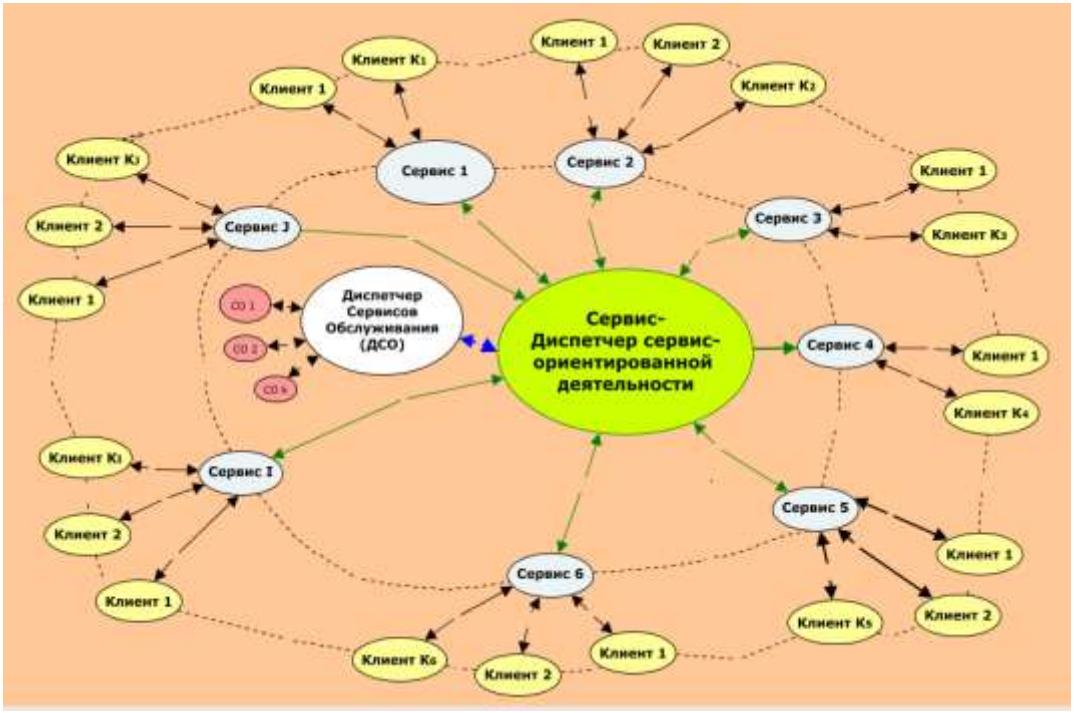


Рис. 1. Концептуальная модель традиционной архитектуры сервис-ориентированных систем

Другой предлагаемый вариант интеллектуализации сервис-ориентированных систем основывается на введении нового сервиса в их архитектуру, именуемого сервисом планирования и диспетчеризации. В этом варианте используется ранее выделенный подход к реализации рациональных действий.

Во вводимом сервисе перед решением задачи диспетчеризации формируется план действий посредством поиска плана на множестве частично заданных планов, которое последовательно сужается с помощью введения

дополнительных ограничений до тех пор, пока оставшиеся элементы не станут являться решениями исходной задачи [2]. Дополнительные ограничения связываются с выполнением постусловий каждого действия и с изменениями факторов в окружении сервис-ориентированных систем. Концептуальная модель интеллектуальных сервис-ориентированных систем с планировщиком действий изображается на рисунке 3. Через планирование действий может обеспечиваться и профилизация интеллектуальных интерфейсов для разделяемых групп клиентов.

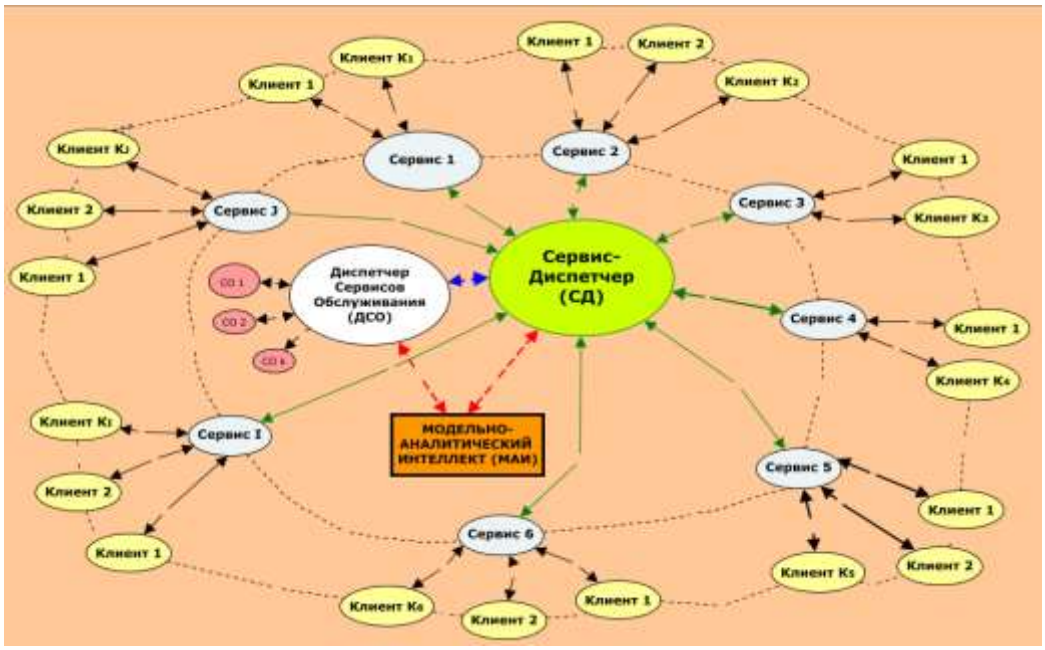


Рис. 2. Концептуальная модель интеллектуальных сервис-ориентированных систем с мониторингом качества их функционирования

Представленная модификация сервис-ориентированной архитектуры ориентируется на достижение целей, поставленных перед сервис-ориентированными системами, за счёт динамических конфигураций, соответствующих формируемым планам.

Условия конфигурирования могут различаться в контексте автономного планирования, распределённого планирования, оперативного планирования и ряда других категорий планирования. С учётом таких различий появляется объективная потребность в выборе типа задачи планирования и способов их реализации в зависимости от состояний окружающей среды.

В силу отмеченных особенностей рациональным представляется решение, связанное с оформлением планировщика в виде самостоятельного сервиса, отвечающего за выбор наилучшего или оптимального метода планирования. Подобный выбор находится в непосредственной связи с мониторингом качества функционирования сервис-ориентированных систем.

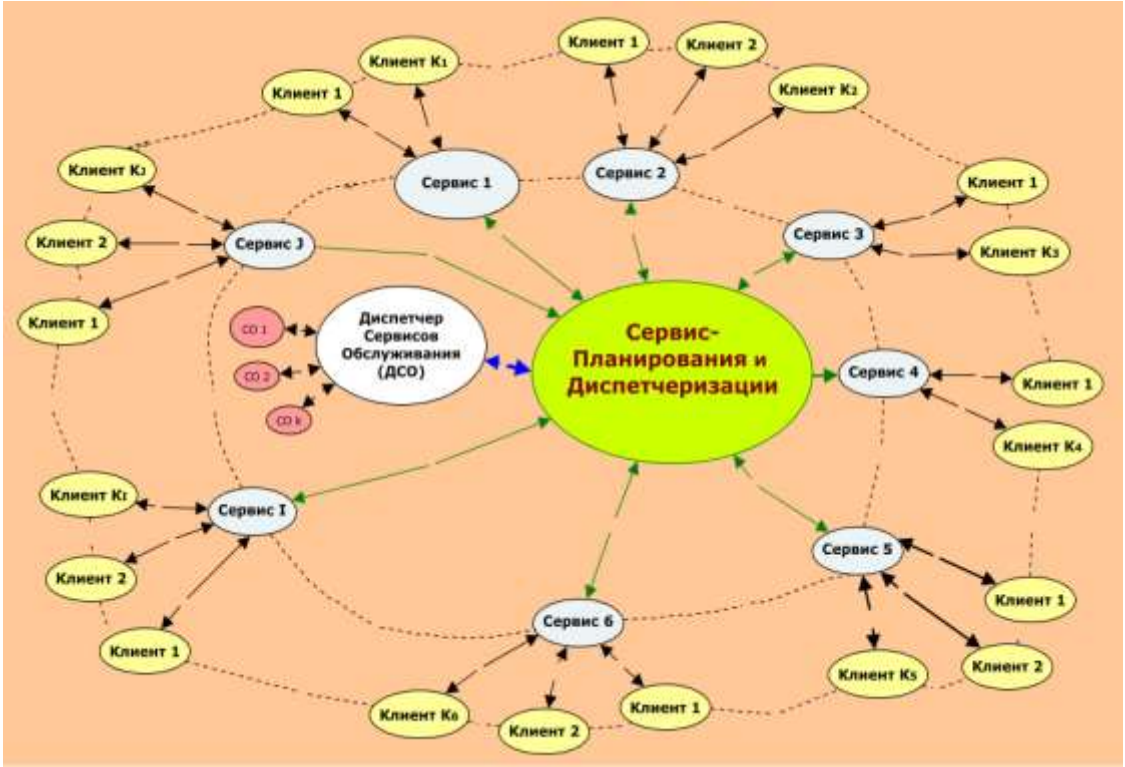


Рис. 3. Концептуальная модель интеллектуальных сервис-ориентированных систем с динамической конфигурацией на базе планировщика действий

Описанные основания являются причиной выдвижения последующей модификации архитектуры сервис-ориентированных систем. Проводимая модификация заключается в сочетании двух новых сервисов: сервиса планировщика и сервиса модельно-аналитического интеллекта. Концептуальная модель интеллектуальных сервис-ориентированных систем, поясняющая отражённую выше идею, приводится на рисунке 4.

Выбор наилучшего или оптимального алгоритма планирования действий может успешно решаться с применением когнитивных технологий. Широкий спектр возможных вариаций в математических формализациях задачи выбора детально раскрывается в [2]. При этом рассматриваются альтернативные постановки задач, позволяющие обеспечивать подтверждение корректности выбираемых решений, что придаёт особую значимость этому свойству в условиях непредсказуемости изменений окружающей среды.

Предложенная система концептуальных моделей интеллектуальных сервис-ориентированных систем может рассматриваться как опорный базис для совершенствования прикладного программного обеспечения информационных инфраструктур.

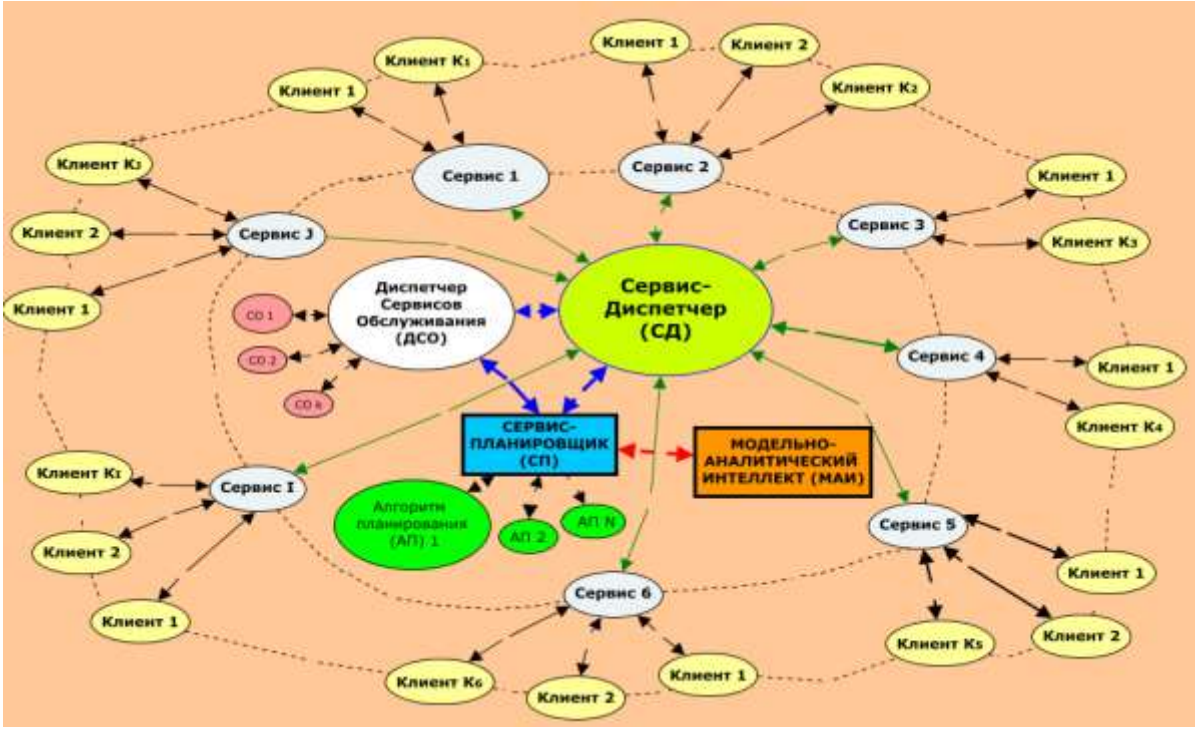


Рис. 4. Концептуальная модель интеллектуальных сервис-ориентированных систем с мониторингом качества их функционирования и с динамической конфигурацией на базе планировщика действий

Список используемых источников

1. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учеб. пособие. СПб. : изд-во Политехн. ун-та, 2011. 105 с. ISBN 978-5-7422-2951-3.

2. Птицына Л. К., Добрецов С. В. Интеллектуальные технологии и представление знаний. Планирование действий интеллектуальных агентов в информационных сетях : учеб. пособие. СПб. : изд-во Политехн. ун-та, 2006. 172 с. ISBN 5-7422-1101-5.

Статья представлена научным руководителем,
доктором технических наук, профессором Птицыной Л. К.

УДК 004.415.2

С. В. Лазев (студент группы СУ-21, СПБГУТ)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УДАЛЕННОГО ТЕСТИРОВАНИЯ ДЛЯ АВТОШКОЛ

В статье рассмотрены вопросы разработки тонкого клиента мультимониторных экзаменационных станций для экзаменационных классов автошкол и отделений ГИБДД, использование которых приводит к материальному выигрышу при закупке ап-

паратной части и экономии потребляемой энергии, а также повышению качества сдачи экзамена.

мультимониторных клиент, автошкола, архитектура клиент-сервер, фотофиксация.

Во многих автошколах проведение занятий и сдача экзамена проходит с использованием персональных компьютеров. Проанализировав данные, полученные от компании “Мобайл Букинг”, которая успешно занимается поставкой программного обеспечения и готовых экзаменационных систем для подразделений ГИБДД, автошкол и транспортных предприятий России и СНГ с 1994 г., выяснено, что, несмотря на внедрение компьютеров, часть работы, выполняемая человеком достаточно велика, а имеющееся программное обеспечение является решением частного случая для конкретной автошколы. В результате чего мы наблюдаем потребность рынка в новом программном обеспечении удаленного тестирования для автошкол. Именно данной теме посвящена эта статья.

Целью работы является разработка и внедрение в автошколы Санкт-Петербурга нового программного обеспечения, восполняющего функционал своих предшественников с добавлением новых возможностей. Для этого выполнен целый ряд задач, таких как:

1) изучение уже имеющегося ПО в автошколах СПб,
2) выявление недостатков таких решений,
3) формирование нового решения,
4) разработка программного обеспечения нового решения,
5) сдача разработанного ПО в тестовую эксплуатацию.

На данный момент, решения, имеющиеся во многих автошколах, были разработаны в 1996 г. и не охватывают весь круг задач, который могли бы выполнять вместо человека, таких как: загрузка новых билетов в связи с изменениями в сфере ПДД, отправка данных об учениках в ГИБДД, сбор разного рода статистики. Разработка программного обеспечения с того времени значительно шагнула вперед и сейчас, с помощью современных инструментов разработки, позволяет создать гибкое решение, позволяющее более эффективно задействовать современное аппаратное обеспечение.

Перед началом разработки собственного решения было выяснено что, аналогов задуманной системы на данный момент нет. Понимая востребованность такой системы было решено реализовать ее на основе клиент-серверного приложения. Клиентская часть которого будет распространяться по всем автошколам, а серверная будет является неким центром, хранящим информацию об автошколах, учениках, их оценках и фотографиях, а также содержимое экзаменационных билетов.

Преимущества

- Актуальность информации. Сервер обновляется каждый раз, когда выходят новые законы или изменения в сфере ПДД.
- Масштабируемость. Легкая горизонтальная масштабируемость позволяет подключать тысячи клиентов.
- Повышение качества проверки. Выбор ответа производится с помощью джойстика, имеющего ограниченное количество кнопок, что предотвращает систему от сбоя из-за человеческого фактора. Также в клиенте реализована фотофиксации: при наличии веб-камеры в случайные моменты времени будет производиться фотофиксация экзаменуемого, которую по желанию администратор может отключить.
- Материальный выигрыш. Экономия проявляется себя при закупке аппаратного обеспечения, на котором будет использоваться тонкий клиент, а также в количестве потребляемой электроэнергии.
- Сбор статистики. Серверная часть позволяет собирать статистику по: стране, городу, автошколе, классу и ученику. Такой сбор статистики имеет государственную важность, т. к. по данным участников ДТП можно узнать в какой автошколе они проходили обучение.
- Гибкость в настройке системы. Выбор языка, реализация джойстиков на базе клавиатуры, задание интервалов фотофиксации, ведение собственной локальной статистики.

Архитектура разрабатываемого ПО для автошкол

Приложение состоит из двух частей: клиент и сервер. Клиент-серверная архитектура позволяет легко масштабировать систему, безболезненно вносить изменения и гибко ее настраивать в зависимости от требуемой производительности.

Серверная часть

Сервер приложения является связующим звеном между пользователем и базой данных. По этой причине на эту часть системы возлагается наибольшая ответственность и требования по функциональности и производительности. Серверная часть реализована на языке PHP 5.2 с использованием свободной объектно-реляционной системы управления базами данных PostgreSQL 9.1.20. Но многие методы, реализующие обращение клиентской части к серверу, написаны с использованием JavaScript ввиду необходимости асинхронной работы сервера. Из соображений безопасности при разработке серверной части было написано собственное ядро. Выбор PostgreSQL объясняется высокой нагрузкой, и с точки зрения производительности дает выигрыш по сравнению со своим основным конкурентом – MySQL.

Одной из главных задач, является реализация методов на клиентской части, обеспечивающих добавление в базу данных записей и фотографий (при включенной фотофиксации). Изначально эти методы работали по средствам FTP-запросов и ответов, что позволяло третьим лица несанкционированный доступ к информации о результатах экзаменов, например, с целью их подмены.

Решение было найдено в реализации POST-запросов и ответов. При таком обмене данными сервер отслеживает откуда идут запросы и работает только с теми пользователями, которые находятся в сети.

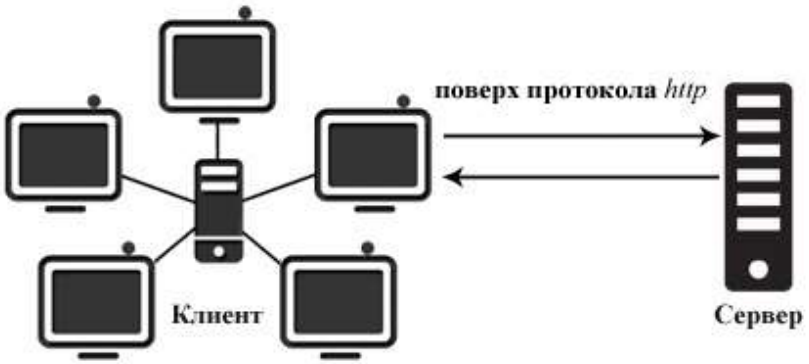


Рис. 1. Архитектура приложения

Клиентская часть

Клиентская часть реализована на языке программирования *C#* совместно с платформой .NET Framework 3.5 [1]. Выбор инструментов не случаен. C# переняв много от своих предшественников – языков C++, Pascal и в особенности Java, является мощным инструментом для разработки приложений на базе ядра Windows NT (т. е. XP, Vista, 7, 8, 10), а это особенно важно, учитывая высокую популярность Windows ОС в России.

Одновременная фотофиксация и загрузка содержимого экзаменационного билета давали ощущение зависания системы. Во избежание такого эффекта было решено использовать распараллеливание процессов [2].

Решением было использование библиотеки потоков System.Thread [3]. Использование библиотеки System.Thread позволяет создавать и контролировать поток, задавать приоритет и возвращать статус потока. Ввиду того, что клиентская часть не производит никаких сложных вычислений, приложение получилось достаточно легким и не ресурснозатратным, что позволяет запускать его на маломощных компьютерах.

Фотофиксация реализована на стороне клиента. Работу с веб-камерами обеспечивае*т C# фреймворк с открытым исходным кодом – AForge.NET, который пре*дназначен для исследований в области компьютерного зрения и искусственного интеллекта. Этот фреймворк состоит из набора библиотек, которые имеют свои особенности. Для приема и обра-

ботки потока видео с камеры нам потребовался только один набор - AForge.Video – набор библиотек видеообработки.

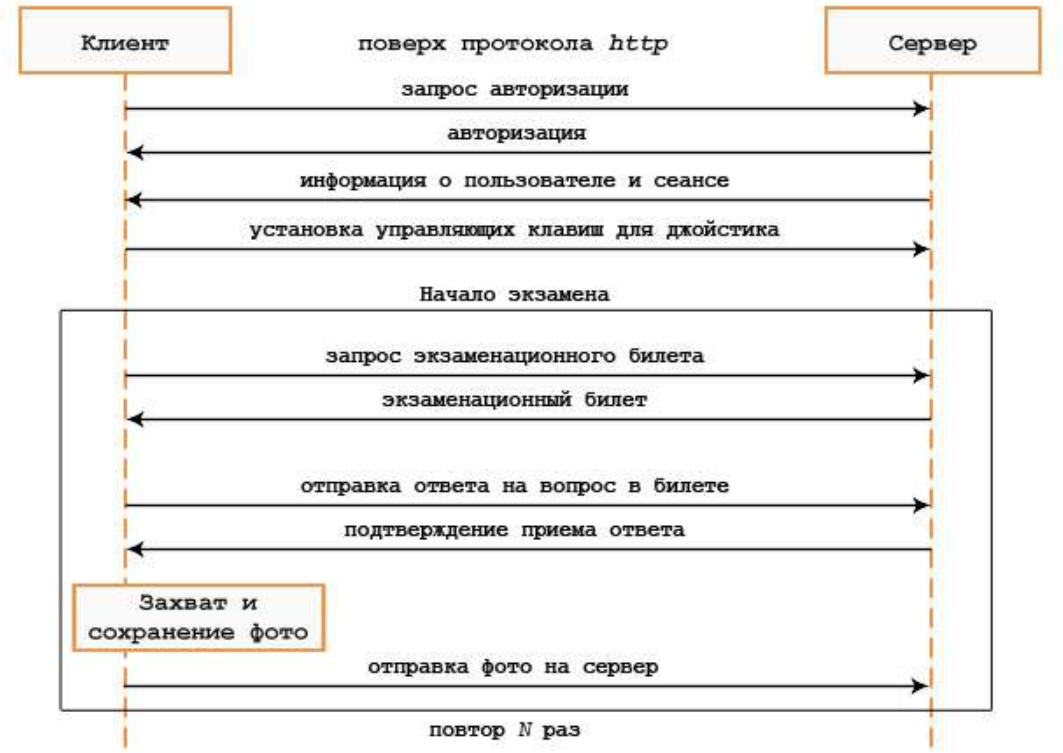


Рис. 2. Взаимодействие клиент-сервер

Минимальные системные требования

- Поддерживаемые ОС: XP, Vista, 7, 8, 8.1, 10.
- Поддерживаемые архитектуры: 32-разрядная (x86), 64-разрядная (x64).
- Требования к процессору: 1,6 ГГц.
- 40 МБ ОЗУ (60 МБ для виртуальной машины).
- 32 МБ (NTFS) свободного дискового пространства.
- .NET Framework 3.5.

Перспективные задачи разработки

После того как приложение пройдет тестовую эксплуатацию и отладку, планируется реализовать следующие улучшения:

- устранение имеющихся недостатков,
- увеличение количества поддерживаемых языков,
- создание более дружелюбного интерфейса, чем имеющийся,
- достижение максимальной оптимизации динамической загрузки объектов.

Список используемых источников

1. .NET Framework [Электронный ресурс] // Википедия – Свободная энциклопедия: [сайт]. URL: https://ru.wikipedia.org/wiki/.NET_Framework (дата обращения: 04.05.2016)
2. Пахомов Б. И. C# для начинающих. СПб. : БХВ-Петербург, 2014. 432 с. ISBN 978-5-9775-0943-5.
3. Павловская Т. А., C#. Программирование на языке высокого уровня : учебник для вузов. СПб. : Питер, 2003. 432 с. ISBN 978-5-91180-174-8.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Небаевым А. И.

УДК 004.7:004.422.8

А. А. Лебедева (аспирантка, СПбГУТ)
С. В. Хроменков (студент группы ИСТ-511м, СПбГУТ)

ПЛАНИРОВАНИЕ ДЕЙСТВИЙ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ АГЕНТОВ С ГАРАНТИЯМИ КАЧЕСТВА ИХ ФУНКЦИОНИРОВАНИЯ

Обоснована необходимость предоставления заказчикам гарантий качества функционирования интеллектуальных информационных агентов. Определены профили их качества. Выделены системообразующие компоненты интеллектуальных информационных агентов, оказывающие существенное влияние на качество их функционирования. Предложено функциональное взаимодействие подсистем планирования действий и подсистем модельно-аналитического интеллекта информационных агентов. Описаны категории исходной информации для выполнения предлагаемого совмещения. Представлены ключевые процедуры планирования с гарантиями качества работы информационных агентов.

информационный агент, система планирования действий, модельно-аналитический интеллект, качество функционирования агента, гарантии качества.

Интенсивное развитие информационных инфраструктур является основной движущей силой для распространения агентных технологий, применяемых в профессиональной и досуговой деятельности. По мере накопления опыта реализации и применения агентных технологий проявляется стремление к их совершенствованию в части обеспечения ими свойств технических реализаций, позволяющих снизить или вовсе исключить влияние человеческого фактора на результаты выполняемой деятельности. Одно из направлений подобного совершенствования ориентируется

на предоставление заказчикам гарантий качества функционирования интеллектуальных информационных агентов.

В информационных инфраструктурах интеллектуальные агенты погружаются в среды со стохастическим характером их описания. В связи с этим позиционируется и стохастический характер описаний процессов их функционирования. На основе учёта приведённых оснований в качестве основного фактора, представляющего особую значимость для предоставления гарантий, выбирается длительность выполнения поставленных перед интеллектуальным информационным агентом задач. Согласно этим представлениям возможные профили качества функционирования интеллектуальных информационных агентов заполняются статистическими характеристиками длительностей выполнения поставленных перед интеллектуальным информационным агентом задач. В каждый отдельный профиль может вводиться сочетание различных типов статистических характеристик. При этом опорным базисом для их нахождения являются плотности распределений длительностей.

К системному ядру интеллектуальных информационных агентов, предопределяющих их функциональную спецификацию, относятся подсистемы планирования выполняемых действий. По этой причине появляется целесообразность сочетания процессов функционирования подсистем планирования действий и подсистем модельно-аналитического интеллекта, обеспечивающих мониторинг и соблюдение необходимых гарантий качества. Для реализации подобного сочетания предлагается представляемая ниже система модельных и операционных формализаций.

План решения поставленной перед интеллектуальным информационным агентом задачи строится посредством трансформации исходного частичного плана. Частичный план описывается двумя кортежами.

Первый кортеж представляется тремя множествами

$$\mathbf{P} = \langle \mathbf{T}, \mathbf{ST}, \mathbf{C} \rangle,$$

где **T** – множество временных шагов; $\mathbf{ST}: \mathbf{T} \rightarrow \mathbf{O}$ – отображение шагов плана на множество базисных операторов **O**.

Среди множества **T** отмечаются два обязательных шага t_0 и t_∞. Первый обязательный шаг ставится в соответствие началу плана, а второй – концу плана. Отображения обязательных шагов оформляются следующим образом:

$$ST(t_0)=start, \;\; ST(t_\infty)=finish.$$

Второй кортеж образуется тремя множествами ограничений

$$\mathbf{C} = \langle \mathbf{C}_O , \mathbf{C}_B , \mathbf{C}_L \rangle,$$

где $\mathbf{C}_O$ – множество отношений частичной упорядоченности на множестве **T**, такое что: $t_0 < t_i$ и $t_i < t_\infty$ для любого $t_i \in \mathbf{T}$, $i > 0$; $\mathbf{C}_B$ – множество связывающих ограничений на вхождение переменных в пред- и постусловия операторов, реализующих действия; $\mathbf{C}_L$ – множество дополнительных ограничений.

Во множество $\mathbf{C}_O$ вводятся требования на порядок шагов в плане. Указанные требования оформляются как относительные, т. е. используются неравенства типа $t_i < t_j$. Задаваемыми подобным образом неравенствами не определяется полная упорядоченность множества **T**.

Во множестве $\mathbf{C}_B$ представляются наборы пар двух видов: $\langle q_1, q_2 \rangle$ или $\neg\langle q_1, q_2 \rangle$.

Первый вид условия используется в том случае, когда на переменные q_1 и q_2 накладывается условие унификации. Второй вид условия применяется при выдвижении предположения о том, что q_1 и q_2 не могут считаться унифицированными ни в одной правильно построенной формуле.

Во множестве $\mathbf{C}_L$ концентрируются все другие необходимые ограничения. Среди ограничений во множестве $\mathbf{C}_L$ различаются две группы. К первой группе относятся монотонные интервальные ограничения. Во вторую группу объединяются точечные ограничения значений. Каждое монотонное интервальное ограничение задаётся тремя элементами $\langle t', q, t'' \rangle$, где $t', t'' \in T$ и $t' < t''$. Указанным ограничением представляется необходимость соблюдения условия q на всем интервале между шагами t' и t''. Ограничения значений, относящиеся ко второй группе, описываются в виде двух элементов $\langle q, t \rangle$. Подобным образом фиксируются требования на соблюдение условия q на указанном шаге $t \in \mathbf{T}$.

Обобщённый алгоритм планирования действий интеллектуального информационного агента описывается с помощью пяти процедур: процедура завершения, процедура уточнения, процедура рационализации, процедура проверки состоятельности плана, процедура рекурсивного вызова.

В процедуре завершения проверяется условие окончания процесса построения плана. Предусматриваются три случая окончания:

0) находится решение задачи в рамках трансформации исходного частичного плана;

1) регистрируется невозможность построения плана посредством трансформации исходного частичного плана;

2) определяется неготовность плана на данном этапе из-за необходимости его доработки.

В первых двух случаях планирование завершается с соответствующим заключением. В третьем случае осуществляется переход к процедуре уточнения.

В процедуре уточнения проводится модификация частичного плана в целях соблюдения некоторого выбираемого целевого условия. При мо-

дификации проводится выбор промежуточной подцели, достижение подцели и консервация.

Для выбора промежуточной подцели $\langle q, t \rangle$ используется частичный план **P**. Для этого могут вводиться различные стратегии. Среди реализуемых стратегий могут применяться следующие: произвольный выбор подцели, назначение приоритетов на основе иерархии ограничений, эвристические способы.

При достижении подцели определяется (при необходимости, добавление нового) шаг t', который обеспечивает выполнение условия q. При необходимости проводится добавление нового шага.

При консервации вводятся дополнительные ограничения с целью предохранения накопленных на данном шаге наработок от последующих изменений.

При рационализации выполняется корректировка плана с целью снижения вычислительной сложности проверки его состоятельности. Типовые приемы рационализации основываются на разрешении обнаруженных конфликтов между шагами и ограничениями плана с помощью дополнительного упорядочивания шагов или введения новых дополнительных ограничений в $\mathbf{C}_L$.

При проверке состоятельности отсекаются несостоятельные частичные планы.

Рекурсивный вызов предназначается для модификации частичного плана.

В реализуемых на практике системах планирования могут исключаться некоторые процедуры обобщённого алгоритма планирования. Исключение сопровождается снижением качества планов [1].

В соответствии с построенным планом формируется модельно-аналитический интеллект. Процесс формирования разделяется на два этапа. На первом этапе определяется расширенная объектно-ориентированная модель интеллектуального информационного агента, а на втором этапе – аналитические соотношения для вычисления значений показателей качества их функционирования.

Построенный план **P** становится основой для формирования расширенной объектно-ориентированной модели процесса функционирования интеллектуального информационного агента в классе диаграмм деятельности. Топология объектно-ориентированной модели предопределяется матрицей инциденций, представляющей связность запланированных действий **A**. Эта матрица формируется по построенному плану. Для параллельных действий добавляется вектор **F**, раскрывающий механизмы их объединений. К определению топологии добавляется множество **U**, описывающее плотности распределения вероятностей длительностей выполнения запланированных действий. Взаимодействие агента с объектами окружающей среды представляется вектором вероятностей **Q**. Во множество

элементов этого вектора включаются: вероятность уточнения информации после взаимодействия с информационным ресурсом и (или) другим агентом; вероятность уточнения знания после взаимодействия с информационным ресурсом и (или) другим агентом; вероятность уточнения модели среды после взаимодействия с информационным ресурсом и (или) другим агентом; вероятность уточнения плана после взаимодействия с информационным ресурсом и (или) другим агентом.

Определение показателей качества функционирования агента проводится на основе применения методов, описанных в [2]. Процесс определения осуществляется посредством преобразований компонентов кортежа описания **M**:

$$\mathbf{M} = \langle \mathbf{P}, \mathbf{A}, \mathbf{F}, \mathbf{U}, \mathbf{Q} \rangle,$$

соответствующих топологии и функциональности модели.

При завершении второго этапа формирования модельно-аналитического интеллекта образуется вектор показателей качества функционирования интеллектуального информационного агента **E**. Если вектор относится к области допустимых ограничений, устанавливаемых согласно требуемым гарантиям качества, то выполненное планирование признаётся успешным. В противном случае процесс планирования возобновляется.

Предлагаемая система формализаций является методической основой для расширения функциональных возможностей интеллектуальных информационных агентов и совершенствования их математического и программного обеспечения, предопределяя научную значимость раскрытого подхода к созданию артефактов. Практическая значимость заключается в предоставлении возможностей расширения областей применения интеллектуальных информационных агентов за счёт охвата тех зон, в которых требуется соблюдение гарантий в их качестве функционирования.

Список используемых источников

1. Птицына Л. К., Добрецов С. В. Интеллектуальные технологии и представление знаний. Планирование действий интеллектуальных агентов в информационных сетях : учеб. пособие. СПб. : изд-во Политехн. ун-та, 2006. 172 с. ISBN 5-7422-1101-5.

2. Птицына Л. К., Добрецов С. В. Модельно-аналитический интеллект мультиагентных систем // III Балтийский форум : материалы Международного морского форума. Составитель Н. А. Кострикова. Калининград, 2015. С. 489–497.

Статья представлена научным руководителем,
доктором технических наук, профессором Птицыной Л. К.

УДК 004.75 (075.8)

А. А. Майоров (аспирант, МТУСИ)
А. В. Тутов (аспирант, МТУСИ)
Н. В. Тутова (доцент, МТУСИ)

ДИНАМИЧЕСКОЕ РАЗМЕЩЕНИЕ ВИРТУАЛЬНЫХ МАШИН В ОБЛАЧНЫХ ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

Рассматривается проблема динамического размещения виртуальных машин (ВМ) в облачных центрах обработки данных (ЦОД). Динамическое размещение необходимо при значительном изменении нагрузки на ВМ, а также в связи с запросами на добавление/удаление ВМ. В работе предлагается методика динамического размещения ВМ, в которой в отличие от известных учитываются критерии, связанные с состоянием центра обработки данных, такие как тепловыделение, энергопотребление и эффективное использование ресурсов.

оптимальное размещение серверов, облачные вычисления, управление ресурсами, размещение виртуальных машин, многокритериальная оптимизация.

Внедрение облачных технологий ставит перед операторами ЦОД задачи эффективного управления виртуальными машинами (ВМ). Технологии виртуализации позволяют разместить несколько ВМ на одном физическом сервере, что в результате ведет к кратному увеличению числа объектов управления. Оптимальное размещение виртуальных машин особенно актуально в связи с высоким текущим уровнем загрузки ЦОД [1].

Проблеме динамического размещения ВМ посвящено множество работ [2, 3, 4, 5]. В большинстве опубликованных работ на данную тему вопрос о динамическом размещении виртуальных машин зависит только от состояния самих ВМ или производительности размещенных на них приложениях без учета большинства критериев, связанных с состоянием самих центров обработки данных, таких как изменения температуры процессоров, энергопотребления и более полного использования ресурсов серверов. В данной работе предлагается методика динамического размещения ВМ, учитывающая перечисленные выше критерии.

Современные гипервизоры VMware ESX, Microsoft Hyper-V или Xen позволяют администратору в ручном режиме осуществлять динамическое распределение ВМ. Однако в условия ЦОД критически важным является оперативное определение оптимального решения с учетом текущих и прогнозируемых параметров состояния системы.

Динамическое распределение ВМ необходимо в трех основных случаях:

1) повышения температуры физических серверов до критического порога (наиболее нагруженные ВМ должны быть перемещены для улучшения ситуации и снижения затрат на охлаждение);

2) недостатка физических ресурсов для работы ВМ (миграция ВМ позволит не потерять их производительности);

3) снижения энергозатрат (при невысокой загрузке физических серверов имеет смысл консолидировать ВМ для отключения части серверов).

Следует отметить, что учет всех критериев является противоречивой задачей.

В системе управления ЦОД функция динамического распределения возлагается на глобальный контроллер (рис. 1), который получает необходимую информацию из системы мониторинга. При динамическом распределении ВМ в ЦОД глобальному контроллеру необходимо решить следующие вопросы:

- Когда нужно производить перемещение ВМ?
- Какие ВМ выбрать для миграции?
- Куда перемещать ВМ?

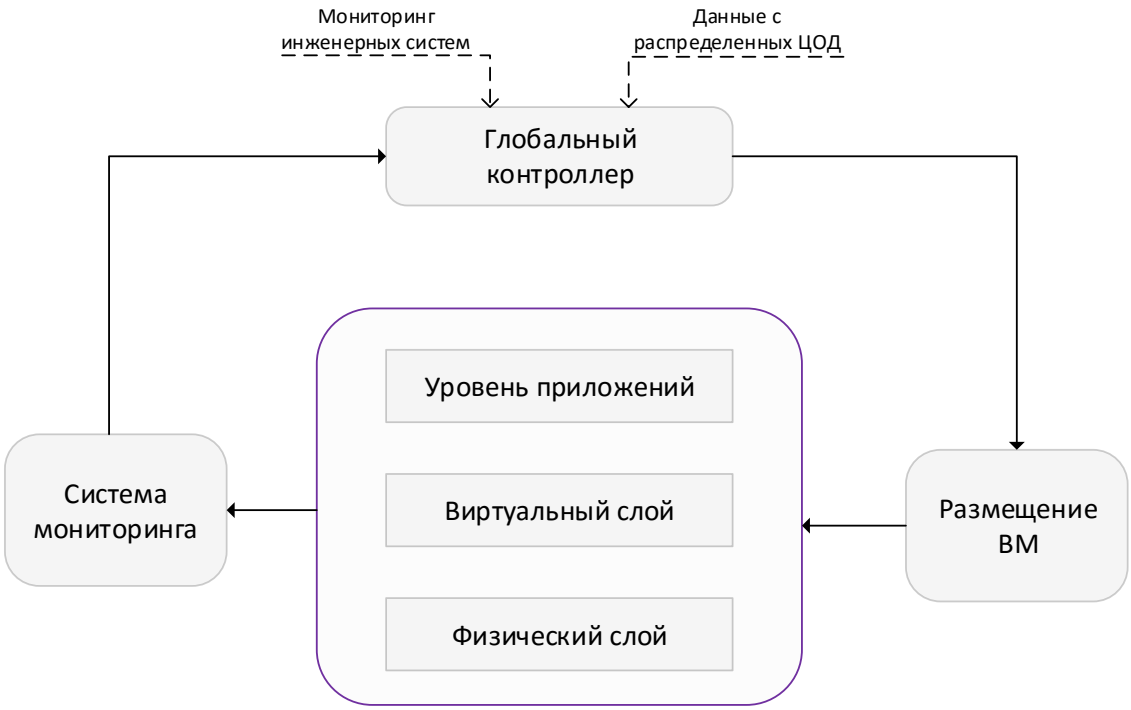


Рис. 1. Глобальный контроллер в системе управления облачным ЦОД

Для этого глобальный контроллер постоянно анализирует данные сенсоров, поступающие из системы мониторинга, и в случае выхода параметров рабочей модели за допустимый уровень, активизирует процесс миграции ВМ.

На глобальный контроллер возложена функция выбора виртуальных машин, которая определяет, какие виртуальные машины должны быть пе-

ренесены с учетом плюсов и минусов возможной миграции. В случае повышения температуры процессора сервера следует выбрать виртуальные машины с высокой загрузкой процессора чтобы эффективнее снизить его температуру. В то же время, миграция ВМ также требует процессорного времени и операций ввода/вывода, что, в свою очередь, увеличивает потребление энергии и температуру сервера. Процесс живой миграции виртуальной машины заключается в копировании файла памяти и образа на хост назначения, а также отслеживание, какие страницы памяти были модифицированы. Поэтому для миграции выбирается виртуальный сервер с меньшим объемом памяти и интенсивностью модификаций страниц, что может сократить время и накладные расходы на миграцию.

В случае конкуренции за ресурсы алгоритму выбора виртуальных машин нужно определить, какие виртуальные серверы конкурируют за ресурсы. Также учитываются накладные расходы на миграцию: конкурирующие виртуальные машины упорядочиваются по возрастанию их объема памяти, а затем виртуальные машины с памятью меньшего объема выбираются для миграции.

Низкая энергоэффективность распознается, когда контроллер определяет простаивающий сервер или сервер с низкой загрузкой ресурсов, тогда все виртуальные машины, работающие на сервере, должны быть перемещены, а сам сервер выключен.

Для того чтобы определить новый хост назначения для выбранной виртуальной машины, в функции выбора хоста вычисляются следующие параметры, которые также можно рассчитать, используя критериальные функции (1)–(3): температура сервера, энергопотребление и производительность [4].

- **Энергопотребление (f_{power}):**

$$f_{power}(u_{CPU}) = \begin{cases} p_0 + (p_1 - p_0) \cdot u_{CPU}, & u_{CPU} > 0; \\ 0, & u_{CPU} = 0, \end{cases} \quad (1)$$

где p_0 – потребление электроэнергии незагруженным сервером; p_1 – потребление электроэнергии полностью загруженным сервером.

- **Неиспользованные ресурсы ($f_{resource}$):**

$$f_{resource}(u_{CPU}, u_{RAM}) = 1 - u_{CPU} \cdot u_{RAM}, \quad (2)$$

где u_{CPU} – загрузка процессора; u_{RAM} – загрузка памяти.

Данный критерий отражает насколько полно загружены ресурсы различных типов.

- **Тепловыделение (f_t):**

$$f_t(T) = 1 - \frac{1}{1 + e^{(T - T_s)}}, \quad (3)$$

где T – текущая температура процессора; T_s – безопасная температура.

Размещение виртуальной машины на самом «холодном» сервере может помочь сбалансировать распределение температуры в ЦОД. Используя модель температуры полученную в результате обработки системных данных мониторинга, функция выбора может спрогнозировать температуру хоста назначения после миграции ВМ.

С точки зрения экономии энергии, предпочтительно помещать виртуальную машину на наиболее загруженный сервер, который еще имеет достаточно ресурсов. Алгоритм выбора хоста может использовать модели энергопотребления для прогнозирования будущего энергопотребления кандидатов в хосты назначения.

Чтобы избежать возникновения нового конфликта за ресурсы и гарантировать производительность каждой ВМ, предпочтение отдается хостам, которые имеют наибольшее количество свободных ресурсов, достаточных для размещения мигрирующих виртуальных машин.

Результаты выбора сервера по различным критериям могут отличаться друг от друга. Для решения этой задачи предлагается использовать обобщенный критерий в виде аддитивной свертки. Оптимизация выполняется при ограничениях на параметры физических серверов.

Для проверки эффективности предложенной методики было выбрано имитационное моделирование с использованием платформы CloudSim (http://www.cloudbus.org/cloudsim). Предлагаемый многокритериальный алгоритм выбора хоста назначения сравнивался с используемыми на практике эвристическими алгоритмами FFD и BFD. Полученные результаты показывают эффективность предлагаемого алгоритма на 10–15 % по критериям энергоэффективности, тепловыделения и равномерности загрузки ресурсов.

Список используемых источников

1. Обзор CNews Analytics «Облачные сервисы 2014» [Электронный ресурс]. URL: http://www.cnews.ru/reviews/cloud2014 (дата обращения 14.04.2016).

2. K. Mills, J. Filliben and C. Dabrowski, “Comparing VM Placement Algorithms for On-Demand Clouds”, Proceedings of IEEE CloudCom 2011, Nov. 29-Dec. 1, 2011, Athens.

3. Соловьев В. П., Удовиченко А. О. Метод планирования размещения группы виртуальных машин с перераспределением ресурсов // Программные продукты и системы. 2012. № 1. С. 134–138.

4. Ворожцов А. С., Тутова Н. В., Тутов А. В. Методика оптимального распределения виртуальных серверов в центрах обработки данных // T-Comm: Телекоммуникации и транспорт. 2015. № 7. С. 5–10.

5. Ворожцов А .С., Тутова Н. В., Тутов А. В. Оптимизация размещения облачных серверов в центрах обработки данных // T-Comm: Телекоммуникации и транспорт. 2015. № 6. С. 4–8.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Ворожцовым А. С.

УДК 004.7: 004.422.8

И. В. Медведев (студент магистратуры, СПбГУТ)

ИНТЕЛЛЕКТУАЛИЗАЦИЯ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ТРАНСПОРТИРОВКИ ГРУЗОВ ПОВЫШЕННОГО КОНТРОЛЯ

Определены правовые нормы и предписания транспортировки грузов повышенного контроля. Проанализированы функциональные спецификации действующих транспортных информационных систем. Представлены необходимые и достаточные методы геопозиционирования грузов повышенного контроля. Выделены возможные направления интеллектуализации геоинформационных систем транспортного комплекса. Предложена система формализаций для интеллектуализации геоинформационных систем транспортного комплекса с подсистемами планирования функциональных действий. Сформирован базис алгоритмов планирования функциональных действий. Раскрыты приоритеты выбора алгоритмов планирования функциональных действий для интеллектуальных геоинформационных систем транспортного комплекса.

геопозиционирование, геоинформационные системы, интеллектуализация, формальные методы, алгоритмы планирования действий.

В современном техногенном промышленном обществе не редко проявляется потребность в различной транспортировке грузов повышенного контроля. При подобных условиях ставятся задачи доставки грузов наиболее быстрым, безопасным и одновременно с этим экономичным путем. Вследствие указанных причин актуализируется создание новых интеллектуальных геоинформационных систем транспортировки грузов повышенного контроля или интеллектуализация существующих реализаций.

К грузам повышенного контроля причисляются объекты, определяемые ГОСТ 19433-88, и объекты, требующие дополнительной защиты при перевозке. В соответствии с указанным стандартом в повышенном контроле нуждаются следующие грузы:

- взрывчатые материалы;

- газы, сжатые, сжиженные и растворенные под давлением;
- легковоспламеняющиеся жидкости;
- легковоспламеняющиеся твердые вещества, самовозгорающиеся вещества;
- вещества, выделяющие воспламеняющиеся газы при взаимодействии с водой;
- окисляющие вещества и органические пероксиды;
- ядовитые вещества и инфекционные вещества;
- радиоактивные материалы;
- едкие и (или) коррозионные вещества;
- прочие опасные вещества.

К грузам, требующим дополнительной защиты при перевозке, относятся:

- сегменты оборонно-промышленного комплекса;
- частные грузы предприятий и фирм.

Опасные грузы нуждаются в дополнительном контроле безопасности их перевозки с целью предотвращения повреждения защитных контейнеров (цистерн) и в динамической фиксации местоположения.

При перевозке частных грузов и сегментов оборонно-промышленного комплекса дополнительно требуется организация секретности транспортировки в различных степенях.

Для обеих категорий грузов осуществляется оформление сопроводительных документов, предусматривающих определение маршрутов транспортировки до начала перевозки, без реализации возможности их изменения в процессе, чем усложняется процесс ее организации.

Среди основных видов транспортировки грузов повышенного контроля различаются следующие:

- автомобильные грузоперевозки;
- железнодорожные грузоперевозки;
- авиаперевозки;
- транспортировка водным транспортом.

Для перевозки грузов на региональном уровне наиболее частыми являются автомобильные грузоперевозки. При их выполнении наблюдаются наибольшие трудности как на этапе оформления и сбора правовых и сопроводительных документов, так и на самом этапе доставки.

Железнодорожные грузоперевозки используются на национальном и континентальном уровне. В случае перевозок внутри страны рассматриваемая деятельность регулируется внутренними правовыми нормами.

Авиаперевозки и транспортировка водным транспортом зачастую используются на межнациональном уровне. Они регулируются международным правом и частными договорами.

В настоящее время сопровождение представленных процессов проводится с применением:

- полуавтоматических систем документирования грузов и разработки маршрутов доставки;
- ручных систем документирования грузов;
- автоматических систем разработки маршрутов доставки;
- систем мониторинга опасных грузов.

В реализуемых решениях либо предусматривается активное участие человека, что сопровождается нерациональным использованием затрачиваемых временных и людских ресурсов, либо обеспечивается малая степень автоматизации сопутствующих процессов без поддержки взаимодействия с государственными и внешними структурами. Выявленная ситуация представляется в виде концептуальной карты на рисунке 1, разработанной в среде CMAPTOOLS.

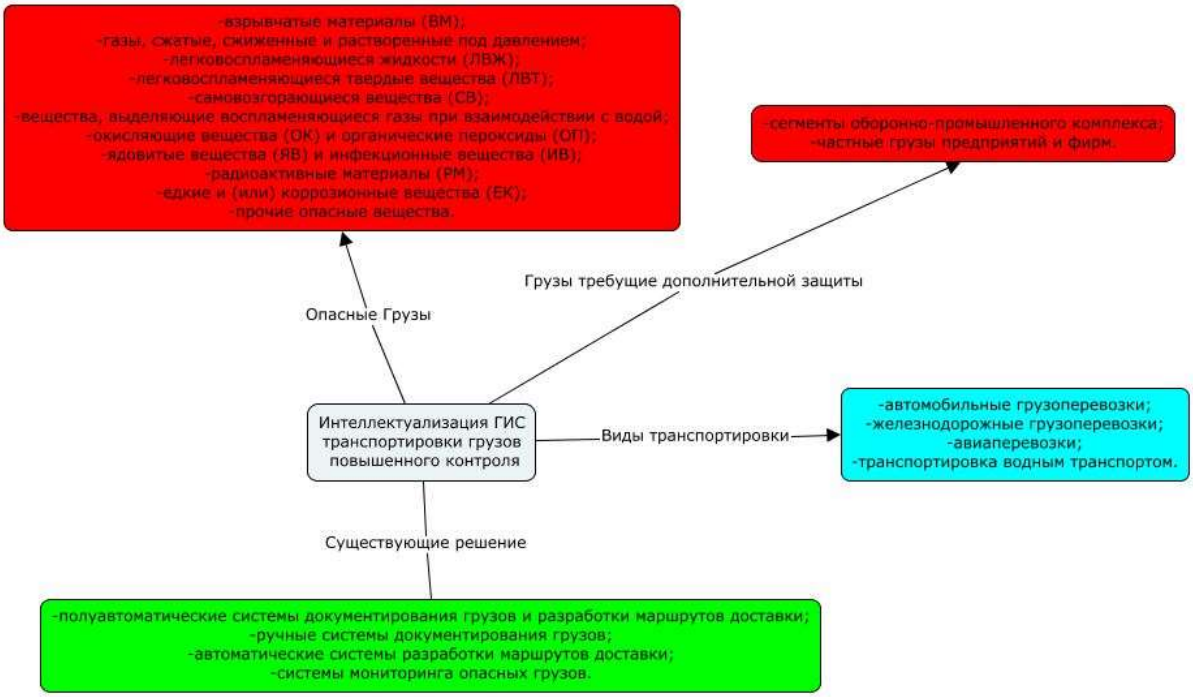


Рис. 1. Концептуальная карта представления знаний об интеллектуализации ГИС транспортировки грузов повышенного контроля

В соответствии с состоянием текущих дел в области развития ГИС транспортировки грузов повышенного контроля проявляется объективная необходимость:

- автоматизации регистрации и типирования грузов, разработка маршрутов и определение составов транспортных средств;
- оформления и составления документов сопровождения, учета и идентификации;

- организации сбора различной информации о грузах и транспортных средствах в динамическом режиме их транспортировки.

Автоматизация регистрации и типирования грузов ориентируется на ускорение данных процессов и снижение влияния на них человеческого фактора.

Автоматическая разработка маршрутов представляется как наиболее актуальной сферой интеллектуализации, так и наиболее трудоемкой из-за необходимости получения и обработки информации от множества различных источников, в том числе дорожных служб и ГИБДД. При этом данная информация должна получаться динамически и быть максимально актуальной в связи с тем, что после построения маршрута при его регистрации дальнейшее изменение затрудняется по объективным причинам.

Составление составов транспортных средств может ограничиваться системами и средствами предприятий и учреждений.

Оформление и составление документов сопровождения, учета и идентификации, в первую очередь, нацеливается на ускорение данного процесса путем рационального взаимодействия различных структур по решениям сопутствующих задач.

Системы сбора различной информации о грузах и транспортных средствах в динамическом режиме при их транспортировке создаются для контроля как за грузами и транспортными средствами в целом, так и за их отдельными элементами. С помощью подобных систем должен осуществляться контроль местоположения грузов с применением ГЛОНАСС и (или) GPS датчиков повышенной точности, а также контроль целостности контейнеров перевозимых грузов различного типа.

Предлагаемый вариант реализации системы с подсистемой построения маршрута представляется в виде интеллектуальной карты на рисунке 2.

Для базового варианта построения маршрутов выбираются методы нелинейного планирования [1, 2]. В базис алгоритмов планирования вводятся алгоритмы NONLIN, SNLP, TWEK, UA, способные обеспечить высокое качество достижения поставленных целей. Оптимизация выбора алгоритма осуществляется согласно методологии, раскрытой в [2]. Преодоление априорной неопределённости при оптимизации проводится с помощью искусственной нейронной сети. Многообразие задач оптимизации профилируется за счёт вариаций в нейросетевом обеспечении.

Предлагаемый подход к интеллектуализации открывает новые возможности по управлению качеством ГИС транспортировки грузов повышенного контроля.

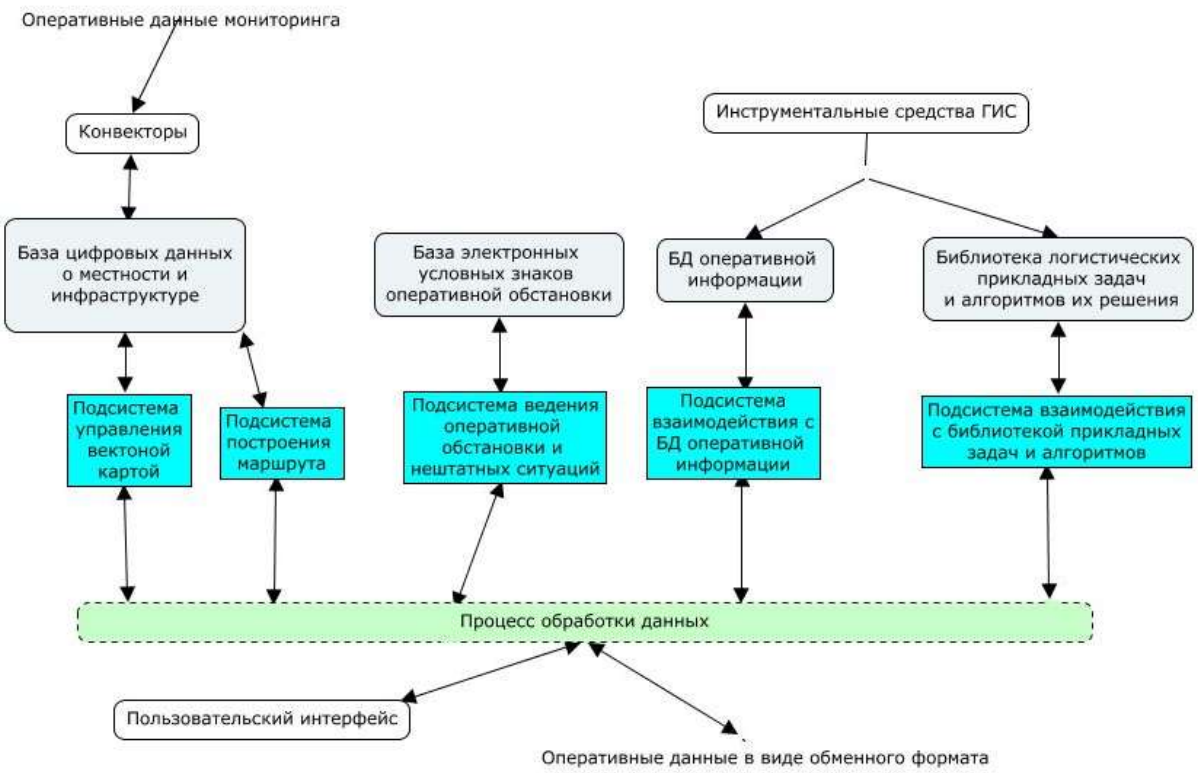


Рис. 2. Интеллектуальная карта представления модели геоинформационного комплекса с подсистемой построения маршрутов для транспортировки грузов повышенного контроля

Список используемых источников

1. Добрецов С. В., Птицына Л. К. Сравнительный анализ нелинейных процедур планирования действий интеллектуальных агентов [Электронный ресурс] // XXX Юбилейная Неделя науки СПбГТУ. Материалы межвузовской научной конференции 2002. Санкт-Петербургский государственный технический университет, 2002, Ч. VII: С. 33–35. URL: http://elib.spbstu.ru/dl/001012.pdf/download/001012.pdf (дата обращения 28.06.2016)

2. Птицына Л. К., Добрецов С. В. Интеллектуальные технологии и представление знаний. Планирование действий интеллектуальных агентов в информационных сетях : учеб. пособие ; Федер. агентство по образованию, С.-Петерб. гос. политехн. ун-т. СПб. : изд-во Политехн. ун-та, 2006. 172 с.

Статья представлена научным руководителем,
доктором технических наук, профессором Птицыной Л. К.

УДК 004.946

А. Б. Менисов (адъюнкт, ВКА им. А. Ф. Можайского)

СИСТЕМА СБОРА ГРАФИЧЕСКИХ ДАННЫХ СОЦИАЛЬНЫХ СЕТЕЙ

Статья посвящена проблеме сбора данных социальных сетей.

Автор не только анализирует современные подходы к сбору графических данных социальных сетей, но сферы применения разработанной системы. Также в статье содержатся примеры решаемых задач.

автоматизированный сбор, социальные сети, API, SMART SITY.

С развитием социальных сетей, а также активностью пользователей и интенсивности добавления данных, эти информационно-коммуникационные системы превратились в большие базы разнородных данных, с помощью которых можно решать проблемы увеличения полноты информации в гражданской и военной сферах. Подробное описание сфер применения представлено на рисунке 1.

Рис. 1. Сферы применения системы сбора данных социальных сетей

В настоящее время существует противоречие, вызванное необходимостью использования *разнородных* данных и несовершенством методов сбора *графических* данных из разных социальных сетей, для решения которого необходим научно-методический аппарат, повышающий полноту выдачи релевантных данных.

Разработанный научно-методический аппарат позволяет решать следующие задачи:

- определение позиций техники и укрепленных сооружений;
- определение подготовки подразделений к переброскам;
- оценивание обстановки;
- выявление учений и используемой техники;

- определения лидеров мнения;
- определение потерь л/с, ВВТ;
- сбор материала для формирования пропаганды;
- обеспечения оперативно-розыскной деятельности.

Процесс сбора информации включает получение и структурирование первичных данных. Собираются тексты сообщений, связи между пользователями, ссылки на внешние ресурсы, фотографические данные. Возможности системы во многом определяются богатством используемых данных и режимом их обработки. Системы, поддерживающие мониторинг в режиме реального времени, сложнее в реализации, чем использующие ретроспективный сбор данных. Работа системы сбора графических данных представлена на рисунке 2.

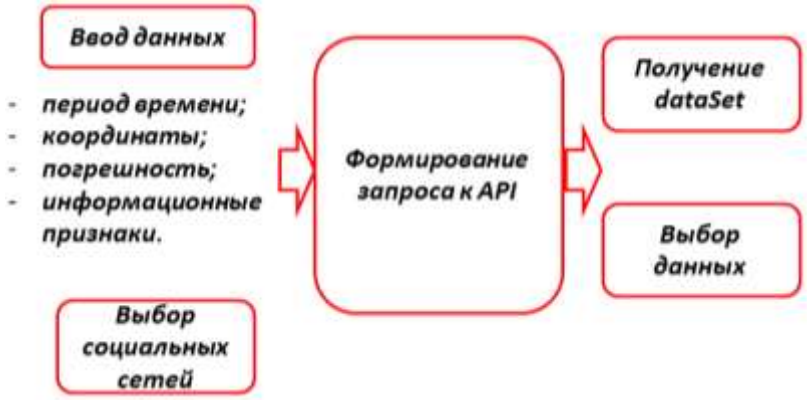


Рис. 2. Алгоритм работы системы сбора данных социальных сетей

На данный момент аналогами данной системы являются программное обеспечение Youscan, Creepy, fbStalker, а также блог Bellingcat, на котором публикуются доклады экспертов по оценке обстановки в разных регионах мира на основе данных социальных сетей. Возможности данных продуктов представлены в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ ПО сбора графических данных социальных сетей

Характеристики	Название ПО				
	BellingCat	Youscan	Creepy	fbStalker	Разработанная система
Выдача данных (шт.)	Доклады экспертов	6–12	30–40	30–40	Все, что есть
Период запроса		7 дней	любой	любой	любой
Задача области сбора (сфера)		1500 м.	+	+	+
Задача сегмента сбора (n-угольник)		-	-	-	+

Характеристики	Название ПО				
	BellingCat	Youscan	Creepy	fbStalker	Разработанная система
Количество социальных сетей		2	3	1	5
Область поиска		Круг	Круг	Круг	Круг/сектор

Таким образом, разработанная система является лучшим предложением для решения задач в военной и гражданских сферах, во-первых, система позволяет собирать больший объем данных, во-вторых, возможностью сбора в режиме реального времени, в-третьих, возможностью задачи сегментированной области поиска.

Список используемых источников

1. Капицын С. Ю., Менисов А. Б., Шастун И. А. История и классификация средств идеологического воздействия [Электронный ресурс] // Экономика и социум. Январь-март, 2015. № 1 (14). URL: http://iupr.ru/osnovnoy_razdel__1_14__2015_g_/

2. Менисов А. Б., Усков А. С. Информационная система автоматизированного сбора данных в социальных сетях // Материалы конференции военно-научного общества ВКА им. А. Ф. Можайского / под общ. ред. Ю. В. Кулешова. СПб. : ВКА им. А. Ф. Можайского, 2015. 377 с., С. 273–275.

3. Менисов А. Б. Система комплексного сбора графических данных в социальных сетях // III Открытая выставка научно-технического творчества ВКА им. А. Ф. Можайского – 2015 г.

4. Менисов А. Б. Система комплексного сбора графических данных социальных сетей // Сборник тезисов докладов V Всероссийского конгресса молодых ученых, 2016.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Капицыным С. Ю.

УДК 004.946

Е. А. Михайлова (курсант 923 уч. группы, ВКА им. А. Ф. Можайского)

ПОСТРОЕНИЕ УЧЕБНО-ТРЕНИРОВОЧНЫХ КОМПЛЕКСОВ С ИСПОЛЬЗОВАНИЕМ ШТАТНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОБРАБОТКИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ

С целью обеспечения возможности совершенствования знаний и умений специалистов пунктов сбора о обработки информации о состоянии ракет-носителей, космических аппаратов и разгонных блоков предложена структура учебно-тренировочного комплекса (УТК), построенного с использованием штатного программного обеспече-

ния обработки и анализа телеметрической информации. Рассмотрены преимущества и недостатки подобного подхода, а также способы управления режимами работы УТК. Предложены подходы к моделированию аварийных ситуаций, как на борту ракеты космического назначения, так и на средствах пунктов сбора и обработки.

учебно-тренировочный комплекс, телеметрическая информация, аварийная ситуация.

Современные тенденции развития систем обработки телеметрической информации (ТМИ) и оценивания технического состояния бортовых систем (ТС БС) ракет космического назначения (РКН) в процессе их эксплуатации предъявляют высокие требования к квалификации специалистов частей запуска и управления. Усложнение объектов ракетно-космической техники, увеличение объемов обрабатываемой информации повышают влияние человеческого фактора на оперативность выработки заключений о ТС БС и их достоверность. Для снижения влияния человеческого фактора необходимо повышать квалификацию специалистов групп обработки ТМИ и анализа ТС БС с использованием учебно-тренировочных средств, позволяющих формировать практические навыки работы в как условиях штатного функционирования РКН, так и при возникновении аварийных ситуаций.

Применение учебно-тренировочных средств является одним из основных подходов к совершенствованию умений и навыков применения и эксплуатации новых и перспективных образцов вооружения и военной техники. В состав тренажерной базы входят учебно-тренировочные комплексы (УТК), оснащенные тренажерами, учебным вооружением и военной техникой, другими тренировочными средствами [1].

Современный уровень развития вычислительной техники обеспечивает возможность создания виртуальных тренажерных комплексов, обладающих рядом достоинств [2]:

1) возможность отработки необходимых действий в штатных и аварийных ситуациях;
2) высокая эффективность обучения при относительно короткой продолжительности;
3) небольшая стоимость виртуального тренажера;
4) возможность группового и дистанционного обучения.

Применительно к группам обработки ТМИ и анализа ТС БС задача создания УТК упрощается еще и тем, что штатные комплексы обработки и анализа построены на базе персональных ЭВМ, а их функциональные возможности определяются установленным специальным программным обеспечением (СПО). На основании этого предлагается следующая структура автоматизированной системы подготовки специалистов, состоящая из следующих основных модулей (рис. 1):

1) Модуль управления конфигурацией УТК. Включает в себя средства авторизации обучающегося и руководителя, задания начальных параметров работы УТК и их смены в ходе проведения тренажа.

Рис. 1. Структурная схема автоматизированной системы подготовки специалистов групп обработки ТМИ и анализа ТС БС РКН

2) Информационно-справочный модуль. Включает в себя справочные файлы по работе с компонентами СПО; методики и инструкции обработки ТМИ и анализа ТС БС РКН; технические описания, схемы и 3D-модели бортовых систем РКН; перечень типовых неисправностей и порядок их выявления.

3) Модуль тестирования. Предназначен для проверки теоретических знаний обучающегося в области обработки и анализа ТМИ, а также знание режимов и особенностей функционирования РКН в штатном режиме и при возникновении аварийных ситуаций

4) Модуль имитационного моделирования. Включает в себя средства имитации источников ТМИ, работы БС РКН и помехового воздействия на каналы передачи информации.

5) Модуль руководителя. Включает в себя средства формирования заданий на обработку ТМИ, отказов БС РКН и технических средств комплекса обработки ТМИ, а также средства управления имитацией возмущающих воздействий на каналы передачи информации.

6) Модули обучающихся. Включают совокупность штатного СПО и позволяют осуществлять операции обработки ТМИ и анализа ТС БС РКН как в режимах нормального функционирования РКН, так и при возникновении аварийных ситуаций.

7) База данных. Обеспечивает хранение сведений о руководителях и обучающихся, справочной и технологической информации, тестовых заданий и результатов тестирования, а также параметров, обеспечивающих управление режимами работы УТК.

Указанные модули условно разделяются на *обучающие* – это модули, которые используются непосредственно при проведении обучения (информационно-справочный модуль, модуль тестирования, модуль имитационного моделирования, модули руководителя и обучающихся) и *обслуживающие* – это модули, не связанные напрямую с процессом обучения, но осуществляющие функции хранения, анализа, обработки информационных потоков тренажерного комплекса (модуль управления конфигурацией УТК, база данных).

Использование штатного СПО при построении одного из важнейших модулей – модуля обучающегося позволяет избежать разработки сложных моделей и алгоритмов обработки ТМИ и анализа ТС БС РКН.

Однако, наряду с достоинствами данному подходу присущи и некоторые недостатки наиболее значимым из которых является некоторые ограничения в возможностях управления режимами работы тренажера, моделировании тех или иных ситуаций и событий, реализации обучения и интерактивных подсказок оператору при выполнении операций обработки. Частично эти недостатки можно нивелировать путем переноса части функций по управлению режимами работы в другие модули.

Управление режимами работы тренажера можно осуществлять путем автоматизированного изменения конфигурации программно средств УТК. Под конфигурацией понимается совокупность специального программного обеспечения и информационных взаимосвязей между ними позволяющая организовать тот или иной вариант построения системы сбора и обработки ТМИ. Автоматизации реконфигурации можно достичь путем создания шаблонов запуска и останова соответствующего программного обеспечения для каждого из учебных мест и их выполнения по командам из модуля руководителя. Кроме обеспечения оперативной смены конфигурации данный подход позволяет имитировать отказ технических элементов наземных пунктов обработки ТМИ.

Имитация аварийных ситуаций на борту РКН может осуществляться двумя способами (рис. 2).

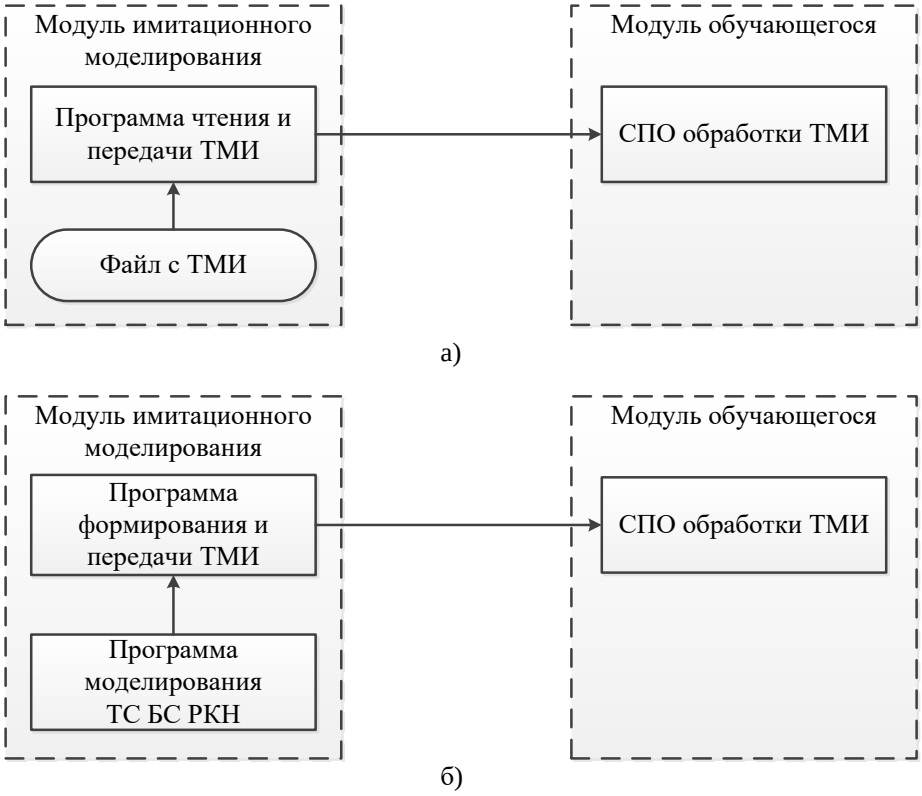


Рис. 2. Имитация аварийных ситуаций на борту РКН:
а) статическая, б) динамическая

Статический способ подразумевает использование заранее подготовленных файлов с ТМИ, которые содержат значения параметров, демонстрирующих проявление той или иной аварийной ситуации. Имитация источника ТМИ осуществляется программой чтения значений телеметрируемых параметров из файла и их передачи по сети потребителям.

Динамический способ подразумевает использование программы, моделирующей состояние бортовых систем РКН в режиме реального времени. В отличии от статического, данный способ обеспечивает возможность задания отказов бортовых систем по решению руководителя в любой момент времени.

Еще одной немаловажной особенностью обработки ТМИ является необходимость выявления и устранения искажений значений телеметрируемых параметров, возникающих на этапе передачи информации с борта РКН по радиоканалу. Обеспечить выработку навыков повышения достоверности телеизмерений можно либо внесением искажений на этапе формирования файла с ТМИ, либо имитировать зашумление на этапе передачи по сети от источника к получателю (рис. 3).

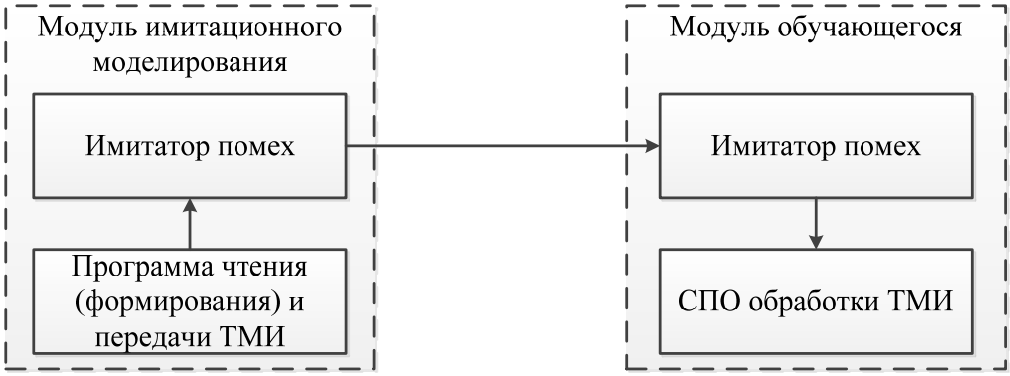


Рис. 3. Имитация искажения ТМИ на этапе передачи по радиоканалу

Имитаторы помех обеспечивают руководителя возможностью оперативного регулирования воздействия на канал передачи ТМИ в диапазоне от 0 (отсутствие помех) до 100 (искажается каждое измерение), а также блокирования передачи информации (отказ канала связи).

Дальнейшее совершенствование предложенной автоматизированной системы подготовки специалистов групп обработки и анализа ТМИ связано с ее сопряжением с аналогичной системой подготовки специалистов группы управления космическими аппаратами в части, касающейся совместного решения задач в рамках единого информационного пространства.

Список используемых источников

1. Приказ Министра обороны Российской Федерации N670 от 15 сентября 2014 г. О мерах по реализации отдельных положений статьи 81 Федерального закона от 29 декабря 2012 г. N 273 – ФЗ «Об образовании в Российской Федерации»

2. Краснянский М. Н., Остроух А. В., Баринов К. А., Дедов Д. Л., Руднев А. А. Виртуальные тренажерные комплексы для обучения и тренинга персонала химических и машиностроительных производств // Вестник ТГТУ. 2011. Т. 17. № 2. С. 497–501.

Статья представлена научным руководителем,
кандидатом технических наук Бородько Д. Н.

УДК 004.89

Д. О. Прохоров (студент группы БСТ1201, МТУСИ)
Н. В. Трофлянина (студентка группы БСТ1201, МТУСИ)
С. А. Фомин (студент группы БСТ1201, МТУСИ)

РАЗРАБОТКА ПРОГРАММНОГО АНАЛИЗАТОРА СЕТЕВОГО ТРАФИКА НА ОСНОВЕ КОЛИЧЕСТВЕННЫХ ХАРАКТЕРИСТИК ПОТОКА ТРАНСПОРТНОГО УРОВНЯ

В современных условиях, когда по сетям передачи данных передаются огромные объёмы информации, остро необходимы программные продукты, позволяющие быстро анализировать сетевой трафик с целью определения его природы. В данной работе представлен способ определения природы передаваемого трафика на основе количественных характеристик потока транспортного уровня. Отличительная черта разработанного способа – его легковесность и нетребовательность к ресурсам машины, на которой выполняется анализ. Разработано приложение, выполняющее поставленную задачу в реальном времени.

анализ трафика, потоки трафика, машинное обучение.

Введение

С каждым годом всё больше растут объёмы сетевого трафика, передаваемого по сети Интернет. Для решения многих прикладных задач требуется проводить анализ этого трафика – например, для организации классов обслуживания, для обнаружения нежелательного и запрещённого трафика и т. д.

Одним из средств, позволяющих проводить анализ передаваемых данных, является глубокий анализ пакетов (DPI). К достоинствам этого способа можно отнести высокую точность анализа, к недостаткам – низкую скорость, что критично при современных объёмах передаваемого трафика.

Другой распространённый способ – анализ TCP- и UDP-портов источника и получателя и определение приложения на основе списка широко известных портов. Недостаток способа в его недостоверности (известный порт может быть использован другим приложением) и в том, что по одному и тому же порту может передаваться трафик разной природы.

В данной работе предлагается быстрый способ анализа трафика, основанный на количественных характеристиках потока транспортного уровня. Этот способ намного быстрее, чем DPI, поскольку при его осуществлении не требуется смотреть и записывать данные прикладного уровня, достаточно запоминать лишь некоторые характеристики потока. Также предложенный способ не использует априорных знаний об использовании приложениями известных номеров TCP- и UDP-портов.

Целью работы ставится разработка способа разделения сетевого трафика на классы обслуживания с целью повышения качества обслуживания интернет-провайдера, а также разработка программного обеспечения, способного выполнять поставленную задачу в реальном времени.

1. Классы обслуживания

При разработке классов обслуживания за основу было взято разделение, предложенное телекоммуникационным стандартизирующим сектором Международного Союза Электросвязи (ITU-T), имеющее название Y.1541. Это разделение содержит 6 классов трафика, каждый из которых в разной степени требователен к одной из четырёх характеристик:

- Задержка (верхняя граница для среднего значения задержки).
- Джиттер (верхняя граница задержки для квантиля 99,9 %).
- Потери (верхняя граница на вероятность потери пакета).
- Ошибки (верхняя граница на вероятность ошибки в пакете).

Так как требования к потерям и ошибкам одинаковы почти у всех классов (они отсутствуют лишь у шестого, «неопределённого» класса»), на основе предложенных *ITU* характеристик были выделены следующие 3 типа сетевых приложений:

- Тип 0: не чувствительные к задержкам и джиттеру. Примеры: браузеры при просмотре веб-страниц (без мультимедиа), BitTorrent.
- Тип 1: чувствителен только к задержкам, но не к джиттеру. Пример: браузеры при просмотре потокового мультимедиа.
- Тип 2: чувствительные и к задержкам, и к джиттеру. Примеры: Skype, Viber при осуществлении аудио- и видеосвязи реального времени.

В данной классификации оказывается, что трафик, генерируемый одним и тем же приложением ОС, может относиться к разным классам обслуживания. В этой связи необходимо уточнить понятие «приложение». В рамках данной работы под приложением понимается владелец одного открытого сокета. Например, приложение ОС chrome.exe может одновременно держать открытым сокет на некотором TCP-порту и принимать через этот порт гипертекстовую разметку веб-страницы (HTML), а также держать открытым сокет на некотором UDP-порту и принимать через этот сокет видеоданные (с такого сайта, как YouTube). В этой ситуации будем считать, что работают два отдельных приложения: одно типа 0 (гипертекст), другое типа 1 (мультимедиа).

2. Обучающая выборка

Для проведения анализа отобраны следующие виды трафика:

- Тип 0: DNS, BitTorrent, HTML поверх HTTP(S).
- Тип 1: видео и аудио поверх HTTP(S) и QUIC.
- Тип 2: видео и аудио в ПО Skype.

Были выбраны именно эти виды трафика по той причине, что именно такой трафик генерируют большинство пользователей сети Интернет.

Было собрано более 3 Гб трафика приведённых выше видов. Для выделения этих видов среди прочего трафика использована библиотека nDPI, осуществляющая глубокий анализ пакетов. Однако nDPI определяет лишь протокол прикладного уровня, а этого оказывается недостаточно для разделения трафика на необходимые классы, так что кроме DPI был проведён дополнительный анализ трафика каждого протокола. Итоговое распределение потоков по классам представлено в таблице 1.

ТАБЛИЦА 1. Критерии отбора трафика для обучающей выборки

Тип трафика	Тип приложения	Критерий разделения
DNS	0	-
BitTorrent	0	-
HTTP.text	0	Анализ HTTP-заголовка, разделение по MIME-типу
HTTP.image	0	
HTTP.audio	1	
HTTP.video	1	
SSL.multimedia	1	Эвристическое разделение: мультимедиа > 1 Мб полезной нагрузки
SSL.other	0	
QUIC.multimedia	1	
QUIC.other	0	
Skype.realtime	2	Эвристическое разделение: realtime > 50 пакетов в секунду и > 3 секунд длительности
Skype.other	0	

3. Обучение классификатора

Следующий шаг – выделение количественных характеристик потока и применение алгоритмов машинного обучения для создания классификатора.

При выделении количественных характеристик потока следует пояснить некоторые используемые понятия:

- порция данных – объём полезной нагрузки, переданный от одной стороны к другой, не прерываемый полезной нагрузкой с противоположной стороны;
- инициатор – инициатор соединения;
- адресат – адресат соединения.

Полный список выделенных характеристик представлен в таблице 2.

ТАБЛИЦА 2. Полный список выделяемых характеристик потока

Характеристика	Пояснение
Средний размер сегмента со стороны инициатора	Среднее значение – статистическая оценка математического ожидания
Средний размер сегмента со стороны адресата	
Средний размер порции данных со стороны адресата	
Средний размер порции данных со стороны инициатора	
СКО размера порции данных со стороны инициатора	Среднеквадратическое отклонение – статистическая оценка дисперсии
СКО размера порции данных со стороны адресата	
СКО размера сегмента со стороны инициатора	
СКО размера сегмента со стороны адресата	
Среднее число сегментов на порцию данных со стороны инициатора	Общее число пакетов, делённое на общее число порций данных
Среднее число сегментов на порцию данных со стороны адресата	
КПД инициатора	Общее количество полезной нагрузки, делённое на общее количество байт
КПД адресата	
Соотношение переданных байт	Во сколько раз адресат передаёт больше, чем инициатор
Соотношение переданной полезной нагрузки	
Соотношение переданных сегментов	
Размеры первых 4 порций данных	2 со стороны инициатора, 2 со стороны адресата
Размеры первых 4 сегментов данных	Не учитывая TCP handshake

Значения характеристик определялись по первой 1 000 пакетов каждого потока.

Было испробовано несколько алгоритмов машинного обучения, однако лучший результат по Ф-мере показал алгоритм «Случайный Лес». Для обучения классификатора было использовано две трети выборки, для проверки его производительности – оставшаяся треть. Результаты работы алгоритма представлены в таблице 3.

ТАБЛИЦА 3. Проверка классификатора на тестовой выборке

		Предсказанные классы		
Реальные классы		0	1	2
	0	1624	1	0
	1	0	36	0
	2	0	0	3

В приведённой таблице значение каждой ячейки – это количество случаев, когда классификатор причислил поток к классу, указанному в заголовке столбца, а на самом деле трафик принадлежат классу, указанному в заголовке строки. Таким образом, главная диагональ – случаи верной классификации, всё остальное – разного рода ошибки.

Кроме того, была предпринята попытка обучить классификатор определять не только тип приложения, но и природу самого трафика. Результаты представлены в таблице 4.

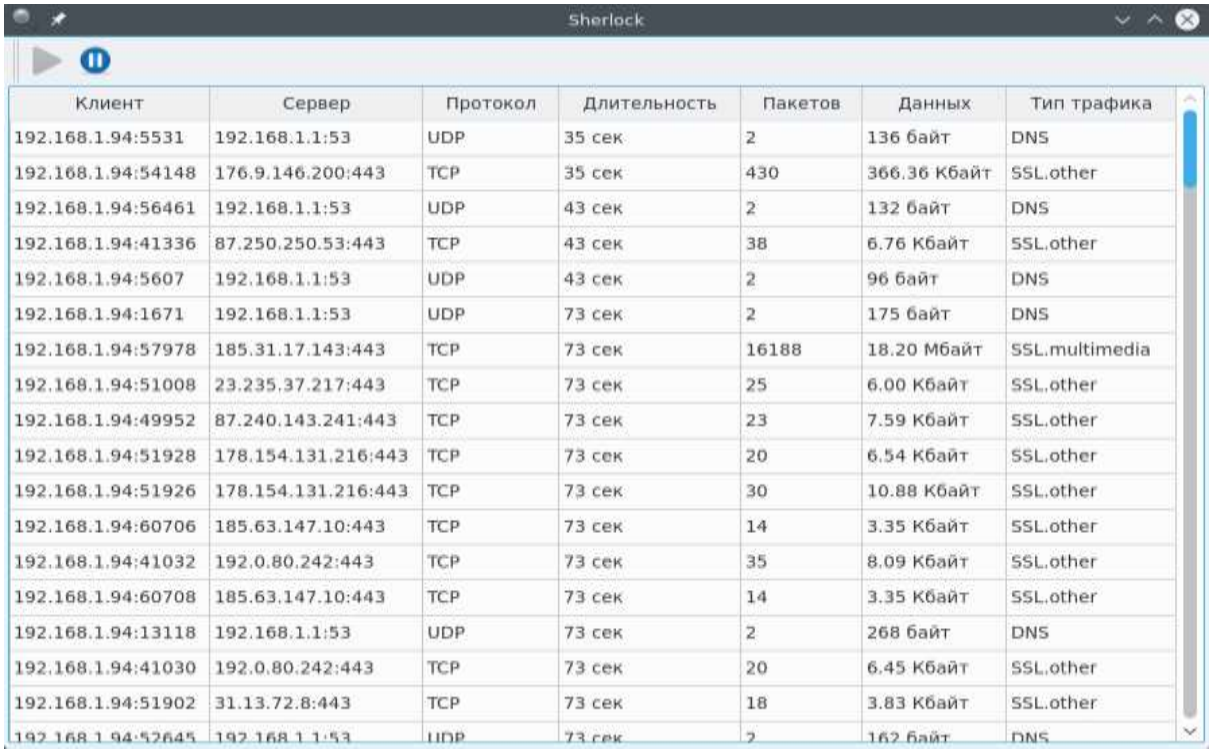
Также было разработано программное обеспечение, способное в реальном времени разделять трафик на потоки, вести учёт количественных характеристик каждого потока и на основе собранных характеристик делать выводы о природе передаваемого трафика. На рисунке 1 представлен скриншот разработанного приложения.

Выводы

В результате эксперимента была доказана принципиальная возможность определения класса сетевого приложения на основе количественных характеристик потока транспортного уровня. Более того, было показано, что с некоторыми погрешностями возможно даже определять протокол 7-го уровня и природу передаваемых данных без анализа содержимого пакетов. Был разработан программный продукт, способный выполнять анализ трафика на основе количественных характеристик потока в реальном времени. Дальнейшее развитие предложенных идей возможно в нескольких направлениях. Во-первых, следует усовершенствовать методы отделения целевого трафика, чтобы устранить эвристические критерии. Во-вторых, представленные идеи требуется проверить на большем объёме трафика, ведь собранные 3 Гб не могут претендовать на полную репрезентативность.

ТАБЛИЦА 4. Результат расширенного обучения классификатора

	Предсказанные классы											
	BitTorrent	DNS	HTTP. audio	HTTP. image	HTTP. text	HTTP. video	QUIC. multimedia	QUIC. other	SSL. multimedia	SSL. other	Skype. other	Skype. realtime
BitTorrent	20											
DNS		1019										
HTTP.audio			6			2						
HTTP.image				139	1							
HTTP.text				4	74					3		
HTTP.video						2						
QUIC.multimedia							1					
QUIC.other								38				
SSL.multimedia			3			1			23	1		
SSL.other				1						239		
Skype.other											88	
Skype.realtime												3



Клиент	Сервер	Протокол	Длительность	Пакетов	Данных	Тип трафика
192.168.1.94:5531	192.168.1.1:53	UDP	35 сек	2	136 байт	DNS
192.168.1.94:54148	176.9.146.200:443	TCP	35 сек	430	366.36 Кбайт	SSL.other
192.168.1.94:56461	192.168.1.1:53	UDP	43 сек	2	132 байт	DNS
192.168.1.94:41336	87.250.250.53:443	TCP	43 сек	38	6.76 Кбайт	SSL.other
192.168.1.94:5607	192.168.1.1:53	UDP	43 сек	2	96 байт	DNS
192.168.1.94:1671	192.168.1.1:53	UDP	73 сек	2	175 байт	DNS
192.168.1.94:57978	185.31.17.143:443	TCP	73 сек	16188	18.20 Мбайт	SSL.multimedia
192.168.1.94:51008	23.235.37.217:443	TCP	73 сек	25	6.00 Кбайт	SSL.other
192.168.1.94:49952	87.240.143.241:443	TCP	73 сек	23	7.59 Кбайт	SSL.other
192.168.1.94:51928	178.154.131.216:443	TCP	73 сек	20	6.54 Кбайт	SSL.other
192.168.1.94:51926	178.154.131.216:443	TCP	73 сек	30	10.88 Кбайт	SSL.other
192.168.1.94:60706	185.63.147.10:443	TCP	73 сек	14	3.35 Кбайт	SSL.other
192.168.1.94:41032	192.0.80.242:443	TCP	73 сек	35	8.09 Кбайт	SSL.other
192.168.1.94:60708	185.63.147.10:443	TCP	73 сек	14	3.35 Кбайт	SSL.other
192.168.1.94:13118	192.168.1.1:53	UDP	73 сек	2	268 байт	DNS
192.168.1.94:41030	192.0.80.242:443	TCP	73 сек	20	6.45 Кбайт	SSL.other
192.168.1.94:51902	31.13.72.8:443	TCP	73 сек	18	3.83 Кбайт	SSL.other
192.168.1.94:52645	192.168.1.1:53	UDP	73 сек	2	162 байт	DNS

Рис. 1. Скриншот разработанного приложения

Список используемых источников

1. Lim Y., Internet Traffic Classification Demystified: On the Sources of the Discriminative Power, конференция CoNEXT 2010.

Статья представлена научным руководителем,
доцентом Беленькой М. Н.

УДК 004.056.5

Ю. Н. Романова (студентка группы Р4155, ИТМО)
К. А. Янюшкин (студент группы Р4155, ИТМО)

ОСОБЕННОСТИ ВЫБОРА CONTENT MANAGEMENT SYSTEM

На сегодняшний день широкое распространение получили системы управления содержимым сайта, позволяющие реализовывать компромиссное решение между низкой стоимостью статических сайтов и высокой гибкостью динамических. В статье рассмотрены общие принципы систем управления контентом, а так же выделены основные критерии выбора подобных систем.

управление контентом, web-сайт, портал, содержимое сайта, безопасность сайта, управление содержимым, администрирование сайта.

Ежедневно попадая в интернет пространство, пользователям приходится сталкиваться с множеством различных web-сайтов. Кроме того, многим из специалистов, хотя бы раз в жизни, приходилось создавать свой сайт. Неважно, что послужило стимулом – какие-либо личные мотивы, служебная необходимость или просто любопытство, в любом случае, в современном интернет пространстве одной из важнейших задач является создание сайта.

В данный момент широкое распространение получили системы управления содержимым сайта (*Content Management System* – CMS), позволяющие реализовывать компромиссное решение между низкой стоимостью статических сайтов и высокой гибкостью динамических. Благодаря подобным системам резко повысилась управляемость сайтом, и значительно снизились расходы на его администрирование.

Выбор CMS кажется простым вопросом только на первый взгляд. На самом деле CMS напрямую влияет на стоимость разработки и владения сайтом. В зависимости от системы, разница в годовых затратах может значительно изменяться особенно, если дело касается посещаемых ресурсов.

И все-таки сделать правильный выбор нелегко. Во-первых, на рынке представлено множество различных систем управления. Во-вторых, нет четкого способа заранее сравнить эффективность систем.

Практически каждый веб-программист выбирает «самую» CMS и останавливается. Решение о выборе системы необходимо принимать заказчику [1].

Общие принципы систем управления контентом (CMS):

1) Доступность. При использовании CMS на сайте нет необходимости устанавливать какое-то специальное программное обеспечение (ПО) – сама система устанавливается на веб-сервер и все операции с контентом осуществляются через любой интернет-браузер (Internet Explorer, Mozilla, Opera, Safari, Google Chrome и т. п.).

2) Функциональность. Большинство CMS сделаны по принципу модульности: имеется какая-то базовая основа, к которой возможно подключение модулей. Модули могут уже входить в состав комплекса, могут быть установлены отдельно, а также многие системы допускают самостоятельную разработку и включение дополнительных модулей.

3) Безопасность. Большинство современных систем предоставляют ряд средств для безопасной работы с сайтом, защиты информации и обеспечения целостности структуры.

4) Общая структура. Так или иначе, все CMS состоят из оболочки (программы управления) и базы данных. Оболочка – это набор программ, которые по запросу пользователя берут информацию из баз данных и пе-

редают ее в виде отдельной страницы браузеру. Такими образом страницы генерируются «на лету» по заданному шаблону.

Критерии выбора CMS*:*

1) Назначение сайта. Самым важным критерием выбора системы управления контентом (CMS) является назначение сайта. От того чем является ваш ресурс или каким вы планируете его сделать – зависит многое. Если ориентирован, прежде всего, на продажу товаров или услуг (интернет-магазин, каталог) – это один вид CMS, с торговой специализацией. Если у вас новостной или информационный портал – это другой вид систем. Если вы планируете создавать сайт большой компании или интернет-портал – нужна будет корпоративная система. Все зависит от направления деятельности и назначения веб-сайта.

2) Функционал. После того, как вы определились с назначением сайта, возникнет перечень функций, которые система должна обеспечивать: размещение информационных материалов (новости, статьи, термины и понятия, вопросы и ответы и т. п.), размещение товарных предложений, перечень услуг (каталог), формы заказа и заявок, обратная связь, поддержка, общение и т.п. Все эти конкретные задачи обеспечиваются функционалом сайта. Поэтому при выборе CMS следует внимательно отнестись к его функциональным возможностям.

3) Удобство. Далее необходимо определить кто, где и как часто будет работать с контентом сайта, каковы его навыки работы с компьютером. Если планируется, что над сайтом будет работать целый коллектив авторов, то и CMS должна предоставлять достаточные возможности по коллективной работе.

4) Технические требования к хостингу. Поскольку CMS устанавливается на сервер (хостинг-площадку) – у всех CMS есть ряд технических требований к серверу, на котором она будет работать. Требуются различные базы данных, поддержка языков программирования, разное доступное пространство на диске и тому подобные особенности. Если у вас уже есть хостинг-площадка, то при выборе CMS следует обратить внимание на техническую возможность использования оной на вашей площадке. Особо сложные, многофункциональные CMS или проекты с большой посещаемостью (новостные сайты, крупные интернет-магазины) могут создавать большую нагрузку на сервер.

5) Безопасность. Существует два типа программных разработок: системы с открытым кодом (исходный код CMS открыт для модифицирования) и коммерческие системы с закрытым кодом (исходный код CMS является собственностью компании-разработчика и не может быть модифицирован). Для первого типа характерны наличие большого количество различных модулей и более простое изменение функционала сайта. Такие системы поддерживаются каким-то сообществом разработчиков на добровольной основе. Для коммерческих (закрытых) систем важны лучшая без-

опасность и поддержка. И, безусловно, для всех типов CMS важны обновления и исправления в системах безопасности.

6) Сколько стоит. Существуют коммерческие и свободно распространяемые системы управления контентом. Причем даже среди коммерческих CMS существуют бесплатные или условно бесплатные редакции. Чаще всего эти бесплатные варианты обладают почти всем необходимым функционалом для небольших интернет-проектов (блог, интернет-магазин, сайт-каталог).

7) Поддержка. Важно определиться, кто и как будет заниматься установкой и поддержкой CMS для вашего проекта. Это может быть собственный специалист компании, или же договор со студией интернет-разработок. При этом значение имеет оперативность и уровень поддержки. Для систем с открытым кодом важно наличие активных участников в сообществе, достойные каналы поддержки, такие как официальные форумы, списки рассылки, вики и базы знаний.

8) Простота развертывания. Немаловажным фактором является простота установки и обновления системы. Если для установки и настройки CMS требуется длительный труд специалистов – это говорит о невнимании разработчиков к администраторам и пользователям CMS.

Наиболее популярные в России свободно распространяемые системы: Drupal, Joomla, MODx, WordPress. Коммерческие системы: 1С-Битрикс, NetCat, UMI.CMS, Host.CMS, Amiro.CMS, S.Builder.

Список используемых источников

1. Денисов А. Системы управления сайтами [Электронный ресурс] // CMSmagazine. 2010. URL: http://www.cmsmagazine.ru/library/items/cms/choice_cms/ (дата обращения 05.02.2016).

2. Басыров Р. Постройте профессиональный сайт сами. СПб. : Питер, 2009. 304 с.

Статья представлена научным руководителем,
доктором технических наук, профессором Ткалич В. Л.

УДК 65.011.56

С. О. Рудик (студент, СПбГУТ)

АВТОМАТИЗАЦИЯ ПРОИЗВОДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ CSRP

Данная статья посвящена решению актуальной задачи: разработки системы автоматизации предприятий на основе технологии CSRP для управления услугами в зависимости от условий клиента В процессе работы было рассмотрена технология CSRP.

система управления, информационные системы, базы данных, информационная система персональных данных, инфокоммуникационные системы, планирование ресурсов предприятия, управление данными, управление, ориентированное на взаимодействие с клиентами, управление отношениями с заказчиками

CSRP (англ. *Customer Synchronized Resources Planning*, управление, ориентированное на взаимодействие с клиентами) – технология, включающая получение заказов, разработку планов, проектов и заданий, техподдержку.

Технология реализует планирование ресурсов, синхронизированное с покупателем. CSRP включает в себя полный цикл – от проектирования будущего изделия с учетом требований заказчика, до гарантийного и сервисного обслуживания после продажи. Суть CSRP состоит в том, чтобы интегрировать покупателя в систему управления предприятием, причем сам покупатель размещает заказ на изготовление продукции, сам отвечает за правильность его исполнения и при необходимости отслеживает соблюдение сроков производства и поставки. Предприятие же может очень четко отслеживать тенденции спроса на его продукцию.

В настоящее время корпоративные информационные системы на основе технологии CSRP набирают все большую популярность на предприятиях. Методология CSRP основана на синхронизации исполнительных и планирующих центров с клиентом, что позволяет быстро влиять на производство того или иного товара, или предоставления услуг. Целью данной статьи является рассмотрение стандарта CSRP для автоматизации производственной деятельности предприятия связи.

При использовании модели бизнеса CSRP, традиционные бизнес-процессы пересматриваются в направлении к обслуживанию покупателей и создании продуктов, удовлетворяющих их потребности. Внедрение приложений CSRP подталкивает руководителей предприятия к изменению. Внутренняя сфокусированность традиционных производственных структур, сегментированная по отделам и функциональности, перефокусируется

наружу. CSRP позволяет построить двунаправленный свободный поток информации между покупателем и производителем.

С точки зрения программных технологий, общий вид CSRP как системы представляет собой набор программных комплексов. Можно составить структурную модель информационной системы (рис. 1), выделив ее основные компоненты, которые содержат программные модули определенного класса. Нижним уровнем информационной системы является, хранилище, в котором содержится вся интеллектуальная собственность предприятия. Прямого доступа к хранилищу не должно быть ни у какого сотрудника на предприятии. Прямой доступ имеет лишь система управления знаниями, которая служит шлюзом для остальных систем и формирует информационное окружение предприятия.

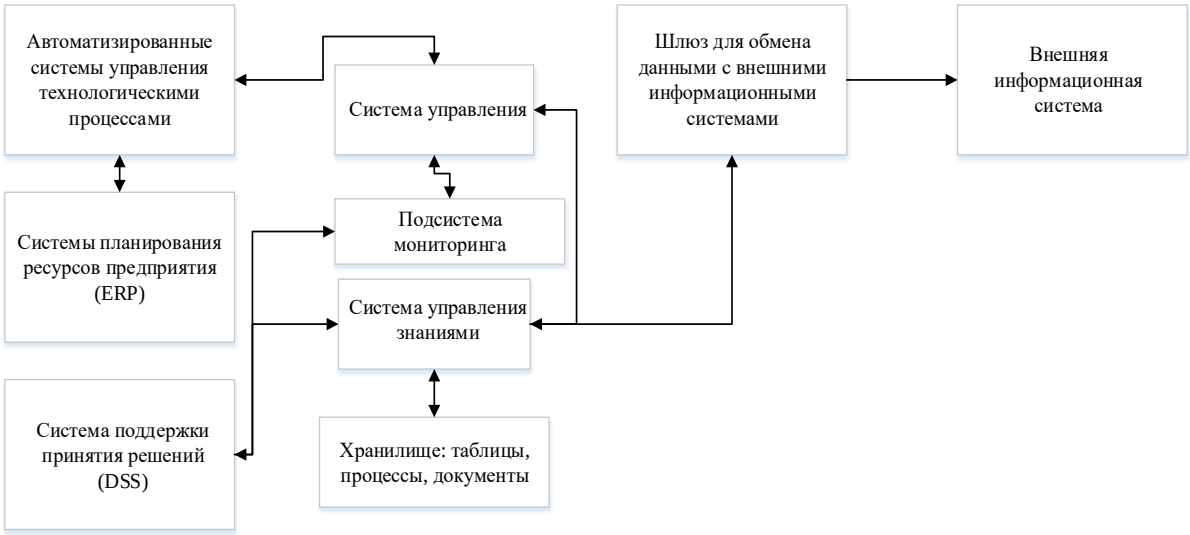


Рис. 1. Структурная модель CSRP как системы

CRM (англ. *Customer Relationship Management*, управление отношениями с заказчиками) – технология, осуществляющая отслеживание истории развития взаимоотношений, координирование многосторонних связей, централизованное управление продажами и клиент-ориентированным маркетингом.

Концепция построения автоматизированных систем обслуживания клиентов компании. CRM подразумевает накопление, обработку и анализ не только финансово-бухгалтерской, но и прочей информации о взаимоотношениях с клиентами. Это способствует повышению производительности менеджеров, улучшает качество обслуживания клиентов и способствует увеличению продаж.

На этапе планирования продаж осуществляется оценка объема и динамики продаж необходимых для выполнения поставленных задачи. Изменение плана продаж повлечет за собой изменение в результатах других модулей. Планирование закупки материалов проходит на основе производственной программы для каждого вида готовой продукции, определяет

необходимое количество материалов, осуществляет закупку ресурсов. При планировании производства утверждается порядок изготовления всех видов изделий.

Для каждого изделия в рамках выпускаемой линии продукции существует своя собственная технология производства. Совокупность программ по выпуску продукции представляет собой производственный план. Обратная связь необходима для решения возникших проблем с поставщиками комплектующих материалов и партнерами, необходима при изменении отдельных планов, оказавшихся невыполнимыми и подлежащих перезаписи.

CSRP – интегрированная электронная информационная система управления, реализующая концепцию управления ресурсами предприятия, главным предназначением является создание продуктов с повышенной ценностью для покупателя, то есть продуктов, которые подходят требованиям каждого покупателя. Систему CSRP называют интегрированной системой поддержания функционального жизненного цикла изделия.

CSRP технология предназначена для создания продуктов с повышенной ценностью для покупателя, то есть товаров или услуг, которые удовлетворяют специфическому набору требований каждого конкретного покупателя. Обработка заказов включает в себя, кроме функции ввода заказа, функции продажи и маркетинга.

Активизация производства за счет внедрения требований покупателя вынуждает руководителя предприятия акцентировать свое внимание не только на производстве, но и учитывать различные рыночные факторы. Имея анализ о продажах товаров и услуг, можно систематизировать подход к решению следующих вопросов: какие продукты производить, на какие новые рынки необходимо акцентировать внимание.

Система CSRP является первой технологией, которая интегрировала в себя взаимодействие с клиентом. Информация о клиентах влияет: на разработку продуктов, закупки, управление запасами, на управление финансами, на управление информацией о продуктах. Использование CSRP систем повышает качество товара, снижает время поставки, повышает ценность товара для клиента, снижает производственные издержки, а также улучшает обратную связь клиентом.

ERP (англ. *Enterprise Resource Planning*, планирование ресурсов предприятия) – организационная стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и оптимизацию ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности.

Деятельность предприятия определяется процессом производства, если в ERP системе товары производится только на заказ, то в CSRP системе

существует способность создавать и управлять уникальным списком комплектующих изделий и соответствующими производственными процедурами для уникального заказа клиента.

Рассмотрим стандартную производственную ситуацию: оператор call-центра связывается с новым клиентом, вместе они обсуждают текущие и будущие требования к продукту. Обсуждают конфигурации, цены и услуги, подбирают решение, которое будет удовлетворять клиента по всем пунктам. В конечном итоге после обсуждения всех критериев они смогут подобрать то решение, которое ни один другой конкурент не может предложить сейчас.

Используя приложение, продавец способен зафиксировать требования к продукту, цену и автоматически послать эту информацию в непосредственно в конструкторский отдел, где информация используется в виде детальных инструкций по производству и планированию. После этого создаются спецификации на материалы и комплектующие для производства, автоматически определяются производственные маршруты, резервируются и заказываются необходимые материалы, создается заказ в производство. Ключевая информация о клиенте динамически используется в основной деятельности предприятия. Информация о предпочтениях покупателя сохраняется в общей базе данных, используемой в сервисных подразделениях, отделах технического обслуживания, исследований, планирования производства, что позволяет достичь необходимого уровня синхронизации деятельности предприятия с потребностями клиентов.

Заключение

С развитием новых технологий стал возможен прием сложных заказов на расстоянии: покупатель, используя средства Интернет для доступа к Web-серверу производителя, вводит заказ – стандартный или видоизменённый и отправляет заказ в любое время суток, минуя продавца, либо оператора call-центра. Клиент может редактировать предыдущие заказы, проверить состояние заказов, которые находятся в обработке или запросить добавить новые пункты. Действия клиента автоматически влияют на планирование, производство и обслуживание покупателей, так как сам покупатель интегрирован в бизнес-процесс. Результатом успешного применения CSRP технологий, является повышение качества товаров, увеличение прибыли предприятия, снижение времени производства и доставки. Еще одним важным результатом применения технологии, является развитие инфраструктуры для создания индивидуальных, конфигурируемых решений, также улучшение обратной связи с клиентами и обеспечение лучшего сервиса для покупателя.

Список используемых источников

1. Гольдштейн Б. С., Фрейнкман В. А. Call-центры и компьютерная телефония. СПб. : БХВ-Петербург, 2002. 373 с.
2. Де Роза К. Планирование ресурсов в зависимости от потребностей клиента (CSRP – Customer Senchreniced Resource Planning): Новый норматив для изготовителей / пер. с англ. М. : СОКАП. 2000. 10 с.
3. Когаловский М. Р. Перспективные технологии информационных систем. М. : ДМК Пресс; Компания АйТи, 2003. 288 с. SBN 5-94074-200-9.
4. Минцберг К. Структура в кулаке: создание эффективной организации / пер. с англ. под ред. Ю. Н. Каптуревского. СПб. : Питер, 2004. 512 с.
5. Новикова Г. М. Корпоративные информационные системы: учебное пособие. М. : РУДН. 2008. 94 с.

Статья представлена научным руководителем,
кандидатом технических наук Белоусом К. В.

УДК 004.7:004.422.8

А. В. Савлиш (студент группы ИСТ-22, СПбГУТ)
П. В. Смирнова (студентка группы ИСТ-511м, СПбГУТ)

ИНТЕГРАЦИЯ СЕРВИС-ОРИЕНТИРОВАННЫХ СРЕДСТВ ДЛЯ СИСТЕМ СИТУАЦИОННОГО УПРАВЛЕНИЯ

Представлены основания необходимости учёта специфики ситуационного управления при интеграции средств сервис-ориентированной архитектуры. Рассмотрены механизмы интеграции сервис-ориентированных средств для систем ситуационного управления. Предложены математические объекты для описания рассмотренных механизмов в классе расширенных объектно-ориентированных моделей. Выбраны показатели качества интеграции сервис-ориентированных средств. Описан метод определения показателей качества интеграции сервис-ориентированных средств при темпоральной логике их объединения.

сервис-ориентированная архитектура, сервис, ситуационное управление, интеграция сервисов, качество сервис-ориентированной архитектуры.

По мере совершенствования технологического базиса информационных инфраструктур расширяется сфера применения сервис-ориентированных архитектур. Одно из перспективных направлений подобного расширения ориентируется на ситуационное управление. Ситуационное управление активно используется в инфраструктурах, технологических процессах, энергетике, бизнесе, предпринимательстве, коммерции, менеджменте, банковских системах, транспорте, строительстве, связи, телекоммуникациях, медицине, образовании, сфере сервиса, медиа-

индустрии. Основной причиной востребованности ситуационного управления является объективная необходимость отслеживания изменений, происходящих в окружающих средах различного рода и масштаба. Парадигма сервис-ориентированных архитектур согласуется с вариативным характером функциональных спецификаций соответствующих систем, образуемых посредством интеграции сервис-ориентированных средств. На этом основании проявляется привлекательность создания систем ситуационного управления в соответствии с концепцией сервис-ориентированной архитектуры.

При широкой палитре особенностей ситуационного управления основное внимание уделяется масштабируемости, асинхронности и оперативности. Предпочтительность таких акцентов предлагается учитывать в механизмах интеграции сервис-ориентированных средств.

Наряду с традиционными механизмами параллельной масштабируемой интеграции сервис-ориентированных средств, представленными в [1], вводятся механизмы интеграции с темпоральной логикой. Они подобны схемам комплексирования решающих функций с временными задержками, описанным в [2].

Введение новых механизмов интеграции нуждается в математическом сопровождении анализа их качества. В позиций обеспечения полного профиля качества новых механизмов интеграции выбирается плотность распределения вероятностей времени выполнения поставленной перед системой задач. При таком выборе сохраняется и методологическое единство профилирования качества разнообразных механизмов интеграции средств в сервис-ориентированной архитектуре, предложенное в [2].

В качестве исходной информации для профилирования качества новых механизмов интеграции сервис-ориентированных средств воспользуемся плотностями распределений длительностей исполнения сервисных функций. Для их нахождения могут применяться формализации, представленные в [2, 3, 4] и ориентированные на разнообразие традиционных схем интеграции сервисов в пассивных и в активных инфокоммуникационных средах.

Пусть переменными M_1, M_2,..., M_I обозначаются произвольные дискретные временные задержки в объединении 1-го, 2-го, ..., I-го сервисов. В условиях ситуационного управления временные задержки могут регулироваться в соответствии с контекстом решаемой задачи.

Каждый i-м сервисом из объединяемых по окончании своего выполнения ожидается дискретное время M_i на подтверждение готовности всех других сервисов к объединению. Если в течение этого времени не подтверждается их готовность, то сервис исполняется заново. В соответствии с описанной схемой событий $f[k]$ плотность распределения вероятностей длительности исполнения I объединяемых сервисов определяется соотношением:

$$f[k] = f_{first}[k] + \sum_{j=1}^{k-2} f_{first}[j]\Phi_{сбр}(k-j),$$

$$f_{first}[k] = f_1[k] \sum_{j_2=k-M_2}^{k} f_2[j_2] \ldots \sum_{j_I=k-M_I}^{k} f_I[j_I] +$$

$$+ f_2[k] \sum_{j_1=k-M_1}^{k-1} f_1[j_1] \sum_{j_3=k-M_2}^{k} f_3[j_3] \ldots \sum_{j_I=k-M_I}^{k} f_I[j_I] + \ldots$$

$$\ldots + f_I[k] \sum_{j_1=k-M_1}^{k-1} f_1[j_1] \sum_{j_2=k-M_2}^{k-1} f_2[j_2] \ldots \sum_{j_{I-1}=k-M_{I-1}}^{k-1} f_{I-1}[j_{I-1}],$$

$$\Phi_{сбр}(k) = P_{1сбр}(k) + \sum_{i=\min(M_1,M_2,\ldots M_I)+2}^{k-\min(M_1,M_2,\ldots M_I)-2} P_{1сбр}(i)\Phi_{сбр}(k-i),$$

$$P_{1сбр}(k) = \prod_{i=1}^{I}\left(1 - \sum_{j=1}^{k-M_i-1} f_i[j]\right) - \prod_{i=1}^{I} \sum_{j=k-M_i}^{k} f_i[j] - \prod_{i=1}^{I}\left(1 - \sum_{j=1}^{k-M_i} f_i[j]\right) + \prod_{i=1}^{I} \sum_{j=k-M_i+1}^{k} f_i[j],$$

где $f_1[j_1]$, $f_2[j_2]$, …, $f_i[j_i]$, …, $f_I[j_I]$ – плотности распределений вероятностей длительностей исполнения интегрируемых сервисов.

На основе $f[k]$ плотности распределения вероятностей длительности исполнения I объединяемых сервисов может находиться любая временная динамическая характеристика профиля качества.

Предлагаемое математическое обеспечение является расширением формализаций жизненного цикла сервис-ориентированных систем ситуационного управления. Указанная особенность характеризует научную значимость рассмотренных решений по интеграции сервис-ориентированных средств.

Практическую значимость отражают новые профили качества интегрируемых сервис-ориентированных средств с расширенным составом регулируемых параметров в виде вектора временных задержек в их объединении.

Список используемых источников

1. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учеб. пособие. СПб. : изд-во Политехн. ун-та, 2011. 106 с. ISBN 978-5-7422-2951-3.

2. Птицына Л. К., Соколова Н. В. Параллельные вычислительные процессы в системах мониторинга и управления : учеб. пособие; Федер. агентство по образованию, С.-Петерб. гос. политехн. ун-т.. СПб. : изд-во Политехн. ун-та, 2008. 134 с. ISBN 978-5-7422-2066-4.

3. Птицына Л. К., Веселов В. О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Наукоёмкие технологии в космических исследованиях Земли. H&ES RESEARCH. М. : ООО «Издательский Дом Медиа Паблишер», 2015. № 2. С. 42–47.

4. Птицына Л. К., Веселов В. О. Моделирование интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV-я Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб. : СПбГУТ, 2015. С. 465–470.

Статья представлена научным руководителем,
доктором технических наук, профессором Птицыной Л. К.

УДК 004.056

Семенов А. В. (студент группы ИКТм-52, ПГУТИ)
Киреева Н. В. (кандидат технических наук, доцент, ПГУТИ)

ВЫБОР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ АНАЛИЗА ИМЕЮЩИХСЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В докладе описывается защита персональных данных, обрабатываемых в ИСПДн (информационных системах персональных данных), а также соответствие системы защиты законодательным актам РФ. Кроме того, выявлена необходимость проводить классификацию ИСПДн по уровню защищенности, приведены требования к каждому классу ИСПДн, а также указаны типы ИСПДн, и угрозы безопасности информации для каждого типа.

ИСПДн, угрозы безопасности информации, НСД, АРМ.

Основной акцент при определении класса информационных систем персональных данных (ИСПДн) делается на категорию обрабатываемых данных: биометрическую, специальную, общедоступную и иную. В зависимости от того, обрабатываются ли данные о расовой и национальной принадлежностях, физиологические и биологические особенности конкретного человека, были ли они получены из открытых источников, определяется необходимый класс ИСПДн.

Также большую роль играет наличие подключения к различным сетям информационного обмена (например, глобальной сети Интернет), что приводит к необходимости выбора одной из типовых моделей угроз.

Отдельно стоит остановиться на требованиях к организации защиты информации, содержащейся в информационной системе. Объектами защиты в ней являются информация, содержащаяся в информационной системе; любые технические средства; общесистемное, прикладное, специальное программное обеспечение; информационные технологии, а также средства защиты информации (СЗИ). Применяемые СЗИ должны пройти оценку со-

ответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

Предъявление требований к СЗИ для ИСПДн производится в два этапа:

1) Проводится оценка класса защищенности (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)), в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

2) Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации (табл. 1).

Степень возможного ущерба может быть высокой, средней и низкой.

ТАБЛИЦА 1

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	**Региональный**	**Объектовый**
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

В качестве примера рассмотрим реально внедренную ИСПДн на одном из российских предприятий (табл. 2).

Состав системы программ 1С:

- 1С Бухгалтерия 7.7;
- 1С Торговля и склад 7.7;
- 1С Зарплата и кадры 7.7.

Возможна реализация следующих основных угроз безопасности:

- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте (АРМ);
- угрозы утечки видовой информации;
- угрозы из внешних сетей.

ТАБЛИЦА 2

№ п/п	Наименование базы данных с ПДн	Тип ПДн	Примечание	Класс защищенности ИСПДн
1	«1С Предприятие 7.7»	ФИО, паспортные данные, ИНН, номер медицинского и пенсионного страхования, заработная плата (биометрические)	Сетевая БД; работа по клиент-серверной технологии с файловым сервером БД	3 класс

Реализация утечки видовой информации возможна за счет просмотра графической, видеоинформации и цифро-буквенной информации с экранов дисплеев и других средств отображения средств вычислительной техники (СВТ).

Угрозы НСД в АРМ связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн. Также источниками угроз могут служить внешние носители информации, содержащие вредоносные программы.

Угрозы из внешних сетей включают в себя:

- угрозы выявления паролей,
- угрозы получения НСД путем подмены доверенного лица,

- угрозы удаленного запуска приложений,
- угрозы внедрения по сети вредоносных программ.

Установленные СЗИ на системах персональных данных (СПДн):

1) ПАК Аккорд-NT/2000 v.3.0.

2) Настройка операционной системы (ОС) и системы 1С таким образом, чтобы вход в ОС и систему1С осуществлялся по индивидуальным идентификаторам и паролям, содержащим не менее 6 символов. Причем, идентификаторы и пароли, используемые для входа в операционную систему и в 1С различные.

3) Антивирусная программа Kaspersky Enterprise Space Security, а также установка его на рабочие станции, настройка защиты и процессов обновления.

В результате было определено, что на рассматриваемом предприятии используется ИСПДн, относящаяся к 3 классу.

В заключении хочется отметить, что защита персональных данных является одним из наиболее быстро развивающихся направлений в сфере информационной безопасности. Появляются новые угрозы безопасности информации, что требует развития систем защиты информации. Таким образом, Таким образом, в соответствии с угрозами безопасности информации, постоянно пополняется рынок средств защиты информации. Требуется учитывать необходимость соответствия действующей системы защиты организации с требованиями законодательства в области персональных данных.

Список используемых источников

1. О персональных данных : федеральный закон : принят Гос. Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. // Российская газета. 2006. 29 июля.

2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2012. 7 ноября.

3. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2013. 22 мая.

УДК 681.7

Т. Д. Фатхулин (аспирант, МТУСИ)

ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ ПО УВЕЛИЧЕНИЮ ПРОПУСКНОЙ СПОСОБНОСТИ ОПТИЧЕСКИХ ВОЛОКОН

Целью данной статьи является рассмотрение технических решений, позволяющих значительно увеличить пропускную способность современных оптических волокон. Проведен анализ ограничений, обусловленных использованием стандартных оптических волокон. Показана необходимость в разработке новых типов оптических волокон, позволяющих уменьшить влияние нелинейных эффектов. Приведены данные эксперимента по передаче 255 Тбит/с и рассмотрены конструктивные особенности используемого оптического волокна. В заключении сделаны выводы о необходимости разработки как активных, так и пассивных компонентов для нового типа оптических волокон.

суммарная мощность, маломодовое волокно, диаметр модового поля, скорость передачи, полоса усиления, формат модуляции, пропускная способность.

Предполагается, что в ближайшее десятилетие емкость систем передачи увеличится в тысячу раз и достигнет Петабит/с [1]. Это позволит внедрить телевидение формата UltraHD, 3D и использовать приложения, требующие сверхскоростных систем связи. Все это потребует создать новую оптическую инфраструктуру для поколения Петабитовых скоростей.

Стоит отметить, что используемые одномодовые оптические волокна рекомендаций G.652, G.653, G.655 на существующих волоконно-оптических системах передачи с использованием современных форматов модуляции скоро достигнут предельных для них показателей. Это обусловлено ограниченностью широкополосности современных оптических усилителей (ОУ) (EDFA, Рамановских и их комбинаций), а также ограничениями, связанными с уровнем вводимой оптической мощности в волокно. Так, при уровне оптической мощности в 1–2 Вт, вводимого в волокно, наблюдается плавление сердцевины оптического волокна. Если же используется волокно для компенсации хроматической дисперсии, то уровень оптической мощности, при котором начинает плавиться сердцевина, достигается уже при 0,5 Вт. Все это не позволяет увеличивать уровень передаваемой оптической мощность в современных волоконно-оптических системах передачи со спектральным разделением каналов (WDM). Особенно эти ограничения влияют на подводные протяженные ВОСП, построенные на таких волокнах.

Современные ОУ способны поднять уровень мощности оптического излучения на 25–30 дБ на передаче. При этом стоит заметить, что уже при уровне оптического излучения больше 17 дБ в оптическом волокне начинают проявляться нелинейные эффекты (например, эффект Бриллюэна).

При превышении некоторого уровня (экспериментально компания Alcatel-Lucent определила этот порог равным примерно 20 дБм) наблюдается сильное уширение спектра оптического сигнала на выходе ОУ, что может привести к недопустимому перекрытию между каналами в DWDM-системах. Зависимость ширины спектра оптического излучения на выходе ОУ от мощности выходного сигнала ОУ показана на рисунке 1 [2]. Компания Alcatel-Lucent рекомендует устанавливать мощность на уровне 19 дБм.

То есть, 17 дБ рекомендуется считать максимальным уровнем излучения в современных оптических волокнах, что значительно сокращает длину регенерационного участка. Использование предусилителей в волоконно-оптических системах передачи на приеме позволяет получить до 14 дБ выигрыша в бюджете мощности.

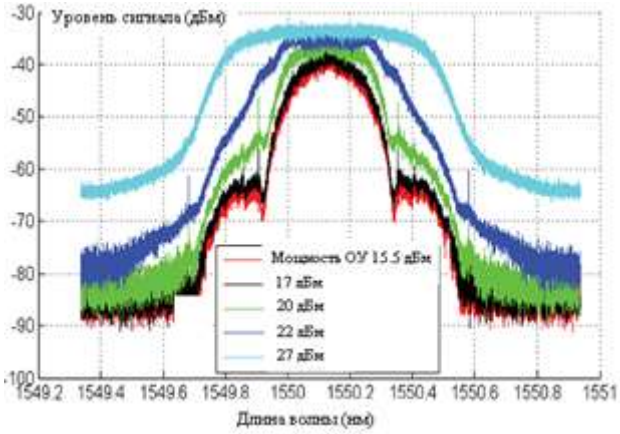


Рис. 1. Зависимость ширины спектра оптического излучения на выходе ОУ от мощности выходного сигнала ОУ

Рамановские усилители, которые усиливают оптический сигнал в волокне распределенным образом, часто имеют мощность лазера накачки порядка 1,2–1,5 Вт. При этом длина волны накачки выбирается 1 450 нм, излучение накачки вводится с приемной стороны, то есть рассматривается рамановский предусилитель. Однако имеются варианты использования рамановских усилителей и на передаче. Все это дает основания сделать выводы о том, что во многих случаях уже достигнут предельный уровень оптической мощности и необходимо находить инновационные пути для передачи сигналов.

Таким образом, можно определить факторы, которые ограничивают использование оптических волокон в современных ВОСП:

1) ограничения, обусловленные вводимой суммарной мощностью в оптическое волокно;

2) ограничения полосы усиления современных ОУ;

3) ограничения по потребляемой мощности.

Считается, что максимальная емкость современных оптических волокон может быть не более 100 Тбит/с. Это почти в 1,5 раза больше суще-

ствующей емкости оптического волокна. Скорость передачи по оптическим волокнам определяется в значительной степени полосой усиления современных оптических усилителей. Они могут работать в *S*-диапазоне 1460–1530 нм (70 нм – 9.4 ТГц), *C*-диапазоне 1 530–1 565 нм (35 нм – 4,4 ТГц) и *L*-диапазоне 1 565–1 626 нм (60 нм – 7,1 ТГц). Полная полоса усиления 1 460–1 625 нм (165 нм – 20,9 ТГц). Сегодня максимальная емкость межматериковой подводной системы передачи составляет около 10 Тбит/с (используется 8 пар оптических волокон с 1,28 Тбит/с на волокно).

Стоит отметить, что отечественные системы передачи лишь недавно смогли достичь суммарной емкости системы в 25 Тбит/с. При этом использовался формат модуляции DP-QPSK [3, 4], 25 суперканалов и одномодовое оптическое волокно. При разработке такой системы необходимо применение усилителей с полосой около 70 нм, использование сетки частот с шагом 33 ГГц и *EDFA* или гибридных усилителей, работающих в диапазонах *C* и *L*. Необходимо отметить, что требуется разработка активных и пассивных компонентов, работающих с нестандартной сеткой частот в 33 ГГц. В предлагаемых оптических модулях необходимо создание задающих, а также опорных лазеров, которые могут перестраивать длину волны излучения в диапазонах *C* и *L* с шагом 33 ГГц. Полоса усиления оптических усилителей, составляющая 70 нм, может быть достигнута путем использования двухканальных усилителей с полосовым мультиплексором и демультиплексором. Структурная схема реализуемой системы представлена на рисунке 2 [5].

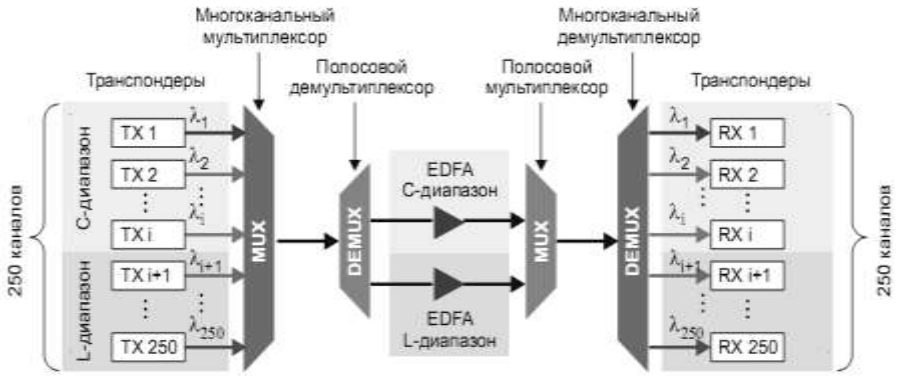


Рис. 2. Структурная схема реализуемой системы связи:
TX i – передающие части транспондеров,
RX i – принимающие части транспондеров

Обобщив вышесказанное можно заключить, что для преодоления ограничений по мощности оптического излучения необходимо создать и внедрить в производство оптические волокна с увеличенным диаметром сердцевины, либо с большим количеством сердцевин под оболочкой. Что-

бы увеличить диаметр модового поля следует создать оптическое волокно с сердцевиной из чистого кварца и дипрессировать оболочку фтором. Площадь модового поля такого оптического волокна будет порядка 112 мкм^2, то есть для длины волны 1 550 нм диаметр модового поля больше 10 мкм [2]. Если и дальше увеличивать диаметр модового поля, то получим маломодовое оптическое волокно. Для подводных систем передачи может использоваться маломодовый режим работы одномодового волокна с площадью модового поля 160 мкм^2 (длина волны 1 550 нм) [1].

В настоящее время предпринимаются попытки по применению технологий, сочетающих в себе решения с маломодовыми и многосердцевинными оптическими волокнами. Так, летом 2014 г. международная рабочая группа High-Speed Optical Communications Group, используя кабель японской компании Telekom NTT, установила новый рекорд скорости в 43 Тбит/с. Использовался один лазер, который создавал сигнал в многосердцевинном кабеле с семью сердцевинами. Через некоторое время международная исследовательская команда из Нидерландов и США достигла скорости передачи уже 255 Тбит/с. При этом применялись маломодовые сердцевины, в каждой из которых передавались 3 моды. Передавалось 50 оптических несущих с шагом сетки частот 50 ГГц. Для эффективного экранирования сердцевин друг от друга использовались небольшие отверстия, проделанные вокруг сердцевин (рис. 3). Однако такой кабель способен передавать сигнал только на расстояние до 1 км без искажений. Компании Alcatel-Lucent совместно с British Telecom удалось при проведении полевых испытаниях уменьшить интервал между каналами с 50 до 35 ГГц. Таким образом, рекордная скорость передачи данных уже в ближайшее время может увеличиться с 255 до 365 Тбит/с.

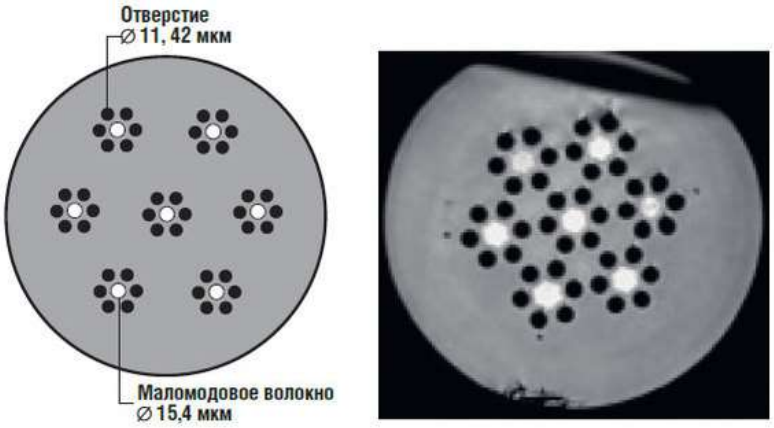


Рис. 3. Многосердцевинное волокно
с семью маломодовыми сердцевинами

Важно отметить, что создание и разработка новых типов оптических волокон требует создания элементной базы для таких ОВ. Волоконно-оптические кабельные линии состоят не только из передатчиков сигнала,

кабеля и приемников сигнала, но и из большого числа элементов, необходимых для функционирования ВОСП. Это и активные, и пассивные элементы. Активные элементы: лазерные диоды, модуляторы, различные виды фотоприемников, регенераторы, усилители (EDFA, рамановские и их комбинации) и фотодиоды разного применения. Согласно рекомендации G.671, к пассивным оптическим компонентам относятся: мультиплексоры и демультиплексоры, включая WDM устройства:

- изоляторы;
- аттенюаторы;
- переключатели, коммутаторы;
- разветвители, ответвители, разделители (сплиттеры);
- коннекторы и другие соединители;
- адаптеры;
- пассивные компенсаторы дисперсии;
- оконцеватели для подавления отражений;
- волоконно-оптические циркуляторы;
- соединительные муфты;
- ремонтные вставки.

Для каждой конкретной ВОСП требуется определенное количество тех или иных элементов. Высокую спектральную эффективность можно получить, применяя когерентные методы приема и передачи, а также модовое или пространственное мультиплексирование. Для широкого внедрения Петабитовых скоростей следует создавать новые технологии, позволяющие решить проблему ограничения полосы пропускания усилителей, вводимой в оптическое волокно мощности и потребляемой мощности, учитывая все элементы ВОЛС (волоконно-оптической линии связи).

Список используемых источников

1. Портнов Э. Л. Новые типы оптических волокон в телекоммуникациях и их применение // T-Comm: Телекоммуникации и транспорт. 2013. № 8. С. 96–98.

2. Портнов Э. Л., Фатхулин Т. Д. Технологии достижения высоких скоростей передачи в современных когерентных DWDM-системах связи // T-Comm: Телекоммуникации и транспорт. 2015. Том 9. № 8. С. 34–37.

3. Портнов Э. Л. Оптические кабели и пассивные компоненты волоконно-оптических линий связи. М. : Горячая линия-Телеком, 2007. 464 с.

4. Трещиков В. Н., Гуркин Н. В., Новиков А. Г., Наний О. Е. Российское DWDM-оборудование с канальной скоростью 100 Гбит/с // T-Comm: Телекоммуникации и транспорт. 2012. № 4. С. 65–67.

5. Трещиков В. Н. Разработка DWDM-системы емкостью 25 Тбит/с // Фотон-экспресс. 2013. № 2 (106). С. 24–28.

Статья представлена научным руководителем,
доктором технических наук, профессором Портновым Э. Л.

УДК 378.14

К. А. Фролов (студент группы ИСТ-442, СПбГУТ)

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО МОДУЛЯ АВТОМАТИЗИРОВАННОГО УЧЕТА ПОСЕЩЕНИЯ ЗАНЯТИЙ СТУДЕНТАМИ В ТЕЧЕНИЕ СЕМЕСТРА

Рассматриваемая в работе система позволяет создать информационный сервис, способствующий сокращению числа отстающих студентов за счет автоматизации внутрисеместрового учета посещения занятий.

информационные технологии, автоматизация, учебный процесс, контроль.

Рассматриваемый вариант автоматизации предполагает наличие в зданиях вуза системы контроля доступа, использующей индивидуальные пластиковые карты. На базе такой системы существует возможность создать подсистему учета посещений занятий по каждой дисциплине в соответствии с расписанием.

Решить эту задачу можно двумя способами: либо установить считыватели данных с пластиковых карт на входе в каждую аудиторию, либо использовать мобильные считыватели, подключенные к персональным ноутбукам преподавателей. Можно использовать и комбинированный вариант, когда часть аудиторий оборудована считывателями, а часть – нет.

Для реализации второго и третьего вариантов необходимо разработать программное обеспечение для локального рабочего места (ЛРМ) преподавателя.

Состав программно-аппаратного комплекс ЛРМ преподавателя должен включать в себя:

- ноутбук, имеющий USB порт и Wi-Fi адаптер;
- считыватель данных с пластиковых карт;
- специализированное программное обеспечение (ПО).

Предлагаемый вариант локального рабочего места преподавателя должен решать следующие задачи:

- ввод данных о посещении занятий;
- хранение данных в локальной базе данных;
- синхронизацию обмена информацией между локальной и центральной базами данных.

Для реализации поставленной задачи дополнительно к типовому программному обеспечению ЛРМ преподавателя разработан и установлен специализированный программный модуль, к которому, в частности, относятся:

- локальная база данных (ЛБД);

- подсистема считывания данных с пластиковых карт;
- интерфейс ввода, обработки и вывода данных.

Учет присутствия на занятиях автоматизируется путем считывания данных с индивидуальных пластиковых карт студентов прямо в аудиториях.

Как показано на рисунке 1, после аутентификации пользователя и выбора режима работы система должна определить наличие связи с ЦБД. Если связь с ЦБД установлена, то происходит обмен данными между локальной и центральной базами данных. Таким образом, система практически всегда содержит актуальные данные.

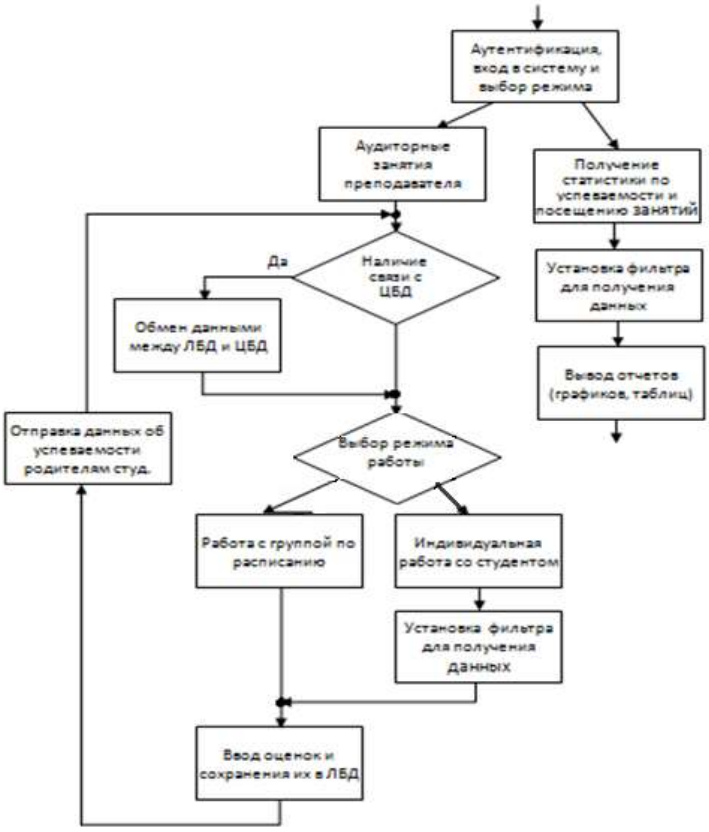


Рис. 1. Фрагмент алгоритма работы системы ЛРМ преподавателя

При работе преподавателя в аудитории в рамках занятий по расписанию на экране ноутбука открывается таблица со списком студентов соответствующей группы.

После считывания номера с индивидуальной пластиковой карты студента в таблице автоматически отмечается присутствие студента на занятии, и эти данные сохраняются в ЛБД. Полученные таким образом данные (при наличии соединения с корпоративной сетью вуза или сетью Интернет) выгружаются в центральную базу данных вуза (алгоритм работы системы приведен на рисунке 1).

Список используемых инструментов:

- язык программирования Python 3.4;
- IDE JetBrains PyCharm;
- ПО для считывания данных с пластиковых карт IronLogic PlaceCard [2];
- Microsoft Excel;
- модули pywin32 и PyQt4 для организации работы Python с Microsoft Excel [2].

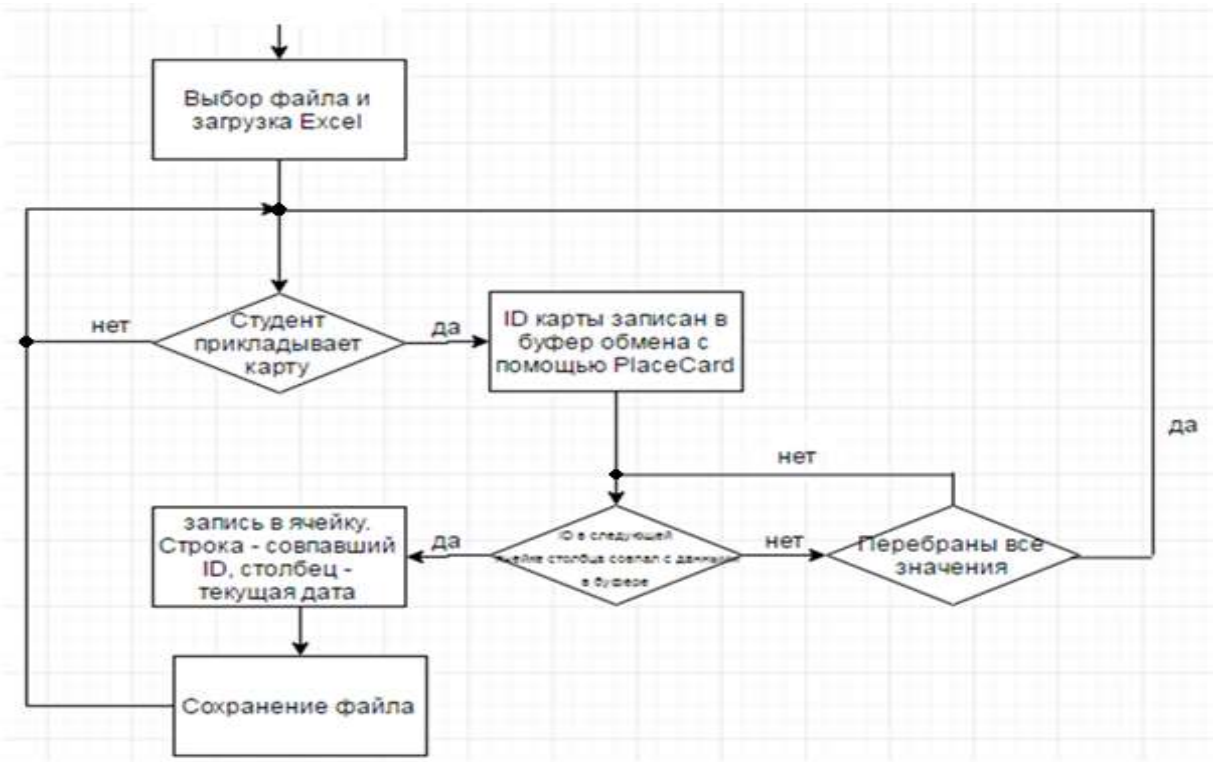


Рис. 2. Фрагмент алгоритма работы ЛРМ во время аудиторных занятий

В режиме работы аудиторных занятий с группой по расписанию преподавателю предлагается выбрать группу и дисциплину занятия. После этого программа ожидает, пока студент приложит пластиковую карту к считывателю. Если номер приложенной карты совпал с одним из номеров карт в ЛБД, то в таблице автоматически появляется отметка о том, что студент присутствует на этом занятии, а также запись об этом автоматически заносится в ЛБД. Алгоритм работы в режиме аудиторных занятий с группой по расписанию приведен на рисунке 2. Пример результата работы ПО приведен на рисунке 3.

Группа РТ-51 Дисциплина АиП

	Номер занятия	1	2	3	4	5	6	7	8	9	10	11	12	
	Номер учебной недели	2	4	5	6	7	8	9	10	11	12	13	15	
	День	15.02	29.02	09.03	14.03	23.03	25.03	06.04	11.04	20.04	25.04	04.05	06.05	
№ п/п	ФИО Время	14:45	14:45	14:45	14:45	14:45	14:45	14:45	14:45	14:45	14:45	14:45	14:45	Посещ.
1	Абдусаитов Александр Хусенович													0
2	Барышева Милана Вячеславовна	1	1	1	1	1	1	1	1	1	1			100
3	Бойко Дмитрий Игоревич	1					1							20
4	Ганина Наталья Алексеевна	1	1	1	1	1	1	1	1	1	1			100
5	Григорьева Ксения Владимировна	1	1	1	1	1	1	1	1	1	1			100
6	Ешникова Алина Сергеевна	1	у	1	1	1	1	1		1	1			80
7	Заостровский Александр Александрович	1	1	1	1	1	1	1	1	1	1			100
8	Коваль Алексей Александрович	1	1	1	1	1		1		1	1			80
9	Коломеец Данил Алексеевич	1	1	1	1	1	1	1	1	1	1			100
10	Кононов Даниил Николаевич									1				10
11	Кунышев Алексей Сергеевич													0
12	Лунёв Вадим Константинович	1	1	1	1	1	1	1	1	1	1			100
13	Макаричев Артём Павлович	1			1									20
14	Мухин Александр Геннадьевич	1	1	1	1	1	1	1	1	1	1			100
15	Николаев Дмитрий Юрьевич	1	1	1	1	1	1	1	1	1	1			100
16	Сатаев Тимур Ильдарович	1	1	1		1			1		1			60
17	Скиданов Ефим Викторович													0
18	Томачек Григорий Алексеевич													0
19	Устинов Кирилл Владимирович	1	1	1	1	1		1		1	1			80
20	Халабурдин Максим Николаевич	1	1	1	1		1		1					60
21	Шулипа Дарья Александровна	1	1	1	1	1	1	1	1	1	1			100
	Процент посещений занятий	76	62	67	67	62	57	57	52	62	62	0	0	

Рис. 3. Вид таблицы 25 апреля во время аудиторных занятий

Внедрение системы локального рабочего места преподавателя в общую информационную систему вуза предполагает реализацию следующих этапов:

- инсталляция системы на ноутбуке преподавателя;
- первичная загрузка данных из ЦБД в ЛБД;
- текущая работа по учету посещений занятий.

В настоящее время реализовано ЛРМ преподавателя, выполняющее функцию автоматического сбора информации о присутствии студентов на занятии.

Список используемых источников

1. Руководство пользователя ПО PlaceCard / Ironlogic.ru: [сайт]. URL: http://www.ironlogic.ru/ il.nsf/file/ru_placecard.pdf/$FILE/placecard.pdf

2. Интеграция MS Excel и Python / Habrahabr.ru: [сайт]. URL: https://habrahabr.ru/post/232291

Статья представлена научным руководителем,
старшим преподавателем Евстигнеевым В. А.

УДК 004.5

Е. С. Хайбрахманова (студент группы Ист-23, СПбГУТ)

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ «ТЕЛЕФОННЫЙ СПРАВОЧНИК СПбГУТ»

На сегодняшний день телефонный справочник, обеспечивающий доступ к информации в режиме онлайн, становится востребованным и необходимым информационным ресурсом сети Интернет. Многие организации, в том числе некоторые университеты имеют телефонные справочники, что значительно повышает эффективность поиска контактной информации и существенно сокращает затраченное на поиск время.

web-приложение, телефонный справочник, онлайн.

Телефонный справочник онлайн – это, прежде всего, автоматизированная система поиска информации, которая должна предоставлять функциональные возможности, обеспечивающие удобный поиск информации различными способами.

Предметом исследования является телефонный справочник, опубликованный на официальном сайте Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Доступ к телефонному справочнику организован в виде ссылки с главной страницы сайта университета.

Назначение телефонного справочника – обеспечение быстрого доступа к необходимой информации. Кроме того, он должен быть удобен как для сотрудников университета, так и для сторонних лиц.

Область применения – информационный ресурс сети Интернет, реализованный как web-приложение, ссылка на который должна располагаться на официальном сайте университета, в связи с этим необходимо поддержание корпоративного стиля.

Сравнительный анализ телефонного справочника СПбГУТ и других университетов направлен на поиск сходных и различных элементов структуры и дизайна. Проведенный анализ позволил сделать следующие выводы:

1) Все справочники, кроме СПбГУТ, обеспечивают доступ, к информации используя организационную структуру университета.

2) Все справочники, кроме СПбГУТ, являются неотъемлемой частью официального сайта университета, т.е. при работе со справочником сохраняется доступ ко всем главным навигационным элементам ресурса, он как бы «вмонтирован» в единую структурную оболочку системы.

3) Все ссылки на справочники с главной страницы сайта университета, кроме СПбГУТ, очень трудно обнаружить, ссылка располагается либо в нижней части страницы, либо расположена на третьем уровне иерархии.

4) Форма вывода справочной информации на всех ресурсах различная: текст, таблица, карточка. В большинстве случаев данные выводятся в табличной форме, но если осуществляется поиск конкретного сотрудника, то вывод информации в форме карточки является предпочтительным, т. к. она может предоставить больше персональных данных, включая фотографию.

Трудно найти идеальный справочник, потому что в каждом есть свои достоинства и недостатки. Для разработки нового телефонного справочника, определены следующие функциональные особенности:

- поисковая система должна включать как строчный поиск, так и поиск по структуре университета;
- данные должны выводиться в виде таблицы и карточек;
- в оформление справочника должны участвовать, как текстовый выделитель, так и визуальный, например, пиктограммы.
- исходные данные содержат не только людей, но и подразделения;
- на странице телефонного справочника не должно быть лишней информации, которая бы перегружала страницу.

Для исследования потребностей пользователя было проведено анкетирование сотрудников.

ТАБЛИЦА 1. Результаты анкетирования

Вопросы	**Порядковый номер респондента**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Актуально ли переделывать справочник	да	да	да	да	да	да	нет	з/о	да
Нужно ли сохронять искомые номера	да	да	нет	да	з/о	з/о	нет	да	з/о
Должен ли сотрудник вносить изменения в справочник	нет	з/о	з/о	нет	з/о	з/о	нет	нет	да
Должны ли быть личные данные	нет	нет	з/о	нет	нет	да	з/о	нет	нет
Важно ли оставить корпоративный стиль	нет	да	нет	да	нет	да	да	з/о	з/о
Нужна ли фотография сотрудника, при выводе данных	з/о	да	з/о	да	з/о	нет	з/о	да	з/о
Устраивает ли телефонный справочник в данном виде	нет	нет	да	нет	з/о	да	нет	нет	нет
Вы пользуетесь телефонным справочником	да	да	нет	да	нет	нет	да	да	да

* з/о – затрудняюсь ответить

Проведенное анкетирование позволило сделать следующие выводы:

- телефонный справочник должен включать в себя такие функции как: поиск телефона, так и поиск по основным данным о сотруднике;
- появление «формы изменения данных», поможет упростить процесс редактирования информации о человеке или подразделение, который сейчас занимает около недели;
- многие сотрудники недовольны телефонным справочником визуально, а именно устаревшим списком, который существует сейчас;
- функционал справочника расширится при добавлении «поля» или «формы», которая будет сохранять часто искомых людей;
- нужна фотография при выводе исходной информации, благодаря этому будет проще найти человека, потому что в университете много однофамильцев, и не всегда известны полные инициалы человека, но можно узнать его внешне.

Визуальное проектирование пользовательского интерфейса

Прототипирование интерфейса

Для создания прототипа пользовательского интерфейса была взята модульная сетка (рис. 1).

Рис. 1. Модульная сетка

Параметры модульной сетки следующие:

Колонка высоту – 1 305 px;

Колонка в ширину – 62 px;

Кол-во колонок – 16;

Расстояние между колонками – 7 px.

За основу была взята модульная сетка, благодаря которой создан внешний вид интерфейсов дня всех страниц приложения. Для примера представлен прототип главной страницы телефонного справочника (рис. 2).

Рис. 2. Прототип главной страницы приложения

При проектировании интерфейсов нужно придерживаться корпоративного стиля университета: логотипа университета и корпоративных цветов (рис. 3 и 4).

Рис. 3. Логотип университета

Рис. 4. Фирменные корпоративные цвета

При работе с цветом нужно учесть, что оранжевый должен быть представлен как доминирующий; черный, белый и серый должны использоваться как фоны или акценты, в поддержку основного [1].

Для удобства, визуально были выделены информационные блоки. На первом блоке размешен логотип и название университета. Второй блок выделен черным цветом, поверх которого название «телефонный справочник» и основные номера. Третий блок – это поисковая система, которая выделена темно-серым цветом, который включает в себя интуитивный поиск и поиск по структуре.

Рис. 5. Главная страница

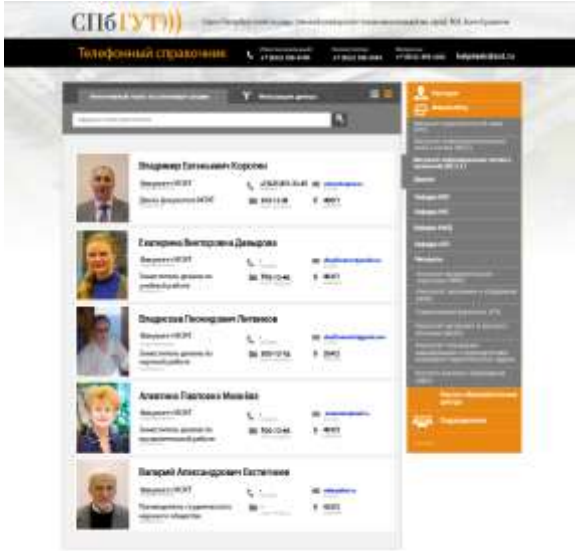


Рис. 6. Поиск по структуре

Внедрение телефонного справочника позволит повысить эффективность работы не только отдельных подразделений ВУЗа между собой, но и повысит удобство коммуникации сторонних лиц с сотрудниками университета.

Список используемых источников

1. СПбГУТ телефонный справочник [Электронный ресурс]. URL: http://tel.sut.ru (дата обращения 15.05.16)

2. СПбГУТ телефонный справочник [Электронный ресурс]. URL: http://tel.sut.ru (дата обращения 15.05.16)

3. Официальный сайт СПбГУТ. URL: http://www.sut.ru/sveden/struct (дата обращения 10.05.16)

Статья представлена научным руководителем,
старшим преподавателем Кисленко Л. С.

УДК 004.932

Л. П. Шукюрова (студентка группы БПЗ1201, МТУСИ)

ВНЕДРЕНИЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В ЧАСТОТНУЮ ОБЛАСТЬ ИЗОБРАЖЕНИЯ МЕТОДОМ БЕНГАМА-МЕМОНА-ЭО-ЮНГ

Одним из средств зашиты мультимедийной информации является встраивание в защищаемый контент невидимых человеческому глазу отметок – цифровых водяных знаков (ЦВЗ). Встраивание ЦВЗ в информацию, представленную в цифровом формате,

происходит при помощи стеганографических методов. В данном докладе используется метод Бенгама-Мемона-Эо-Юнг (БМЭЮ), выполняющий скрытие данных в частотной области растрового графического стегоконтейнера. Метод БМЭЮ позиционируется как стойкий к атакующим искажениям в виде JPEG-компрессии.

ЦВЗ, стеганография, защита авторских прав.

Защита авторских прав мультимедийных файлов от несанкционированного доступа является важнейшей и нерешенной на сегодняшний день проблемой. Одним из средств зашиты мультимедийной информации является встраивание в защищаемый контент невидимых человеческому глазу отметок – цифровых водяных знаков (ЦВЗ) [1]. Встраивание ЦВЗ в информацию, представленную в цифровом формате, осуществляется при помощи стеганографических методов [2].

Рис. 1. Блок-схема алгоритма встраивания

Одним из часто используемых на практике стеганографическим алгоритмом является метод Бенгама-Мемона-Эо-Юнг (БМЭЮ), выполняющий скрытие данных в частотной области растрового графического стегоконтейнера, благодаря чему позиционируется как стойкий к атакующий искажениям в виде JPEG-компрессии.

Рассмотрим блок-схему алгоритма встраивания ЦВЗ (рис. 1).

Сперва мы получаем RGB-составляющие изображения, так как для встраивания будем использовать только синюю (B) составляющую изображения. Обусловлено это тем, что изменения именно в этой цветовой составляющей зрительная система человека воспринимает хуже всего, что

способствует сокрытию факта встраивания. Далее делим составляющую на сегменты и применяем к каждому сегменту ДКП. Полученные блоки подвергаются классификации на пригодные и непригодные для встраивания в них стегоинформации. Пригодными считаются блоки, которые одновременно удовлетворяют нижеперечисленным двум условиям:

- блоки не должны иметь резких переходов яркости,
- блоки не должны быть слишком монотонными.

Блоки, не удовлетворяющие первому условию, обладают слишком большими значениями низкочастотных коэффициентов ДКП. Для блоков, не отвечающих второму условию, характерно равенство нулю большинства высокочастотных коэффициентов. Перечисленные требования являются критерием отбраковки непригодных блоков. Вышеуказанные условия классификации учитываются с использованием двух пороговых коэффициентов: P_L (для первого условия) и P_H (для второго условия) превышение (P_L) или недобор (P_H) будет указывать на непригодность рассматриваемого блока. Встраивание в блок бита информации происходит следующим способом (формулы (1)): выбираются три коэффициента ДКП из среднечастотной области с координатами (υ1, ν1), (υ2, ν2) и (υ3, ν3). Для встраивания «0» коэффициенты меняются таким образом, чтобы третий коэффициент был меньше первого или второго коэффициентов, а для встраивания «1» третий коэффициент должен быть больше первых двух. Также для принятия решения о достаточности различения вышеупомянутых коэффициентов ДКП используется порог различения P:

$$\begin{cases} \left|\Omega\left(u_3, v_3\right)\right| < \min\left(\left|\Omega\left(u_1, v_1\right)\right|, \left|\Omega\left(u_2, v_2\right)\right|\right) - P, \text{ при } m = 0; \\ \left|\Omega\left(u_3, v_3\right)\right| > \max\left(\left|\Omega\left(u_1, v_1\right)\right|, \left|\Omega\left(u_2, v_2\right)\right|\right) + P, \text{ при } m = 1. \end{cases} \quad (1)$$

В данном докладе использовались пороги со следующими значениями: $P = 50$, $P_L = 2\,600$, $P_H = 40$.

Для встраивания информации использовалось изображение-контейнер размерностью 400×400 пикселей и ЦВЗ размерностью 32×32 пикселей.

На рисунке 2*а* проиллюстрировано изображение до встраивания, на рисунке 2*б* представлено стегоизображение, не трудно заметить, что видимые искажения отсутствуют, а значит встраивание ЦВЗ было проведено корректно. Следует отметить, что конечный результат всегда будет зависеть от значения порога и меняя его, мы сможем получать разные результаты.

а) *б)*

Рис. 2. Исходное изображение и стегоизображение

Рассмотрим процесс извлечения ЦВЗ, представленный на рисунке 3.

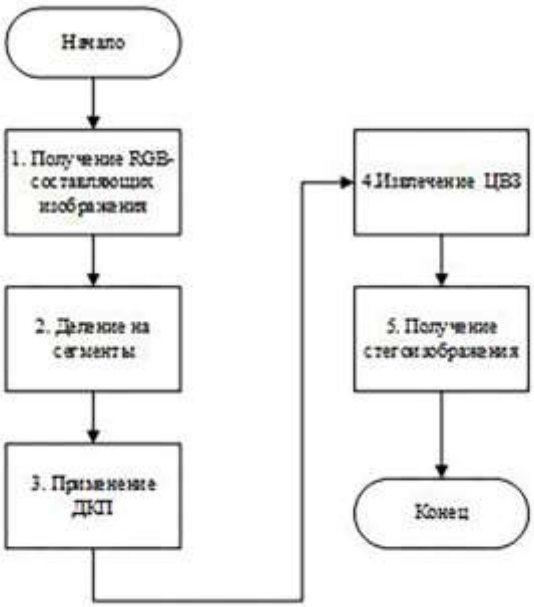
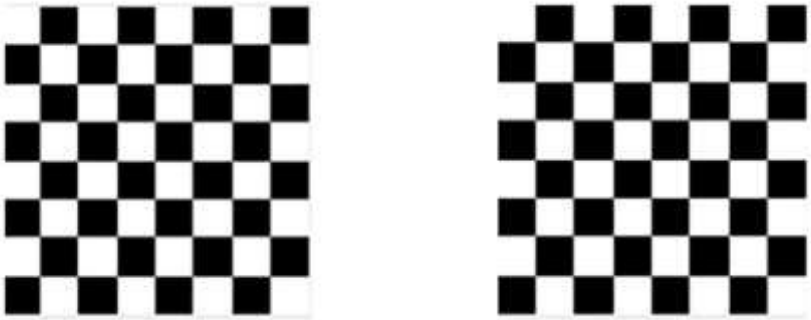


Рис. 3. Блок-схема алгоритма извлечения

Для извлечения информации из изображения на приемной стороне должны быть известны пороги P, P_L и P_H, а также три коэффициента ДКП. Таким образом, на приемной стороне можно определить блоки, в которые проводилось встраивание, повторив аналогичный на передающей стороне анализ.

ЦВЗ до встраивания проиллюстрирован на рисунке 4*а*. Результат после извлечения ЦВЗ представлен на рисунке 4*б*.



а) *б)*

Рис. 4. Исходный ЦВЗ – *а)*, извлеченный ЦВЗ – *б)*

Визуальные изменения отсутствуют, а значит ЦВЗ извлечен корректно и полностью. Таким образом, данный метод можно использовать в целях защиты авторских прав медиа-файлов.

Список используемых источников

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К. : "МК-Пресс", 2006. 288 с.
2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М. : СОЛОН-ПРЕСС, 2009. 272 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Лариным А.И.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ

УДК 621.375

Д. Ю. Абраменкова (студентка группы ИКТК-35, СПбГУТ)
Е. А. Шербашов (студент группы ИКТК-35, СПбГУТ)

ГОДОГРАФЫ ГЛУБИНЫ ОБРАТНОЙ СВЯЗИ ONLINE

В усилительных устройствах широко используется отрицательная обратная связь (ООС). За счёт фазовых сдвигов на краях диапазонов она может превратиться в положительную обратную связь (ПОС), что может привести к существенным изменениям АЧХ, а при больших фазовых сдвигах и к самовозбуждению. В статье показана методика построения годографа глубины ОС. Он позволяет узнать имеются ли участки частотной характеристики на которой ОС является положительной. Наличие ПОС выражается на годографе, потому заходит ли он в единичную окружность в начале координат, т.е. становится ли модуль F меньше 1. Рассмотрены примеры решения таких задач. Для наглядности годографы глубины ОС построены с помощью передвижения векторов в виде анимации.

возвратная годограф, петлевое усиление, полюсы, обратная связь, частота, инструментальный усилитель.

В схемах с обратной связью годограф используется для определения устойчивости. Кроме определения устойчивости, возникает вопрос определения вида ОС.

Количественной мерой оценки влияния ОС на параметры усилительного тракта является возвратная разность. Она представляет собой разность между сигналом, поданным на вход в разрыв петли ОС, и сигналом, возвратившимся к тем же точкам петли после её прохождения. В общем случае сигнал ОС может либо суммироваться с входным сигналом усилителя, либо вычитаться из него. В зависимости от этого различают положительную и отрицательную ОС. Если фазы сигнала ОС и входного сигнала противоположны, то возвратная разность всегда число положительное. Это приводит к уменьшению коэффициента усиления. Такая ОС называется отрицательной.

В инженерной практике знак ОС определяют в области средних частот, где и организуется необходимая для усилителей внешняя ОС. Сигналы в петле ОС могут быть точно противофазными лишь на одной частоте. На высоких и низких частотах могут появляться дополнительные фазовые

сдвиги, которые превращают отрицательную обратную связь в положительную. Поэтому вид ОС по её знаку правильно определять, используя модуль возвратной разности, т. е. глубину ОС. Глубина отрицательной ОС всегда характеризуется числом, большим единицы.

Определение вида ОС можно выполнить по годографу глубины обратной связи, либо по её АЧХ. Рассмотрим первый вариант.

Годограф вектор-функции $x(t)$ – это кривая, описываемая концом переменного вектора $x(t)$, начало которого при всех значениях t – постоянная точка O (t – действительная переменная величина, например, время), он *позволяет определить вид обратной связи и устойчивость*.

Наиболее удобным и наглядным критерием устойчивости является критерий Найквиста. В этом случае строят годограф петлевого усиления

$$T = \beta \cdot K.$$

Вид обратной связи можно определять по годографу возвратной разности. Для этого необходимо построить годограф функции возвратной разности. Рассмотрим простейшие звенья с ОС.

На рис.1 показан усилитель, выполненный на базе ИНУН. Его передаточная функция имеет один полюс в области верхних частот. Ниже приведены аналитические выражения для каждой части усилителя и для глубины ОС F.

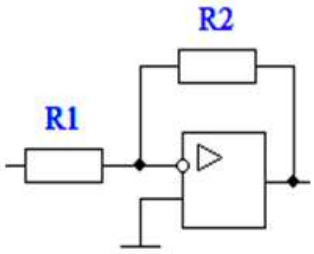


Рис. 1. Усилитель с однополюсной функцией передачи в области ВЧ

Аналитические выражения:

$$A(p) = \frac{-\mu}{1 + p\tau},$$

$$B = \frac{R_1}{R_1 + R_2},$$

$$1 - A(p)B = \frac{1 + \mu B + p\tau}{1 + p\tau} = \frac{F + p\tau}{1 + p\tau}. \qquad (1)$$

Предварительно покажем построение годографа петлевого усиления на рисунке 2.

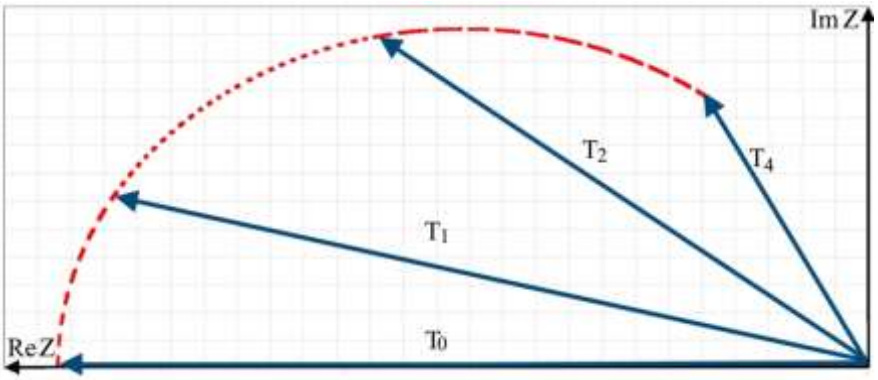


Рис. 2. Годограф однополюсной функцией передачи

Годограф был выполнен в движении векоторов, но так как на бумаге этого не показать, то на рисунке показаны несколько веторов T_0, T_1, T_2, T_4 которые как и в анимации рисуют постепенно линию гадогрофа.

Аналогично были построены рисунки годографа для двух- и более полюсной функции передачи. Они строились по соответсвтующим схемам и аналитическими выражениями в программе Fastmean. После этого построение рисунков было снято на видео и замедленно для того, чтобы создать наглядную анимацию.

Построение годографа возвратной разности показано на рисунках 3 и 4.

На рисунке 3 годограф больше единицы на всех частотах, о чём подтверждает окружность радиусом равным единице.

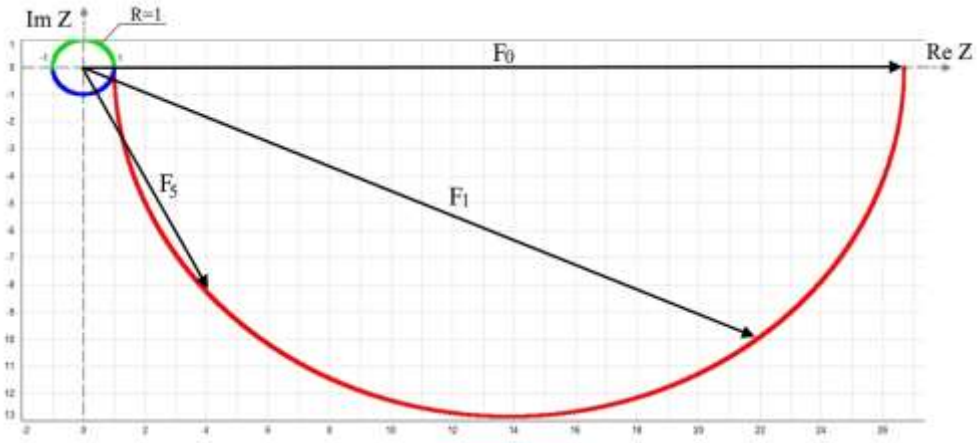


Рис. 3. Годограф однополюсной функцией передачи *F*

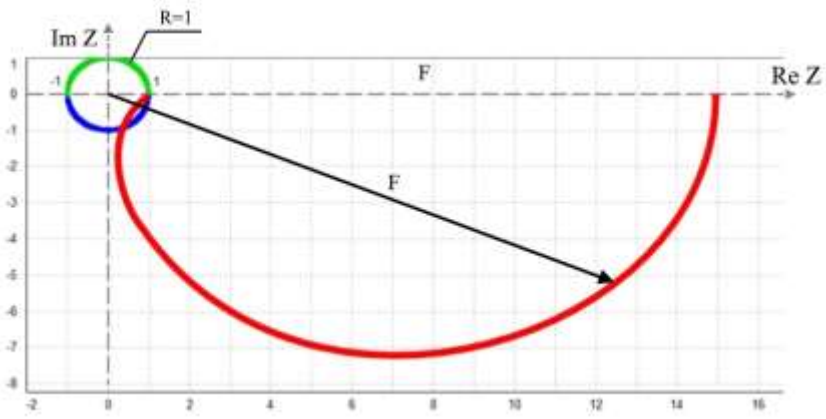


Рис. 4. Годограф двухполюсной функцией передачи *F*

Для проверки на устойчивость строим годограф петлевого усиления *T*, а для определения знака глубины обратной связи строим её годограф *F*. Оба этих годографа изображены на рисунке 5.

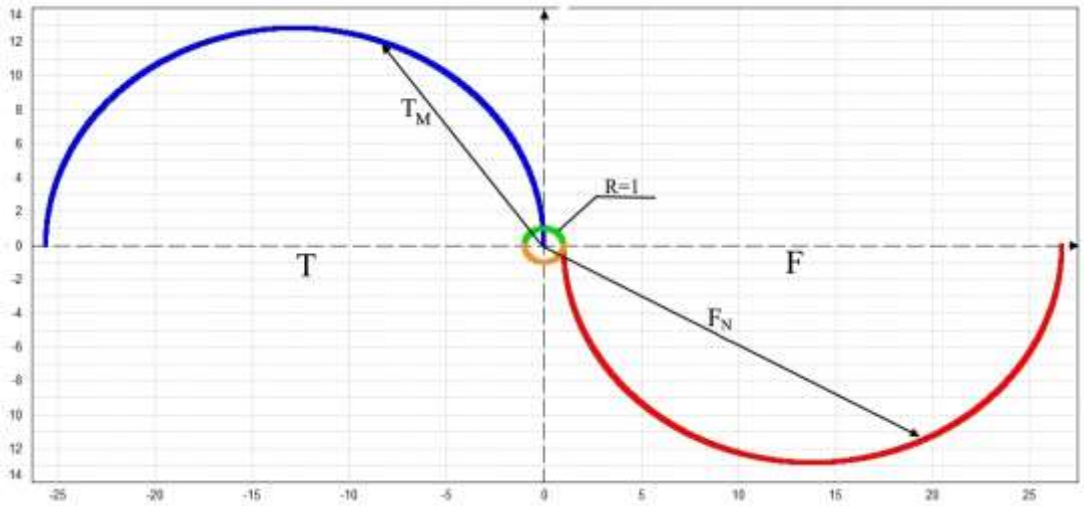


Рис. 5. Годографы *T* и *F*

В любом годографе оказывается сложным определение частоты сигнала *f*, и поэтому исследование проще проводить по логарифмическим АЧХ и ФЧХ.

В отличие от прямой передачи возвратное отношение имеет не только полюс f_p, но и нуль f_z (1). За частотой нуля действие ОС прекращается. (рис. 6)

Если усилитель имеет два полюса в функции передачи на ВЧ, то в этом случае возвратная разность приобретает нули, которые располагаются между исходными полюсами (рис.7).

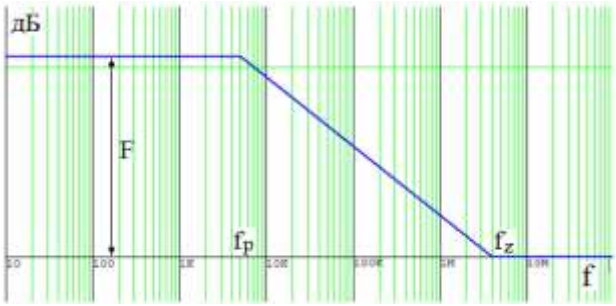


Рис. 6. Асимптотическая АЧХ глубины ОС при однополюсной функции передачи

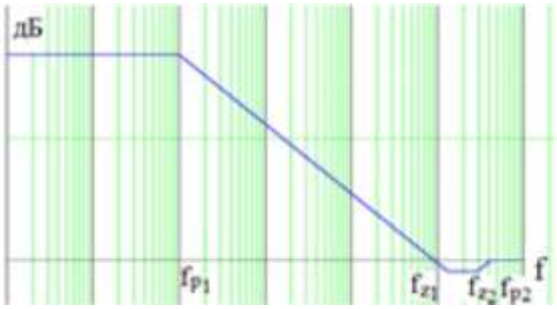


Рис. 7. Асимптотическая АЧХ глубины ОС при двухполюсной функции передачи

Корни числителя в многополюсной функции передач могут быть вещественные и комплексно-сопряжённые. Их влияние на АЧХ глубины ОС иллюстрирует рисунок 8. Некоторые АЧХ пересекают уровень 0 дБ, что свидетельствует о наличии положительной обратной связи.

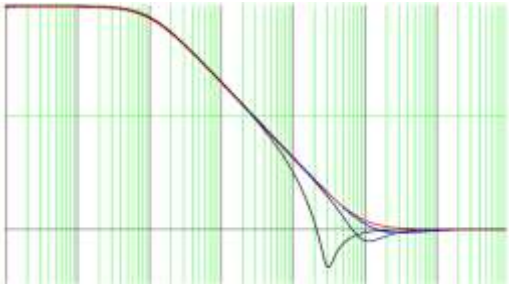


Рис. 8. АЧХ глубины ОС при изменении корней двухполюсной функции передачи

В области НЧ частотные характеристики возвратного отношения показывают их зеркальное отражение области ВЧ.

Список используемых источников

1. Перепёлкин Д. А. Схемотехника усилительных устройств: уч. пос. для вузов. 2-е изд., испр. и перераб. М. : Горячая линия – Телеком, 2014. 238 с. ISBN 978-5-9912-0456-9.

2. Алексеев А. Г., Климова П. В. Определение глубины ОС на ПК // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II-я Международная научно-техническая и научно-методическая конференция: сб. науч. статей. СПб. : СПбГУТ, 2013. С. 41–43.

3. Прянишников В. А. Электроника. Курс лекций. 2-е изд. исп. и доп. СПб. : КОРОНА принт., 2000. 415 с.

4. Ибрагим К. Ф. Основы электронной техники: элементы, схемы, системы / пер. с англ. М. : Мир, 2001. 398 с.

Статья представлена научным руководителем,
кандидатом технических наук, профессором Алексеевым А. Г.

УДК 621.396.67.01

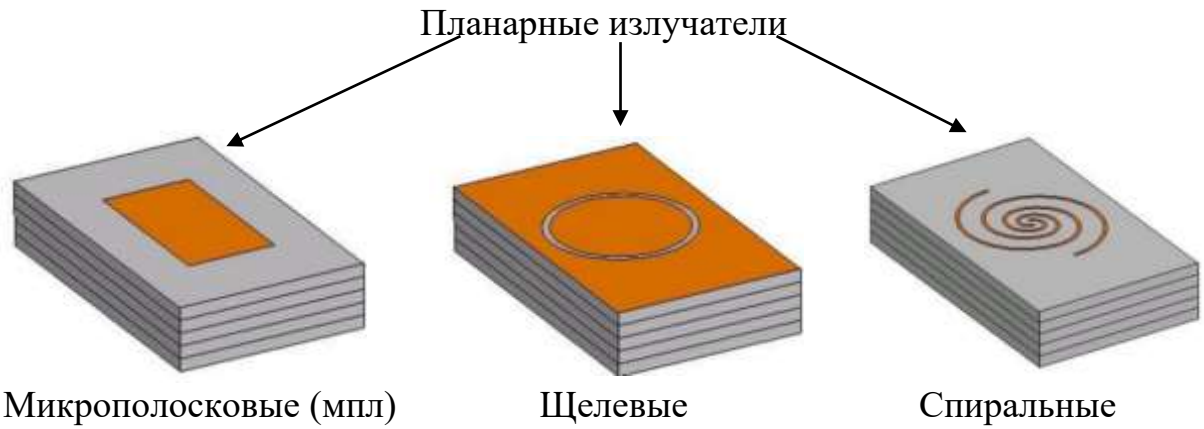
Р. Р. Ахметов (студент, СПбГУТ)

СПИРАЛЬНЫЕ ПЛАНАРНЫЕ ИЗЛУЧАТЕЛИ

На данный момент перед разработчиками объёмных интегральных схем СВЧ остро стоит вопрос интеграции антенны непосредственно в схему. Самый подходящий вариант излучателей в данном случае – планарные излучатели.

объёмные интегральные схемы, планарные излучатели, спиральные антенны, круговая поляризация, коэффициент усиления.

Планарные излучатели, используемые в объемных интегральных схемах (ОИС) СВЧ в качестве антенны, делятся на три типа.



В таблице 1 показано сравнение характеристик различных типов антенн. В данной таблице красным цветом отмечены недостатки, желтым – более-менее приемлемые характеристики, зелёным – достоинства данных планарных излучателей.

ТАБЛИЦА 1. Сравнение характеристик мпл, щелевых и спиральных планарных антенн

	мпл	**Щелевые**	**Спиральные**
По рабочему диапазону частот	Узкополосный	Узкополосный	Широкополосный
Коэффициент усиления	Низкий коэффициент усиления	высокий коэффициент усиления	Высокий коэффициент усиления
Возможность получения циркулярно (эллиптически) поляризованного сигнала	Сложность получения эллиптической поляризации	эллиптически поляризованное поле основной волны H	Позволяют осуществлять прием и передачу при круговой поляризации

	мпл	Щелевые	Спиральные
Реализация связи между модулями схемы	Не реализуема	Реализуема связь между модулями ОИС при помощи данной антенны	Реализуема связь между модулями ОИС при помощи данной антенны
Питание антенны	Наиболее эффективное питание антенны при помощи МПЛ	Наиболее эффективное питание антенны при помощи щелевых линий	При питании могут использоваться оба типа линий

Ввиду того, что спиральные антенны имеют целый ряд преимуществ, они приобретают всё больший интерес среди производителей.

Рабочий диапазон частот

В случае с МПЛ и щелевыми излучателями один из способов расширение диапазона – использование т. н. фрактальных антенн (уменьшенных копий исходных планарных излучателей).

Фракта́л – объект, в точности или приближённо совпадающий с частью себя самого. Имеет ту же форму, что и одна или более частей. Пример фракталов приводится на рисунке 1.

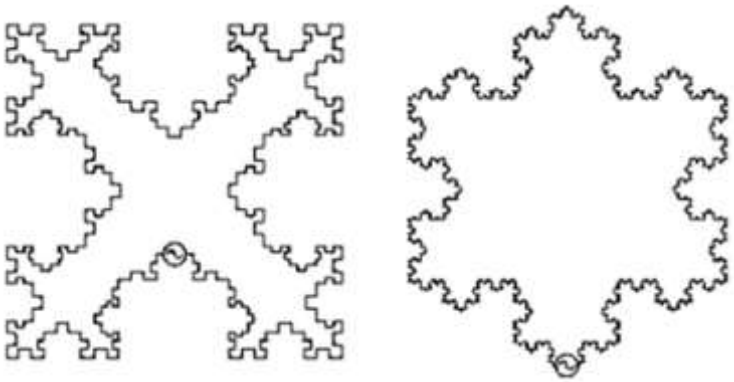


Рис.1. Пример фракталов

Почему спиральные планарные излучатели широкополосные? Ответ, предположительно, кроется в геометрической форме спирали. Спираль имеет форму кривой, постепенно приближающейся к центральной точке (оси), достигается тот же «фрактальный эффект». Спиральные планарные антенны способны эффективно работать во всём диапазоне СВЧ.

Круговая поляризация

Для антенны важна возможность приема и передачи циркулярно или эллиптически поляризованного сигнала при космической связи и связи в целом, так как объект приема – излучения регулярно меняет своё положение, постоянно находится в движении.

Круговая поляризация сигнала в спиральных планарных излучателях объясняется геометрической формой спирали. Стоит отметить, что в зависимости от направления намотки спирали излученное антенной поле право- или лево- поляризовано.

Разнонаправленное излучение спиральных антенн

Связь между модулями ОИС может быть реализована ввиду того, что спиральные планарные антенны позволяют получать и осевое излучение, и излучение в плоскости антенны.

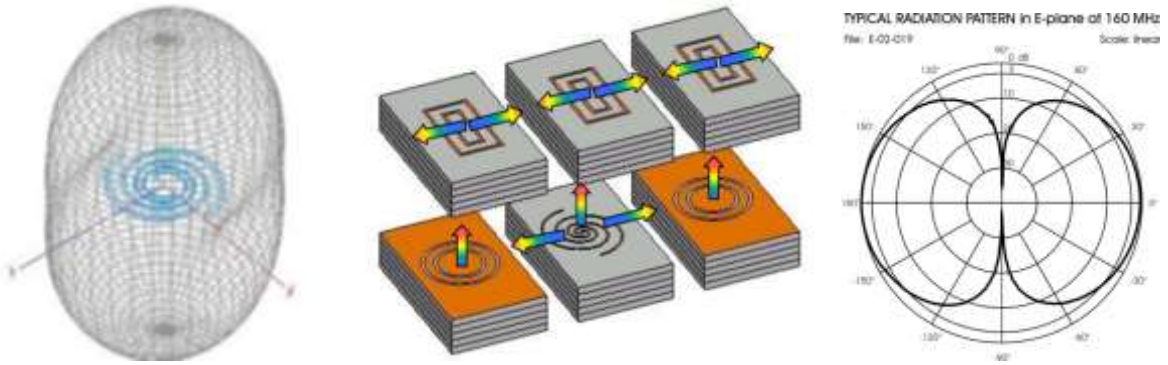


Рис. 2. Спиральные антенны, в отличие от мпл и щелевых,
способны излучать сигнал как в осевом, так и в плоскостном направлении

Каким образом достигается разнонаправленное излучение спиральных антенн:

- при изменении рабочей частоты;
- при изменении толщины металлизированной подложки;
- в зависимости от питания (синфазное, противофазное).

Рабочая частота

При различных частотах одна и та же антенна способна переключаться из осевого излучения в плоскостное излучение, при том осевое излучение характерно высоким частотам, а плоскостное – низким.

Питание антенны. Толщина металлизированной подложки

Для питания антенн используется подложка из метаматериала. Обязательной является металлизация подложки, чтобы защитить остальную часть модуля от высокочастотных помех.

Рис. 3. Схематическое изображение ОИС

При металлизации подложки регулируется её толщина (этим мы регулируем направление). Так же есть возможность изменять толщину слоя между линией питания и металлизацией (этим регулируются остальные характеристики).

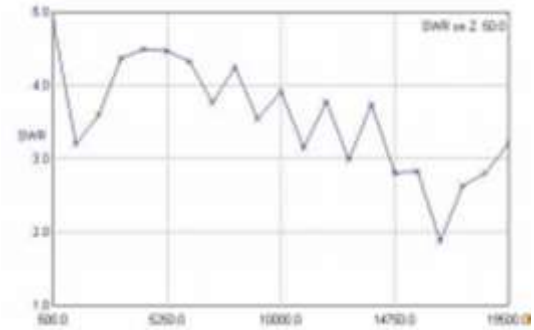


Рис. 4. График КСВн в диапазоне частот 500 МГц – 19,5 ГГц.
Толщина подложки составила λe (длина волны в диэлектрике)
Синфазное и противофазное питание антенны

Синфазное питание антенны – питание, при котором токи в точках питания антенны находятся в одной фазе, противофазное – разность фаз токов = 180 град

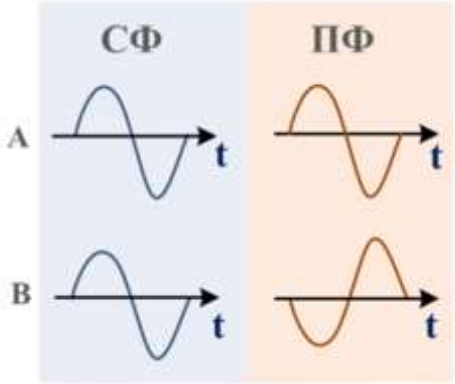


Рис. 5. Синфазный сигнал (СФ) и противофазный сигнал (ПФ)

В случае, когда питание антенны синфазное, наблюдается осевое излучение

В случае, когда питание противофазное – излучение в плоскости антенны

Выводы

Используемые в настоящее время планарные излучатели удовлетворяют заданным требованиям и обладают нужными характеристиками.

Однако спиральные планарные излучатели как таковые не имеют проблем МПЛ и щелевых излучателей, усложняющих конструкции, требующих от разработчиков дополнительных усилий, что говорит о рациональности и перспективности их использования.

Список используемых источников

1. Бочаров Е. И., Ветров В. В., Седышев Э. Ю., Усатова И. А. Планарные излучатели объёмных интегральных схем СВЧ // Всероссийская конференция «Электроника и микроэлектроника СВЧ» 3–6 июня 2013 года. СПб. : СПбГУТ, 2013.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Седышевым Э. Ю.

УДК 621.375.026

А. А. Ганбаев (аспирант, СПбГУТ)

АНАЛИЗ МЕТОДОВ МОДУЛЯЦИИ ВЧ КОЛЕБАНИЙ В КЛЮЧЕВЫХ ГЕНЕРАТОРАХ

Рассмотрены методы модуляции ВЧ колебаний в ключевых генераторах и усилителях мощности. Проанализированы варианты получения модулированного ВЧ радиосигнала на малом уровне мощности с последующим усилением, а также формирования модулированного сигнала в мощном выходном каскаде ключевого генератора. Приведена схема управляемого ключевого генератора на основе резонансного инвертора тока, обеспечивающего высокий КПД и линейную модуляционную характеристику.

Широтно-импульсная модуляция, амплитудная модуляция, КПД.

В данной работе предпринята попытка проанализировать существующие методы управления ВЧ колебаниями в ключевых генераторах и усилителях мощности. Интерес к этой тематике за последнее десятилетие заметно возрос в связи с состоявшимся технологическим прорывом в области полупроводниковых приборов. Создание транзисторов с высокой по-

движностью электронов на основе арсенида и нитрида галлия открыло возможность практической реализации высокоэффективных ключевых режимов усиления колебаний на частотах до 3 ГГц. В этой связи применение высокоэффективных ключевых режимов генерирования и усиления и колебаний в диапазонах ВЧ и СВЧ (от десятков мегагерц до единиц гигагерц) приобретает первостепенно значение для широких классов радиотехнических устройств.

В зарубежных исследованиях по ВЧ ключевым транзисторным усилителям мощности в последние годы вновь проявлен интерес к применению радиочастотной широтно-импульсной модуляции (РЧ-ШИМ). Идея такого метода управления ВЧ колебаниями была опубликована в 1973 году американским ученым Раабом (Raab) [1]. Данный вид модуляции имеет преимущество над $\Delta\Sigma$-модуляцией, которая все чаще используется в ключевых генераторах в последние годы. Недостаток $\Delta\Sigma$-модуляции – это наличие шумов квантования, которые отсутствуют в РЧ-ШИМ, соответственно сигнал не искажается и не нуждается в последующей сложной фильтрации [1, 2].

Ниже представлена компьютерная модель, реализующая РЧ-ШИМ и позволяющая исследовать процесс модуляции во временной области с последующим анализом спектрального состава. На рисунке 1 приведена схема РЧ-ШИМ модулятора, построенная в программе FASTMEAN. Для упрощения моделирования была выбрана несущая частота f_0 = 200 кГц и частота модуляции $f_м$ = 10 кГц. Полученные результаты с применением масштабирования по частоте использованы для оценки реального СВЧ усилителя мощности, работающего на частоте 1 ГГц и имеющего полосу частот в 50 МГц.

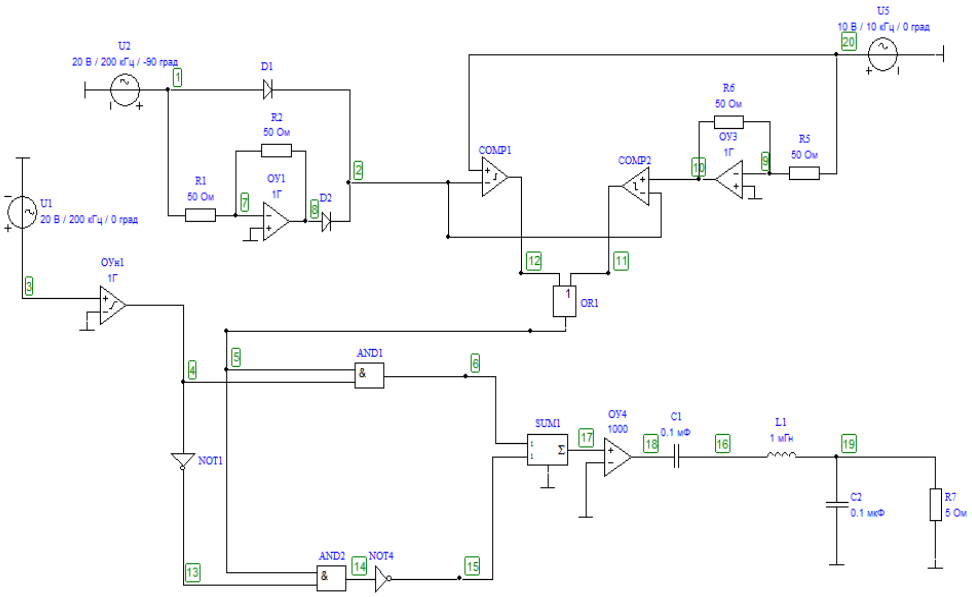


Рис. 1. Компьютерная модель РЧ-ШИМ модулятора

На основе разработанной компьютерной модели сняты для РЧ-ШИМ модулятора временные диаграммы на выходе компаратора, ограничителя и на выходе модулятора которые показаны на рисунке 2.

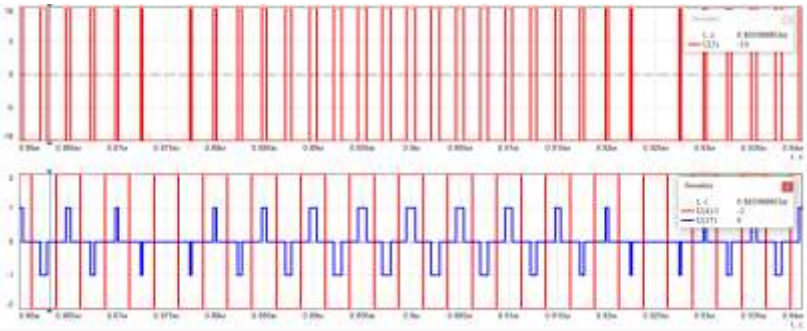


Рис. 2. Диаграммы на выходе компаратора, ограничителя и модулятора

На выходе РЧ-ШИМ формируются ВЧ биполярные импульсы с изменяющейся длительностью, после фильтрации которых формируется амплитудно-модулированный сигнал, который изображен на рисунке 3.

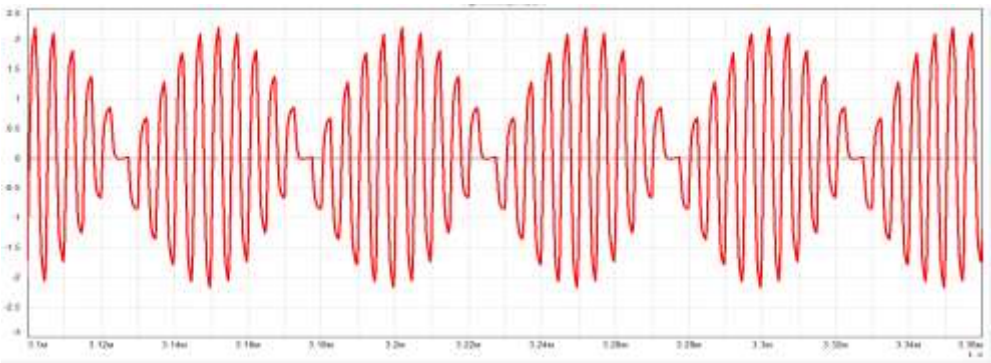


Рис. 3. Амплитудно-модулированный сигнал на выходе РЧ-ШИМ

В программе FASTMEAN также был рассчитан амплитудный спектр сигнала для тактовой частоты равной 200 кГц, который изображен на рисунке 4.

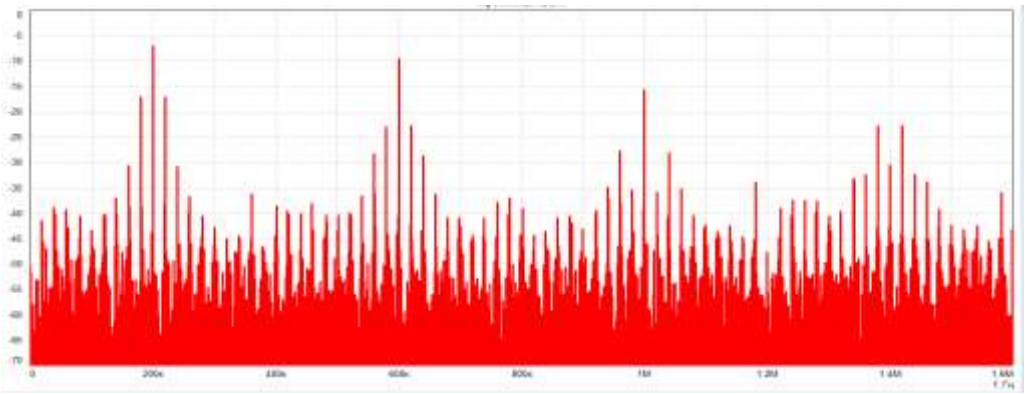


Рис. 4. Амплитудный спектр на выходе РЧ-ШИМ модулятора

Кроме РЧ-ШИМ также известны другие виды модуляции, одна из которых использует метод цифровой широтно-импульсной модуляции с использованием технологии Кана (Khan) схема которого изображена на рисунке 5 [3].

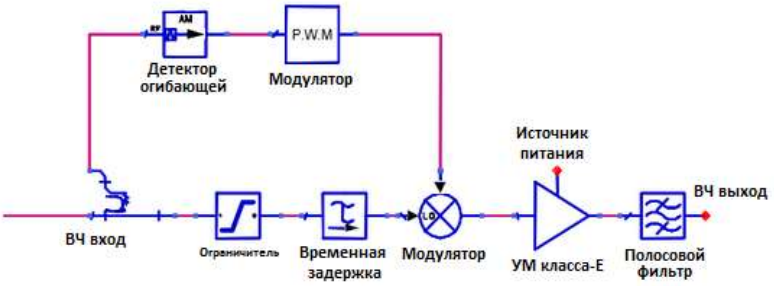


Рис. 5. Схема модулятора по технологии Кана

Такой способ модуляции был применен в усилителях мощности класса Е при тактовой частоте 2,4 ГГц и частоте модуляции 10 МГц, КПД по добавленной мощности при этом составил около 70 %, что является хорошим результатом.

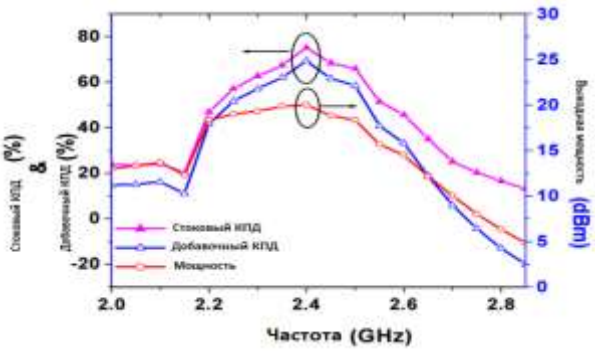


Рис. 6. КПД модулятора на частоте 2,4 ГГц

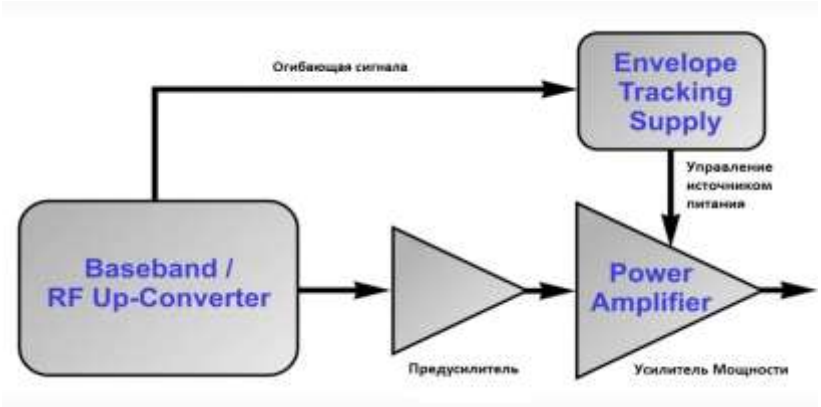


Рис. 7. Схема метода отслеживания огибающей (Envelope Tracking)

Также, в передатчиках используется метод отслеживания огибающей (Envelope Tracking). Преимуществом Envelope Tracking является то что,

огибающая ВЧ сигнала управляет напряжением питания усилителя мощности. Таким образом, уменьшается уровень потерь мощности источника питания и повышается КПД усилителя мощности.

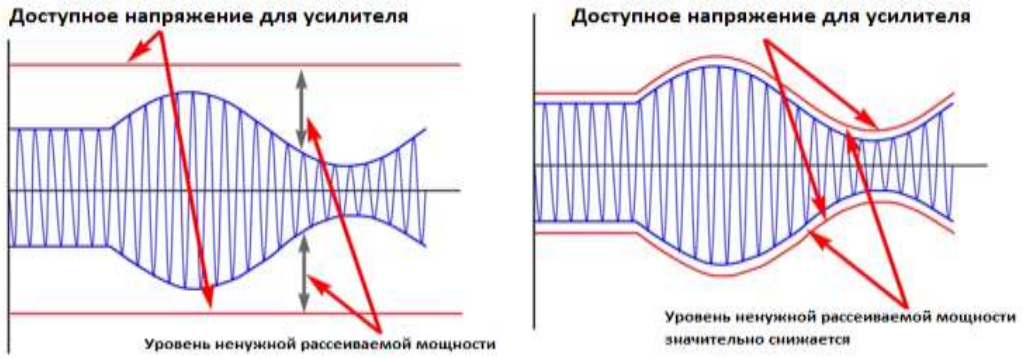


Рис. 8. Сравнения уровней ненужной выделяемой мощности
с использованием метода отслеживания огибающей (Envelope Tracking)

Рассмотрим управляемый резонансный инвертор тока (рис. 9). Данная схема может работать на высокой частоте радиосигнала, преобразуя ШИМ сигнал в ВЧ АМ (рис. 10) сигнал. Схема имеет высокий КПД (более 90 %) и линейную модуляционную характеристику, что делает ее конкурентоспособной по отношению к другим схемам.

Для данной схемы была разработана компьютерная модель, которая исследована в программе FASTMEAN. Для параметров модели, указанных на рисунке 9 временная диаграмма напряжения в нагрузке и ее амплитудный спектр приведены на рисунке 10.

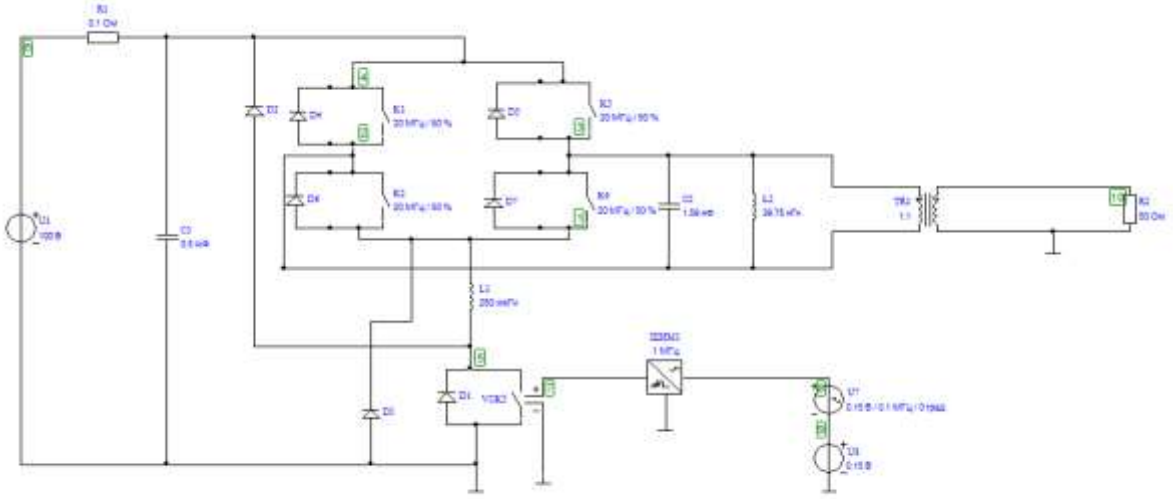


Рис. 9. Схема управляемого инвертора тока

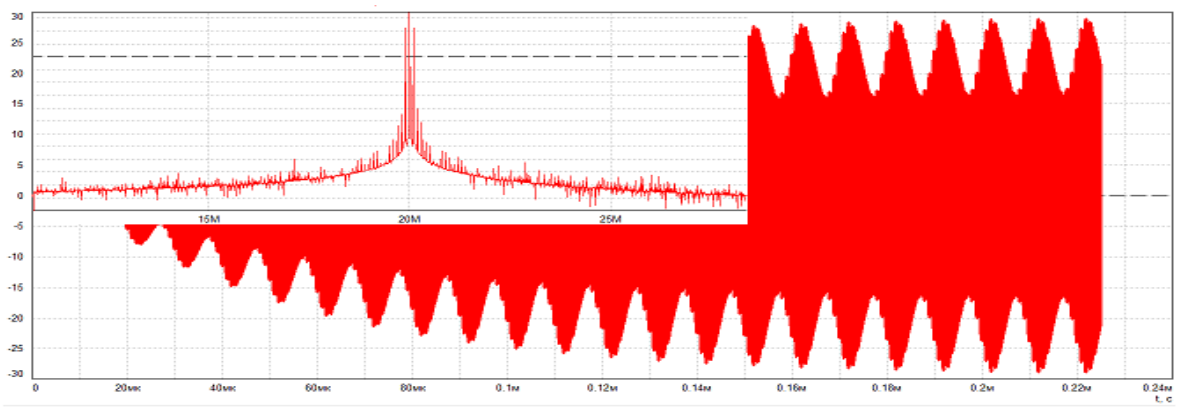


Рис. 10. Временная диаграмма и спектр напряжения
на выходе управляемого инвертора

Выполненный сравнительный анализ и результаты моделирования свидетельствуют о важных достоинствах предложенной схемы управляемого резонансного инвертора тока и ее перспективности применения в радиосвязи.

Список используемых источников

1. Raab F. H., Radio frequency pulse width modulation, IEEE Transactions on Communications, vol. 21, pp. 958–966, Aug. 1973.
2. Dr. Andrzej Samulak. System Analyses of Class-S Power Amplifier. Germany: Erlangen, 2010.
3. Kahn L. R., Single sideband transmission by envelope elimination and restoration, Proc. IRE, vol. 40. no.7, pp. 803–806, july 1952.

Статья представлена научным руководителем,
доктором технических наук, профессором Филиным В. А.

УДК 53.04, 536.03, 539.06

Н. В. Домрачев (студент группы ФП–41, СПбГУТ)
Н. Ю. Сазоненко (студент группы ФП-41, СПбГУТ)
А. Д. Сединин (студент группы ФП-41, СПбГУТ)
И. Л. Тхоржевский (студент группы ФП-41, СПбГУТ)

АНАЛИЗ РЕЗУЛЬТАТОВ РАСЧЁТА ДИСПЕРСИОННОГО ДАВЛЕНИЯ В СЛОИСТЫХ СТРУКТУРАХ НА ОСНОВЕ КРЕМНИЯ

В работе получены расчетные значения величины давления дисперсионных сил, действующих в наноразмерных структурах на основе Si-подложки, с разным типом материала слоя металлизации. Проведена оценка влияния параметров слоя металлизации структур металл–диэлектрик–полупроводник (МДП), изготовленных на основе

кремниевой пластины, в диапазоне актуальных для современной электроники значений этих параметров.

дисперсионные силы, металл, диэлектрик, полупроводник, МДП–структуры.

Развитие электронной техники направлено, прежде всего, на уменьшение массогабаритных размеров устройств, что позволяет снизить их энергопотребление и увеличить время автономной работы. Эта тенденция также открывает возможности для разработки и построения новых устройств электроники, принцип работы которых основан на действии межмолекулярных взаимодействий и квантовых явлений. К таким явлениям относятся дисперсионные силы, обусловленные длинноволновым флуктуационным электромагнитным полем, в которых учитываются эффекты запаздывания электромагнитного поля. В большинстве работ по исследованию дисперсионных сил рассматривается взаимодействие некоторых абстрактных систем. Однако в ряде работ прикладного характера установлено, что именно эти силы являются причиной выхода из строя устройств, размеры которых составляют несколько нанометров. В то же время ведутся работы по созданию наноэлектромеханических устройств (NEMS), принцип действия которых основан на действии дисперсионных сил. Поэтому актуальной является задача исследования проявления дисперсионных сил в структурах, активно используемых в современной электронике, с параметрами, которые соответствуют реальным элементам.

Значение дисперсионного давления, как величину силы, приложенной к единичной площади поверхности слоя, можно получить с помощью выражения:

$$P(a_{Diel},T) = -\frac{k_B T}{8\pi a_{Diel}^{\ 3}} \sum_{l=0}^{\infty}{}' \left(1-\frac{\delta_{l0}}{2}\right) \int_0^{\infty} k_\perp dk_\perp K_l^{(0)} \times$$
$$\times \sum_q \left[\frac{e^{2K_l^{(0)} a_{Diel}}}{r_q^{(0,1)}(i\xi_l,k_\perp)\cdot r_q^{(0,2)}(i\xi_l,k_\perp)} - 1 \right]^{-1}. \qquad (1)$$

Это выражение (1) применимо для расстояний между взаимодействующими слоями от доли нанометров до нескольких сотен микрон [1, 2], то есть для случаев, когда толщины слоев исследуемых структур металл–диэлектрик–полупроводник превышают размеры атомного слоя (он составляет величину порядка 5 – 10 Å).

Частоты Мацубары $\xi_l = 2\pi \cdot k_B T \cdot l / \hbar$ являются не зависящими от времени функциями и используются для перехода от интегрирования в бесконечных пределах по времени к проведению интегрирования в пределах от нуля до $1/T$ по “мнимому” времени. При этом сохраняется формальное сходство с уравнениями движения электромагнитного поля.

Значения коэффициентов отражения Френеля от границы раздела кремниевой пластины Si (или слоя металлизации) и диэлектрического слоя для двух поляризаций падающей электромагнитной волны вычисляются при мнимых значениях частоты:

$$r_{TM}^{(\mathrm{Diel},n)}\left(i\xi_l,k_\perp\right)=\frac{\varepsilon_l^{(n)}K_l^{(Diel)}-\varepsilon_l^{(Diel)}K_l^{(n)}}{\varepsilon_l^{(n)}K_l^{(Diel)}+\varepsilon_l^{(Diel)}K_l^{(n)}} \text{ и } r_{TE}^{(Diel,n)}\left(i\xi_l,k_\perp\right)=\frac{K_l^{(Diel)}-K_l^{(n)}}{K_l^{(Diel)}+K_l^{(n)}},$$

где коэффициент $K_l^{(Diel,n)}\equiv\sqrt{k_\perp^2+\varepsilon_l^{(Diel,n)}\frac{\xi_l^2}{c^2}}$,

причем c – скорость распространения электромагнитной волны в вакууме.

Диэлектрическая проницаемость является комплексной величиной, зависящей от частоты $\omega(t)=\omega_1+i\cdot\omega_2$, где ω_1 и ω_2 – действительный и мнимый аргументы соответственно, i – мнимая единица.

Мнимая часть диэлектрической проницаемости всегда имеет положительные значения и определяет диссипацию энергии электромагнитной волны, распространяющейся внутри тела.

Для качественного и более полного описания комплексной диэлектрической проницаемости применяют соотношения Крамерса–Кронига, которые позволяют получить значения диэлектрической проницаемости в широком диапазоне частот и, таким образом, дать полное представление об электрооптических свойствах материалов:

$$\varepsilon(i\xi)=1+\frac{2}{\pi}\int_0^{\omega_{\min}}\frac{\omega\varepsilon_2(\omega)}{\omega^2+\xi^2}d\omega+\int_{\omega_{\min}}^{\omega_{\max}}\frac{\omega\varepsilon_2(\omega)}{\omega^2+\xi^2}d\omega+\frac{2}{\pi}\int_{\omega_{\max}}^{\infty}\frac{\omega\varepsilon_2(\omega)}{\omega^2+\xi^2}d\omega. \qquad (2)$$

Первый интеграл в правой части данного уравнения близок к нулю для большинства материалов. Второй интеграл в пределах от $\omega_{\min}$ до $\omega_{\max}$ может быть вычислен численно с использованием экспериментальных данных.

Третий интеграл в правой части уравнения (2) можно оценить, принимая во внимание общий закон убывания функции комплексной диэлектрической проницаемости. Обычно оказывается, что этот вклад настолько мал, что им можно полностью пренебречь.

Большинство устройств современной электроники (более 90 %) изготавливаются на основе кремния. В качестве диэлектрического слоя часто используют диоксид кремния. Поверх диэлектрического слоя, как правило, формируют металлический слой, образующий контактные площадки и необходимые соединения между отдельными областями. Этот тип слоистых структур называют структуры металл–диэлектрик–полупроводник (МДП).

Чтобы адекватно описать функцию комплексной диэлектрической проницаемости металлов, в исследованиях явления дисперсионного взаимодействия используют модель Друде или плазменную модель. Эти модели различаются особенностями учета энергии рассеяния в процессах столкновения свободных электронов проводимости с ионами решётки и влияния межзонных переходов. В области низких частот разложение функции диэлектрической проницаемости металлов в ряд Тейлора по степеням ω начинается со значения действительной составляющей диэлектрической проницаемости ε_1 при $\omega = 0$ и содержит только чётные степени ω.

Поскольку в расчётах используются экспериментальные данные о вещественной и мнимой частях комплексного показателя преломления, полученные при взаимодействии слоя металлизации с реальными электромагнитными полями соответствующих частот, при низких частотах они естественным образом включают вклад свободных электронов проводимости с учетом рассеяния энергии.

Таким образом, экспериментальные данные для комплексного показателя преломления отражают вклад свободных электронов проводимости в диэлектрическую проницаемость металла в соответствии с описанием модели Друде при низких частотах:

$$\varepsilon_{Dr}(i\xi) = 1 + \frac{2}{\pi}\int_0^\infty \frac{\omega\varepsilon_2(\omega)}{\omega^2 + \xi^2}\,d\omega .$$

Для плазменной модели диэлектрической проницаемости уравнение имеет вид:

$$\varepsilon(i\xi) = 1 + \frac{2}{\pi}\int_0^\infty \frac{\omega\varepsilon_2^{(cl)}(\omega)}{\omega^2 + \xi^2}d\omega + \frac{\omega_p^2}{\xi^2},$$

где $\varepsilon_2^{cl}(\omega)$ – вклад в мнимую часть диэлектрической проницаемости, обусловленный внутренними электронами.

В рамках исследования были рассмотрены структуры металл–диэлектрик–полупроводник при температуре $T = 300$ К с диэлектрическим слоем, выполненным из диоксида кремния SiO_2 с толщиной, равной $a_{diel} = 50$ нм. На рисунке 1 представлена полученная расчетная зависимость модуля величины дисперсионного давления от толщины слоя металлизации для структур металл–диэлектрик–полупроводник.

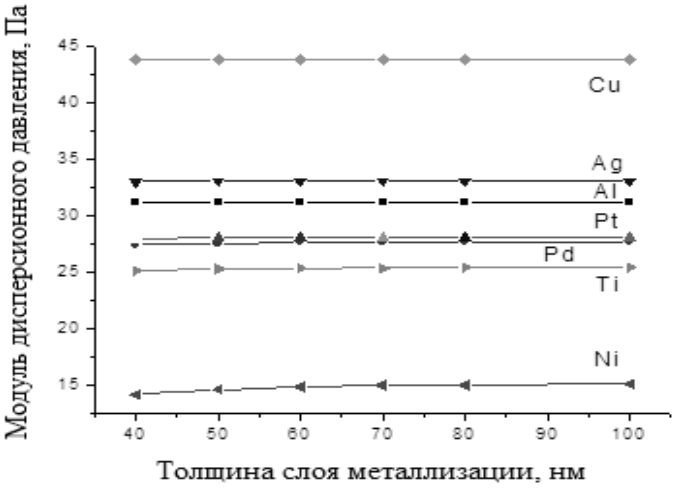


Рис. 1. Расчетная зависимость модуля величины дисперсионного давления от толщины металлического слоя d_{Me}

Из рисунка 1 видно, что при уменьшении толщины слоя металлизации от 100 до 40 нм расчетная величина дисперсионного давления изменяется менее чем на 1 %. Относительное изменение значения дисперсионного давления сохраняется при изменении толщины диэлектрического слоя диоксида кремния от 50 до 10 нм и связано с соотношением диэлектрических проницаемостей типа материала, используемого в качестве слоя металлизации, в области малых и средних частот. В таблице 1 представлены полученные значения модуля дисперсионного давления в структурах металл–диэлектрик–полупроводник с разными типами металлизации и фиксированной толщиной, которая составляла 80 нанометров.

ТАБЛИЦА 1. Модуль расчетной величины дисперсионного давления от толщины слоя диоксида кремния SiO_2 в МДП-структурах при d_{Me} = 80 нм

a_{diel}, нм	Модуль величины дисперсионного давления $\|P\|$ в МДП-структурах, Па						
	Al	**Pd**	**Pt**	**Ni**	**Cu**	**Ti**	**Ag**
50	31,24	27,66	28,09	15,014	43,80	25,08	33,07
40	69,32	61,45	62,71	30,12	101,32	55,83	74,99
35	110,90	98,48	100,80	45,19	166,168	88,84	121,64
30	189,58	168,82	173,36	71,50	292,09	151,11	211,26
25	354,29	316,87	326,58	121,54	563,35	280,77	402,35
20	752,20	677,04	700,75	229,12	1239,30	592,39	873,76
15	1 948	1 770	1 841	509,27	3 341	1 524	2 327
10	7 215	6 643	6 851	1 542	12 961	5 603	8 925
5	63 310	59 474	62 676	10 377	121 129	48 825	82 108

Также в ходе проведенного исследования было установлено, что расчетное значение дисперсионного давления слабо зависит от моделей (модель Друде и плазменная модель), которые используются для описания диэлектрической проницаемости $\varepsilon(i\xi)$ слоя металлизации в рассмотренных МДП-структурах на основе Si. Расхождение результатов вычислений величины дисперсионного давления с использованием обеих моделей $\varepsilon(i\xi)$ составляет менее 10 %.

Полученные результаты согласуются с данными работы [3], в которой проводилось исследование влияния моделей описания диэлектрической проницаемости для различных конфигураций взаимодействующих объектов и типов металлов, из которых они выполнены.

Анализ полученных результатов в ходе выполнения работы показывает, что относительное изменение расчетной величины дисперсионного давления слабо зависит от типа материалов, которые используются в качестве металлического слоя в структурах металл–диэлектрик–полупроводник. Толщина металлического слоя в диапазоне толщин, используемых в современной электронной технике, практически не оказывает влияния на эту величину. Использование в вычислениях величины дисперсионного давления различных моделей (плазменной и Друде) диэлектрической проницаемости слоя металлизации дает близкие по значению результаты, расхождение которых не превышает 10 %.

Список используемых источников

1. Parsegian V. A. Van der Waals forces: a handbook for biologists, chemists, engineers and physicists // Cambridge: Cambridge University Press, 2005. 394 p.

2. Бараш Ю. С. Силы Ван-дер-Ваальса. М. : Наука, 1988. 344 с.

3. Klimchitskaya G. L., Mostepanenko V. M. Casimir free energy of metallic films: Discriminating between Drude and plasma model approaches // Phys. Rev. A. 2015. Vol. 92, 042109. pp. 1–30.

Статья представлена научным руководителем,
кандидатом физико-математических наук, доцентом Юровой В. А.

УДК 621.375.026

Д. С. Прялухин (студент группы ФМ-51м, СПбГУТ)

ПРИМЕНЕНИЕ КЛЮЧЕВОГО РЕЖИМА E_m В СВЧ УСИЛИТЕЛЯХ МОЩНОСТИ

В настоящее время при разработке транзисторных усилителей мощности СВЧ диапазона остро стоит вопрос получения максимальной радиочастотной мощности при наибольших КПД и коэффициенте усиления по мощности. Данная статья посвящена вопросам построения и применения усилителей мощности режима E_m на рабочей частоте 2,45 ГГц, приводится математическая модель данного усилителя.

усилитель мощности, ключевой режим, СВЧ, GaN, КПД.

Известно из теории, что максимальный КПД усилителя в режиме А составляет 50 %, максимальный КПД в режиме АВ 70–72 %, но на практике при усилении радиочастотных сигналов с меняющейся огибающей эта цифра существенно меньше и не превышает 15–20 %. Именно пониженным КПД обусловлены такие факторы как нагрев транзисторов усилителя, снижение его эффективности и срока службы.

Одним из перспективных способов достижения наибольшего КПД является применение ключевого режима работы транзисторов. В 1975 г. американскими специалистами была опубликована работа [1], в которой предлагается новый класс усилителей мощности работающих в ключевом режиме – «класс Е». Популярность режима *E* объясняется высоким КПД и сравнительно простой схемой. На рисунке 1*а* показана форма напряжения на транзисторе в режиме *E*, а на рисунке 1*б* – форма тока (пунктирной линией).

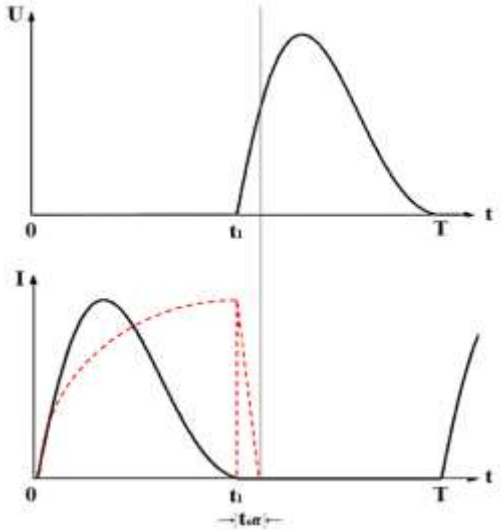


Рис. 1. Временные диаграммы изменения напряжения и тока нагрузки:
а) – режим E_m (верхняя диаграмма), *б*) – режим *E* (нижняя диаграмма)

В последнее время эффективность ВЧ усилителей мощности оценивается КПД по добавленной мощности:

$$\eta = \frac{P_{\text{н}} - P_{\text{возб}}}{P_0}, \qquad (1)$$

где Pн – средняя мощность в нагрузке; Pвозб – мощность возбуждения; P_0 – мощность источника питания. Как видно из формулы (1), при большей мощности возбуждения КПД снижается.

Во временном интервале падения тока t_{off} (рис. 1) возрастает напряжение, в связи с этим для режима E возникают потери мощности. Для уменьшения значения t_{off} и увеличения КПД (1) используют быстродействующие транзисторы или увеличивают мощность усиливаемого сигнала на входе. Первый вариант отличается высокой стоимостью реализации усилителя, второй вариант значительно влияет на эффективность усиления.

Применение новой модификации, т. е. режима E_m [2], предложенного в 2002 г. известным радиоинженером Сокалом (N. O. Sokal), является одним из возможных решений данной проблемы. Благодаря использованию дополнительного канала в схеме усилителя и соответственно его настройке резкая (скачкообразная) форма тока меняется на плавную кривую, достигающую нулевого значения к моменту выключения транзистора, что дает весомый прирост КПД с 80 до 92 % (рис. 2).

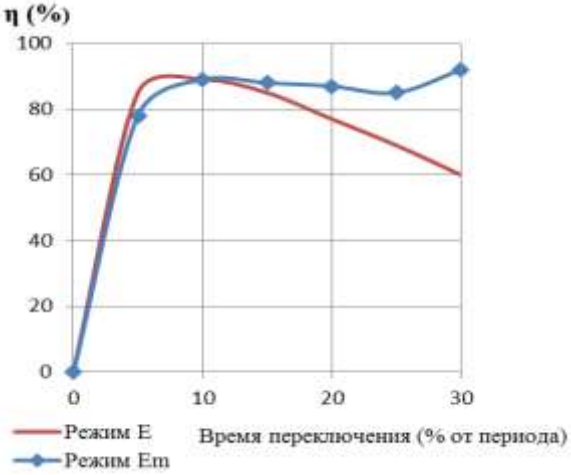


Рис. 2 Зависимость КПД (η)
от времени переключения

На рисунке 3 представлена схема усилителя в режиме E_m, в котором наряду с основным каналом вводится дополнительный маломощный канал усиления, работающий на второй гармонике основной частоты, вклад которого в общую мощность составляет не более 30 %.

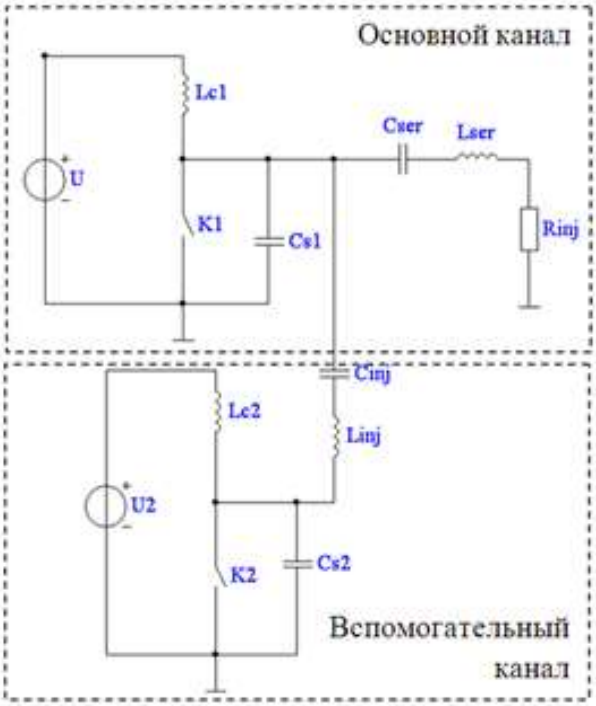


Рис. 3. Схема усилителя в режиме E_m

Формулы расчета параметров режима E_m:

$$L_{ser} = \frac{Xl}{\omega},$$

$$C_{ser} = \left(\frac{1}{f \cdot 2\pi \cdot \sqrt{L_{ser}}} \right),$$

$$R_{inj} = \frac{128 \cdot (U)^2}{9 \cdot (\pi^2 + 16) \cdot P},$$

$$X_{inj} = \frac{16 \cdot (\pi^2 \cdot 3 + 16) \cdot (U)^2}{9 \cdot \pi \cdot (\pi^2 + 16) \cdot P},$$

$$Xl = \omega \cdot L,$$

U – напряжение источника питания; P – заданная средняя мощность в нагрузке.

Таким образом, в отличие от режима E в режиме E_m фазовые соотношения между отдельными каналами подбираются так, что ток основного по мощности канала естественным образом спадает до нуля без скачка при выключении транзистора.

Мягкий режим переключения (без скачков) обеспечивает возможность перехода в более высокочастотный диапазон (до 10 ГГц), а применение новых видов транзисторов, разработанных на основе нитрида галлия

(GaN) открывают возможность для практической реализации таких усилителей.

Приведенный в данной статье сравнительный анализ режимов работы транзисторных усилителей мощности СВЧ диапазона позволяет выделить режим E_m как наиболее перспективный для последующего изучения. Цель дальнейшей работы: исследование электрического режима E_m и создание топологии усилителя мощностью 10 Вт в режиме E_m на рабочей частоте $f = 2{,}45$ ГГц, а также изучение предельных частотных свойств нитрид-галлиевых транзисторов для обеспечения функционирования этого режима на частотах выше 3 ГГц.

Список используемых источников

1. Sokal N. O., Sokal A. D., High-efficiency tuned switching power amplifier / U. S. Patent 3,919,656, Nov. 11, 1975.

2. Telegdy A., Molnar B., Sokal N. O., Class-E´ M Switching-Mode Tuned Power Amplifier—High Efficiency With Slow-Switching Transistor / IEEE Trans. Microwave Theory Tech., vol. 51, no. 6, June, 2003.

Статья представлена научным руководителем,
доктором технических наук, профессором Филиным В. А.

УДК 535

Н. Ю. Сазоненко (студентка ФП-41, СПбГУТ)
А. Д. Сединин (студент ФП-41, СПбГУТ)
И. Л. Тхоржевский (студент ФП-41, СПбГУТ)

ФРЕНЕЛЕВСКАЯ ДИФРАКЦИЯ НА КРУГЛОМ ОТВЕРСТИИ. ЛАБОРАТОРНАЯ РАБОТА НОВОГО ТИПА

Авторы поставили себе цель разработать компьютерную работу нового типа, одинаково пригодную для применения как в условиях недостаточного аппаратного обеспечения лабораторного практикума, так и для дистанционного применения. Работы такого типа существуют в большом количестве, однако обычно они являются легко воспроизводимыми механически, без глубокого понимания исследуемого процесса. Используя случайную генерацию, удалось исключить возможность угадывания или повторного воспроизведения результата. Попутно была написана программа автоматизированного допуска, имеющая самостоятельную ценность. В развитие работы, необходимо усовершенствовать методику оценки.

дифракция Френеля, лабораторная работа.

Введение

В курсе общей физики большое внимание уделяется непосредственно практическому наблюдению изучаемых процессов. В частности, это осуществляется в процессе лабораторных работ. Некоторые явления, такие как, например, различные взрыва, высокотемпературные процессы, ядерный распад и т. п., невозможно воссоздать на практике в условиях учебного заведения. С развитием информационных технологий появилась возможность компьютерного моделирования указанных и многих других явлений. Это позволяет решить множество проблем реальных лабораторных установок, например, сложной калибровки и настройки измерительных приборов. К тому же это открывает новые возможности для заочного и дистанционного обучения.

Выполнение работ в электронном варианте обладает своей спецификой, и при постановке подобной лабораторной работы необходимо решить некоторые вопросы:

1) автоматизировать систему получения допуска к лабораторной работе, который предполагает достаточное усвоение студентом необходимого теоретического материала;

2) решить проблему “шаблонного” выполнения поставленной задачи, без понимания самой сути физического процесса, сделав такое выполнение невозможным.

Авторы поставили задачу создать лабораторную работу, в которой оба этих вопроса будут успешно решены.

Теоретический материал

Дифракция в ближнем поле качественно хорошо описывается приближенной теорией Френеля [1], краткое изложение которой приводится ниже. Окружим источник света S произвольной замкнутой поверхностью F. В соответствии с принципом Гюйгенса-Френеля, каждая точка поверхности F является источником вторичных волн, распространяющихся по всем направлениям. По принципу Гюйгенса-Френеля, световое поле, возникающее в пространстве вне поверхности в результате интерференции вторичных когерентных волн, совпадает с полем реального источника света. Рассмотрим амплитуду световой волны в точке P (рис. 1). Разобьем поверхность на участки (зоны), проведя несколько концентрических сфер с центром в точке P (на рисунке зоны заштрихованы). Выберем радиусы сфер равными b, $b + \lambda/2$, $b + \lambda$, …, $b + \lambda/2$ (где $m = 1, 2, 3, \ldots$).

Тогда соответствующие кольцевые области на поверхности F называются зонами Френеля. С помощью геометрических построений можно показать, что, в случае $b >> \lambda$, разница в площадях соседних зон очень мала. Так как при равенстве площадей количество светящихся точек в соседних зонах примерно одинаково, то колебания от них в точке P должны

практически полностью погасить друг друга. Поставим на пути световой волны диафрагму, диаметр которой совпадает с границей четной зоны Френеля; тогда колебания от всех пар соседних зон скомпенсируют друг друга и в точке *P* будет наблюдаться темное пятно. Если же диафрагма открывает нечетное число зон Френеля, то колебания от одной из них останутся некомпенсированными и в точке *P* будет светлое пятно.

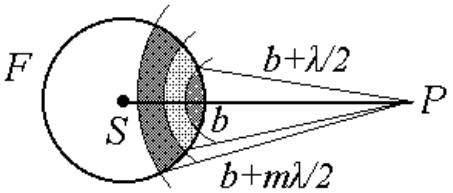


Рис. 1. Зоны Френеля
для сферической волны

Можно определить количественное значение интенсивности в точке P, воспользовавшись так называемой спиралью Френеля. Мысленно разобьем зоны Френеля на более мелкие подзоны. Будем изображать суммарное колебание от подзоны в виде вектора (рис. 2). Вектор от следующей подзоны должен быть повернут на некоторый небольшой угол $\delta\varphi = 2\pi\delta x/\lambda$, где δx – разность хода между лучами от соседних подзон. Кроме того, из-за уменьшения коэффициента Кирхгоффа, амплитуда колебаний от следующей подзоны чуть меньше, чем от предыдущей. Результат сложения колебаний от отдельных подзон представлен на рисунке 2. Нетрудно сообразить, что к концу первой зоны Френеля вектор от подзоны развернется на "π", а к концу второй зоны – совершит полный оборот.

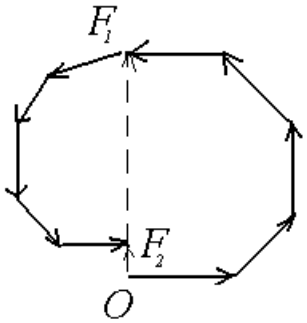


Рис. 2. Схема построения
спирали Френеля

В пределе бесконечно малых подзон, ломаная линия с рисунка 2. Переходит в непрерывную кривую, называемую спиралью Френеля (она изображена на рисунке 3). С ее помощью можно получить количественную оценку интенсивности света в центре дифракционной картины. В самом

деле, амплитуда колебания от первой открытой зоны Френеля изображается вектором OF_1, длина которого на рисунке 3 обозначена как E_1. Очевидно, что амплитуда колебаний от полностью открытого волнового фронта изображается вектором с длиной E_0. Из-за близости первого витка спирали к окружности, можно предположить, что $E_1 \approx 2E_0$, или, то же самое $\mathfrak{I}_1 \approx 4\mathfrak{I}_0$.

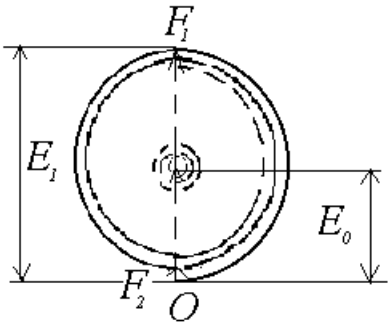


Рис. 3. Спираль Френеля

Оценим размеры зон Френеля и предельные расстояния для начала френелевской дифракции для простейшего случая плоской волны.

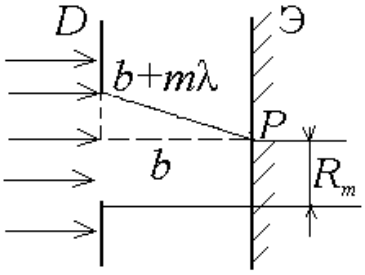


Рис. 4. К определению размера
зон Френеля для плоской волны

Непосредственно из рисунка 4, по теореме Пифагора, следует:

$$R_m = \sqrt{(b + m\lambda/2)^2 - b^2} \approx \sqrt{m\lambda b}. \quad (1)$$

Выражая из (1) количество зон, укладывающихся в отверстии, будем иметь, что дифракция Френеля наблюдается при необходимом условии:

$$m \approx \frac{d^2}{4b\lambda}. \quad (2)$$

Количество зон Френеля можно определить по графику. Число горбов на графике для интенсивности в зависимости от прямолинейной координаты «*x*», ось для которой проходит через точку *P*, совпадает с числом открытых зон.

Порядок выполнения работы

Программа состоит из двух блоков: опроса в форме теста и самой лабораторной работы.

Рис. 6. Пример работы программы

Тест состоит из пяти вопросов, для ответа на которые можно воспользоваться учебниками по волновой оптике [2, 3, 4]. Особенность алгоритма в том, что формулировки вопросов, варианты ответа и порядок вопросов при каждом запуске программы изменяется. После прохождения теста программа выведет на экран сумму баллов. При наборе 4 из 5 возможных баллов, программа переходит на экран с лабораторной работой. В случае невыполнения теста, программа автоматически завершает работу.

Перед началом непосредственного выполнения работы, программа случайным образом генерирует длину волны из оптического диапазона, которая никому заранее не известна и подлежит определению на основе теоретических знаний, почерпнутых студентами из теоретического описания. После загрузки лабораторной работы необходимо, манипулируя бегунками, добиться открытия целого числа зон Френеля. Бегунки отвечают за расстояние от диафрагмы до экрана и за ширину диафрагмы. График, представленный в работе, демонстрирует зависимость интенсивности света на экране. Получив количество зон Френеля, необходимо ввести это значение в специальное поле. После этого по нажатию кнопки, программа подсчитает значение длины волны для заданных параметров. После повторения опыта ещё два-три раза, программа высчитает среднее от полученных длин волн и погрешность измерения; если они будут согласовываться с той длиной волны, что была сгенерирована изначально, работа будет считать выполненной.

Заключение

Поставленная задача была, в основном, выполнена авторами. В будущем авторы хотели бы доработать данную систему и внести в неё следующие элементы:

- автоматизировать процесс оценки данной работы и разработать систему дистанционного отчета;
- разработать набор подобных лабораторных работ по другим физическим явлениям;
- приспособить опрос для автономного использования в других работах.

Список используемых источников

1. Борн М., Вольф Э. Основы оптики. М. : Наука, 1973. 720 с.
2. Калитеевский Н. И. Волновая оптика. М. : Высшая школа, 1995. 463 с.
3. Сивухин Д. В. Общий курс физики. Т. IV. М. : ФИЗМАЛИТ, 2005. 792 с.
4. Савельев И. В. Курс физики. Т. III. Квантовая оптика. Атомная физика. Физика твердого тела. Физика атомного ядра и элементарных частиц. М. : Наука, 1989. 304 с.

Статья представлена научным руководителем,
доктором технических наук, профессором Колгатиным С. Н.

УДК 378.02:37.016

Р. С. Хачин (студент группы ФП-41, СПбГУТ)

РЕАЛИЗАЦИЯ ЗАДАНИЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ФИЗИКЕ С ПОМОЩЬЮ МАТЕМАТИЧЕСКОГО РЕДАКТОРА MATHCAD

Увеличение объема информации и способов ее представления дает возможность решения образовательных задач не только традиционными методами, но и с помощью информационных технологий, повышая, таким образом, не только качество образования, но и конкурентоспособность будущего инженера.

самостоятельная работа, Mathcad, информационные технологии, инженерное образование.

Изменения, происходящие в системе высшего технического образования, направлены на повышение качества подготовки инженерных кадров страны. Содержание образования, его стратегия направлены на развитие самостоятельности, проявление инициативы и активности будущих инженеров. В результате, доля самостоятельной работы в учебном процессе

растет, что, в свою очередь, требует методического сопровождения от преподавателей и готовность выполнять подобного рода работу от студентов.

Исследования явлений в физике полагает не только вычисление параметров изучаемых систем, но и составление схем, пояснительных рисунков, построение графиков, наглядно представляющих происходящие изменения в системе. При решении подобного рода задач применение компьютера позволяет уменьшить трудоемкость и визуализировать процесс.

Известный факт, что в силу простоты применения, наглядности математических действий, благодаря хорошему аппарату представления результатов, Mathcad является наиболее популярным математическим редактором среди студентов, ученых и технических специалистов. Перечисленные факторы позволяют реализовать определенный объем самостоятельной работы по физике с помощью математического редактора Mathcad. Таким образом, появляется комплекс заданий, связанных не только содержанием, но и единой методикой выполнения расчетов, построения графиков, оформления отчетов.

Например, изучение колебаний и волновых процессов – это решение задач многих параметров. Построение графиков данных процессов в Mathcad, применение режима трассировки позволяет найти ответ с малым объемом временных затрат, представить состояние системы в данный момент времени (рис. 1–3).

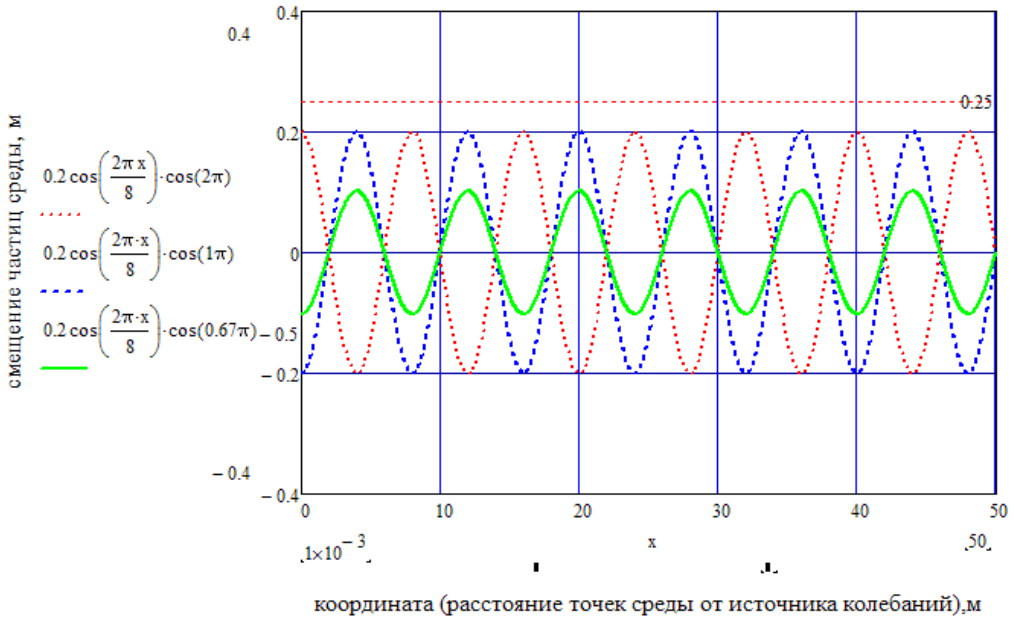


Рис. 1. График смещения частиц среды
при распространении стоячей волны в разные моменты времен

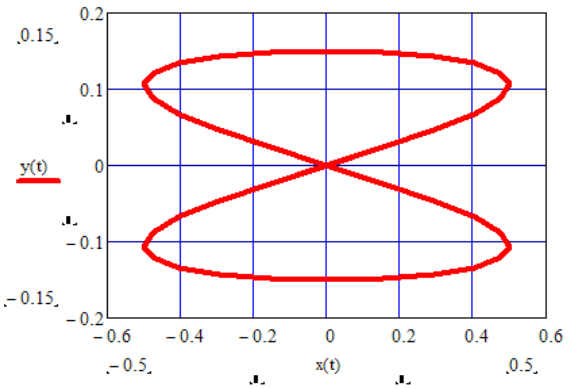


Рис. 2. График траектории точки при сложении колебаний с соотношением частот 1:2

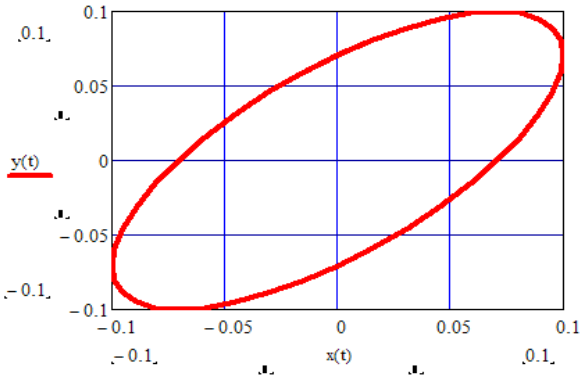


Рис. 3. График траектории точки при сложение колебаний равных частот

Так же, описание поведения микрочастиц осуществляется с помощью волновой функции, являющейся комплексной величиной, формально, обладающей волновыми свойствами. Благодаря волновой функции, можно определять вероятность нахождения частицы в том или ином состоянии. Такой процесс становится особенно наглядным при построении графиков соответствующих функций в Mathcad для частиц в малой области пространства. Используя график плотности вероятности, можно определить вероятность нахождения частицы в соответствующей области, продемонстрировать дискретность энергетических состояний частицы, перемена условия задания позволяет проследить процесс изменения состояния частицы (рис. 4–6).

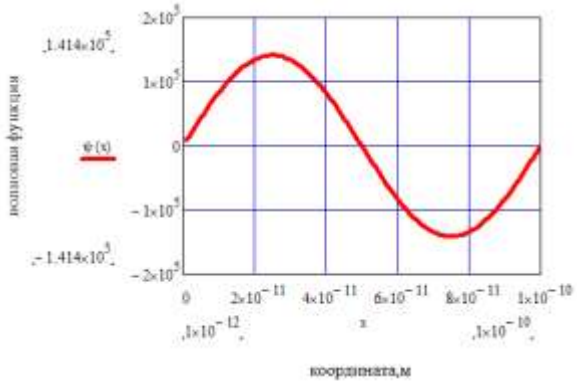


Рис. 4. График волновой функции для электрона в одномерной бесконечной потенциальной яме шириной 0,1 нм в состоянии с главным квантовым числом – 2

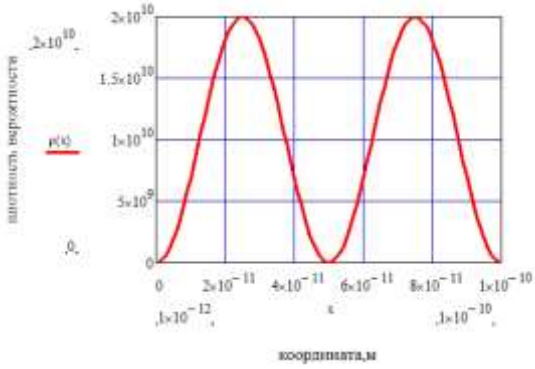


Рис. 5. График плотности вероятности для электрона в одномерной бесконечной потенциальной яме шириной 0,1 нм в состоянии с главным квантовым числом – 2

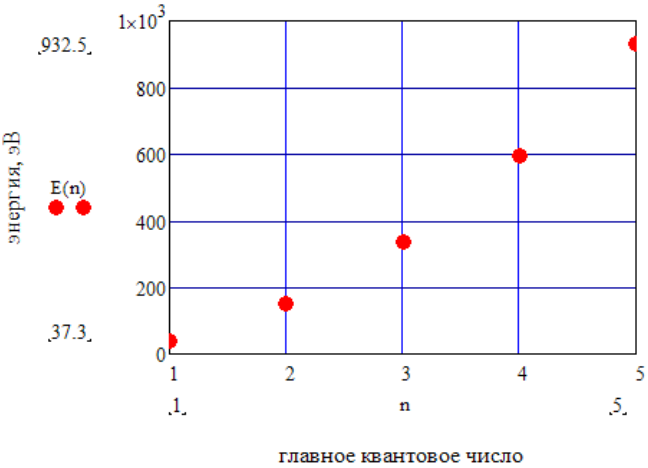


Рис. 6. График энергии частицы для электрона
в одномерной бесконечной потенциальной яме шириной 0,1 нм

Таким образом, применение возможностей компьютера способствует продуктивному решению образовательных задач, формированию культуры самостоятельной работы, как у студента, так и у преподавателя, основанной на информационных технологиях.

Список используемых источников

1. Жукова Е. Д. Технология организации и реализации самостоятельной работы студентов: рабочая тетрадь. Уфа: изд-во БГПУ, 2004. 32 С.

2. Ваганова Н. С. Самостоятельная работа как путь формирования методологической грамотности будущих бакалавров профессионального обучения в вузе // Вестник Томского государственного педагогического университета. 2015. № 1. С. 33–37.

3. Гальперин П. Я. Организация умственной деятельности и эффективности учения // Теория учения: хрестоматия. Ч. 1 / под ред. Н. Ф. Талызиной, И. А. Володарской. М. : Помощь, 1996. 139 с.

4. Лаптенков Б. К., Тихомиров Ю. В. Опыт организации и проведения виртуального лабораторного практикума по курсу физики // Физическое образование в вузах. 2005. № 2. С. 90–100.

5. Эшназарова М. Ю. Применение электронных учебников в учебном процессе // Молодой ученый. 2013. № 9. С. 433–434.

6. Федоров И. Б. О концепции инженерного образования // Высшее образование России. 1999. № 5. С. 3–9.

Статья представлена научным руководителем,
кандидатом педагогических наук, доцентом Первушиной М. О.

УДК 621.375.026

В. В. Черненко (магистрант, СПбГУТ)

РАБОТА КЛЮЧЕВОГО ГЕНЕРАТОРА РЕЖИМА *E* НА НЕЛИНЕЙНУЮ НАГРУЗКУ

Объектом исследования является высокоэффективный транзисторный ключевой генератор, работающий на выпрямляющую антенну (rectenna), предназначенную для преобразований СВЧ колебаний в энергию постоянного тока. Проводится анализ схемы и формулируются условия согласования СВЧ генератора с нелинейной нагрузкой.

микроволновые ключевые усилители мощности, rectenna, нелинейная нагрузка.

Работа ключевого генератора с внешним возбуждением (усилителя мощности класса Е) на выпрямитель представляет большой практический интерес. Подобное устройство в литературе получило название DC-DC конвертора класса Е (рис. 1) [2].

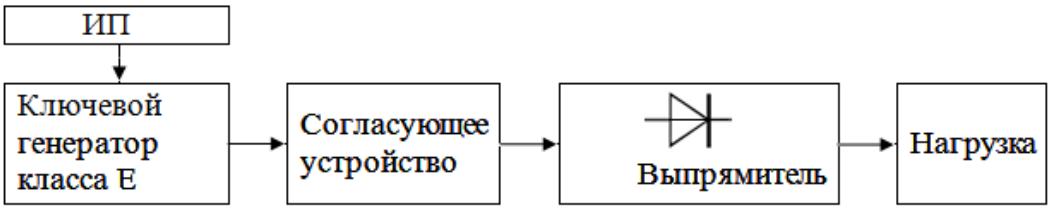


Рис. 1. Структурная схема DC-DC конвертора класса Е

Благодаря реализации мягкого режима переключения транзистора в режиме *E* (переключение в нуле напряжения и $du/dt = 0$) резко снижаются потери мощности, особенно на высоких частотах (10–100 МГц). Создание миниатюрных высокоэффективных резонансных преобразователей для радиоаппаратуры связано именно с использованием режима Е на этих частотах. Более высокие частоты (до 1–1,5 ГГц и выше) также представляют интерес для решения проблемы беспроводной передачи СВЧ энергии и ее преобразования в энергию постоянного тока (Rectifying antenna) (рис. 2). [1, 3].

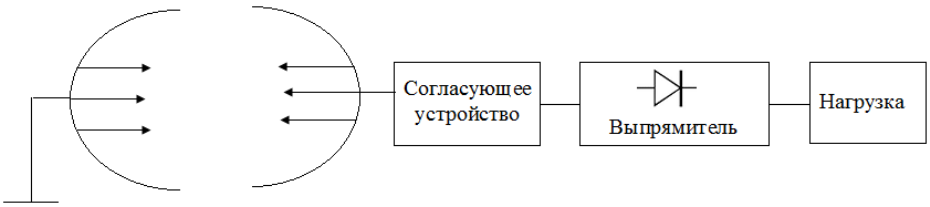


Рис. 2. Rectifying antenna

Для реализации режима *E* при работе генератора на выпрямитель необходимо обеспечить на рабочей частоте со стороны входа выпрямителя требуемое (оптимальное) резистивное сопротивление. Схема на рисунке 3 представляет собой выпрямитель с диодом Шоттки, на входе которого действует СВЧ колебание, которое требуется преобразовать в энергию постоянного тока.

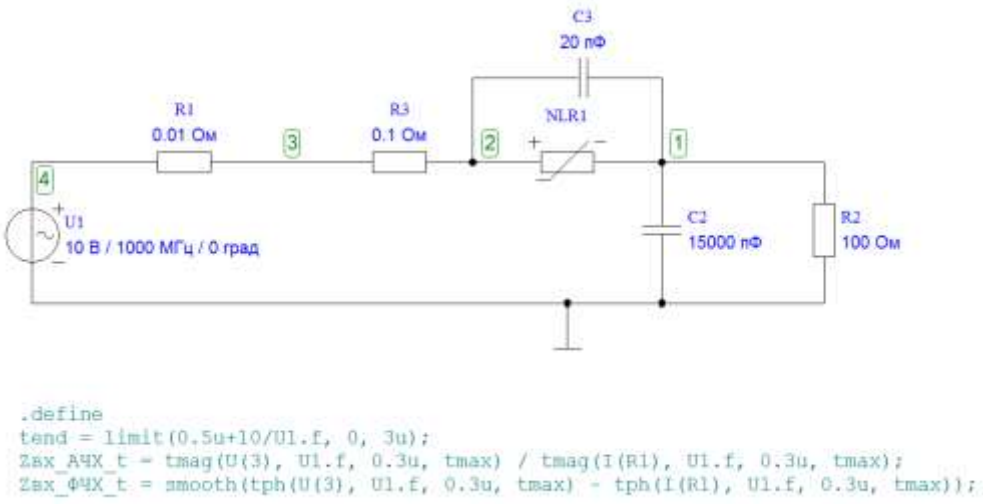


Рис. 3. Компьютерная модель выпрямителя с диодом Шоттки

Задачей исследования в последней главе диссертации и темой данного доклада было компьютерное моделирование частотной зависимости модуля и фазы входного сопротивления нелинейного двухполюсника с нагрузкой, которое в целом представляет собой выпрямитель. Модель диода Шоттки, которая была использована, состоит из нелинейного резистора с соответствующей ВАХ, зашунтированная небольшой емкостью C3 (20 пФ, учтены потери диода резистором R3), емкость C2 представляет собой сглаживающий фильтр, уменьшающий остаточные пульсации ВЧ/СВЧ-колебаний.

Методом гармонической линеаризации с использованием программы FASTMEAN определялась амплитуда и фаза первой гармоники напряжения в точке 3 и соответственно тока, протекающего в этой ветви (R1). Для интересующего диапазона частот вычислялось отношение амплитуд напряжения к току и сдвиг фаз между ними, что и определяло модуль и фазу комплексного сопротивления данного двухполюсника. Необходимо отметить, что погрешность метода гармонической линеаризации зависит от уровня высших гармоник тока через диод. На рисунке 4 представлена осциллограмма тока для частоты воздействия 1 ГГц и соответствующий ей спектр. Из анализа представленных зависимостей видно, что уровень высших гармоник значителен, что может привести к значительной погрешности метода гармонической линеаризации. Увеличение частоты воздействия до 2 ГГц приводит к существенно лучшему результату (рис. 5).

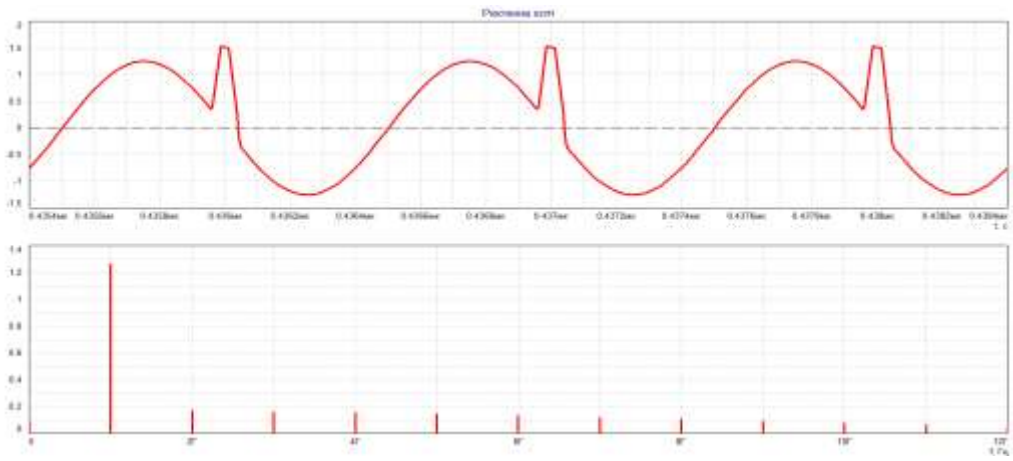


Рис. 4 Осциллограмма тока через диод для частоты воздействия 1 ГГц
и соответствующий ей спектр

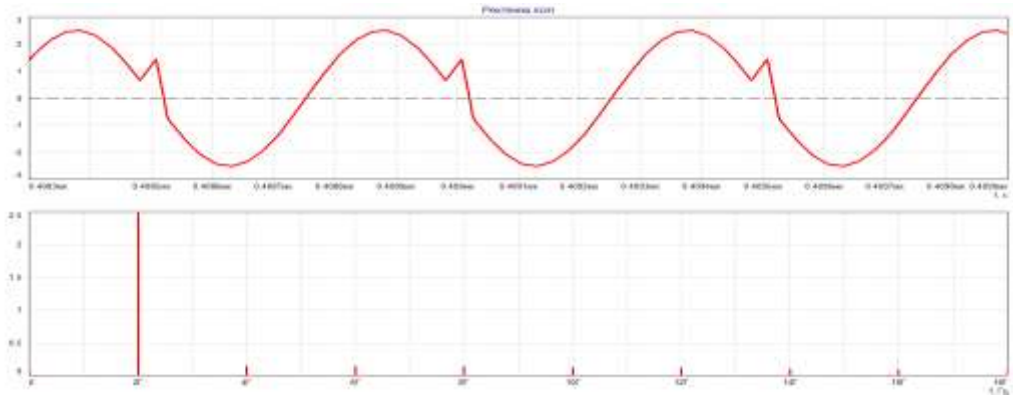


Рис. 5. Осциллограмма тока через диод для частоты воздействия 2 ГГц
и соответствующий ей спектр

Для параметров модели, приведенной на рисунке 5 результаты компьютерного расчета по указанной методике, приведены на рисунке 6.

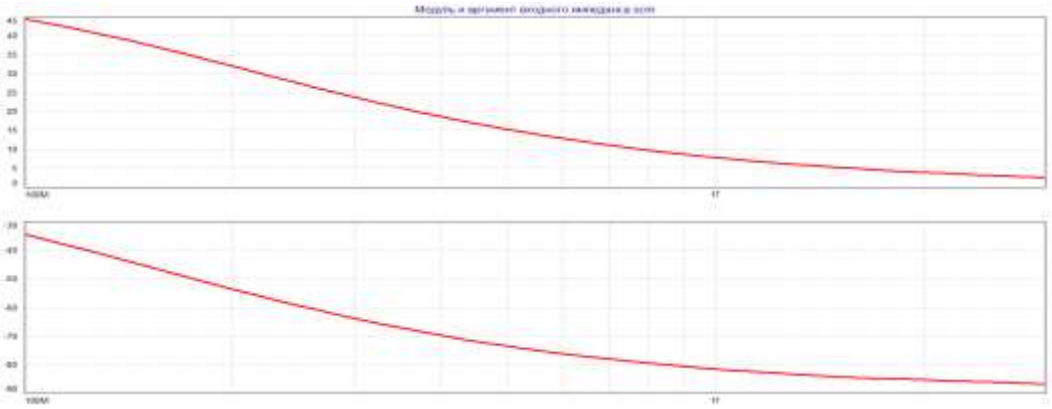


Рис. 6. Результаты компьютерного расчета модуля (*a*)
и аргумента (*b*) комплексного входного сопротивления нагруженного выпрямителя

Полученные частотные зависимости позволяют заменить нелинейную цепь диода и нагрузки на рабочей частоте эквивалентным комплексным

сопротивлением. Так, например, как следует из графика, для рабочей частоты 2 ГГц модуль сопротивления составляет 4 Ом, а фаза – 85 градусов, т.е. преобладает емкостная составляющая. Полученные данные являются основой для расчета согласующей цепи, обеспечивающей режим Е микроволнового генератора.

По формулам, известным из курса теории цепей проведен расчет эквивалентной схемы. Линейная эквивалентная цепь выпрямителя с нагрузкой 100 Ом на частоте 2 ГГц имеет вид рисунка 7:

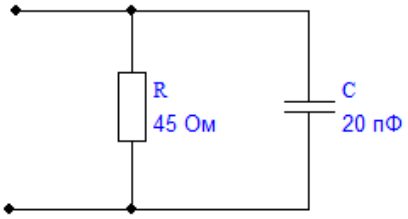


Рис. 7. Линейная эквивалентная цепь выпрямителя

С целью компенсации емкости C на рабочей частоте $f = 2$ ГГц необходимо добавить резонансную индуктивность $L = 0{,}64$ нГн. Эквивалентная схема генератора будет иметь вид рисунка 8.

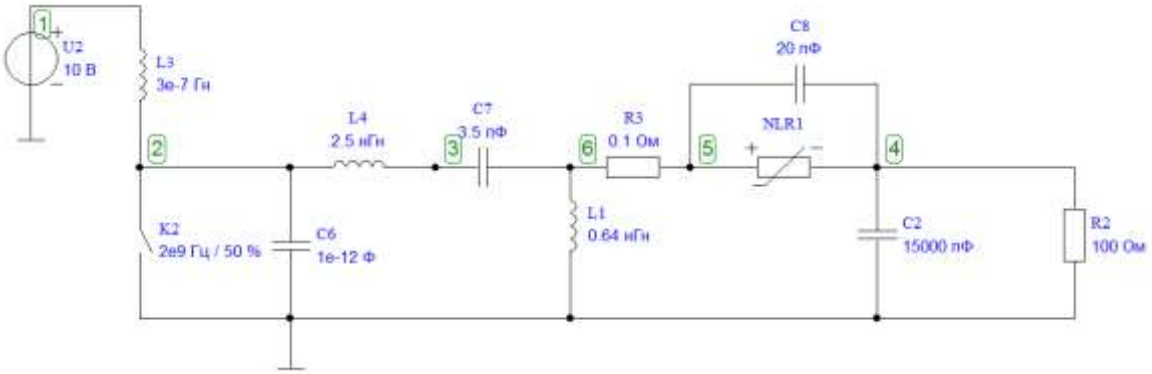


Рис. 8. Компьютерная модель эквивалентной схемы генератора, работающего на выпрямитель

Осциллограммы напряжения и тока на транзисторе для схемы рисунка 8 приведены на рисунке 9. Таким образом, проведенное согласование позволяет реализовать режим Е при работе ключевого генератора на нелинейную нагрузку.

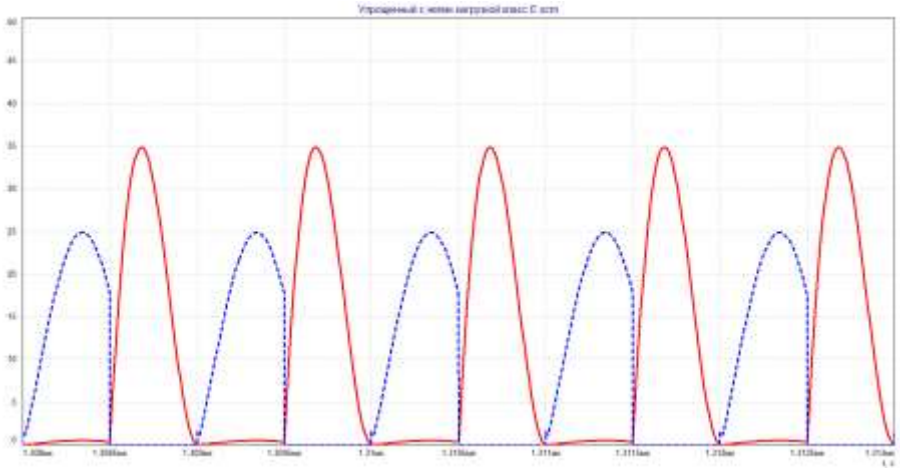


Рис. 9. Кривые напряжения и тока на транзисторном ключе (транзистор на GaN)

Список используемых источников

1. Ching-Hong K. Chin, Quan Xue, Chi Hou Chan. Design of a 5.8-GHz Rectenna Incorporating a New Patch Antenna. IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, VOL. 4, 2005.

2. Dr. Andrei Grebennikov, Nathan O. Sokal, Marc J. Franco. Switchmode RF Power Amplifiers. UK: Elsevier Inc., 2012.

3. J. A. G. Akkermans, M. C. van Beurden, G. J. N. Doodeman, and H. J. Visser. Analytical Models for Low-Power Rectenna Design . IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, VOL. 4, 2005 187.

Статья представлена научным руководителем,
доктором технических наук, профессором Филиным В. А.

ЭКОНОМИКА И УПРАВЛЕНИЕ В СВЯЗИ

УДК 621.398

М. В. Авраменко (студент группы ИКТК-27, СПбГУТ)
В. А. Диптан (аспирант, СПбГУТ)

ИССЛЕДОВАНИЕ СПРОСА НА M2M РЕШЕНИЕ ДЛЯ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА ОКРУЖАЮЩЕЙ СРЕДЫ

У технологии межмашинных коммуникаций есть огромный потенциал для улучшения охраны окружающей среды, она может приносить пользу различным формам сельского хозяйства, производить замеры качества воздуха и т. д. В статье рассматриваются результаты маркетингового исследования, проводимого путем анкетирования людей на улице.

machine-to-machine, интернет вещей, маркетинг, носимые устройства, качество воздуха.

В современном мире нас окружает огромное количество устройств – бытовая и офисная техника, всевозможные системы охраны и безопасности, промышленное оборудование: датчики, системы доступа, измерительные и контрольные системы и т. д. Многие из них требуют постоянного мониторинга, контроля, выставление определенных параметров, или сбора данных, измерений. В большинстве случаев требуется обеспечение передачи данных или сигналов управления к таким устройствам, а так же получения информации от них. Именно это и называется M2M технологии (*Machine-to-Machine*). M2M технологии уже используются с целью улучшения состояния окружающей среды, например для вывоза мусора, переработки нефти, переработки электрических лампочек, сокращения выбросов CO2, контроля шумового загрязнения, очистки сточных вод [1]. Регулярные измерения состояния атмосферы в крупных мегаполисах помогут не только понять жителям чем они дышат, но и помочь государственным органам бороться с опасными загрязнениями. Согласно обзору исследовательской компанией Garthner [2] технология M2M среди 2 тыс. технологий отмечена как одна из наиболее востребованных, позволяющих получить хорошую обратную связь от современного потребителя, значительно улучшить качество существующих продуктов и сервисов. Разрабатывае-

мый проект нацелен решить задачи мониторинга окружающей среды, а так же иметь минимальную сложность интеграции устройств и отображать данные от датчиков с любых устройств в режиме реального времени.

Суть проекта заключается в разработке бюджетного и надежного носимого устройства контроля за качеством воздуха. Современный рынок носимых медицинский устройств, способных контролировать физическое состояние организма, его двигательную активность, находится в стадии активного роста [3]. Из этого развивается и новая потребность – контролировать не только свое внутреннее состояние, но и состояние происходящего в окружении человека, то что также непосредственно влияет на состояние человека. К сожалению, у потребителя нет возможности измерить основные показатели окружающего воздуха, и тем более сравнивать их. На рынке представлено значительное количество приборов по контролю за качеством воздуха, но все они являются либо профессиональными для специалистов в области экологии и вентиляции, либо стационарными домашними приборы. Носимые приборы, которые были бы общедоступны по цене и интерфейсу, на рынке только начинают появляться.

Помимо общего для всех желания наблюдать за состоянием окружающего воздуха, у людей есть и другие важные мотивы к приобретению данного прибора. Одним из мотивов станет значительное загрязнение воздуха в мегаполисах. Имея данный прибор, потребитель сможет с легкостью сравнить загрязнённость воздуха в районе где он работает и где проживает, более того, вероятно, что данная информация позволит выбрать оптимальное место для проживания и побудит потребителей выбирать более экологически чистые места. Еще одним немаловажным мотивом является контроль за концентрацией пыльцы и аллергенов в воздухе, что с учетом растущего числа аллергиков немаловажно. С учетом вышесказанного можно сделать вывод, что предпосылок к востребованности данного продукта много и для авторов статьи встала цель исследовать реальную востребованность подобного гаджета.

Целью данного исследования является изучение потребности у людей живущих в крупных мегаполисах в подобных устройствах. Для проведения исследования был составлен список из 40 респондентов. Для выявление отношения у разных возрастных категорий граждан к новым инновационным устройствам и сервисам была сделана выборка по возрастному критерию:

1) до 30 лет,
2) до 50 лет,
3) свыше 50 лет.

Был выбран разведочный тип исследования, так как производился предварительный анализ информации, необходимой для более глубокого понимания задачи. Для проведения эксперимента был выбран полевой метод, то есть проводилось анкетирование людей на улице.

Анкетирование состояло из следующих вопросов:

1) Пользуетесь ли вы современными устройствами такими как: фитнес браслеты, умными мультиварками и т. п.? Каково ваше отношение к подобным устройствам?

2) Хотели бы вы себе приобрести устройство со встроенным датчиком качества воздуха, датчиком температуры, влажности, давления и с удобным приложением на своей смартфон?

3) Какова, на ваш взгляд приемлемая цена, за которую вы бы готовы были купить подобное устройство?

4) Удобно ли вам было бы получать уведомления на свой смартфон от устройства, например, при изменении каких-нибудь параметров, влажности в комнате или температуры за окном?

5) Что бы вы хотели добавить в устройство и каким вы его видите?

Результаты ответа на первый вопрос анкеты среди группы респондентов до 30 лет – 23 человека. Из 23 человек 19 ответили о том, что используют подобные устройства, у 4 человек подобных устройств нет, но они отнеслись к ним весьма положительно и хотели бы приобрести в будущем.

На первом графике показаны результаты ответов на первый вопрос у группы респондентов до 50 лет – 10 человек. На данном графике наблюдается противоположная тенденция. Из 10 опрошенных респондентов лишь двое ответили положительно, остальная группа ответила отрицательно, отметив, что в подобных устройствах пока не нуждаются либо не интересовались.

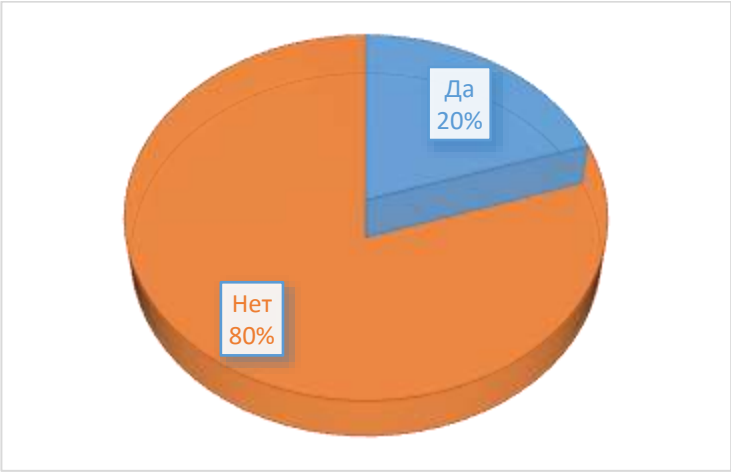


Рис. 1. Результаты ответа на первый вопрос
среди категории граждан в возрасте до 50 лет

У граждан в категории “свыше 50 лет” – 7 человек, не было представления о подобных устройствах.

На вопрос “Хотели бы вы приобрести устройство, разрабатываемое в проекте?”, первая группа респондентов до 30 лет ответила в 96 % случаев – положительно – это 22 человека. Один опрошенный не захотел бы

приобрести подобное устройство, так как посчитал, что данный сервис можно реализовать в приложении для смартфонов.

Среди группы опрошенных до 50 лет – 60 % (6 человек) ответили положительно и заинтересовавшись подобным девайсом. Остальные 40 % ответили отрицательно аргументировав, что в подобных сервисах не нуждаются. Группа респондентов свыше 50 лет ответили отрицательно.

На вопрос о стоимости подобного устройства 65 % – 15 человек ответили, что готовы бы купить устройство в ценовой категории 1 500–2 000 р., 35 % – 8 людей готовы были отдать за подобный девайс 1 000–1 500 р. Категорию от 500–1 000 р. никто не выбрал (рис. 2).

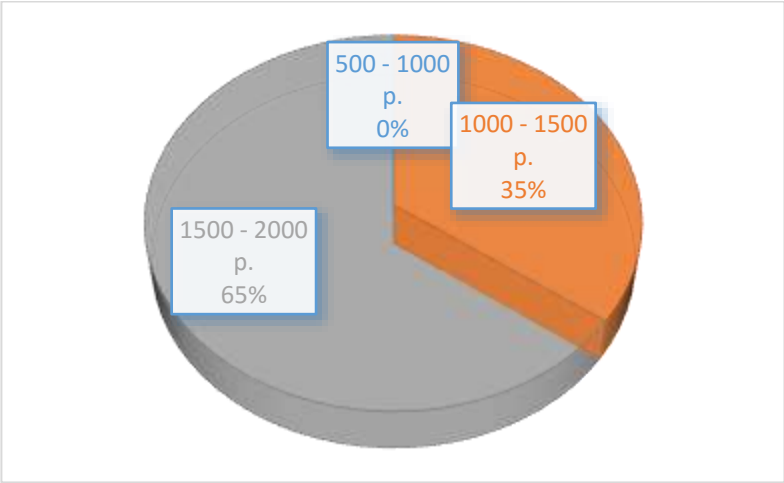


Рис. 2. Результаты ответа на третий вопрос
среди категории граждан в возрасте до 30 лет

Среди опрошенных респондентов в возрасте до 50 лет результаты практически одинаковые рис.3. Семь опрошенных готовы были заплатить за девайс от 1 500–2 000 р., четверо выбрали второй вариант ответа – 1 000 1 500 р. Категорию от 500–1 000 р. так же никто не выбрал.

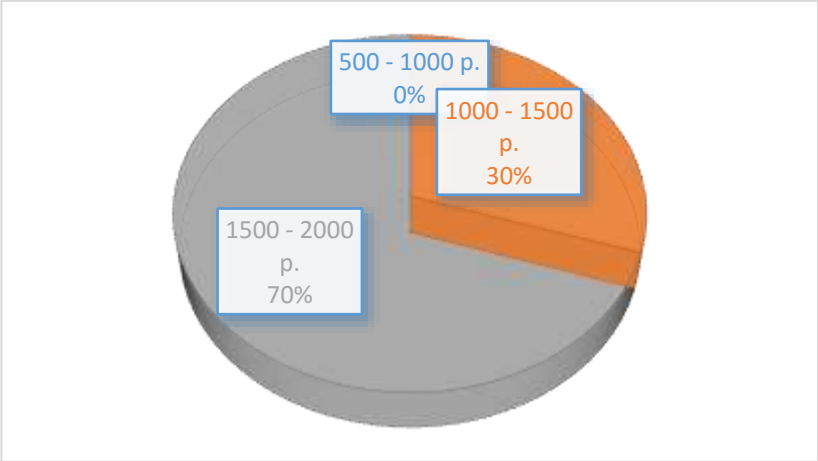


Рис. 3. Результаты ответа на третий вопрос
среди категории граждан в возрасте до 50 лет

Среди опрошенных людей в возрасте от 50 лет – 4 человека выбрали ответ 1 000–1 500 р., остальные опрошенные воздержались от ответа.

На четвертый вопрос о уведомлениях на смартфон, в группе респондентов до 30 лет, положительно ответило все 100 %, отметив как полезную функцию. Группа опрошенных людей до 50 лет, так же отметили данную функцию полезной. Среди респондентов свыше 50 лет данная функция не вызвала особого интереса, пояснив это тем что удобнее было использовать устройство в стационарном режиме с дисплеем.

На вопрос о том, чтобы вы хотели добавить в устройство и каким вы его видите, многие затруднялись ответить. Во многих ответах респонденты желали добавить простоту в установке устройства: «открыл, установил, подключил к смартфону и все». Некоторые предлагали добавить функцию дистанционного управления, подсветку, режим наименьшего энергопотребления и режим озвучивания текста. Еще одним предложением было добавить линейку подобных устройств с разной комплектацией, например, только с датчиком влажности, либо с датчиком качества воздуха.

Выводом данного исследования можно указать, что большинство анкетированных людей было заинтересовано в подобных решениях и сервисах. Как видно из результатов опроса больший интерес проявила группа респондентов до 30 лет. Уже сейчас видно, что M2M все крепче связывается с автоматизацией, особенно это видно в домашнем сегменте и будет продолжать развиваться в ускоренном темпе роста.

Список используемых источников

1. Stryjak J., Sharma A. Analysis Agricultural machine-to-machine (Agri M2M): a platform for expansion // GSMA. 2015.

2. Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor [Электронный ресурс]. URL: http://www.gartner.com/newsroom/id/3114217.

3. Маляревский А. IDC о рынке носимых устройств // Инновации в ИТ. 2015. N7-8 [Электронный ресурс]. URL: http://www.crn.ru/numbers/reg-numbers/ detail. php? ID=104051.

Статья представлена научным руководителем,
доктором экономических наук, профессором Макаровым В. В.

УДК 339.113

А. П. Баулина (студентка группы ИКТЗ-24, СПбГУТ)
Ю. Р. Шарафитдинова (студентка группы ИКТЗ-24, СПбГУТ)

УНИВЕРСАЛЬНЫЙ МЕССЕНДЖЕР

В статье рассмотрена проблема с использованием большого числа современных мессенджеров и переключением с одного мессенджера на другой. Для ее решения было проведено исследование, показывающее потребность среди молодежи создания универсального мессенджера, который включил бы в себя наиболее популярные существующие мессенджеры. По результатам проведённого исследования сделаны выводы о создании универсального мессенджера.

универсальный мессенджер, messenger, социальные сети, исследование, сообщения, приложения, iOS, Windows, Android.

Приложение было условно названо «Универсальным мессенджером», так же и мы его будем называть в этой статье.

Коммуникации между людьми сегодня достигли высочайшего уровня технологичности. Прогресс в области компьютерных и мобильных разработок сделал возможным обмен сообщениями за считанные секунды (или мгновенно). Это позволяет людям общаться в режиме реального времени, находясь при этом даже за сотни тысяч километров друг от друга. С помощью системы мгновенных сообщений обмениваться можно не только текстовыми посланиями, но также изображениями, звуковыми сигналами и видеозаписями. На сегодняшний день действительно существует множество социальных сетей, пользующихся большой популярностью, легкий доступ к каждой из которых могут получить владельцы смартфонов, установив соответствующее приложение.

Наверняка многие задумывались, – а если бы все мессенджеры соединились в одно единое приложение? Нельзя сказать, что все мессенджеры повторяют функционал друг друга, но каждый сервис имеет свои уникальные стороны. А постоянное переключение между мессенджерами часто утомляет.

В связи с вышесказанным у потребителя возникает проблема с использованием большого числа современных мессенджеров и переключением с одного мессенджера на другой. Для решения подобной проблемы мы поставили перед собой цель исследовать потребность среди молодежи создания универсального мессенджера, который включил бы в себя наиболее популярные существующие мессенджеры. Давайте же разберемся с тем, что такое мессенджер, каким он может быть и какие возможности он дает современным пользователям.

Messenger – от английского "курьер" или "связной". Это программа для мгновенного обмена сообщениями между пользователями. Именно в скорости состоит его главное преимущество перед обычной электронной почтой. Здесь послание передается невероятно быстро, тогда как обновление почтового ящика происходит раз в несколько минут.

Мы провели исследование среди студентов СПбГУТ разных факультетов. Средний возраст более чем 150 опрошенных преимущественно составляет 18–25 лет.

Среди них 37,6 % женщин и 62,4 % мужчин.

Как выяснилось далее, 92,7 % от общего числа опрошенных имеют современные смартфоны.

Большей популярностью пользуются мобильные устройства на базе операционной системы Android (55,7 %), второе место занимает iOS (35 %) а тройку лидеров замыкает Windows Phone (6,4 %).

Для любого обладателя мобильного устройства, если он является активным пользователем социальных сетей, важно получать уведомления или сообщения, следить за новостной лентой и быть в курсе всех событий. Решением стали приложения, разработанные социальными сетями для удобного доступа к сервису. Такие приложения оказались очень популярными среди нашей аудитории. 98,6 % опрошенных используют их. Однако интерес пользователя, как правило, не ограничивается одним-двумя сервисами. На сегодняшний день существует ряд наиболее популярных среди пользователей мессенджеров. Мы спросили, какими приложениями пользуются владельцы телефонов. Самыми популярными оказались Вконтакте, Skype, Instagram, Viber, WhatsApp, Telegram, iMessage, Facebook, их используют более 20 % респондентов (рис. 1).

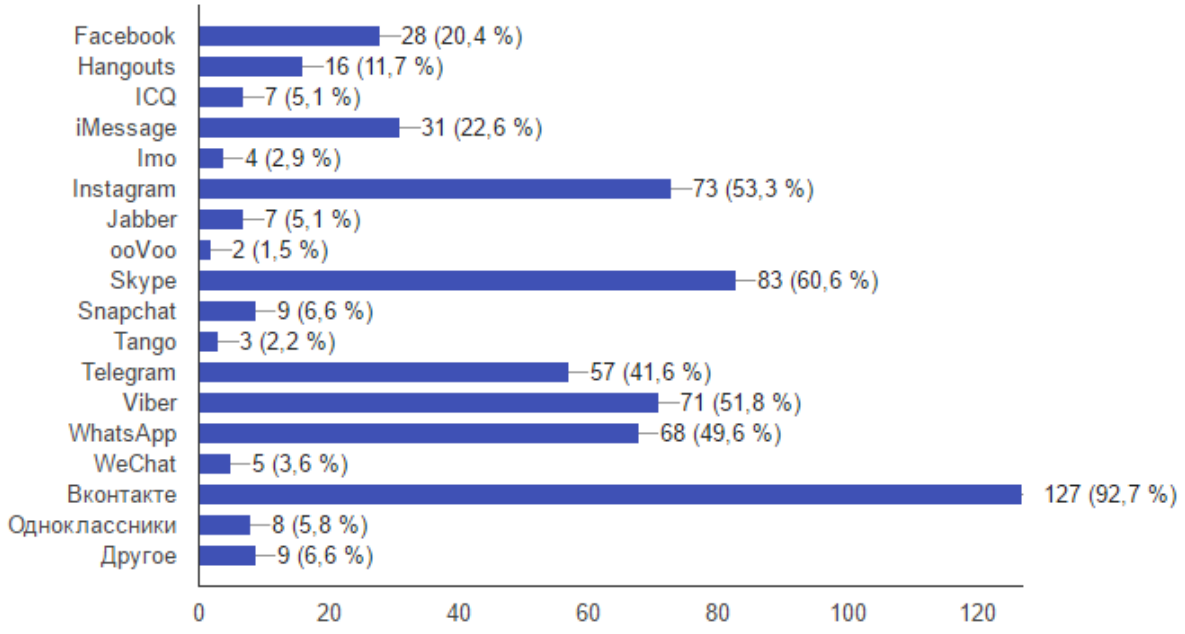


Рис. 1. Используемые приложения социальных сетей

Между тем, остановиться на одном мессенджере современному пользователю просто не получается. Как видно из графика, любой из опрошенных использует как минимум один, а чаще всего одновременно несколько мессенджеров. Редко кому удается подобрать такой, который использовался бы всеми его знакомыми.

Каждая из социальных сетей предоставляет определенные сервисы для общения, но количество таких сервисов ограничено удобством доступа к ним, поэтому каждая сеть имеет свой набор предоставляемых услуг, и, если этот набор не удовлетворяет вашим потребностям, вам приходится использовать несколько приложений.

98,6 % опрошенных используют приложения на смартфоне именно для общения в социальных сетях. И не удивительно, ведь некоторые социальные сети создавались исключительно, как приложения для телефонов. Другие же соц. сети наоборот первоначально были созданы в web-интерфейсе. Но, наверное, каждая социальная сеть сейчас имеет свое приложение для удобного пользования на смартфоне. Мы спросили, хотел бы пользователь объединить все приложения в одном? 60,3 % опрошенных ответили «да» (рис. 2).

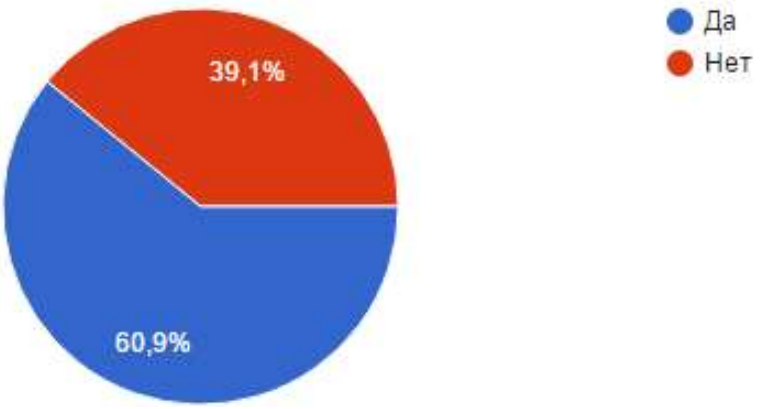


Рис. 2. Потребность в объединении нескольких приложений социальных сетей

По результатам исследования мы определили, что «Универсальный мессенджер» будет пользоваться спросом среди аудитории. Мы предлагаем разработчикам выпустить приложение в 2 видах, бесплатная версия с рекламой и ограниченным функционалом, и платная версия. Оба варианта нашли своих почитателей (рис. 3, 4).

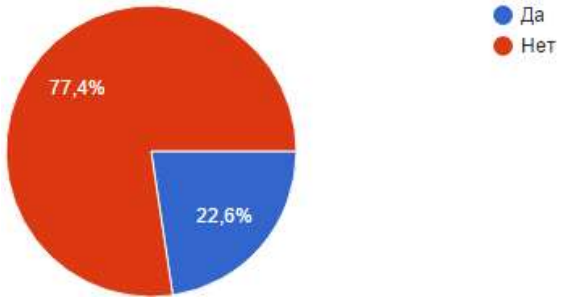


Рис. 3. Готовность потребителей платить за приложение

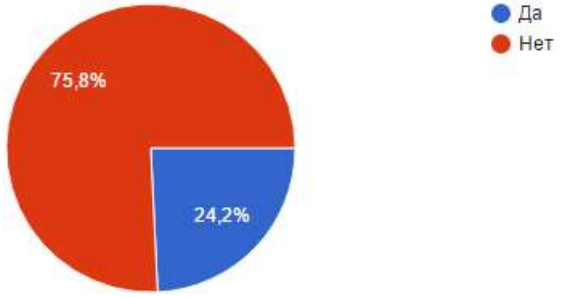


Рис. 4. Готовность потребителей платить за версию без рекламы

На данный момент уже были попытки создания прототипа данного мессенджера. Однако, почему они не увенчались успехом? Они не обладали необходимым пользователю функционалом.

В ходе исследования мы пообщались с разработчиками приложений для мобильных устройств и узнали их профессиональное мнение: потребуется весьма много времени потратить, чтобы обеспечить необходимую безопасность, подстроить приложение под все API и адаптировать на все устройства.

О том, что такое мессенджер, знает сегодня каждый. Это непременный атрибут современного общества, позволяющий выстраивать коммуникации и общаться легко, быстро и часто бесплатно. Наличие Интернета сегодня – не проблема, он есть везде. А потому мессенджеры активно вытесняют (и довольно успешно) SMS как самостоятельный способ связи. Выбор удобных и многофункциональных сетей мгновенного обмена сообщениями с каждым годом становится все шире.

По-настоящему универсальный мессенджер может не появиться никогда, но появление опции соединения с различными аккаунтами из одной программной оболочки могло бы стать замечательной функцией для множества пользователей.

Список используемых источников

1. Система мгновенного обмена сообщениями [Электронный ресурс] // Википедия – свободная энциклопедия: [сайт]. URL: http://ru.wikipedia.org/?oldid=77950828 (дата обращения 20.06.2016).

2. Службы мгновенных сообщений, или мессенджеры, постепенно замещают сервис SMS-сообщений. А вы еще не отказались от устаревших «эсэмэсок»? [Электронный ресурс] // Известия: [сайт]. URL: http://izvestia.ru/news/552406#ixzz4D2VxnOiy (дата обращения 20.06.2016).

3. Кузнецов А. Franz – универсальный мессенджер с Telegram, WhatsApp, Skype и другими сервисами [Электронный ресурс] //. URL: http://w7phone.ru/franz-universalnyj-messendzher-s-telegram-whatsapp-skype-i-drugimi-servisami-131312/ (дата обращения 20.06.2016).

4. Силонов А. Мобильные мессенджеры вытеснили sms // Ведомости – электронное периодическое издание: [сайт]. URL:

http://www.vedomosti.ru/technology/articles/2013/04/29/mobilnye_messendzhery_vytesnili_sms (дата обращения 20.06.2016).

Статья представлена научным руководителем,
ассистентом Диптаном В. А.

УДК 338.4

М. П. Белянчикова (аспирант, МТУСИ)

МОДЕЛИРОВАНИЕ ФИНАНСОВОЙ УСТОЙЧИВОСТИ КОМПАНИЙ ПОДВИЖНОЙ СВЯЗИ

Специфические черты финансовых ресурсов компаний подвижной связи определяют необходимость использовать для прогнозирования финансовой устойчивости специальных эконометрических моделей финансового прогнозирования. Представлена разработанная эконометрическая модель оценки перспективной финансовой устойчивости организаций подвижной связи.

подвижная связь, финансовые ресурсы, финансовая устойчивость.

Важнейшим, завершающим этапом анализа финансового состояния организаций подвижной связи является оценка перспективной финансовой устойчивости. Вопросам финансового управления и прогнозирования в отрасли телекоммуникаций посвящены работы Т. А. Кузовковой, В. Б. Козлова, Р. Н. Накозина, Г. Н. Шаманского, О. И. Шаравовой, Ю. С. Тереховой. Необходимость применения для прогнозирования финансовой устойчивости компаний подвижной связи специфичной эконометрической модели обусловливает актуальность создания такой модели.

В зарубежной литературе для прогнозирования вероятности банкротства предлагаются модели Э. Альтмана, У. Бивера, Э. Таффлера. Однако их применение в современных условиях российской экономики для оценки возможной платежеспособности компаний подвижной связи видится весьма проблематичным в силу несоответствия как весовых коэффициентов, так и экзогенных переменных внешним и внутренним условиям деятельности.

В национальной экономике России роль подвижной связи в настоящее время определяется ее принадлежностью к производственной и социальной инфраструктуре. Доступность и качество предоставления услуг подвижной связи относятся к всеобщим условиям, без которых

невозможны нормальное функционирование производства и обращения товаров, а также жизнедеятельность людей.

Необходимость применения специфичных методов хозяйствования, принципов государственного регулирования и экономических взаимоотношений на рынке услуг предопределены инфраструктурной ролью подвижной связи в экономике страны и сетевым характером производства ее услуг. Особенности состояния и использования производственных ресурсов подвижной связи обусловлены своеобразием действия экономических законов в секторе подвижной связи, возникающим вследствие специфики производимого ею продукта – услуг, особенностями состава и структуры производственных ресурсов, технологий и организации процессов передачи информации и потребления услуг [1, с. 8].

Финансовые ресурсы, включающие основной и оборотный капитал, являются одним из важнейших видов ресурсов, необходимых для производства услуг подвижной связи.

Особенности финансов отрасли инфокоммуникаций и специфика структуры активов и пассивов организаций подвижной связи, невещественный характер продукта и оказание услуг различным группам потребителей, как юридическим, так и физическим лицам, определяют особые, отличные от других отраслей производства, состав, состояние, движение и процесс использования финансовых ресурсов [2, с. 35].

Невещественный характер продукции – услуг подвижной связи определяет незначительный размер запасов, в том числе сырья и материалов, в активах организаций подвижной связи [3, с. 84].

Удельный вес оборотных средств в структуре финансовых ресурсов организаций подвижной связи так же значительно невелик. Их доля в общей стоимости активов операторов подвижной связи составляет лишь 7–23 %, в то время как российские предприятия отраслей материального производства демонстрируют наличие оборотных средств в размере не менее 40 % активов.

Удельный вес основных средств в структуре имущества в виде дорогостоящих сооружений, базовых станций, оборудования, сетей, аппаратно-программных средств для производства услуг занимает ведущее положение, которое предопределено необходимостью своевременного и полного удовлетворения потребностей пользователей в доступности и качестве услуг подвижной связи.

На долю дебиторской задолженности крупнейших национальных операторов подвижной связи приходится более 50 % оборотных средств, вследствие преобладания в системе оплаты услуг тарифных планов с постоплатной системой расчетов, широкому применению которой способствует конкуренция на рынке услуг подвижной связи.

Вышеприведенные факторы, характеризующие особенности формирования и использования финансовых ресурсов российских операторов подвижной связи, оказывают структурно-стоимостное влияние на значения показателей финансовой устойчивости, а также такие показатели, как платежеспособность и ликвидность.

Результатом этого влияния стало использование для оценки текущего финансового состояния организаций подвижной связи особых, отличных от используемых в финансовом анализе предприятий других отраслей национальной экономики, нормативных ограничений ряда важнейших финансовых показателей (коэффициента маневренности, коэффициента обеспеченности оборотных средств собственными источниками, коэффициента ликвидности) в целях достоверной и объективной оценки их реального финансового положения [3, с. 85].

Перспективная финансовая устойчивость организации подвижной связи, отражающая такое состояние финансовых ресурсов, при котором организация, свободно маневрируя денежными средствами, способна путем их эффективного использования обеспечить непрерывный процесс производства и реализации услуг подвижной связи, является важнейшим индикатором будущего состояния финансовых ресурсов, от которого зависит обеспечение нормального функционирования организации.

С учетом специфики деятельности, производства и потребления услуг, особенностей состава, структуры, движения и использования финансовых ресурсов сектора подвижной связи, рыночной среды и макроэкономической ситуации в целом, для прогнозирования финансового состояния организаций подвижной связи в соавторстве с О. И. Шаравовой автором статьи разработана *эконометрическая модель оценки перспективной финансовой устойчивости,* в которой в качестве экзогенных переменных выступают коэффициенты финансовой устойчивости, соотношения заемных и собственных средств, обеспеченности оборотных средств собственными источниками:

$$y = 0,659k_{\text{ФУ}} + 0,168k_{\text{З/С}} + 0,481k_{\text{ОС}},,$$

где $k_{\text{ФУ}}, k_{\text{З/С}}, k_{\text{ОС}}$ – коэффициенты финансовой устойчивости, соотношения заемных и собственных средств, обеспеченности оборотных средств собственными источниками соответственно.

Перспективное финансовое положение организации подвижной связи оценивается как устойчивое, если эндогенная переменная $y \geq 0$, в случае $y \prec 0$ – как неустойчивое.

Выбор эндогенной переменной представленной эконометрической модели оценки перспективной финансовой устойчивости организаций подвижной связи определен тем, что она представляет собой

относительную величину – удельный вес излишка или недостатка величины собственных и долгосрочных заемных источников формирования наиболее существенной для организаций подвижной связи доли оборотных активов в виде денежных средств и дебиторской задолженности в общем итоге баланса, являющийся основополагающей характеристикой финансовой устойчивости организации подвижной связи.

Оценка адекватности полученной эконометрической модели произведена на основании коэффициента детерминации и критерия Фишера – Снедекора. Значение коэффициента детерминации на уровне 0,87 свидетельствует о возможности использования эконометрической модели оценки перспективной финансовой устойчивости организаций подвижной связи в прогнозных целях, а допустимые значения критерия Фишера – Снедекора позволяют отклонить гипотезу о незначимости уравнения регрессии.

Список используемых источников

1. Кузовкова Т. А., Салютина Т. Ю., Шаравова О. И. Статистика инфокоммуникаций: учебник для вузов / под ред. проф. Т. А. Кузовковой. М. : Горячая линия – Телеком, 2015. 554 с.
2. Кузовкова Т. А., Шаравова О. И. Особенности финансовых ресурсов организаций инфокоммуникаций // Международный научно-исследовательский журнал. 2014. № 10–3 (29). С. 34–36.
3. Шаравова О. И. Методологические особенности диагностики финансового положения инфокоммуникационных компаний (DOI 10.18454/IRJ.2015.41.176) // Международный научно-исследовательский журнал. 2015. № 10 (41). Часть 1. С. 84–85.

Статья предоставлена научным руководителем,
кандидатом экономических наук, доцентом Шаравовой О. И.

УДК 004.056.53

Д. А. Гудков (студент группы ИКТЗ-24, СПбГУТ)
С. Е. Дмитриев (студент группы ИКТЗ-24, СПбГУТ)
В. С. Юхневич (студент группы ИКТЗ-24, СПбГУТ)

АНАЛИЗ ИСПОЛЬЗОВАНИЯ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯМИ СЕТИ INTERNET

В работе исследуются проблемы востребованности методов надёжной защиты аккаунтов в сети Internet, а также информированность опрошенных о возможных способах защиты. Рассматривается такое понятие, как многофакторная аутентификация (МФА), и одна из наиболее используемых её реализаций – двухфакторная аутентификация (ДФА).

многофакторная аутентификация, двухфакторная аутентификация, защита личных данных в сети Internet.

Согласно статье 23 Конституции Российской Федерации каждый имеет право на личную и семейную тайну, а также на тайну переписки, почтовых и иных сообщений.

Информация является одной из наибольших ценностей в современной жизни. С появлением глобальных инфокоммуникационных сетей доступ к ней стал чрезвычайно простым. В свою очередь, легкость и скорость доступа к информации ощутимо повысили угрозу безопасности данных в случае отсутствия достаточного уровня их защиты.

Практически у каждого пользователя Интернета имеется множество аккаунтов во всевозможных сервисах, таких как электронная почта (Hotmail, mail.ru, yandex), социальные сети (VK, Facebook, Instagram), универсальные аккаунты, которые используются одновременно для доступа к нескольким сервисам (Google, iCloud), сервисы цифрового распространения компьютерных игр и программ (Steam, Origin).

И всегда есть желающие получить несанкционированный доступ к чужим учетным записям. Причин для этого может быть множество, например, получение управления аккаунтами в социальных сетях для рассылки спама и прочтения личной переписки, потеря контроля над учетными записями в сервисах, занимающихся операциями с банковскими картами, может привести к краже денежных средств и т. д.

В связи с этим возникла необходимость защитить себя от атак злоумышленников. Традиционно для доступа к учетной записи используется пара логин-пароль. При помощи вредоносного ПО или фишинга атакующий легко может узнать логин и пароль при вводе их пользователем, поэтому необходимо помимо защиты паролем использовать дополнительные средства для предупреждения несанкционированного доступа. Такая модель защиты, при которой используется несколько средств аутентификации, называется многофакторной аутентификацией (МФА) [1].

Многофакторная аутентификация намного снижает риск кражи пользовательских учетных записей, так как знания пароля недостаточно для совершения взлома. Тем не менее, многие модели, построенные на МФА, уязвимы для схем взлома вида «человек в середине» (man in the middle).

Одним из типов многофакторной аутентификации является двухфакторная аутентификация (ДФА), или двухэтапная верификация. ДФА представляет собой схему авторизации пользователя с помощью комбинации двух компонентов (разных типов) [2].

Распространена такая схема ДФА, при которой при попытке входа в аккаунт с нового устройства помимо аутентификации по логину-паролю пользователя просят ввести код подтверждения, который можно получить по SMS или с помощью голосового вызова. Также он может быт взят из

списка заранее сгенерированных разовых кодов или при помощи специального приложения-аутентификатора, генерирующего код каждый определенный промежуток времени или по требованию пользователя.

Плюсами такой схемы являются:

- отсутствие нужды в дополнительных токенах – средств аутентификации, которым владеет пользователь – ведь мобильный телефон практически всегда под рукой;
- постоянная смена кода подтверждения, что уменьшает вероятность того, что его узнает злоумышленник.

К минусам данной реализации относятся такие проблемы, как

- необходимость наличия сигнала сети телефоном;
- возможность перехвата SMS;
- некоторая задержка при получении кода (увеличение времени, которое уходит на аутентификацию);
- смешение двух факторов в смартфоне, ведь он используется и как средство входа в аккаунт, когда на нем вводится пароль (первый фактор), и на него же приходит код подтверждения (второй фактор).

Тем не менее, такая реализация ДФА обеспечивает достаточный уровень защиты пользовательских данных от атак злоумышленников.

Целью нашего исследования является анализ использования ДФА в настоящее время. В ходе исследования был проведен опрос, большинством респондентов которого являются студенты обоих полов. Практически все из них обладают средствами связи, а 92 % многозадачными устройствами. Мы учитываем этот факт, так как рассматриваемая схема ДФА имеет второй фактор – одноразовый код, получаемый либо в SMS (и в смартфонах, и в старых телефонах) либо через специальное приложение – генератор паролей (только смартфоны). Также в современных устройствах существует большое количество приложений, требующих наличие персонального аккаунта.

Ожидаемо, у многих респондентов имеется множество аккаунтов в различных сервисах (рис. 1).

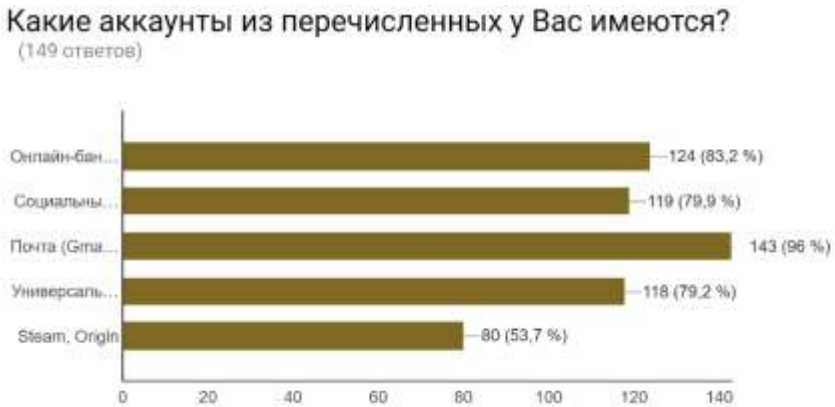


Рис. 1. Наличие аккаунтов у респондентов

Взломав ваш аккаунт, злоумышленник может получить доступ к вашим личным данным, переписке, фотографиям, а также использовать аккаунт для рассылки спама и обмана других пользователей (особенно из списка друзей) или кражи денег [3]. К краже денег можно отнести кражу аккаунта, в который вкладывались деньги.

В ходе опроса было установлено, что более половины респондентов подвергались взлому с разным ущербом для пользователя (рис. 2).

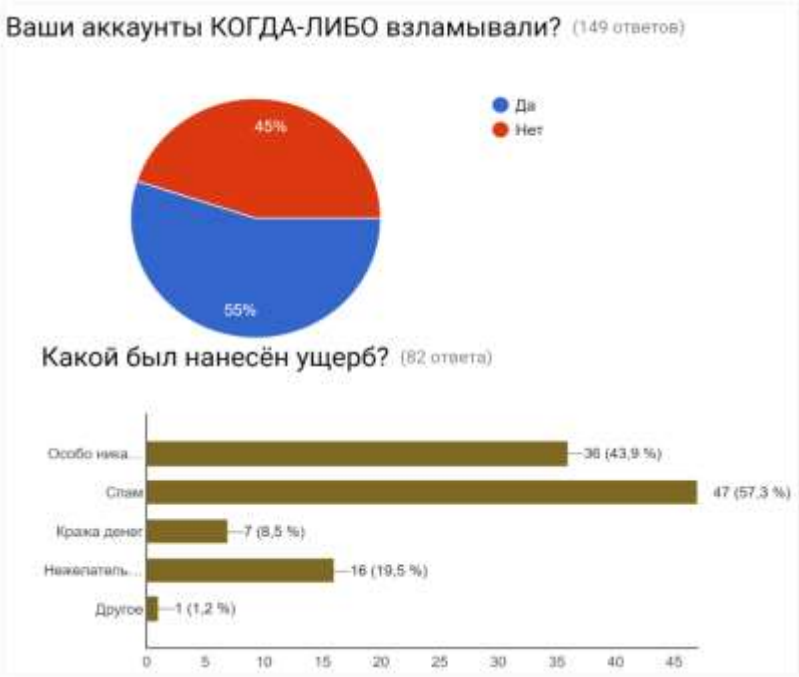


Рис. 2. Взлом аккаунтов

Большинство опрошенных для предотвращения повторных взломов придумывали более сложные пароли, что ненамного увеличивает уровень защиты, очень часто пароли крадут не подбором стандартных фраз, а с помощью фишинга, вирусов и т. д. Так что качество пароля в данном случае не повлияет на успешность атаки. Другая часть начала использовать ДФА, оставшиеся опрошенные не предпринимали мер по увеличению защищенности, создавая новый аккаунт (рис. 3).

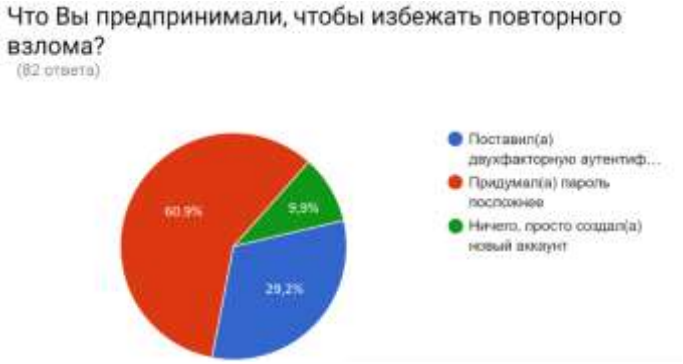


Рис. 3. Действия во избежание повторного взлома

Некоторые сервисы используют принудительную ДФА, например, банки при онлайн-оплате, входе в аккаунт на сайте или в приложении банка на мобильном телефоне. Также без подтверждения номера на устройстве нельзя войти в аккаунты Telegram, Viber и т. д. Также многие сервисы предоставляют пользователям возможность использовать их мобильные телефоны в качестве средства аутентификации, не принуждая их к этому.

По результатам проведенного исследования количество людей, использующих ДФА сейчас примерно равно количеству людей, обходящихся без неё (рис. 4).

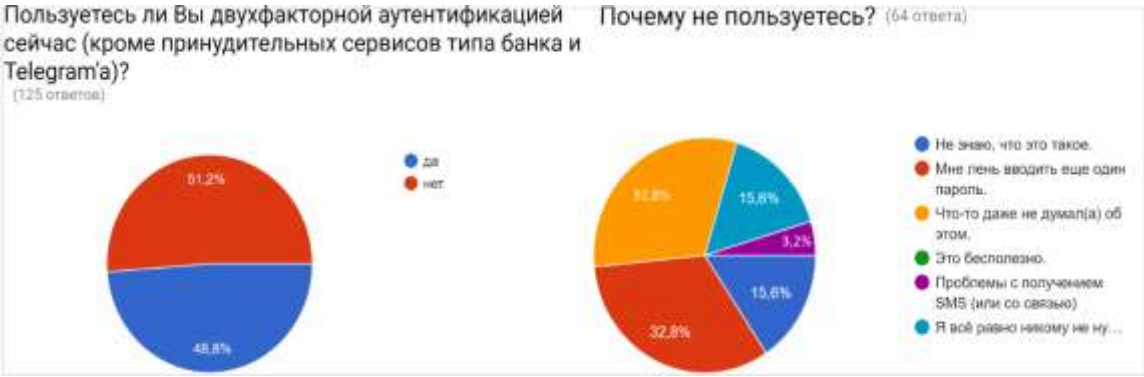


Рис. 4. Использование ДФА

На вопрос о том, почему респонденты не пользуются ДФА, самыми популярными вариантами стали лень и пренебрежение. Около 16 % опрошенных не представляют, что это за технология.

Использование ДФА не столь трудоёмко, как может показаться, так как введя код один раз, устройство можно добавить в список доверенных, и для него не понадобится вводить одноразовый код еще раз.

Если вы считаете, что Ваш аккаунт не может понадобиться злоумышленникам, то вы ошибаетесь, ведь различным базам пригодится ваша учетная запись для рассылки спама или обмана других пользователей, атакующий может получить доступ к Вашим электронным кошелькам, также, получив доступ к вашему устройству злоумышленник может его использовать для DDoS-атак на различные сайты и так далее. Стоит задуматься о том, чтобы лучше защитить свои устройства и аккаунты до того момента, как их взломают.

Выводы

Из результатов проведенного опроса можно сделать вывод о том, что не все пользователи осознают важность защиты своих аккаунтов в интернете. Хотя все больше и больше сервисов внедряют у себя технологию ДФА, многие продолжают использовать традиционную модель однофакторной аутентификации при помощи пароля. Причинами этому являются недостаточная осведомленность и недооценка возможной опасности.

Необходимо внедрять технологии многофакторной аутентификации в большее количество сервисов и настоятельно рекомендовать их использовать.

Список использованных источников

1. Важность многофакторной аутентификации [Электронный ресурс]. URL: http://www.securitylab.ru/analytics/425166.php
2. Двухфакторная аутентификация: что это и зачем оно нужно? [Электронный ресурс]. URL: https://blog.kaspersky.ru/what_is_two_factor_authenticatio/4272/
3. Всё о web-дизайне. Безопасность пользователя интернета [Электронный ресурс]. URL: http://wseweb.ru/diz/obzor7.htm

Статья представлена научным руководителем ассистентом Диптаном В. А.

УДК 316

Н. А. Остроущенко (студент группы ИКТЗ-24 СПбГУТ)
М. В. Рогалев (студент группы ИКТЗ-24 СПбГУТ)
С. Э. Тураев (студент группы ИКТЗ-24 СПбГУТ)

ИССЛЕДОВАНИЕ ПОДХОДА К ИСПОЛЬЗОВАНИЮ ПАРОЛЕЙ У МОЛОДЕЖИ

Данное исследование было проведено, чтобы узнать отношение молодежи к парольной политики. Нам было интересно узнать не длину используемых паролей, ни их составляющее, а, конкретно каких принципов придерживаются молодые люди для безопасности своих данных при использовании пароля. Сейчас эта тема является очень важной не только для молодежи, но так же и у более взрослого поколения. Парольная политика является первым звеном защиты информации, как и входная дверь, которая используется для доступа к помещению.

пароль, парольная политика, молодежь.

Что для современного человека электронное устройство? На сегодняшний день обстоятельства складываются таким образом, что в повседневной жизни практически все вынуждены пользоваться цифровыми устройствами. И очень остро стоит вопрос, касающийся безопасности личных данных, которые хранятся на этих устройствах. Как показывает практика, зачастую, слабая парольная политика или ее несоблюдение позволяет злоумышленникам осуществить несанкционированный доступ к информации различного уровня важности. В связи с актуальностью данной про-

блемы, мы решили провести исследование с целью выяснить отношение молодежи к подходу использования пароля.

Устройство, к которому нужно получить доступ, можно сравнить с дверью квартиры. Мы можем подойти к ней, взглянуть на нее, потрогать, попытаться открыть, но наткнемся на препятствие в виде замка. Пароль – как замок от двери, которая ведет к помещению квартиры, открыв его, получаешь доступ к большому объему информации. Поэтому важно, чтобы замок был стойкий, тогда можно предотвратить потерю данных на начальном уровне. Получается, что одна из самых простых мер защиты – выбор сложного пароля.

Для выполнения данного исследования было решено опросить молодых людей с помощь созданного нами в Google Формы анонимного опроса, а также личного общения со знакомыми.

В ранее проведенных исследованиях, приведенном в списке используемой литературы под номером один, учитывалась длина пароля, используемые символы, уникальность и устойчивость к взлому по словарю. Нам же было интересно узнать позицию, которой придерживаются молодые люди, какому способу парольной защиты отдают предпочтение, как они генерируют пароли и т. п.

Для начала нам хотелось узнать, как сильно молодые люди переживают за свои личные данные. Лишь 10% опрошенных не задумываются над данным вопрос. Около трети не используют пароль для доступа к своему устройству, считая, что у них нет информации, о которой стоит беспокоиться или просто ленятся. Из этого можно сделать вывод, что большинство людей задумываются над вопросом о сохранности своих данных, но с другой стороны далеко не все используют даже самый простой способ защиты от несанкционированного доступа – пароль.

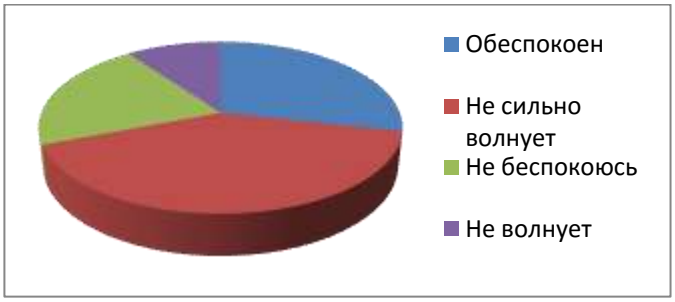


Рис. 1. Результаты опроса
по вопросу обеспокоенности за личные данные

У тех, кто все же использует пароль, нами исследовано, что наиболее популярными технологиями являются отпечаток пальца и графический рисунок. Стандартный пин-код отошел на второй план, а на первый план пришли более современные технологии.

Рис. 2. Результаты опроса
по использованию технологии пароля

Также 62,9 % опрошенных считают используемую технологию стойкой ко взломам, но взломщики паролей в силах ее обойти. Также 22,9 % не боятся взломов даже от силовых структур, таких как ФСБ и уверенны в ней полностью. До момента проведения исследования, взлом техники компании Apple Inc был невозможен, но специалистам ФБР удалось взломать телефон и получить с него необходимые данные. Как сообщают Reuters.com, для взлома телефона компании Apple, ФБР потратила порядка 1,3 млн долларов.

Чтобы придумать новый пароль люди предпочитают использовать свой мозг и ум взамен генераторам паролей, но так же опрос показал, что некоторые используют самые простые и легко взламываемые пароли, такие как 123456, Qwerty, test и другие. Что касается хранения паролей, то 77,1 % отдают предпочтение своей памяти, нежели менеджерам паролей или бумажным носителям. Более 60 % людей не доверяют никому свои пароли, но четверть людей сказали свои пароли близким людям и друзьям. Меняют свои пароли раз в полгода год лишь 48,6 % опрошенных, скорей всего по причине утери пароля, нежели для безопасности, ведь треть людей считает свой пароль идеальным и не учитывает тот факт, что с каждым днем словари паролей и «радужные таблицы» все больше развиваются и пополняются. Сегодня у вас стойкий пароль, а завтра вас уже взломали. В проведенных ранее исследованиях, приведенном в списке литературы под номером три, были получены результаты, что сервисы, связанные с электронной коммерцией и социальными сетями не предъявляют серьезных требований и правил к паролю, тем самым пытаются удержать клиентов. Взлом таких «одноразовых» аккаунтов занимает немного времени, но платежная информация стоит хороших денег. По данным компании Trendmicro, исследование которых приведено в списке использованных источников, стоимость банковского аккаунта может доходить до 500 долларов, а банковской карты – около 100.

Также нами было проведено сравнение ответов двух групп на вопрос «Как часто используют чужие устройства для входа в социальные сети под своим аккаунтом?». Результаты получились, примерно, одинаковы. Однако нашлись такие респонденты, кто используют пароль для доступа к своему устройству и часто используют чужие устройства для доступа в социальные сети. Технологии шагают вперед, и кто знает, чем безобидная проверка почты с чужого устройства может обернуться.

Многие из опрошенных людей, кто сами не используют пароль, знают пароли близких людей и 10 % знают даже множество других паролей. Возможно, знать пароль близких людей в наше время это необходимость, так как далеко не все взрослые люди «дружат» с новыми технологиями и им, безусловна, нужна помощь младшего поколения.

Нам было интересно узнать, что опрошенные люди думают о осведомленности в обществе о важности использования пароля. 55 % респондентов считает, что общество хорошо осведомлено о важности пароля. Результат получился немного странным, ведь как показывает практика, вопрос парольной политики стоит очень остро. Если молодое поколение придумывает стойкие пароли и относится ответственно к данному вопросу, то большинству из взрослого поколения не столь важно какой будет пароль, какова будет его длинна и разнообразие символов, важнее его простота написания на клавиатуре и, чтобы его как можно меньше запрашивали.

В заключении можно сказать следующее: опрос показал, что необходимо подробно осведомить общественность о важности паролей с помощью рекомендательных статей, курсов лекций в вузах и на предприятиях. Ценность различных данных может стоить компании больших убытков, а также репутации. Молодежь задумывается о важности сохранения конфиденциальности своих данных, но используют пароль 6 человек из 10. Также непонятны расхождения в опросе людей, кто не использует пароль по причине отсутствия важной информации, но в тоже время беспокоятся о ней. Но действительно ли нечего «скрывать»? Когда личные фотографии знаменитостей были выложены в сеть, они тоже ничего не скрывали, но хотели ли они того, что произошло? Не всегда даже самые крупные сервисы уделяют достаточное внимание защите от создания простых паролей, а значит, и безопасности аккаунтов пользователей. Поэтому стоит пересмотреть свое отношение к парольной политике, особенно это касается тех областей, где активно используются денежные обращения.

Список используемых источников

1 Bogdan Calin., Statistics from 10,000 leaked Hotmail passwords [Электронный ресурс]. URL: http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/

2 Edwards Julia FBI paid more than $1.3 million to break into San Bernardino iPhone [Электронный ресурс]. URL: http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB

3 Юшкевич Иван Тестирование парольных политик веб-сервисов [Электронный ресурс]. URL: http://dsec.ru/ipm-research-center/research/testing_the_password_policy_web_services/

4 Сколько стоят наши личные данные в интернете? [Электронный ресурс]. URL: http://ibusiness.ru/blog/money/41792

Статья представлена научным руководителем,
ассистентом Диптаном В. А

УДК 339.138

Н. С. Плетнева (студентка группы ИКТК-27, СПбГУТ)

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ «BONCH.ЛИЧНЫЙ КАБИНЕТ»

Переход на уровневую подготовку по программам высшего профессионального образования заметно повлиял на учебный процесс: сократились количество часов по базовым дисциплинам и объем учебного материала. Но при этом возникла нехватка времени для общения преподавателей и студентов и для прохождения полного курса дисциплин. Все эти проблемы и поможет решить специализированное мобильное приложение «Bonch.Личный кабинет».

мобильные приложения, разработка, опрос, push-уведомления, NFC.

С 2011 г. все вузы России перешли на уровневую подготовку специалистов: бакалавр или магистр.

Внедрение уровневой системы подготовки повлияло на учебный процесс: сократилось количество часов обучения как по базовым, так и по профильным дисциплинам, уменьшился объем учебного материала. В результате чего сократилось время на усвоение программы образования, появилась нехватка времени на прохождение полного курса изучения дисциплин, а также времени общения преподавателей и студентов.

Решить все появившиеся проблемы поможет специализированное мобильное приложение, которое способно объединить в себе сразу несколько моментов жизни студентов: обучение, обмен данными, общение и т. д.

На сегодняшний день процесс создания мобильных приложений для российских вузов находится на зачаточном этапе: основная часть приложений представляет собой расписание занятий, которое, как правило, делается даже не самим вузом, а кем-то еще, заинтересованным в размеще-

нии рекламы или желающим любым способом монетизировать показ расписания.

В отличие от российских вузов крупнейшие зарубежные вузы считают делом чести выпустить собственное мобильное приложение, а список возможностей приложения намного шире и не ограничивается только просмотром расписания.

В нашем университете также существует проблема получения актуальной и необходимой информации по процессу обучения и обратной связи с преподавателями, ведь сайт университета крайне неоптимизирован для просмотра хотя бы с планшета.

Для того, чтобы выяснить, действительно ли необходимо внедрение такого онлайн-сервиса, и разобраться в требуемых функциях для него, был проведен опрос при помощи Google-формы среди студентов СПбГУТ. В опросе приняли участия в общей сложности 222 студента с 1 по 4 курс.

По проведенному опросу понятно, что студенты не очень часто используют личный кабинет. Данные по этому вопросу можно увидеть на рисунке 1.

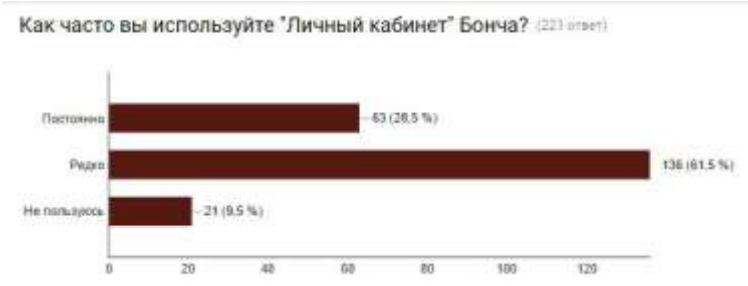


Рис. 1. Использование личного кабинета студентами

Если рассматривать вопрос о том, какие бы разделы из личного кабинета были бы необходимы в мобильном онлайн-сервисе, то можно увидеть, что студентом больше всего важен доступ к расписанию, что представлено на рисунке 2.

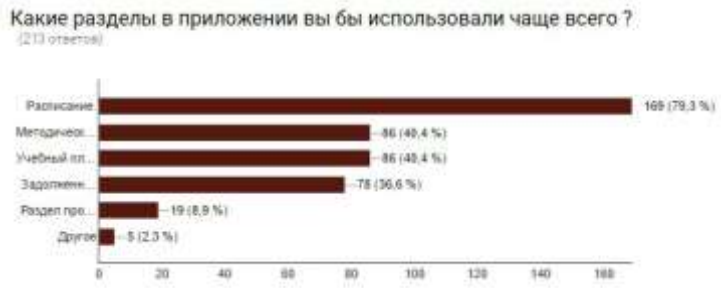


Рис. 2. Необходимые разделы в приложении

Далее были предложены варианты следующих дополнительных возможностей сервиса:

- быстрый доступ к связи с преподавателями, посредствам телефона и почты;
- push – уведомления;
- возможность при помощи сервиса и устройства с NFC, проходить в университет (сам сервис с личными данными студента и является пропуском в университет).

Данные по предложенным возможностям в мобильном приложении представлены на рисунках 3–5.

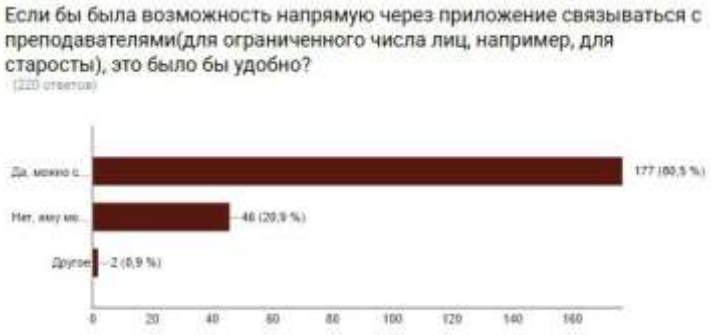


Рис. 3. Быстрый доступ к преподавательскому составу

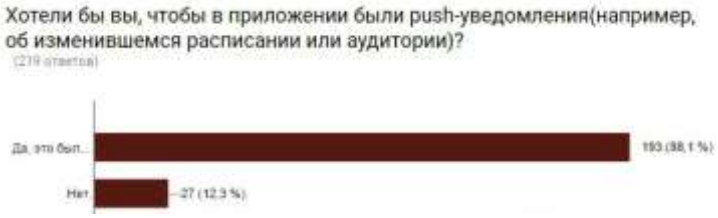


Рис. 4. Необходимость *push* – уведомлений в приложении

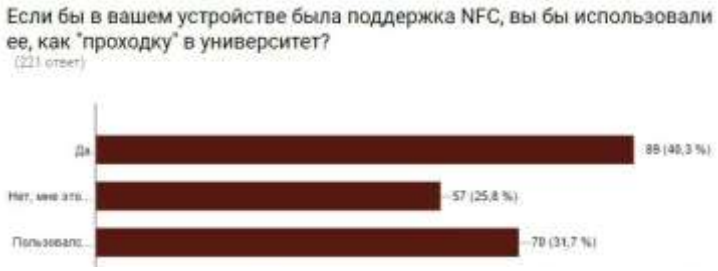


Рис. 5. Использования приложения, как пропуск в Университет

Опираясь на полученные данные можно с уверенностью сказать, что оптимизированное мобильное приложение крайне востребовано среди студентов нашего университета. Основные цели, которые хотели бы видеть сами студенты в разработанном сервисе – это:

- быстрый и удобный доступ к расписанию;
- возможность получения методических материалов;
- получение *push* – уведомлений о последних новостях;
- быстрый доступ к преподавательскому составу университета;

- использование сервиса в качестве пропуска в университет.

В результате можно сделать вывод, что создание данного приложения на сегодняшний день является актуальным и позволит решить ряд задач, упрощающих повседневную жизнь студентов. Его функции позволят сделать процесс обучения более доступным, комфортным и информативным.

Список используемых источников

1. О задачах высших учебных заведений по переходу на уровневую систему высшего профессионального образования: Приказ Федерального агентства по образованию от 10 февраля 2010 г. N 109"// Собрание законодательства. – 2010.

2. Черчилль Гилберт А., Браун Том Дж. Маркетинговые исследования / пер. с англ. под ред. Г. Л. Багиева. 5-е изд. СПб. : Питер, 2007. 704 с.

3. iTunes. [Электронный ресурс]. URL: https://itunes.apple.com/us/app/asu-mobile/ id350504591?mt=8 (дата обращения 28.04.2016)

4. iTunes. [Электронный ресурс]. URL: https://itunes.apple.com/ us/app/uolmobile/ id528649971?mt=8 (дата обращения 28.04.2016)

5. iTunes. [Электронный ресурс]. URL: https://itunes.apple.com/us/app/fsu-mobile/ id372797911?mt=8 (дата обращения 28.04.2016)

6. Google формы. [Электронный ресурс]. URL: https://apps.google.com/ intx/ru/products/ forms/ (дата обращения 28.04.2016)

Статья представлена научным руководителем,
ассистентом Диптаном В. А.

УДК 338.4

И. Н. Проничев (студент группы ЭБ-11з, СПбГУТ)

АКТУАЛЬНОСТЬ ВНЕДРЕНИЯ СИСТЕМЫ ГЛОНАСС НА ПРЕДПРИЯТИИ

Целью любого коммерческого предприятия является получение прибыли, при этом в рыночных условиях при наличии большой конкуренции не каждой компании удается обеспечивать устойчивый рост, наращивая поступление доходов. Поэтому предприятия используют любые возможности, чтобы повысить эффективность деятельности, которой занимается компания. На протяжении всего жизненного цикла предприятия актуальными для него задачами являются поиск скрытых резервов компании, снижение затрат и повышение рентабельности.

спутниковая навигация, автотранспорт, мониторинг.

Почти все организации используют в работе автомобильный транспорт, как легковой, так и грузовой. Задача повышения эффективности ка-

питальных вложений и снижения издержек является частью проблемы рациональной организации автомобильного транспорта и охватывает широкий круг эксплуатационных и технологических вопросов. Решение этой задачи обеспечивается в первую очередь качественным управлением производственным процессом, которое в значительной мере предопределяет рациональное использование основных фондов и высокую эффективность капитальных вложений.

Речь идёт о процессах внедрения и использования спутниковой навигации на транспорте предприятия АО «Кольская Горно-металлургическая компания», в рамках которой реализуется внедрение системы мониторинга.

Практическая значимость заключается в возможности использования её основных разработок и выводов для дальнейшего совершенствования процессов применения системы ГЛОНАСС не только на автомобильном, но и на других видах транспорта. Результаты могут быть использованы региональными и муниципальными органами власти и бизнеса как методическая база разработки и управления проектами внедрения ИТС на подведомственных территориях и предприятиях имеющих транспортные комплексы.

Акционерное общество «Кольская горно-металлургическая компания» – дочернее предприятие ПАО ГМК «Норильский Никель» – ведущий производственный комплекс Мурманской области, созданный на базе старейших предприятий – комбинатов Североникель и Печенганикель, представляет собой единое горно-металлургическое производство по добыче сульфидных медно-никелевых руд и производству цветных металлов.

В современных условиях в связи с быстрым научно-техническим прогрессом, автоматизацией процессов производства существенно возрастают роль и значение внутрипроизводственного транспорта на предприятии. Целью анализа должно быть изыскание возможности выпуска предприятием продукции с наименьшими затратами живого и овеществленного труда, связанные с внутрипроизводственным транспортом.

Задачи анализа хозяйственной деятельности транспортного подразделения: объективная оценка результатов его хозяйственной деятельности, выявление резервов повышения качества оказываемых транспортных услуг и путей снижения их стоимости.

Интерес представляет структура затрат на выполнение работ [2] (рис. 1).

Структура затрат в 2015 г. примерно остается неизменной. Наибольший удельный вес в структуре затрат имеет статья затраты на оплату труда и запасные части. Доля этих статей составляет 25 % в общем объеме затрат подразделения. Также высокий удельный вес имеет статья затраты на горюче-смазочные материалы, она составляет 21 % от всего объема затрат.

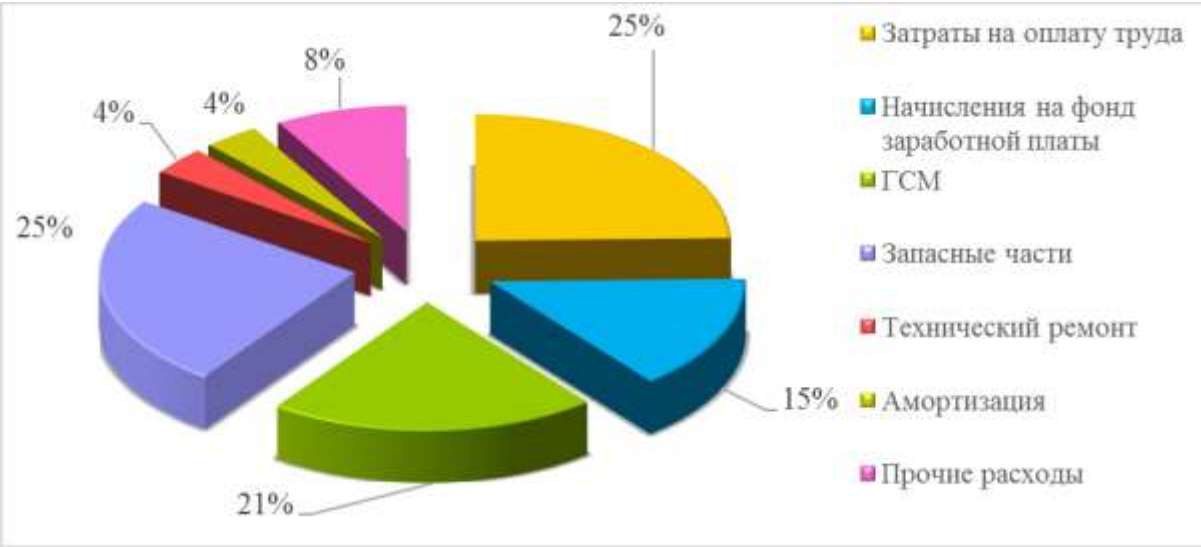


Рис. 1. Структура затрат на производство в 2015 г.

Темп роста статей затрат на горюче-смазочные материалы и запасные части самый высокий на протяжении всего года. В 2014 г. затраты на горюче-смазочные материалы увеличились на 553 тыс. руб., что составило 12 % от уровня 2013 г. В 2015 г. затраты на горюче-смазочные материалы увеличились на 561 тыс. руб., что составило 11 % от уровня 2014 г.

В 2014 г. затраты на запасные части увеличились на 598 тыс. руб., что составило 11 % от уровня 2013 г. В 2015 г. затраты запасные части увеличились на 663 тыс. руб., что составило 11 % от уровня 2014 г.

Таким образом, выделяются проблемы в деятельности автотранспортного подразделения компании:

- снижение производительности автотранспорта;
- неэффективное управление автотранспортом;
- рост затрат на производство, особенно на горюче-смазочные материалы и запасные части [1].

Это говорит о том, что рассматриваемому подразделению необходимо тщательнее контролировать свои расходы и осуществить разработку мероприятий, направленных на повышение эффективности использования транспорта.

Мероприятия по реализации внедрения системы должны обеспечивать достижение целей проекта и быть направлены на снижение затрат. Планирование реализации проекта основывается на следующем:

- проект создания системы мониторинга разделен на этапы, каждый из которых направлен на решение одной или нескольких бизнес-задач;
- каждый из этапов должен планироваться таким образом, чтобы в наиболее короткие сроки могли быть получены результаты, полезные для использования в Компании;

- в рамках реализации первой очереди необходимо выделить пилотные зоны с ограниченным числом рабочих мест;
- для обеспечения полноценной работы пользователей в рамках каждого функционального подпроекта должны быть предусмотрены мероприятия по подготовке (инструктированию) пользователей.

Таким образом, цель проекта создания системы мониторинга автотранспорта является снижение издержек при выполнении производственной деятельности специалистами подразделения за счет обеспечения возможности оперативного и своевременного управления ресурсами автотранспортной техники.

Ожидаемый эффект от внедрения:

- повышение уровня безопасности ведения работ;
- снижение производственных издержек и оптимизация процесса управления автотранспортной техники, технического обслуживания и ремонтов;
- повышение эффективности использования автотранспортной техники за счет сокращения простоев;
- сокращение времени на осуществление оперативного контроля за местоположением транспортных средств в реальном масштабе времени;
- сокращение времени на организацию дистанционного контроля за перемещением транспортных средств в реальном масштабе времени;
- сокращение расхода горюче-смазочные материалы за счет оптимизации перевозок.

Реализация системы мониторинга обеспечит возможность эффективного управления производственной деятельностью автотранспортного подразделения, которая позволит:

- повысить ответственность руководства подразделений за результаты деятельности;
- обеспечить эффективное управление ресурсами подразделений, посредством логически взаимосвязанного единого контура управления;
- организовать планомерную и целенаправленную деятельность по снижению издержек в конкретных подразделениях;
- повысить исполнительскую дисциплину и организовать эффективную систему мотивации персонала, основанную на конкретных показателях производственной деятельности;
- организовать непрерывный процесс измерения, анализа и улучшения ключевых показателей эффективности производственной деятельности, как отдельных руководителей предприятия, так и структурных подразделений.

В качестве платформы системы выбрана система «СКАУТ» – спутниковый контроль автотранспорта и учет топлива, производитель ГК «СКАУТ» (г. Санкт-Петербург).

Важным преимуществом системы ГЛОНАСС/GPS слежения и мониторинга СКАУТ является возможность контроля топлива. Уникальный математический алгоритм анализа графика уровня топлива автоматически определяет заправки и сливы топлива. В отчете по топливу системы слежения СКАУТ диспетчеру выводится список всех заправок и сливов, их адрес, объем и время. Использование датчиков расхода топлива позволяет более точно определять объем потребленного топлива [4].

Экономический эффект при внедрении системы на предприятии проявляется в комплексе факторов и обеспечивается за счет следующих факторов:

1) За счет значительного уменьшения потребления топлива относительно ранее выделяемых объемов, у предприятия освобождаются дополнительные денежные средства.

2) Нецелевого использования техники. Исключаются «левые» рейсы. Уменьшается износ узлов и агрегатов машин и расход топлива, не связанные с производственной деятельностью.

3) Неэффективного использования техники. С помощью данных Системы легко обнаруживаются периоды работы машин на холостом ходу с низкой загрузкой, а также ошибки при составлении плана работ техники предприятия.

4) Нарушений правил эксплуатации техники. С помощью Системы нарушители режимов вождения и технологических процессов выявляются и привлекаются к ответственности [3].

Рассмотрим расчет экономии за счет снижения расхода топлива после внедрения системы на 2 площадках (табл. 1).

Основными источниками экономической эффективности являются (за период 5 лет) снижение расхода топлива.

Срок окупаемости составляет 1, 2 года.

После внедрения системы получается экономия 613 342 л топлива, что в стоимостном выражении составит 17 471 028,07 руб. за 12 месяцев. При этом изменение экономии топлива в целом по компании составит 15,3 %.

Таким образом, проект является эффективным и возможность реализации данного проекта в компании целесообразна.

ТАБЛИЦА 1. Расчет экономической эффективности

Наименование	Расход топлива	Ед. изм.	12 мес. до установки	12 мес. эксплуатации	Изменение экономии топлива после установки	Экономия топлива в руб. без НДС
Экономия по пл. Заполярный	факт	литр	2 656 385	1 641 813		15 441 482,42
	норма	литр	2 787 270	2 376 561		
	экономия	литр	130 885	734 748	542 092	
		%	4,7	30,92	26,22	
Экономия по пл. Мончегорск	факт	литр	1 392 037	1 116 645		2 029 545,65
	норма	литр	1 399 593	1 192 285		
	экономия	литр	7 556	75 640	71 250	
		%	0,54	6,34	5,80	
Итого экономия топлива:	факт	литр	4 048 422	2 758 458		**17 471 028,07**
	норма	литр	4 186 863	3 568 846		
	экономия	литр	138 441	810 388	613 342	
		%	3,31	18,60	15,30	

Список используемых источников

1. Воронов В. В. Экономика предприятия: учебник. М. : Дело и Сервис, 2010. 208 с.
2. Менеджмент в телекоммуникациях: учебное пособие / В. В. Макаров [и др.] ; под ред. В. В. Макарова, Р. Г. Цатуровой ; Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования "Санкт-Петербургский гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича". Санкт-Петербург, 2011. (2-е изд., перераб. и доп.).
3. Соловьев Ю. А. Системы спутниковой навигации. М. : Эко-Трендз, 2003. 320 с.
4. Экономика автомобильного транспорта: учебное пособие / А. Г. Будрин, Е. В. Будрина, М. Г. Григорян / под ред. Г.А. Кононовой. 3-е изд., стер. М. : Издательский центр «Академия», 2011. 320 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Щербаковым И. Б.

УДК 658.012

Х. М. Хамхоева (студентка группы Э2-1, СПб ФУП РФ)

ИСПОЛЬЗОВАНИЕ МАТЕМАТИЧЕСКОГО АППАРАТА ПРИ ФОРМИРОВАНИИ ПОРТФЕЛЯ ЦЕННЫХ БУМАГ

В настоящее время роль управления инвестиционным портфелем резко возрастает и заключается в нахождении той грани между доходностью и рискованностью, которая позволила бы выбрать оптимальную структуру портфеля. В данной статье рассматривается оптимальный портфель ценных бумаг. В частности, портфель минимального риска Гарри Марковица.

оптимальный портфель, рисковые бумаги, безрисковые ценные бумаги, портфель минимального риска, эффективность портфеля.

Одной из причин финансового становления государства является высокая инвестиционная активность, которая обеспечивает экономический рост.

При инвестировании в ценные бумаги инвестор нередко сталкивается с различными проблемами. Инвестиционные вложения в отдельные активы имеют большую прибыльность, а значит и высокий риск, или условно невысокий риск и относительно низкую прибыльность. Для того чтобы достигнуть оптимального соотношения доходности и риска вкладчики формируют портфель ценных бумаг, который содержит в себе разные виды ценных бумаг.

Рассмотрим задачу формирования оптимального портфеля, предложенную американским экономистом Гарри Марковицем в 1952 г., за что ему была вручена Нобелевская премия [1, 2].

Допустим x_i – доля вложенного в ценные бумаги i-го вида капитала. Необходимо найти x_i, при котором риск будет минимальным. Кроме того, должно обеспечиваться заданное значение эффективности m_p, то есть:

$$\sum_i x_i m_i = m_p,$$

$$\sum_i x_i = 1.$$

Решение данной задачи будем обозначать x^*. Если $x_i^* \geq 0$, то рекомендуется вложить долю x_i^* капитала в ценные бумаги i-го вида. А в том случае, если $x_i^* < 0$, то необходимо провести операцию «shortsale» («короткая продажа»).

Что это за операция? Пусть вкладчик, формирующий портфель, дал обязательство через какой-то промежуток времени поставить ценные бумаги i-го вида, вместе с доходом, который бы они принесли их владельцу за этот промежуток времени.

Сейчас он за это получает их денежный эквивалент. На данные средства он приобретает акции иного вида и получает с них прибыль. Так как они оказались более эффективными, то инвестор оказывается в выигрыше.

В том случае, когда имеется более двух видов ценных бумаг, анализ усугубляется. Мера риска оптимального портфеля возрастает с ростом эффективности.

Такой портфель называется портфелем Марковица минимального риска.

В случае, когда на рынке присутствуют безрисковые бумаги, решение данной задачи сильно упрощается.

Допустим, что m_0 – эффективность безрисковых бумаг;

x_0 – доля вложенного капитала в эти бумаги;

m_r – средняя ожидаемая эффективность;

V_r – вариация;

σ_r – среднеквадратичное отклонение эффективности рисковой части портфеля, в который вложено $(1 - x_0)$ часть всего капитала.

Тогда прогнозируемая эффективность портфеля составит:

$$m_p = m_0 x_0 + \left(1 - x_0\right) m_r.$$

Если предположить, что безрисковые бумаги не коррелируют с остальными, то риск будет равен:

$$V_p = \left(1 - x_0\right)^2 V_r$$

$$\Rightarrow \sigma_p = \left(1 - x_0\right)\sigma_r$$

$$\sigma_p = \sigma_r - x_0\sigma_r$$

$$\Rightarrow x_0 = \frac{\sigma_r - \sigma_p}{\sigma_r} = 1 - \frac{\sigma_p}{\sigma_r}$$

Отсюда следует, что ожидаемая эффективность портфеля линейно зависит от риска.

Рисковые ценные бумаги пронумеруем числами 1, 2, …, n.

Задача об оптимальном портфеле Марковица в том случае, когда есть безрисковые бумаги, представлена математической моделью:

$$\begin{cases} \sum_{ij}^{n} x_i x_j V_{ij} \to \min \\ x_0 + \sum_i x_i = m_p \\ x_0 + \sum_i x_i = 1 \end{cases}$$

Изложим теперь окончательный вариант решения этой задачи, полученный американским экономистом Д. Тобиным.

Пусть V – матрица ковариаций рисковых ценных бумаг;

X (x_i) – вектор-столбец долей капитала, вкладываемого в i-й вид ценной бумаги;

M (m_i) – вектор-столбец прогнозируемых эффективностей i-го вида ценной бумаги;

I – n-мерный вектор-столбец, компоненты которого равны 1.

Тогда оптимальное значение долей составит:

$$X^* = \frac{m_P - m_0}{\left(M - m_0 I\right)^T V^{-1}\left(M - m_0 I\right)} V^{-1}\left(M - m_0 I\right).$$

В данном случае V^{-1} – матрица, обратная к матрице V. В числителе формулы – число, в знаменателе тоже получится число, не зависящее от инвестора и определяющееся только рынком.

V^{-1} $(M - m_0 I)$ – вектор-столбец размерности n, который не зависит от эффективности портфеля m_p. Следовательно, вектор долей рисковых ценных бумаг X^*, пропорциональный этому вектору, тоже не зависит от m_p.

Сумма компонента X^* зависит от эффективности m_p, поэтому с ростом эффективности портфеля компоненты вектора будут расти, и доля x_0 безрисковых ценных бумаг будет уменьшаться.

Решение по математической модели формирования оптимального портфеля ценных бумаг проводилось при помощи компьютерной программы MS Excel [3, 4].

Таким образом, согласно теории Гарри Марковица, при формировании портфеля инвестору необходимо руководствоваться ожидаемой доходностью и стандартным отклонением. Причем под ожидаемой доходностью понимается мера потенциального вознаграждения, которая связана с определенным портфелем, а под стандартным отклонением – мера риска, связанная с данным портфелем.

Список используемых источников

1. Буренин А. Н. Управление портфелем ценных бумаг. М. : Научно-техническое общество им. академика С. И. Вавилова, 2014. 81 с.

2. Иванов А. П. Финансовые инвестиции на рынке ценных бумаг: монография. М. : Дашков и К, 2012. 480 с.

3. Трофимец Е. Н., Трофимец В. Я. Пути повышения мотивации к изучению математики у студентов-экономистов на основе профессионально-ориентированных экономических задач // Бесконечномерный анализ, стохастика, математическое моделирование: новые задачи и методы. Проблемы математического и естественнонаучного образования: сборник статей Международной конференции, Москва, 2015. С. 334–338.

4. Трофимец Е. Н. Интегральный подход в обучении математике студентов-экономистов: монография / Федер. агентство по образованию, Яросл. гос. техн. ун-т. Ярославль : ЯГТУ, 2009. 170 с. ISBN 978-5-9914-0094-7.

Статья представлена научным руководителем,
кандидатом педагогических наук, доцентом Трофимец Е. Н.

УДК: 658.012

О. С. Шишмарева (студентка группы Э2-1, СПб ФУП РФ)

К ВОПРОСУ ПОСТРОЕНИЯ МОДЕЛИ ОРГАНИЗАЦИИ РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

Статья посвящена рассмотрению модели оптимальной организации рекламной деятельности на примере автомобильного рынка. В статье приводятся аргументы, почему для получения максимальной прибыли компаниям удобно пользоваться данной математической моделью.

рекламная деятельность, математическая модель, распределение средств, целевая функция.

В век информационных технологий и большого объёма предложения различных товаров и услуг реклама играет значительную роль в экономике организации. Большое значение в формировании потребительского спроса играет рекламирование продукции.

В своей основе реклама – это экономическое явление. К экономико-математической модели организации рекламной деятельности можно отнести: оптимальную организацию рекламной деятельности, модель распространения рекламы, оценка эффективности рекламной деятельности. В данной работе я бы хотела показать только модель оптимальной организации рекламной деятельности, так как, на мой взгляд, она является основной для рекламодателя на начальном уровне рекламной деятельности.

Сместим фокус внимания на автомобильный рынок, он является одним из крупнейших во всем мире. В 2013 г. автопроизводители потратили на рекламу более 24,58 млрд руб. и продолжают наращивать свои маркетинговые бюджеты.

Модель оптимальной организации рекламной деятельности

Согласно предыдущему опыту на рекламу альянса «Renault-Nissan» выделено 3 883 млн руб. на всю продукцию (в 2013 г. было выделено 3 883,6 млн руб. [1]). Альянс рекламирует свою продукцию, используя пять источников массовой информации таких как: реклама на телевидении, наружная реклама (outdoor), реклама в интернете, реклама в прессе, реклама на радио.

Анализ рекламной деятельности корпорации в прошлом показал, что вложенные в рекламу средства приводят к увеличению прибыли на 22, 14, 10, 9, 8 руб. соответственно, в расчете на 1 руб., затраченный на рекламу. Руководство, согласно прошлому опыту, намерено потратить не менее 52 % суммы на рекламу на телевидение, не менее 16 % – на наружную рекламу, не более 13 % – на рекламу в интернете, не менее 10 % выделенной суммы − на прессу, не более 9 % – на радио. Требуется определить оптимальное распределение средств, направляемых на рекламу.

Введём x_i: x_1 – средства, направленные на телевидение, x_2 − средства, направленные на наружную рекламу, x_3 – средства, направленные на рекламу в интернете, x_4 – средства, направленные на рекламу в печатных СМИ (в прессе), x_5 – средства, направленные на рекламу на радио.

Переходим к составлению модели по данному экономическому процессу [2, 3].

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 3883, \\ x_1 \le 0,52*3883, \\ x_2 \ge 0,16*3883, \\ x_3 \le 0,13*3883, \\ x_4 \le 0,1*3883, \\ x_5 \le 0,09*3883, \\ x_1 \ge 0,\ x_2 \ge 0,\ x_3 \ge 0,\ x_4 \ge 0,\ x_5 \ge 0. \end{cases}$$

Целевая функция оптимизации будет иметь вид:

$$f(x) = 22x_1 + 14x_2 + 10x_3 + 9x_4 + 8x_5 \to \max.$$

Решение по математической модели удобно осуществлять, используя табличный процессор Microsoft Excel, с помощью надстройки «Поиск решения» [2, 3].

Все исходные данные сведены в таблице 1:

ТАБЛИЦА 1. Исходные данные

	Виды рекламы				
	Реклама на телевидении	Наружная реклама	Реклама в интернете	Реклама в прессе	Реклама на радио
Прибыль на 1 руб. вложенных средств (руб.)	22	14	10	9	8
Максимальная доля	52 %	16 %	13 %	10 %	9 %
Выделенные средства (млн руб.)	3 883				

Результаты по решению математической модели представлены в таблице 2.

ТАБЛИЦА 2. Результаты решения

	Виды рекламы				
	Реклама на телевидении	Наружная реклама	Реклама в интернете	Реклама в прессе	Реклама на радио
Вложенные средства (млн руб.)	2 019,16	1 863,84	0	0	0
Прибыль (млн руб.)	70 515,28				

Анализируя данные, можно сделать вывод, что для получения максимальной прибыли, компания, проводя рекламную кампанию, должна вложить 2 019,16 млн руб. в рекламу на телевидении, 1 863,84 млн руб. на наружную рекламу, при этом не вкладывать деньги на рекламу в интернете, в прессе и на радио. Наглядно, данный вывод можно представить в виде диаграммы, изображенной на рисунке 1.

Максимальная прибыль альянса «Renault-Nissan» составит 70 515,28 млн руб.

Можно сделать вывод, что организация рекламной деятельности является сложным процессом, который включает множество различных расчётов, поэтому фирмы и компании должны строго следить за тем, чтобы данным видом деятельности занимались только специалисты данной сферы. Они должны иметь большой опыт работы в данной области, владеть информацией об экономической ситуации на рынке [4].

Информационные технологии играют важную роль в организации рекламной деятельности, так как помогают в решении математических моделей, по средствам различных программ.

Рис. 1. Распределение средств по видам рекламы

Рекламная кампания может принести фирме большие деньги, если она правильно организована и составлена, в противном случае компания понесёт убытки. Как сказал известный американский копирайтер, организатор и исследователь рекламы Клод Кларенс Хопкинс: «Один миллион, вложенный в эффективную рекламу, продает больше, чем десять миллионов, вложенных в неэффективную рекламу».

Список используемых источников

1. Рекламные бюджеты [Электронный ресурс] / AdIndex.ru: [сайт]. URL: http://adindex.ru/ publication/analitics/budget/2014/07/30/113265.phtml

2. Трофимец Е. Н. Информационно-аналитические технологии обучения менеджеров в образовательных учреждениях России и за рубежом // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2010. № 1. С. 86–95.

3. Трофимец Е. Н. Интегральный подход в обучении математике студентов-экономистов: монография / Федер. агентство по образованию, Яросл. гос. техн. ун-т. Ярославль : ЯГТУ, 2009. 170 с. ISBN 978-5-9914-0094-7.

4. Основы финансовой грамотности: учебник. / Я. А. Магазинер, А. А. Орлова, Д. А. Жилюк, Р. И. Присяжная, В. А. Фролова. СПб. : Литера, 2015. С. 256.

Статья представлена научным руководителем,
кандидатом педагогических наук, доцентом Трофимец Е. Н.

УДК 338.24.01

У. В. Югова (студентка группы Э-01з, СПбГУТ)

ВОЗМОЖНОСТИ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ МОТИВАЦИИ ТРУДА

В современных условиях эффективное управление персоналом является основной задачей для любой компании. Мотивация действительно повышает базовую производительность труда, а изменение отношения работников к труду увеличивает прибыльность организации. Актуальность обусловлена всевозрастающей ролью личности работника, не только как совокупности функций и должности, а человека – как особого объекта управления, который не может рассматриваться только как ресурс.

система мотивации, управление персоналом, производительность труда.

Мотивация работников является одной из основных сторон в управлении персоналом предприятия, так как именно она считается конкретной причиной их действий. Нацеливание сотрудников на достижение целей предприятия, объединение интересов каждого сотрудника и предприятия в целом – основная задача управления персоналом. Перемена основных черт профессионализации труда, рост уровня образования и общественных ожиданий сотрудников усиливает значимость мотивации как функции менеджмента.

Мотивация – побуждение человека к труду, являющееся результирующей системой внутренних побудительных элементов, таких как потребности, интересы, ценностные ориентиры, с одной стороны, с другой – отражаемые и фиксируемые сознанием человека факторы внешней среды, т. е. внешние стимулы, побуждающие к деятельности [1].

Основные задачи мотивации персонала [2] представлены на рисунке 1.

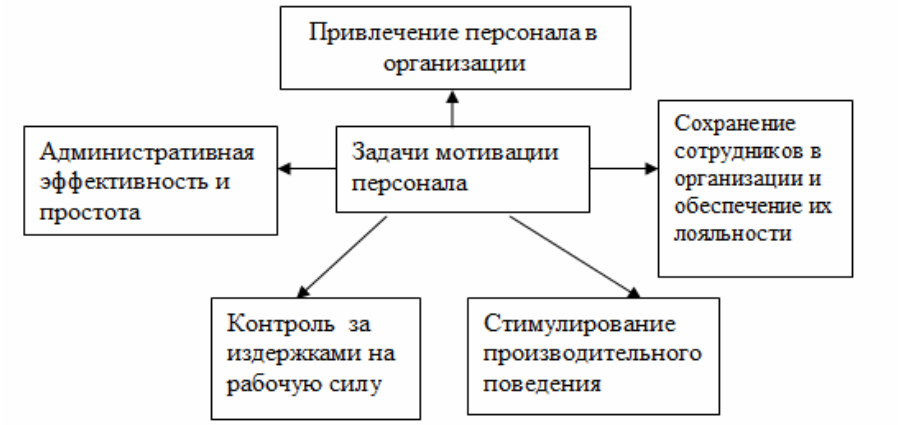


Рис. 1. Основные задачи мотивации персонала

В чем же заключается каждая из данных задач?

1) Втягивание персонала в организацию, которая конкурирует с другими на рынке труда за использование необходимых человеческих ресурсов.

2) Если награда в организации не устраивает работников, то они вынуждены будут покинуть ее.

3) После набора и удержания на работе компетентных сотрудников, менеджер обязан заботиться об увеличении плодотворности и эффективности их работы.

4) Взвешенная система мотивации даёт возможность организации совершать контроль и результативно распоряжаться расходами на рабочую силу, гарантируя при этом присутствие необходимых сотрудников.

5) Система мотивации должна быть доступна в понимании любому сотруднику и проста для организации действий персонала, т. е. не требовать больших ресурсов для гарантирования ее безостановочной деятельности.

Какие мотивационные модели сложились в настоящее время в теориях управления?

Лишь искусно созданная модель мотивации, которая учитывает приобретенные сведения из сферы психологии, менеджмента и т. д., окажется в состоянии результативно функционировать и направлять как команду, так и определенного индивида к достижению общих целей.

Всякая модель мотивации содержит в себе модели мотивации. В теории и практике менеджмента нет совершенной многофакторной и альтернативной модели стимулирования, отвечающей всем вероятным запросам. Но имеются известные модели, различные по направленности и действенности.

Ниже приводится классификация моделей мотивации, широко используемая фирмами ряда стран. Это следующие модели [3]:

- кнута и пряника;
- первичной и вторичной потребности;

- внутреннего и внешнего вознаграждения;
- факторная модель стимулирования;
- справедливости;
- ожидания;
- социальной справедливости и др.

Главные принципы теории ожиданий заключаются в следующем: эта теория ищет ответ на вопрос, как ожидания воздействуют на мотивацию сотрудника и как мотивация воздействует на итоги труда любого сотрудника. Также доказывается, что мотивация определяется тремя моментами: ожиданий 1-го уровня (старания – результат), ожиданий 2-го уровня (результаты – поощрение) и валентности результатов 2-го уровня.

Мотивация как совокупность мотивов обусловливается множеством социальных факторов. К ним принадлежат верность коллективу, опасения выглядеть смешным, наклонность поддержать свой авторитет, тяготение к общественному порядку и повышение квалификации. В процессе повышения квалификации человек усваивает такие стимулы, как жажда быть понятым, склонность быть главным, увлекать за собой остальных людей, быть направляемым и пр.

На рисунке 2 показана классификация методов мотивации [4].

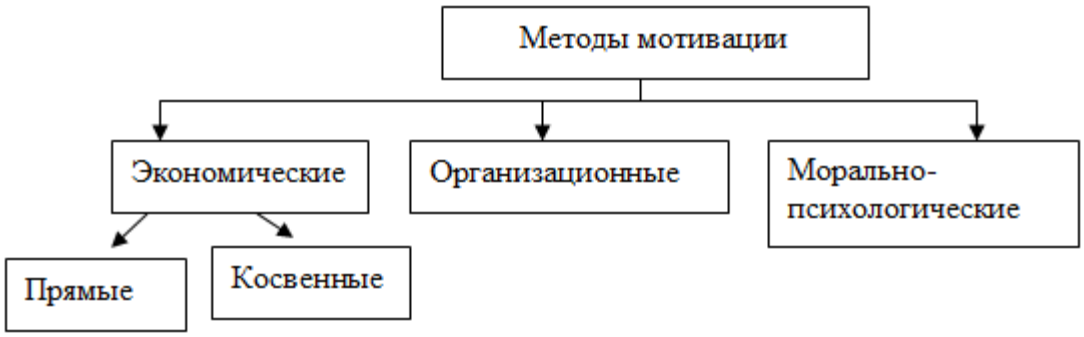


Рис. 2. Классификация методов мотивации

Формы прямой экономической мотивации - это:

- базисная оплата труда (финансовый измеритель стоимости деятельности работника);
- второстепенная оплата труда (с учетом опытности работника, сложности его труда, объединения специальностей, сверхнормативной работы, общественных гарантий организации);
- вознаграждение (устанавливает личный вклад сотрудников в итоговые результаты работы в определённое время);
- премия (объединяет итоги труда каждого структурного подразделения предприятия и сотрудника с основным критерием благополучной деятельности организации – прибылью);

- другие виды платежей (к примеру, оплата проезда до места работы и по населённому пункту; выплаты нескольких официальных жалований при выходе сотрудника на пенсию и т. д.).

Косвенная экономическая мотивация:

- разрешение пользоваться служебным транспортом;
- использование социальных институтов предприятия;
- пользование детскими лагерями (для детей работников) по льготным путевкам; домами отдыха;
- обеспечение на льготных условиях местами в детских дошкольных организациях; закупка изделий, производимых предприятием, по более низким ценам и т. д.

К организационным методам мотивации относят:

- мотивацию целями (увлекательные цели);
- мотивацию обогащением сути работы (предоставление разной интересной работы, с безграничными перспективами роста, повышающими качества сотрудника);
- мотивацию причастностью к делам фирмы (позволить сотрудникам участвовать в решении некоторых проблем, привлечение их в процесс командного творчества, действительная передача им прав и ответственности).

Морально-психологические методы стимулирования включают:

- образование условий, при которых работники чувствовали бы профессиональную гордость за участие в какой-либо работе, персональную ответственность за результаты.
- наличие вызова, предоставление возможности каждому работнику проявить свои способности, лучше совладать с задачей. Поэтому задание должно включать в себя не только риск, но и шанс на удачу.
- выделившиеся сотрудники имеют право подписывать бумаги, в разработке которых они участвовали.
- личная или публичная оценка.

Для разработки систем мотивации, подходящих для практического применения руководством, можно рекомендовать следующие элементы: финансовое стимулирование; повышение квалификации и карьерный рост; признание успехов; приемлемость корпоративной этики. Степень оплаты труда – один из главных для работников мотиватор, влияющий на продуктивность и благонадёжность людей. На предприятиях применяются такие виды материального стимулирования, как:

1. Заработная плата.

А) Главная часть – стойкий оклад (выплачивается в суммарном объеме, если отсутствуют грубые нарушения рабочих обязанностей).

Б) Дополнительная часть, включающая: премиальные; надбавки за профессионализм; сверхурочные; оплата совместительства; доплаты

кормящим матерям, за руководство отделом; выплаты за неиспользованный отпуск и т. д.

2. Бонусы – единичные выплаты, объём которых зависит от: трудового стажа; размера заработной платы; общих итогов деятельности отдела; собственного вклада каждого работника.

3. Участие в прибыли – этот тип одобрения, распространяющийся на топ-менеджеров и специалистов по продажам, так как их деятельность влияет на рентабельность организации в целом. Исходя из финансовых успехов организации, создается целевой фонд, в который отчисляется доля от выручки. Объём вознаграждения зависит от уровня, на котором эти работники находятся в иерархии компании.

4. Добавочные выплаты для сотрудников отделов продаж и сбыта – механизм, призванный поощрять работников к отыскиванию свежих рынков сбыта изделий компании, путем максимизации дохода. К ним относятся платежи, восполняющие собственные затраты работников, не связанные напрямую с работой сотрудника.

Еще одним важным компонентом системы мотивации является подсистема повышения квалификации и карьерного роста. Главными инструментами тут является целенаправленная работа по образованию кадрового резерва и проектирование карьеры.

На данном этапе уместно обговорить стремление сотрудника к обучению и участию в различных программах. Такой подход показывает работнику неравнодушие компании, ее внимание к тревожащим сотрудника проблемам роста.

Оценка штата и планирование персональных планов роста являются для работника доказательством его возможностей. Руководство предприятия должно показывать направление совершенствования фирмы по отношению к карьерным предпосылкам сотрудников – какие вакансии будут возникать, где, когда и как будет расширяться компания и какие требования родятся к работникам, исходя из намеченной политики и целей становления организации.

Третье звено системы мотивации – признание достижений. Работа над ним должна предполагать: создание названий и критериев достижений работников; выбор каналов общения для свободного оповещения о достижениях работников.

Итоговое звено в цепи действий по сооружению системы мотивации – интерес к корпоративной культуре компании.

Следовательно, создание системы мотивации предполагает на практике интерес к четырем главным моментам, но не ограничивается ими. Достижение успеха мотивацией определяется единым подходом к ней, базирующимся на глубоком и всеобщем исследовании положения дел на предприятии и мотивационной структуры действий ее штата.

Список используемых источников

1. Экономическая энциклопедия / авт.- сост. Н. В. Федоров, Е. Я. Бутко, В. Л. Кураков, А. Л. Кураков и др. М. : Гелиос АРВ, 2010. 1024 с.

2. Трофимов А. Г. Работа с персоналом на предприятии // Управление персоналом. 2010. № 3. С. 15–19.

3. Кокорев В. П. Мотивация в управлении. Курс лекций. Рекомендовано Советом учебно-методического объединения по образованию в области менеджмента. 183 с.

4. Веснин В. Р. Менеджмент: учебник. 4-е изд., перераб. и доп. М. : Проспект, 2012. 613 с.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Щербаковым И. Б.

ГУМАНИТАРНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

УДК 177.3

Т. А. Баранова (студентка группы ИСТ-511, СПбГУТ)
А. О. Жаранова (студентка группы ИСТ-511, СПбГУТ)
В. В. Капитоненко (студентка группы ИСТ-511, СПбГУТ)

МЕТАФИЗИКА НРАВСТВЕННОСТИ ТРОЛЛИНГА И АВТОНОМНАЯ ВОЛЯ

В статье проводится нравственный анализ явления троллинга в пространстве интернета, включающего в себя блогосферу и социальные сети. Основанием нравственного анализа данного явления служит моральная философия Иммануила Канта, изложенная им в работах «Критика практического разума», «Основы метафизики нравственности», «Метафизика нравов». В докладе освещаются основные положения моральной философии Канта, их практическое применение к различным сферам человеческой деятельности. Приводятся примеры явления троллинга в пространстве интернета, после чего делается заключение о соответствии их категорическому императиву и автономной воле.

троллинг, хамство, интернет, Иммануил Кант, свободная воля, автономная воля, гетерономная воля, максима, императив, категорический императив, кантианский философский подход, критика практического разума, нравственность поступков.

Виды троллинга в пространстве Интернета

Троллинг – специфический вид социальной коммуникации в пространстве Интернета, связанный с провокационной деятельностью отправителя сообщения, преследующего различные цели. Разумеется, нельзя дать однозначную нравственную оценку этому явлению. В пользу этого говорит тот факт, что далеко не все виды троллинга в пространстве Интернета ставят в качестве своей цели желание оскорбить собеседника намеренно или невольно. Так, существуют примеры троллинга, которые не только не имеют ничего общего с хамством, но также и со злым умыслом.

Например, провокационный характер *trolling*-сообщения, если он произнесен «к месту», может иметь лишь шуточный, игривый характер ради эстетического удовольствия от «удачно» придуманного каламбура или игры слов. Это вполне безобидно, при условии, что такая эстетика радует

не только отправителя, но и получателя сообщения, а не оскорбляет последнего.

Например, некто X на молодежном форуме размещает провокационное сообщение: «Хочу начать верить в Бога, но не знаю в какого? Посоветуйте». Дождавшись в ответ сообщения, в котором некто Y заявляет, что «неважно в какого, поскольку Бог – один», X реагирует удачным каламбуром: «Спасибо. Теперь начну веровать в бога Одина». Это удачная шутка, и всем становится весело. Однако если подобное сообщение размещено на сайте какой-нибудь благотворительной организации, содействующей религиозному образованию в России, то это действительно хамство.

Существуют далеко не безобидные виды троллинга, которые, тем не менее, также нельзя отнести к хамству:

1. Провокационный характер *trolling*-сообщения может преследовать цель распространения через сеть Интернет вирусов и вредоносных программ. Отвлекаясь от факта производства вирусов, являющегося самостоятельным преступлением, мы могли бы этот вид троллинга связать с имеющимся историческим типом «сплетен», в которых тиражируется образ всем известной персоны.

Например, некто X размещает провокационное объявление с текстом «Страна скорбит о безвременно ушедшем “короле” поп-музыки Филиппе Киркорове. Похороны состоятся…». Целью такого провокационного объявления является привлечение внимания читателя к сайту, который, скорее всего, содержит вирусы или вредоносные программы.

2. Провокационный характер *trolling*-сообщений может использоваться для управления каким-то сообществом, социальной группой, когда отправитель сообщения мастерски использует такой прием для прекращения или начала той или иной беседы. Такому виду троллинга можно было бы присвоить историческое название «интриги».

Например, обычно в таких сообщениях, некто, играя роль шута-зачинщика в беседе (чате, форуме), устраняет в группе тему беседы, или ссорит участников, или, наоборот, способен подбросить новую тему и привлечь сторонников.

3. Без провокаций нельзя обойтись и тем отправителям *trolling*-сообщений, чье намерение – собрать достаточно информации косвенного характера о каком-либо человеке или организации. Это можно было бы назвать провокационным «сбором слухов» или «шпионажем».

В этих случаях отправитель сообщения обычно своими репликами вынуждает кого-то произнести вслух и выдать требуемую информацию, или просто подсчитывает количество голосов, высказавшихся «за» и «против» его поста.

4. Наконец, самыми опасными были бы *trolling*-сообщения с целью «шантажа» или «запугивания».

Такие сообщения обычно рассылаются лично адресату и содержат угрозы в адрес получателя сообщения, или его родственников.

В отечественной литературе можно найти множество других классификаций троллинга. Так, например, Р. А. Внебрачных, однозначно вынося нравственно-отрицательный, но крайне расплывчатый приговор этому явлению в своей статье «Троллинг как форма социальной агрессии в виртуальных сообществах», выделяет еще несколько видов троллинга: «тролль-комментатор», «тролль-герой-любовник», «тролль-советчик» [1, с. 50–51].

Гетерономная и автономная воля в философии нравственности Канта

В отличие от спекулятивного, т. е. «умозрительного» разума, где познавательная функция сознания передается рассудку [2], который ограничен в знании истины, практический разум в философии Канта сам осуществляет контроль над способностью суждения и способностью желания в случае совершения индивидом нравственного поступка.

Всякий поступок, согласно Канту, обусловлен либо желанием, либо волей так, что воля в каких-то случаях следует желанию, а в каких-то – способна противостоять ему. В этом простом факте Кант видит указание на существование свободной воли, не обусловленной причинно-следственной связью опыта жизни. Оговорка Канта о воле не случайна: разумным субъектом Кант называет того, кто осознает свое существование как существование само по себе, «поскольку оно не подчинено условиям времени <…> и в этом его существовании для него нет ничего предшествующего определению его воли» [3, с. 426]. Согласно «Критике чистого разума» свобода присуща лишь разуму и является трансцендентальной («безусловной») и трансцендентной, т. е. «запредельной познанию» причинностью [2, с. 384–385]. Свободную волю разумного субъекта Кант определяет как автономную и помещает её исключительно в пределах разума [3, с. 351]. В то же время воля как таковая в её исполнении не может быть «оторвана» от желания и жизни, поскольку воля оформляется как личный поступок, совершаемый во времени и обусловленный природной причинно-следственной связью. Таким образом, воля изначально проявляется в состоянии гетерономии – т. е. в разнородности содержания желаний, долженствований, стремлений к удовольствию, к отсутствию страха, избегания смерти, и т. д. Гетерономии природы сознания с необходимостью передается свободная компонента автономной воли разума в виде свободы выбора. Этим способом практический разум осуществляет контроль над способностью суждения, которая, в случае нравственного суждения, преодолевает ограниченность опыта сознания и увеличивает саму свободу разума в нем.

То, как Кант провозглашает автономию свободной воли, рисует нам следующую схему: автономия воли как присущее природе сознания изначально-нравственное стремление к свободе создает свободу выбора в гете-

рономной среде желаний, но свобода выбора не порождает обязательность нравственного поступка, увеличивающего свободу разума и, поэтому, способна как увеличивать, так и уменьшать степень человеческой свободы. Кант пишет: «Автономия воли есть единственный принцип всех моральных законов и соответствующих им обязанностей; всякая же гетерономия произвольного выбора не создает никакой обязательности, а, скорее, противостоит её принципу и нравственности воли» [3, с. 350].

Регулятивный принцип практического разума в отношении способности суждения и способности желания проявляется как «нравственный закон». Таким образом, нравственный закон автономной воли не побуждает человека совершать нравственные поступки, а определяет мотивы поступков. Мотивы поступков Кант описывает в самом начале «Критики практического разума»: в случае, если человек мотивирован знанием социальных норм, то такой мотив называется максимой или императивом; в случае неосознанного следования желанию или незнания закона – такой мотив остается без специального названия. Однако именно наличие воли определяет, является ли безнравственный поступок человека злом, или нет. «Человека, однако, называют злым не потому, что он совершает злые (противные закону) поступки, а только потому, что эти поступки таковы, что дают возможность сделать вывод о его злых максимах», – пишет Кант в трактате «Об изначально злом в человеческой природе» [4, с. 21].

То, что Кант называет максимой, можно было бы определить как любую установку воли субъективного характера [3, с. 331]. Установки воли объективного характера (нормативы) – долженствования, запреты, разрешения – Кант называет законами, но они его как исследователя нравственности не интересуют. Сферу теоретического обнаружения нравственного поступка составляют такие максимы, которые называются императивами [3, с. 332]. Единственным императивом, способным определить условия автономной воли, направленной на увеличение свободы разума, является категорический императив: «Поступай так, чтобы максима твоей воли могла в то же время иметь силу принципа всеобщего законодательства» [3, с. 347]. Однако на практике, как правило, человеку бывает некогда анализировать логику своих поступков. Поэтому Жиль Делёз в работе «Критическая философия Канта: учение о способностях» охарактеризовал «голос» автономной воли в сознании человека с помощью понятия «общее моральное чувство»: «Общее моральное чувство – это согласие рассудка с разумом под законодательством самого разума» [5, с. 182].

Степень участия автономной воли в явлении троллинга

Теперь можно приступить к нравственной оценке многочисленных видов троллинга в сети Интернета. Как уже говорилось, формальным критерием нравственности троллинга как поступка, согласно И. Канту должна быть степень присутствия автономной воли в процессе волеизъявления

в гетерономной среде. Таких степеней возможно всего две: 1) либо автономная воля только создает свободу выбора для того или иного поступка, 2) либо поступок, находясь в согласии с принципом категорического императива автономной воли, не только совершается свободным выбором, но и увеличивает свободу выбора в нравственно возрастающем самосознании личности. Ранее ы выделили несколько видов троллинга: 1. троллинг-шутка; 2. троллинг-хамство; 3. троллинг-сплетни; 4. троллинг-интриги; 5. троллинг-шпионаж; 6. троллинг-шантаж.

Первый вид троллинга – шутка – формально находится в согласии с категорическим императивом Канта, поскольку несвободными в случае, если они являются объектом шутки, могут чувствовать себя только люди, лишенные чувства юмора, что само по себе является неразвитостью морального чувства.

Второй вид троллинга – хамство – является безнравственным поступком, даже в случае, если совершающий этот поступок делает это по незнанию (непониманию): это также говорит о нравственной неразвитости личности. Если же хамство творится с умыслом, то это говорит о злонамеренности и о наличии у человека максимы, разрешающей хамство в отношении других людей.

Третий вид троллинга – сплетни – является безнравственным как со стороны отправителя сообщения, так и со стороны адресата, поскольку жажда получения сплетен так же не согласуется с категорическим императивом.

Четвертый вид троллинга – интриги – будучи самоцелью, является безнравственным поступком, однако в составе гипотетически благой цели, может использоваться в качестве метода. Так, например, если кто-то пытается подобными методами развалить Интернет-сообщество, на котором пропагандируется ксенофобия.

Пятый вид троллинга – шпионаж – также является безнравственным сам по себе, но может оправдываться опять-таки в качестве «метода» для раскрытия какой-либо безнравственной деятельности и её пресечения.

Наконец, шестой вид троллинга – шантаж – лишен нравственного принципа, будучи преступлением.

Выводы

Можно сделать следующие выводы на основании результатов исследования:

1. Далеко не все виды троллинга являются безнравственными.

2. Троллинг как явление нельзя однозначно относить к разновидности социальной агрессии или хамства, реализуемых в пространстве Интернета.

3. Некоторые виды троллинга следует отнести к долженствованиям и анализировать не как троллинг сам по себе, а как процесс, являющийся частью долга, а уже в свою очередь долг анализировать не предмет нрав-

ственности. Поскольку, как замечает Кант, «… в этике понятие долга должно вести к целям, а максимы в отношении целей, которые нам следует себе ставить, должны быть обоснованы согласно моральным основоположениям» [9, с. 316].

Список используемых источников

1. Внебрачных Р. А. Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник удмуртского университета. Философия. Социология. Психология. Педагогика. Ижевск: УГУ, 2012. Вып. 1. С. 48–51, 112 с.
2. Кант И. Критика чистого разума. — Ростов н/Д. : Феникс, 1999. 672 с.
3. Кант И. Критика практического разума // Собр. соч. в 6 тт., Т. 4, Ч. 1. М. : Мысль, 1965. С. 311–504, 544 с.
4. Кант И. Об изначально злом в человеческой природе // Собр. соч. в 6 тт., Т. 4, Ч. 2. М. : Мысль, 1965. С. 5–58, 478 с.
5. Делёз Ж. Критическая философия Канта: учение о способностях // Эмпиризм и субъективность. Критическая философия Канта. Бергсонизм. Спиноза. М. : ПЕР СЭ, 2001. С. 145–225, 480 с.

Статья представлена научным руководителем,
кандидатом философских наук, доцентом Вязьминым А. Ю.

УДК 30 428

Т. Д. Басова (студентка группы РСО-51м, СПбГУТ)

МИФ КАК СРЕДСТВО ФОРМИРОВАНИЯ НОВЫХ СМЫСЛОВ В РЕКЛАМЕ

В статье рассматривает миф и реклама как феномены современной культуры, прослеживается аналогия между этими понятиями. Рассматривается взгляд философов XIX – XX в. на миф и мифотворчество. Само понятие рекламы рассматривается с точки зрения создания смыслов, формирование новой культуры и героев современного общества, которую принимают и руководствуются в жизни.

миф, реклама, символическая система, коннотация.

Мифология и реклама на первый взгляд совершенно разные понятия. Но оба являются феноменами культуры. Мифы всё больше ассоциируются с Древней Грецией, с богами Олимпа и подвигами Ясона, Геракла и других героев. Казалось, все это кануло в лету. Что касается рекламы, то это феномен массового общества XX в. Несмотря на то, что многие пытаются найти зачатки рекламы еще в далёкие времена, именно как институт реклама зарождается с появлением радиовещания, телевидения и других

средств телекоммуникации. Поэтому рекламу можно сравнить с лакмусовой бумажкой, которая проявляет характерные черты современного общества.

Реклама и мифология тесно переплетены между собой. Неправильно думать, что мифология навсегда осталась в Древнем мире. Ведь что такое миф? Это прежде всего, способ понять окружающий мир и представить какой он есть, это способ видения ситуации и разрешение возникших противоречий. Если взглянуть на хронологическую цепочку истории, то мировоззрение делилось на:

- мифологическое;
- религиозное;
- антропоцентричное.

Казалось бы, права человека упоминаются повсюду, везде им отведено ключевое место… Но! Можно ли сказать, что мифологии нет в нашем современном мире?

Миф есть. Он везде, он среди нас. И он внутри рекламы. Смотря на рекламу через призму мифологии, можно увидеть и скрытую сторону послания, а именно под «рентгеновскими лучами» мифологического инструмента можно увидеть изнанку массового общества потребления. «То есть мифологическое сознание, подобно шифрованному письму, понятно только тому, кто обладает необходимым для этого ключом» [1].

Э. Кассирер определяет миф как вторую символическую систему, в который выражен не просто знак, но именно связи, между символами, которые выступают как реальные [1]. Р. Барт описывая миф как вторую семиотическую систему. Объект его внимания связан с анализом формирования значения, в частности, с разработкой собственной концепции мифа. Он подчеркивал, что в мифе имеются две семиологические системы, т. е. миф является «вторичной семиологической системой». Также указывал, что миф нельзя рассматривать с точки зрения истины, «...миф не есть ни ложь, ни искренне признание, он есть искажение» [2].

Одним из способов, с помощью которого знак «работает» во втором порядке означивания, Р. Барт назвал «коннотацией». Коннотативные значения несут дополнительную смысловую нагрузку, они латентны и лишь подразумеваются. Они могут актуализироваться в сознании людей либо нет, поскольку их восприятие зависит от социокультурного контекста, а понимание – от «чутья» интерпретатора. Коннотативные смыслы существуют пока присутствует породивший их идеологический контекст.

Таким образом, миф надстраивается над первичной системой знаков и в дискурсивном значении придаёт им иной смысл. С помощью этих латентных сообщений разговаривает с нами реклама. Мифологи, а именно те, кто создает рекламу, создают для общества новых героев, идеальную жизнь, работу, условия, показывают людям как нужно делать и с помощью чего.

Мифы характерны и для современного общества. И в обществе потребления они играют одну из важных ролей, все также миф отражает мировоззренческую функцию, но теперь в руках рекламистов, которые пользуются этим инструментом для привлечения внимания потребителей.

Список используемых источников

1. Барт Р. Мифологии / пер. с фр. С. П. Зенкина; [вступ. ст. и коммент. С. П. Зенкина]. М . : Изд-во им. Сабашниковых, 2000. 320 с. С. 52.

2. Кассирер Э. Философия символических форм. В 3-х т. Т. 2. Мифологическое мышление. М. ; СПб. : Университетская книга, 2001. 280 с.

3. Притчин А. Н., Теременко Б. С. Миф и реклама // Общественные науки и современность. 2002. № 3. С. 149–163.

Статья представлена научным руководителем,
доктором культурологии, профессором Маняхиной М. Р.

УДК 654.739

А. А. Бычкова (студентка группы РСО-51М, СПбГУТ)

ВИРТУАЛЬНОЕ ПРОСТРАНСТВО КАК НОВЫЙ КАНАЛ ПРОДВИЖЕНИЯ

На сегодняшний день актуальна тема трансформации традиционных технологий рекламы в виртуальное пространство. Важным вопросом является то, что быстрое развитие технологий практически определяет их роль в коммерческой сфере, особенно в сфере маркетинга и рекламной деятельности. Инструменты коммуникации изменяются изо дня в день, так же как и меняется определения социальных ролей. Так, например, сегодня появляются новые социальные характеристики, такие как количество друзей в социальных сетях или количество читателей блога. То есть, если смотреть на рекламу как на коммуникационный процесс, то изменяется сама основа рекламной деятельности. Лидирующие места среди каналов распространения рекламы всё больше занимают виртуальные пространства Интернета. Поэтому для всех участников рекламного рынка сегодня важно вовремя изменить каналы общения с потребителями и перейти от традиционных средств продвижения к современным виртуальным.

соцсети, геймификация, аккаунт, визуальный контент.

На сегодняшний представители российского бизнеса характеризуют SMM как инструмент маркетинга и PR, при этом деятельность организации в социальных сетях чаще всего сопровождается только созданием группы и её технической поддержкой. Так как мало кто осмеливается посмотреть на социальные сети шире и начать использовать их разнообраз-

ней. Для тог, чтобы определить варианты использования социальных сетей и способы адаптации фирмы под них, нужно разобраться с тем, что такое социальные медиа.

Социальные медиа – это, во-первых, платформа коммуникации, которая содержит в себе различные сервисы, благодаря которым процесс общения становится интереснее и насыщеннее. То есть сферы применения социальных сетей ограничивает область, где могут быть коммуникационные процессы. Обобщая, можно сказать, что ключевая характеристика социальных медиа и их применения состоит в том, чтобы налаживать и развивать отношения между людьми. В нашем случае, отношения между сотрудниками компании с сотрудниками других компаний и клиентами.

Исходя из вышесказанного, можно ограничить сферы, в которых использование социальных медиа будут релевантны: маркетинг, PR, B2B – продажи, B2C – продажи, работа с поставщиками, работа с партнерами, техническая поддержка, *HR*.

Маркетинг. Социальные сети могут быть одним из средств реализации комплексных кампаний. Потому что социальные медиа – хороший инструмент для посева вирусных видео: например, *Y*ouTube на сегодняшний день посещает большое количество пользователей, в том числе, которые не зарегистрированные. Так с помощью SMM можно протестировать визуальную и аудиальную составляющую бренда. Можно узнать точку зрения на рекламную кампанию не только креативного агентства и точку зрения самой организации – заказчика, но также и мнение клиентов. Которое иногда не совпадает с мнением заказчика и производителя рекламы. Социальные медиа позволяют получить отклик практически мгновенно на вашу кампанию, благодаря чему её можно быстро откорректировать.

PR. Соцсети помогают эффективно работать с общественностью. В чатности, с помощью них можно консолидировать положительные отзывы на странице организации, на вкладках продуктов. Кроме того, социальные платформы подходят для нейтрализации негативного отношения. Но при одном условии, если организация готова к восприятию конструктивной критики. Вообще, соцсети – хороший PR – инструмент для превращения «хэйтеров» (*hate* – из англ. яз. – ненавидеть, люди, негативно относящиеся к продуктам/услугам организации) в лояльных клиентов, а иногда даже в адвокатов бренда.

B2B – продажи. В социальных сетях большое количество возможностей для поиска людей, которые работают в организациях – потенциальных клиентов, с которыми можно налаживать отношения и продавать свой продукт посредством соцсетей. После продажи можно и следует поддерживать общение, получать обратную связь, оставаясь полезными для клиента.

B2C – продажи. Вопреки распространенному мнению, в социальных медиа можно продать практически всё. На основных площадках, таких как

Вконтакте, Instagram, Facebook, есть возможность создания собственного полноценного интернет – магазина внутри паблка или группы. Данная система продаж в соцсетях сегодня особенно популярна среди молодых начинающих дизайнеров одежды и аксессуаров.

Работа с поставщиками. В соцсетях можно работать с поставщиками, а также с их конкурентами. В результате такой работы, можно получить либо более низкие цены, либо более выгодные условия по сделке.

Работа с партнерами. Важная составляющая работы организации в социальных медиа. Благодаря им возможно более тесное сотрудничество с партнерами организации: теми компаниями, которые своими товарами или услугами дополняют товары или услуги организации. За счет хороших отношений с партнерами можно добиться обмена клиентами.

Техническая поддержка. Все люди решают проблемы по-разному. Кому-то проще позвонить на горячую линию, кому-то вести текстовую переписку. Это означает, что организации техподдрежки в некоторых сферах нужно организовывать в социальных сетях. Сегодня это успешно используется у телекоммуникационных и других компаний.

HR. Социальные сети помогают формировать имидж организации, как интересного и хорошего работодателя. Благодаря чему можно привлечь более квалифицированных сотрудников. SMM помогают подобрать потенциальных кандидатов в среднее и высшее управленческое звено. Кроме того, с помощью соцсетей можно лучше оценить потенциального сотрудника, понять его сильные и слабые стороны. Как итог, найти действительно подходящего работника на вакансию.

Состояние SMM сегодня и инструменты онлайн-маркетинга в социальных сетях

Социальные сети – обязательная составляющая большинства онлайн-кампаний. Если в 2012–2013 гг. организации еще думали вести или нет соцсети, то теперь однозначно выбирают первый вариант.

Контент – один из основных аспектов рекламных кампаний в сетях. Кроме того, дело во всем не в постоянно улучшающихся алгоритмах поисковых систем. Сегодня нужно предлагать разнообразный интересный контент (образовательный, развлекательный), если вы хотите привлечь внимание к своему бренду.

Social + mobile. Соцсети и мобильная сфера сегодня взаимозависимы. Поэтому оптимизация контента под мобильные приложения сосетей обязательна. Так, как количество пользователей социальных сетей, заходящие в них через мобильные увеличивается с каждым годом [1].

Мониторинг и аналитика в социальных сетях позволяют пользователям оценивать эффективность проводимых онлайн-акций. Оценивать охват и целевую аудиторию коммерческих аккаунтов в соцсетях.

На сегодняшний день популярно использование рекламных посланий типа Promoted Tweets и Sponsored Stories, позволяющие сделать рекламу не похожей на себя и привлечь больше клиентов [2].

Улучшение квалификации SMM – специалистов. Сегодня умения делать посты в соцсетях для хорошего «сммщика» мало, поэтому проходит большое количество образовательных курсов по повышению квалификации.

Рост геймификации. сегодня наблюдается увеличение взаимосвязи маркетинга и игровой индустрии. Одним из основных инструментов геймификации сегодня является брендирование элементов/локаций/героев в играх.

Увеличение спроса на визуальный контент. Instagram и Pinterest в настоящее время переживают свое лучше время для монетизации аккаунтов. Использование инфографики, фото, видео, гиф-анимаций в контенте является обязательным для эффективности аккаунтов.

Использование локального маркетинга, то есть геолокация. Для успешности продвижения страниц в соцсетях следует использовать геолокационные инструменты – чекины, рекомендации, хэштеги. Эти инструменты помогают привлечь внимание новых клиентов, которые раннее не знали об организации.

Подводя итог, можно сказать что развитие SMM идет быстрым ходом, так всего за 2 последних года качество контента коммерческих и тематических аккаунтов увеличилось, как и квалификация специалистов данной сферы. Кроме того, развиваются инструменты работы с общественностью в социальных медиа. Организации постепенно переходят в соцсети для продвижения, из-за чего возможно в скором времени будут расти рекламные бюджеты в соцсетях.

Список использованных источников

1. Халилов Д. Маркетинг в социальных сетях. М. : Манн, Иванов и Фербер, 2013. 240 с.
2. Румянцев Д. Продвижение бизнеса в Вконтакте: новые практики и технологии. СПб. : Питер, 2016. 400 с.

Статья представлена научным руководителем,
кандидатом философских наук, доцентом Антоновым С. Н.

УДК 308

М. Д. Голубкова (студентка группы РСО-21, СПбГУТ)

СПЕЦИАЛЬНЫЕ МЕРОПРИЯТИЯ КАК ИНСТРУМЕНТ ДЛЯ ПРОДВИЖЕНИЯ АВТОСПОРТИВНЫХ КОМПАНИЙ

Данная статья посвящена вопросу выбора средств продвижения автоспортивных компаний. Рассматриваются результаты эмпирического исследования применения специальных мероприятий в продвижении компании ООО «Драйв Класс», а также рекомендации по повышению эффективности продвижения данной компании. Рассматриваются конкуренты компании ООО «Драйв Класс», ее целевая аудитория, специфика специальных мероприятий компании.

специальные мероприятия, продвижение компании ООО «Драйв Класс», автоспортивные компании.

В настоящее время большинство руководителей в России не считают, что специальные мероприятия – это эффективный подход к осуществлению коммуникаций как с потребителями и партнерами, так и с сотрудниками компаний, являющимися внутренними потребителями. К сожалению, не все руководители компаний готовы к нововведениям и придерживаются устаревших методов, что пагубно влияет на продвижение их дела [1].

Организация специальных мероприятий, как самостоятельная сфера рекламы и связей с общественностью, появилась всего 20 лет назад. Специальные мероприятия способствуют: формированию отношений и новых знакомств; созданию положительного имиджа организации; привлечению внимания СМИ и общественности и т. д. Наиболее популярными видами специальных мероприятий являются презентации, конференции, праздники, корпоративные события, фестивали, выставки и ярмарки, мероприятия для СМИ [3].

Актуальные методики организации и проведения специальных мероприятий является мало изученной темой в России. Несмотря на обилие качественной англоязычной литературы, например, серия книг «Special Events» Джо Голдблатта, и переведенной литературы таких авторов, как Ульрих Хальцбаур и Синди Лемер, сложно найти пособия, учитывающие российскую специфику. Кроме того, стоит отметить, что большая часть источников предлагает лишь практические решения, а не теорию.

При самостоятельной организации мероприятий следует последовательно выполнять следующие этапы: формулирование цели и задач; проведение исследования; проектирование, этап творческой разработки; планирование мероприятия: определение времени и места проведения, аудитории, определение необходимых ресурсов и распределение работ: персонала, техники и оборудования, бюджета; продвижение мероприятия

и приглашение участников; взаимодействие с партнерами, спонсорами, СМИ; работа во время мероприятия; оценка эффективности [2].

Все специальные мероприятия, как инструменты PR, направлены на продвижение товаров или услуг и формирования положительного образа бренда, однако возможны различные методы выполнения данной цели, поэтому классифицировать их можно различными способами. Так, целевой аудиторией компании ООО «Драйв Класс» с самого её зарождения были женщины от 27 лет с собственным автомобилем и достатком выше среднего. Именно направленность на женские группы отличало «Драйв Класс» от других компаний. В связи с тем, что руководитель «Драйв Класс» – женщина, данная компания выделяется на фоне конкурентов и стилем управления. Согласно данным экспертного интервью с ведущим тренером «Драйв Класс» Максимом Белюковым, женские группы подготовки с психологической точки зрения намного эффективнее, чем смешанные: в них нет давления, нет мужчин, у которых, как правило, обучение управлением автомобиля быстрее приносит результаты.

Согласно данным мониторинга сайта и анализа документов компании «Драйв Класс» существуют следующие основные услуги компании: курсы для начинающих водителей: подготовка водителей с реальным стажем вождения не более 6 месяцев; спортивная подготовка: подготовка спортсменом для участия в соревнованиях; детско-юношеское направление: управление автомобилем для детей от 12 до 17 лет; гоночная команда *JuniorRallyTeam* (собственная спортивная команда для молодых пилотов и штурманов).

Ключевыми корпоративными клиентами являются: Аксель групп, Банк Санкт-Петербург, Сбербанк, Газпром, Аларм Моторс и т. д.

В данный момент компания «Драйв Класс» использует три направления коммуникаций: целевая аудитория (дополнилась мужчинами от 27 лет с достатком выше среднего и собственным автомобилем, а также детьми от 12 до 17 лет); партнёры – сотрудничество с известными компаниями (один из наиболее эффективных способов рекламы и поиска новых клиентов, который используется исследуемой компанией); контрагенты.

По данным опроса клиентской базы ООО «Драйв Класс» было выявлено, что наиболее эффективным способом представления компании «Драйв Класс» является мероприятие за городом в выходной день (рис. 1). Опрос проводился по телефону, приняло участие 78 человек, являющихся клиентами ООО «Драйв Класс.

Сравнительный анализ среди наиболее крупных конкурентов по показателям эффективности (опыт работы на рынке; количество крупных клиентов за последние пять лет; уровень подготовки тренеров; количество призов и наград; количество основных услуг; участие в спортивных мероприятиях) позволил разработать сравнительную таблицу деятельности данных компаний (табл. 1).

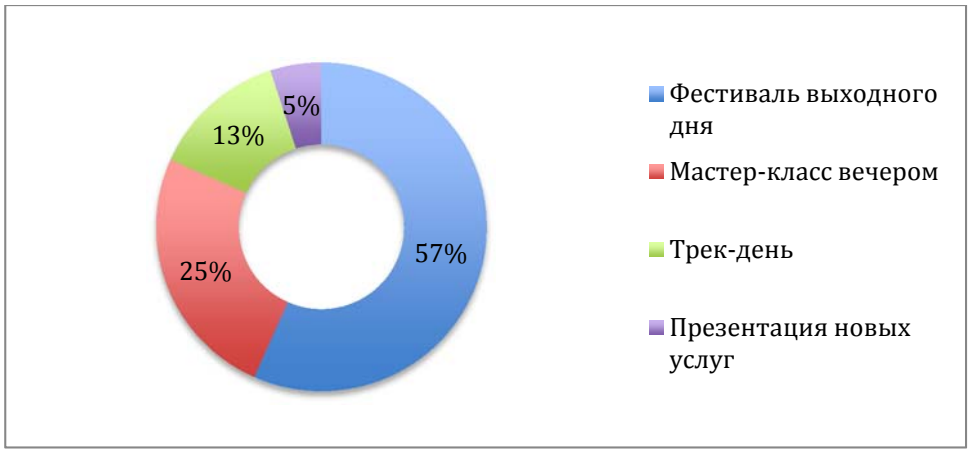


Рис. 1. Результаты опроса потенциальных участников

ТАБЛИЦА 1. Анализ конкурентов компании

	Опыт работы на рынке (лет)	Количество крупных клиентов за последние пять лет	Уровень подготовки тренеров	Количество наград, призов	Количество основных услуг	Участие в мероприятиях
ДрайвКласс	11	21	высший	30	12	+
Моисеев-Грахов	19	15	высший	27	10	+
Автошкола Добрецова	6	0	средний	5	3	+
Bashmakov DS	1	2	высший	3	7	+
ФизикаДвижения	8	14	средний	23	9	+

Таким образом, данные таблицы 1 показывают, что лидером по определенным конкурентным показателям стал ЦВТ Драйв Класс. Для определения наиболее оптимального способа продвижения были проведены исследования PR-деятельности компании Драйв Класс.

На данный момент, основываясь на документации компании, можно заключить, что для продвижения своих услуг ЦВТ Драйв Класс использует следующие PR-технологии: комментарии; интервью и статьи руководителя компании; публикации в СМИ об удачных проектах; участие в отраслевых мероприятиях и конкурсах; использование фирменного стиля организации; специальные мероприятия.

Одним из самых удачных проектов компании за последние годы стало создание уникального автомобильного фестиваля «ФИЛОДРАЙВ». 22 февраля 2015 г. был проведен первый фестиваль, включающий в себя соревновательную часть для участников фестиваля и обширную развлекательную программу для спонсоров.

Подобная деятельность увеличивает количество упоминаний компании в средствах массовой информации и повышает её узнаваемость.

Для более эффективного продвижения компании необходимо делать акцент именно на компании «Драйв Класс» как организаторе: это позволит

повысить количество упоминаний о компании, привлечь новых спонсоров и партнеров, а также создать информационный повод. В качестве инструментов для привлечения внимания к фестивалю необходимо приглашать «звёзд», которые будут взаимодействовать со зрителями на фестивале, проводить мастер-классы от компаний-участников фестиваля. Использование бартерных условий также станет удачным приёмом в продвижении, но основной составляющей, учитывая целевую аудиторию, должно стать активное продвижение в социальных сетях. Важно создание группы или публичной страницы компании в таких социальных сетях, как Вконтакте, Facebook, Instagram и Twitter.

Для привлечения аудитории необходимо постоянное обновление и создание уникальной информации. Рекомендуется вести видеосъемку, брать интервью у участников во время мероприятия и распространять данную информацию в социальных сетях; поддерживать интерактивный формат с помощью проведения конкурсов и розыгрышей. В социальных сетях возможно раскрытие персональной информации об организаторах и участниках. Рекомендуется проведение мониторинга обратной связи с помощью «лайков», «репостов», «комментариев» и статистике посетителей группы или публичной страницы; а также развитые группы и публичной страницы в социальных сетях, что может привлечь большее количество спонсоров и партнеров, а также поможет в оценке эффективности мероприятия.

Список используемых источников

1. Романцов А. Н. Event-маркетинг : Сущность и особенности организации: практ. пособие. 2-е изд. М. : Дашков и К, 2012. 116 с.

2. Шишкин Д. П., Гавра Д. П., Бровко С. Л. PR-компании : методология и технология : учеб. пособие. СПб. : Роза мира, 2004. 187 с.

3. Шумович А. В. Великолепные мероприятия: Технологии и практика event management. 3-е изд. М. : Манн, Иванов и Фербер, 2008. 336 с.

Статья представлена научным руководителем,
кандидатом психологических наук, Беловой Е. В.

УДК 308

Е. А. Дорохова (студентка группы РСО-51м, СПбГУТ)

СПОСОБЫ ПРОДВИЖЕНИЯ КОМПЬЮТЕРНЫХ ИГР В ИНТЕРНЕТЕ

Данная статья посвящена вопросу продвижения компьютерных игр. Индустрия развлечений, в частности компьютерных игр, имеет свою специфику электронного продвижения игрового продукта. Для наилучшего формирования, поддержания имиджа, интереса у игроков или информирования аудитории о выходе новой видеоигры, какого-либо обновления используют различные сочетания интернет-технологий. Рассматривается авторская модель продвижения видеоигр.

продвижение компьютерных игр, интернет-технологии, электронное продвижение, модель продвижения видеоигр, продвижение онлайн.

В конце 30-х годов XX в. известный нидерландский философ, Йохан Хейзинга [1] высказал мысль, что, если продумать до конца все, что мы знаем о человеческом поведении, оно покажется нам всего лишь игрою: человеческая культура возникает и разворачивается в игре, как игра. Игра – это форма деятельности, наделенная смыслом, социальная функция, игра основывается на обращении с определенными образами, рассматривается как фактор культурной жизни, аспект социализации.

Сегодня общество уходит от прежних «игр», предназначенных для скорейшего обучения, т. е. вовлечения подрастающего поколения во взрослую жизнь. Имитационные игры, социально-ролевые игры, настольные игры, компьютерные игры, – перечень форм современных игр почти бесконечен. Игра и жизнь, в определенном смысле, неразделимые понятия, они всегда присутствовали в жизни человека, позволяя тренировать навыки, решать сложные задачи. Например, знаменитый исследователь креативного мышления Пол Слоан [2] рекомендует играть в игры (шахматы, монополия и др.) для развития незаурядного, инновационного, изобретательского мышления.

Игры эволюционировали в те формы, которые позволяют приспосабливаться к потребностям среды обитания. Для того, чтобы играть в игры, необходимо, знать о них. В силу данной причины, способы продвижения компьютерных игр являются важнейшей детерминантной, обуславливающей их деструктивное или конструктивное влияние. Проект системной модели продвижения компьютерных игр представлен на рисунке 1.

Как видно из рисунка 1, в создании благоприятного продвижения видеоигры участвуют такие параметры, как: условия игры (наличие финансов, свободного времени, информации об игре и т. д.), особенности целевой аудитории (в первую очередь возрастные, которые являются основным

классифицирующим критерием, а также мотивационные, как ведущие потребности, которые реализуются в игре); способы продвижения игр (которые зависят от характеристик целевой аудитории), а также характеристики самой игры (жанр, сюжет и т. д.).

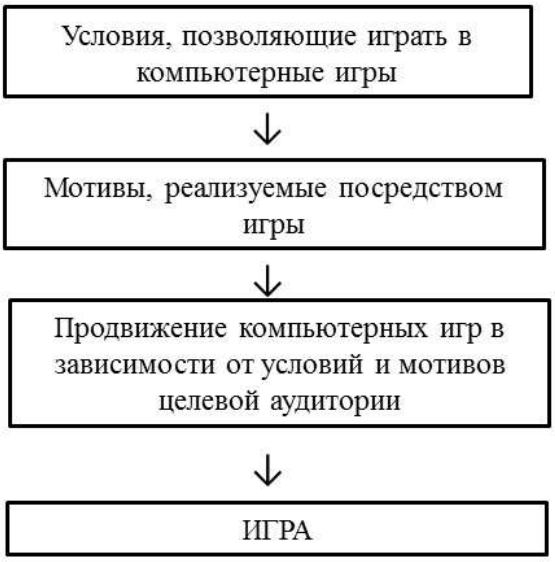


Рис. 1. Проект системной модели продвижения компьютерных игр

На сегодняшний день Интернет – это один из самых мощных и эффективных каналов продвижения видеоигр. День за днем конкуренция между компаниями-разработчиками и их желание заинтересовать, как можно большую аудиторию игроков различных стран, растет в геометрической прогрессии. Для того, чтобы выбраться в ТОП самых популярных разработчиков видеоигр наряду с Blizzard Entertainment, IdSoftware, Ubisoft и т. д., поддерживать себя на вершинах рейтинга, мало выпускать качественный по всем параметрам продукт, необходимо продвижение продукта и его производителя на специализированном рынке компьютерных игр.

Данный медиа канал позволяет более точно сегментировать и быстро доносить сообщения до целевой аудитории, также этот способ коммуникации удобно использовать при малобюджетном продвижении компании и при определении критериев измерения его эффективности.

Продвижение компьютерных игр и компаний-разработчиков может осуществляться более эффективно, если повысить доверие аудитории к данному продукту при помощи современных интернет-технологий [3].

Во-первых, необходимо применять взаимодействие с помощью корпоративного сайта. Официальный корпоративный сайт – неотъемлемая часть продвижения любого бизнеса в Интернете, а тем более игрового. Продвижение любого коммерческого предприятия сети Интернет начинается с создания корпоративного сайта: это удобный, современный и перспективный способ привлечения внимания как целевой аудитории, так и остальных. Очень важен тот факт, что интерактивные узлы веб-сайтов поз-

воляют ознакомиться с информацией о товарах, услугах компании, оформить заказ, оставить комментарии на форумах, отзывы и т. д.

Во-вторых, возможна оптимизация сайта для социальных сетей (Social Media Optimization, SMO). Суть данной технологии заключается в принятии мер по привлечению на корпоративный сайт пользователей социальных сетей. Оптимизация сайта для социальных сетей подразумевает работу по видоизменению сайта для лучшего его восприятия пользователями, повышения его цитируемости и ссылок на него в социальных медиа.

В-третьих, возможна поисковая оптимизация (Search Engine Optimization, SEO) – комплекс изменений контента сайта для того, чтобы тот считался поисковой системой наиболее релевантным определенному запросу.

Реклама в сети Интернет отличается разнообразием. Так, баннерная реклама – это графическое рекламное сообщение (баннеры), размещаемое на тематических площадках сети и имеющее гиперссылку на веб-сайт продвигаемой фирмы. Баннерная реклама является самым популярным способом увеличения посещаемости веб-сайта. Контекстная реклама – текстовое сообщение, которое размещается в результатах запроса в поисковых системах. Подобного рода реклама зависит от поискового запроса пользователя или от тематики страницы, на которой данная реклама размещена. Видео-реклама – это размещение рекламных видео-роликов (онлайн-видео) на различных тематических сайтах, способствующих повышению имиджа компании, продвижению ее товаров и услуг, формированию узнаваемости бренда. Иногда выделяют еще одну составляющую поисковой рекламы – медийно-контекстную рекламу (контекстно-баннерную). В отличие от обычной контекстной рекламы данный вид рекламы представляет собой не короткое текстовое объявление, а показ графических объявлений, рекламных баннеров.

Реклама в социальных сетях – это размещение рекламы в социальных сетях с учетом таргетинга и ретаргетинга, а также в сообществах социальных сетей с большим количеством подписчиков определенной аудитории. Преимущества данного типа рекламы в том, что он позволяет точно определить целевую аудиторию. Реклама игр внутри других игр (в виде видеоролика или баннерной рекламы) время от времени появляется во время схожей по тематике игры.

Рассмотрим еще несколько способов продвижение компьютерных игр в Интернете. Продвижение в социальных сетях (Social Media Marketing, SMM) – это продвижение интернет-ресурсов в социальных сетях, блогах, на форумах, порталах и т. д., задачей которого является привлечение внимания аудитории. Под e-mail маркетингом подразумевается рассылка сообщений, содержащих информацию о компании-производителе, ее видеоиграх, обновлениях и бонусах игрокам или потенциальным игрокам при помощи электронной почты.

Так, например, существует реклама, распространяющаяся с помощью электронной почты: это и рассылки подписчикам, которые осуществляются при условии подписки пользователя на информирование о новостях, обновлениях, и реклама веб-сайта компании-разработчика. Размещение рекламы в новостных рассылках, как правило, осуществляется аналогично баннерной рекламе в Интернете, но отличается по способу ограничения целевой аудитории, т.к. в данном случае интересы аудитории могут зависеть не только от тематики рассылок, но и от информации в анкете подписчика. Несанкционированная рассылка (спам) – рассылка рекламы без согласия на то пользователя.

Медиарилейшнз – это построение отношений и работа со средствами массовой информации в Интернете, в рамках данной технологии можно также говорить о создании PR-текстов, информационных поводов, о материалах для распространения в процессе организации и проведения новостных событий и публикаций в СМИ. Вирусный маркетинг – это технология распространения рекламы, при которой продукт или его реклама так влияют на получателя информации, что он «заражается» идеей распространения этого продукта или его рекламы и становится главным распространителем информации. Оформление мобильного приложения в магазинах приложений (например, AppStore)– технология, позволяющая привлекать игроков при помощи необычного, уникального оформления приложения и положительных отзывов (в результате определяющего рейтинг приложения). Данная технология больше подходит для мобильных игр и онлайн игр.

Таким образом, для эффективного продвижения необходимо использовать комплекс способов продвижения компании в сети Интернет. Системный подход к продвижению компьютерных игр требует оценки множества параметров: условий самого процесса игры (как внешних факторов игровой деятельности), особенностей целевой аудитории (возрастных и мотивационных), способов продвижения игр (которые зависят от характеристик целевой аудитории), а также характеристики самой игры.

Перспективы развития индустрии компьютерных игр безграничны. Инновационные способы продвижения можно использовать для продвижения в игровой индустрии не только самой игры, но и вопросов науки, культуры, образования, социально-значимых тем. Компьютерные игры – это инновации в сфере компьютерных технологий, это постоянно растущая целевая аудитория. Как позитивный ресурс развития общества, компьютерные игры можно использовать по-разному: в самом контенте компьютерных игр решать социально значимые задачи; в рамках PR-сопровождения компьютерных игр возможно продвижение других, значимых для общества проектов.

Список используемых источников:

1. Хейзинга Й. HomoLudens. Человек играющий. СПб. : Изд-во Ивана Лимбаха, 2011. С. 20, 22
2. Слоан П. Искусство мыслить незаурядно / пер. с англ. К. : Companion Group, 2011. 224 с.
3. Ринин Ф. Ю. Интернет-маркетинг. Полный сборник практических инструментов. М. : Эксмо, 2012. 224 с.

Статья представлена научным руководителем,
кандидатом психологических наук Беловой Е. В.

УДК 94(47).084.8

С. М. Елисеев (студент группы ИКТ-402, СПбГУТ)
К. О. Кобзев (студент группы ИКТ-402, СПбГУТ)

ЛЕНД-ЛИЗ В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

В данной статье рассмотрен один из самых спорных и обсуждаемых в настоящее время эпизодов Великой Отечественной войны – лend-лиз. В чём правда, а в чём вымысел? Вокруг чего сохраняется столько загадок, тайн и нерешённостей? Какое значение лend-лиз имел для СССР? Дать точный ответ на эти вопроса помогут только факты и реальные цифры.

лend-лиз, Великая Отечественная война, антигитлеровская коалиция, СССР, США, Англия.

До настоящего времени остается большое число эпизодов, имен и событий в истории СССР, о которых стараются много не говорить, а некоторые важные факты не достигли достойной огласки. В числе таких - американский лend-лиз Советскому Союзу. По определенным политическим соображениям точные цифры этих поставок были строго засекречены вплоть до 1992 года. Мифы о лend-лизе – одна из самых популярных тем в истории Второй мировой войны.

Внешняя экономическая помощь

Лend-лиз (от англ. «lend» — давать взаймы и «lease» – сдавать в аренду) – своеобразная программа кредитования союзников Соединенными Штатами Америки посредством поставок техники, продуктов питания, оборудования, сырья и материалов.

Закон о лend-лизе (англ. *Lend Lease Act*; полное название – «Закон по обеспечению защиты Соединенных Штатов», англ. *An Act to Promote the*

Defense of the United States) был принят конгрессом США 11 марта 1941 г. СССР присоединился к программе в ноябре этого же года.

Советскому Союзу после разрушительных Первой мировой и Гражданской войн достались экономические проблемы, кризис системы образования, голод, нищета, тлеющие конфликты почти по всей протяжённости границ.

В таком состоянии СССР принял участие в Великой Отечественной войне, спешно эвакуируя промышленность, разворачивая новые производства и перестраивая на ходу экономику страны. Любое оружие, любые припасы требовались незамедлительно и в несколько раз больше, чем было на момент начала боевых действий. В таких условиях, безусловно, ценна любая внешняя экономическая помощь. Ею и стал ленд-лиз.

Рис. 1. Английские женщины готовят танк «Матильда»
к отправке в СССР по ленд-лизу

Проблемы доставки

Как только стало очевидным, что вскоре в Советский Союз начнут поступать грузы из Великобритании и США, сразу встал вопрос о маршрутах их доставки. Три основных маршрута – арктический, персидский и тихоокеанский – обладали каждый как своими преимуществами, так и недостатками.

- Тихоокеанский. Самый близкий и безопасный путь из Америки в СССР летом и осенью 1941 г. пролегал через Тихий океан.

Этот маршрут функционировал всю войну, и по нему в Советский Союз доставили 47 % импортных грузов.

• Персидский. Этот маршрут пролегал через Персидский залив и Иран. Для поставок по нему потребовалось отстроить с нуля современную автомобильную дорогу буквально через всю страну.

Из-за этого Персидский маршрут смог начать функционировать только в середине 1942 г. Впоследствии, он принял на себя 23,8 % всех поставок союзников.

• Арктический. Этот маршрут являлся самым целесообразным – через Норвежское и Баренцево моря в Архангельск и Мурманск. В решающий период 1941–1942 гг. северное направление оказывалось наиболее эффективным. Всего за годы войны северным маршрутом доставлено 36 % всех военных грузов.

Кроме того, существовал и воздушный путь ленд-лиза – трасса Уэлькаль-Красноярск. По ней своим ходом, в тяжелейших климатических и погодных условиях, удалось перегнать несколько тысяч самолётов: истребителей, бомбардировщиков и транспортников.

Оружие и военная техника

Говоря о ленд-лизе, наибольший интерес вызывает союзническая военная техника.

• Танки. В годы войны в СССР было поставлено из США: легкий M3A1 “Стюарт”, средний M4A2 “Шерман” и др. Из Англии: пехотные “Валентайн” и «Матильда», тяжелый «Черчилль» и др. Всего в период боевых действий было поставлено по ленд-лизу 12 980 тыс. танков. Помимо этого, в СССР поставлялись самоходные артиллерийские и зенитные установки, а также принципиально новый класс техники для Красной Армии – бронетранспортеры.

• Авиация. Поставки самолетов по ленд-лизу пришлись как раз в самое трудное для советских ВВС время. Среди них были: Белл P-39 «Аэрокобра», Кертисс «Китихоук» и «Томагаук», Дуглас A-20 «Бостон» и другие самолеты из США. Англия поставляла: Хоукер "Харрикейн", Супермарин "Спитфайр" и Хендли-Пейдж "Хемпден". В общей сложности за все время СССР получил 22 206 самолетов.

• Флот. Ощутимо пополнился импортными кораблями и судами, различным вооружением и техникой советский флот.

Так, в результате ленд-лизовских поставок количество сторожевых кораблей на Тихоокеанском флоте в 1945 г. по сравнению с началом войны увеличилось в 4–5 раз. Число тральщиков в составе ВМФ СССР увеличилось вдвое. В период 1943–1945 гг. из США поступали десантные судна специальной постройки, которых советский флот фактически не имел, хотя потребность в них была велика. Северный флот начал пополняться американскими торпедными катерами типа "Воспер" (A-1), "Хиггинс" (A-2) и ЭЛКО (A-3). Кроме всего этого, Красная Армия получила более 6 мил-

лионов винтовок и пулеметов, 14 тысяч артиллерийских орудий, 345 тыс. т боеприпасов. Ленд-лизовским порохом и взрывчаткой было снаряжено около трети выпущенных по врагу боеприпасов за все годы войны. Каждый пятый истребитель и каждый пятый бомбардировщик военного времени в СССР были произведены за границей. Около четверти парка зенитной артиллерии, включая орудия больших калибров, прибыли в страну по ленд-лизу.

Транспорт

Автопарк Красной Армии также в большой степени был обеспечен за счет западных поставок. К концу войны в автомобильном парке РККА поставленные по ленд-лизу машины составляли 32,8 %.

Здесь можно было встретить Dodge WC 51, Chevrolet G-7107, Dodge T-203-B, International M-5–6 и ряд других. Наиболее популярным и массовым ленд-лизовским автомобилем в СССР в годы войны был Studebaker US6 U3, который использовался в основном в качестве артиллерийского тягача.

Однако вплоть до конца войны использование автотранспорта сковывалось недостатком автобензина.

Еще более заметной была роль поставок по ленд-лизу в сохранении на необходимом уровне численности советского парка локомотивов и железнодорожных вагонов. Поставки по ленд-лизу превосходили общее советское производство паровозов в 1941–1945 гг. в 2,4 раза, электровозов в 11 раз, а вагонов в 10,2 раза, тем самым предотвратив паралич железнодорожного транспорта в Советском Союзе.

Также функционирование советского железнодорожного транспорта было бы невозможно без ленд-лизовских поставок железнодорожных рельсов.

Вспомогательное оборудование и ресурсы

Высокотехнологичные и наукоёмкие производства в годы войны для СССР были непозволительной роскошью. Радиостанции, в том числе дальней связи, миллионы километров телефонного провода, многоканальные телефоны, телетайпы, радиомаяки, радары и прочая сложная аппаратура прибывали в СССР в огромных количествах. Советские танки оснащались ленд-лизовскими радиостанциями, например, «Беспроводным набором № 19, Мк. III» канадского производства.

Также в СССР по ленд-лизу поставлялись сложное медицинское оборудование, лекарства, расходные материалы, хирургические передвижки, рентгеновские аппараты, стерилизаторы и прочие медицинские приспособления.

Наиболее важными для Советского Союза были поставки сложных станков и промышленного оборудования.

Поставки союзниками металлопроката и чистых материалов (алюминия, меди, легирующих добавок) имели решающее значение для многих отраслей советской промышленности.

Одним из наиболее узких мест советской экономики перед войной было производство авиационного бензина. Особенно не хватало высокооктановых бензинов. В Советском Союзе импортный авиабензин и светлые бензиновые фракции использовались почти исключительно для смешивания с советскими авиабензинами с целью повышения их октанового числа.

Американские поставки играли существенную роль в снабжении СССР автопокрышками. Ленд-лизовские покрышки составили 43,1 % от советского производства.

Бытовые товары

Материально-техническая база аграрного сектора оказалась почти разрушенной. Основную часть техники, обслуживавшей колхозы и совхозы, пришлось передать фронту. Требовалась помощь союзников в поставке продовольствия.

Для Советского Союза значительная часть продуктов поступала в виде: консервированной или мороженой свинины и баранины, концентратов, сливочного масла, яичного порошка, сгущенного и порошкового молока. Поставки отборного зерна посевного фонда в 1942 г. позволили закрыть даже вопрос сорванных посевных работ.

Ленд-лизовский сахарный песок составил около 41,8 % от общего уровня советского производства. Наряду с этим, союзники поставляли хлопок, кожу, одеяла, спирт.

Общее количество произведённой для СССР обуви измеряется миллионами пар в год. Даже после войны американские ботинки остались на советских складах в количестве более четырёх миллионов.

По нормам питания ленд-лизовские поставки закрывали потребность десяти миллионов бойцов на протяжении более чем полутора тысяч дней – дольше, чем продлилась Великая Отечественная война!

Значение для СССР

Одну из самых красноречивых оценок ленд-лизу дал И. В. Сталин в письме президенту США Трумэну от 11.06.1945:"соглашение, на основе которого США на протяжении всей войны в Европе поставляли СССР в порядке ленд-лиза стратегические материалы и продовольствие, сыграло важную роль и в значительной степени содействовало успешному завершению войны против общего врага – гитлеровской Германии".

Роль ленд-лиза – не в относительной цене поставок и не в том, какой процент от совокупного производства СССР они составили, а в их абсолютной значимости. Всякий раз, говоря о каком-то из видов поставленной техники, следует задаваться вопросом, а мог бы он вообще быть построен в СССР в таком количестве за приемлемый срок – и от продукции какого военного завода пришлось бы ради этого отказаться?

Значимость западных поставок в годы Великой Отечественной войны традиционно преуменьшается советской историографией еще со времен начала "холодной войны".

Это было направлено на поддержание утверждения об "экономической победе социализма" в Великой Отечественной войне и о превосходстве советской военной экономики над военными экономиками капиталистических стран. Касательно этого на сегодняшний день существует множество мнений, как и о самом ленд-лизе.

Вопрос оплаты и политическая составляющая

Вопрос оплаты – одна из самых обсуждаемых тем, говоря о ленд-лизе. Этот момент стал настолько выгодным инструментом холодной войны, что от него нельзя было отказаться. Поэтому западные страны не списали СССР долг по ленд-лизу, как остальным государствам-должникам.

А в современном типичном споре о фактической стоимости поставленного товара и требуемой сумме выплат может прозвучать практически любая цифра. Окончательные выплаты закончились только в 2006 г.

Насколько полезен был ленд-лиз для СССР, настолько и выгоден для союзников. Это был дальний продуманный расчет.

Соединенные штаты выжали экономический максимум с этой войны. Масштабные военные заказы повлекли за собой рост военного производства и американской экономики в целом.

Как бы там ни было, ленд-лиз занимает значительное место среди иных крупных военных, политических или экономических операций Союзников против стран Оси. Благодаря ему эффективность ведения боевых действий РККА из-за военных и экономических потерь не упала так сильно, как могла бы, а тяготы и лишения мирного населения в тылу и на пострадавших от войны территориях СССР были заметно сглажены.

Но никогда нельзя забывать, что светлым будущим и мирным небом над головой мы обязаны павшим на фронтах воины солдатам, ветеранам, несломленному духу и великому патриотизму советского народа!

Список используемых источников

1. Лапиков М. Мифы и факты о ленд-лизе [Электронный ресурс]. URL: http://warspot.ru/3724-mify-i-fakty-o-lend-lize (дата обращения 01.05.2016).

2. Стеттиниус Э. Ленд-лиз – оружие победы [Электронный ресурс]. URL: http://militera.lib.ru/memo/usa/stettinius/06.html (дата обращения 01.05.2016).

3. Баранов А. Е. Ленд-лиз. Северные конвои. Стратегическое назначение [Электронный ресурс]. URL: http://mil.ru/ winner_may/ allied_troops/ more.htm?id= 12008558@ cmsArticle (дата обращения 01.05.2016).

4. Документальный фильм "Война и мифы". 5 серия: "Ленд-лиз. Вклад союзников" [Электронный ресурс]. URL: https://cont.ws/post/253100 (дата обращения 01.05.2016).

Статья представлена научным руководителем,
кандидатом исторических наук, доцентом Мосеевым В. И.

УДК 308

А. А. Ильменев (студент группы РСО-21, СПбГУТ)

ВОЗМОЖНОСТИ ПРОДВИЖЕНИЯ БИЗНЕСА СРЕДСТВАМИ PR

Данная статья посвящена вопросу продвижения малого и среднего бизнеса на примере компании «Tyre Plus». Рассматриваются результаты эмпирического исследования (экспертного интервью, опроса, мониторинга сайтов и анализа документов) продвижения компании «Tyre Plus», перспективы развития бизнеса в современных экономических условиях.

продвижение компании «Tyre Plus», малый и средний бизнес.

Возможности продвижения бизнеса средствами PR – это перспективное направление исследований, позволяющее сделать организации более конкурентоспособными. При этом каждый год появляются всё новые способы продвижения компаний, которые требуют уточнения эффективности их использования. На примере шинных центров, рассмотрим приёмы, которые позволяют в условиях высокой конкуренции в бизнесе повысить успешность компаний и их продукции благодаря правильному продвижению организации и ее товаров на рынке.

Малый бизнес – это крупный сектор рынка, среда которого постоянно развивается, меняясь не только качественно, но и количественно. Даже за последние годы кризиса в нашей стране, согласно данным федерального бизнес агентства, «количество индивидуальных предпринимателей в России увеличилось до 3,5 млн человек». Как сказал Джорж Кохон – создатель сети ресторанов быстрого питания «McDonald`s» в России: «Конкуренция – это здорово, ведь в результате мы только становимся сильнее. В лю-

бом случае, посетители голосуют ногами: если они приходят, значит, проголосовали за нас» [1, 2].

Анализ литературных данных [1, 2] показал, что продвижение является совокупностью маркетинговый мероприятий, действий, с помощью рекламы, PR, персональных продаж, стимулирования сбыта, а также применение иных маркетинговых коммуникаций, которые предпринимаются товаропроизводителями, преследуя цель увеличения сбыта, повышения спроса, повышения лояльности потребителей и привлечение новых.

Следует отметить, что важными являются функции продвижения: создание образа престижности, низких цен, инноваций; информация о товаре и его параметрах; сохранение популярности товаров или услуг; изменение образа использования товара; создание энтузиазма среди участников сбыта; убеждение покупателей переходить к более дорогим товарам; ответы на вопросы потребителей; благоприятная информация о компании.

С развитием информационных технологий происходит и развитие маркетинга, появляются новые технологии рекламирования и информирования общественности. С недавнего времени появились такие известные и широко применяемы методы продвижения в Интернете, как поисковая оптимизация и SEO; контекстная реклама; маркетинг в социальных сетях; управление репутацией в Интернете и видеореклама [1, 2].

В ходе эмпирического исследования были проанализированы данные министерства экономического развития Российской Федерации, а также данные, полученные в результате посещения конференции стратегического партнера – российского производителя автомобильных шин «Cordiant». Экономические факторы, влияющие на бизнес представлены в таблице 1.

ТАБЛИЦА 1. Экономические факторы, влияющие на бизнес в России

	2015 г.	2016 г.
Цены на нефть Urals (мировые), дол./бар.	53,0	50,0
Индекс потребительских цен на конец года	12,2	6,4
Курс доллара среднегодовой, рублей за доллар	61,0	63,3
Темп роста ВВП, %	−3,9	0,7
Промышленность, %	−3,3	0,6
Инвестиции в основной капитал, %	−9,9	−1,6
Реальные располагаемые доходы населения, %	−4,0	−0,7
Реальная заработная плата, %	−8,1	−0,2
Оборот розничной торговли, %	−8,5	0,4

Таблица 1 показывает состояние рынка на данный момент и прогноз на 2016 г., на ней можно увидеть, насколько платежеспособны будут клиенты и в каких условиях придется работать малому бизнесу.

Рассмотрим данные о новых продуктах компании и рекомендации по ведению успешного бизнеса в сложный кризисный период: инвестиции в сервис; участие в программе расширенной гарантии на продукцию; активная работа с грузовым и сельскохозяйственным сегментами. По результатам эмпирического исследования были получены данные о рейтинге продаваемых автомобилей. Данный показатель является важным, т. к. от него зависит прогноз по продажам шин на определенные автомобили со своими уникальными типоразмерами колес тройка лидеров: «Lada Granta», «Hyundai Solaris» и «KIA Rio».

Следует отметить, что согласно прогнозу продаж легковых автомобилей, начиная с 2012 г., продажи новы автомобилей неуклонно падают [1, 2]. При этом согласно данным компании «Cordiant», в 2016−2017 гг. шинный рынок продолжит снижение.

Результаты экспертного интервью с владельцем сети шинных центров «Tyre Plus», позволили прийти к следующим основным выводам, что с учетом перспектив развития компании, в данный момент бизнес продвигается следующими дополнительными способами: дополнительные услуги в подарок − дополнительными услугами является бесплатный шиномонтаж при покупке комплекта шин; топливные карты выдаются при покупках во время акции, с помощью которых можно получить скидку на автозаправочных станциях; реклама на радио – реклама на местных радиостанциях до сих пор активно используется, ибо целевая аудитория «автолюбители» активно слушают радио в своих автомобилях; наружная реклама − также используется собственная наружная реклама в городе и области, представленная виде дорожных баннеров; промо-акции «Проверь давление в шинах». Так, несколько раз применялась промо-акция «Проверь давление в шинах»: на парковках крупнейших магазинов города ставилась большая палатка с логотипами Michelin и Tyre Plus, а также работал аниматор в костюме Бибендума и приглашал поучаствовать в акции, так любой желающий мог проверить давление в шинах автомобиля, подкачать их если потребуется и за это получить купон на скидку в магазинах и оперативную консультацию. Как способы продвижения применяется и интернет-магазин (общий интернет магазин (tyreplus.ru)), баннерная реклама в интернете (присутствие местных шинных центров в интернете выражено интернет-магазином и баннерной рекламой на городских порталах города).

Согласно проведенному опросу клиентов шинных центров (опрос проводился в шинных центрах в Оренбургской области, а котором участвовало 76 клиентов), узнаваемость шинного центра основана на эффективности осуществления рекламы в Интернете, промо-акций, баннерах в городе, радио, рекомендаций знакомых, работы в социальных сетях.

На данный момент, разработана анкета для клиентов, для получения актуальной информации, которая поможет выстроить дальнейшую стратегию продвижения компании, а также собраны контакты опрашиваемых для создания базы потенциальных клиентов.

Дальнейшие перспективы исследований – дополнительное эмпирическое исследование по поиску самых эффективных каналов продвижения. Исходя из собранных данных, можно сделать вывод, что на данный момент эффективными и перспективными методами продвижения будут: создание интернет магазина (сайта); регистрация сервера компании; создание рекламы в сети Интернет; прямой-маркетинг; вирусный маркетинг.

Список используемых источников

1. Душкина М. Р. PR и продвижение в маркетинге: коммуникации и воздействие, технологии и психология. СПб. : Питер, 2009. 560 с.
2. Ринин Ф. Ю. Интернет-маркетинг. Полный сборник практических инструментов. М. : Эксмо, 2012. 224 с.

Статья представлена научным руководителем,
кандидатом психологических наук Беловой Е. В.

УДК 004.42

С. А. Королёв (студент группы ИСТ-21, СПбГУТ)
М. В. Котлова (старший преподаватель, СПбГУТ)

ОПЫТ РАЗРАБОТКИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ

Различные организации используют электронные табличные документы в совершенно различных областях, благодаря их широким возможностям, для небольшого количества данных они удобны как в качестве аналитической системы, так и системы хранения данных. Когда количество информации возрастает, без базы данных становиться сложно обходиться. Сложность в том, что интеграция базы данных в существующие бизнес процессы не так проста, потому что электронные таблицы являются важной частью информационного взаимодействия и не предусматривают дополнительного промежуточного сервиса работы с данными в виде БД. Поэтому задача работы проектирование системы и разработка элементов ИС для сбора табличных документов, хранения анализа и отчета данных из них.

информационная система, электронный документооборот, табличные документы, анализ данных, web технологии.

Во всех сферах деятельности, люди, так или иначе, работают с большим объемом информации. Для ее получения, обработки и передачи используют различные способы группировки и представления. Таблицы представляют собой один из наиболее простых и эффективных способов группировать и представлять данные.

На компьютерах таблицы хранятся в электронных документах различного формата. Одним из наиболее популярных форматов являются форматы «xls» и «xlsx», которые соответствуют офисному программному пакету MS Office, в частности Excel. Это программное обеспечение используется практически повсеместно, в том числе государственными учреждениями и частными предприятиями, благодаря множеству возможностей по работе данными. Такая широкая функциональность привела к тому, что MS Excel используют в документообороте предприятия, и в его аналитике.

Автоматизация управленческого учета часто является следствием поэтапного развития компании. По мере увеличения количества учетных операций и ответственных за ввод данных, увеличивается потребность в оперативной обработке и автоматизации большинства операций. С ростом клиентской базы и ассортимента, растет объем анализируемой информации и количество пользователей этой информацией.

На этапе образования компании или филиала, как правило, предприятие начинает вести учет в excel, где можно быстро настраивать и формировать различные виды отчетов.

С ростом предприятия, резко возрастает количество финансовых и производственных операций. Неавтоматизированная система с применением электронных таблиц начинает не поспевать за этим ростом, становится трудоемкой и неповоротливой, как следствие не позволяет оперативно получать необходимую управленческую информацию. Особенно это касается не регламентируемой нормативными документами информации, или данных, комплексно собираемых по ряду информационных систем, не взаимодействующих друг с другом.

Когда необходимо собрать ряд данных, то для этого часто используют корпоративную электронную почту, что приводит к завалу ее различными не классифицируемыми документами (рис. 1).

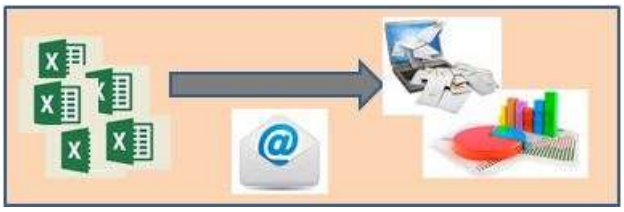


Рис. 1. Схема сбора документов
по электронной почте

Так как информация идет о документах, то логично использовать электронные системы документооборота чтобы автоматизировать процесс. Эти системы имеют большой набор функций, есть продукты как заграничного, так и отечественного производства. Но все это множество функций не включает в себя анализ информации из таблиц.

Задача предлагаемого программного обеспечения сохранить информационные потоки предприятия и соответствующий им электронный документооборот с минимальными изменениями, но, при этом, интегрировать в него базу данных. Такой подход позволит управлять централизованным сбором документов, собирать информацию предприятия в БД посредством предоставления возможности удобного взаимодействия между пользовательскими типовыми электронными таблицами и базой данных. Факт того, что разработка отечественная, позволит использовать ее в государственных структурах, упрощая сбор и анализ не стандартизированных документов и данных [3].

Концепция системы, изображенная на рисунке 2, заключается в том, что разрабатывается приложение, представляющее собой веб-сервис, выполняющий ряд необходимых функций. Сотрудники через сайт могут загружать шаблоны документов для заполнения, отправлять файлы на сервер в зависимости от категории просматривать данные об отправленных документах. На сервере информация из таблиц переносится в базу, и руководители, могут получать отчеты гораздо быстрее, пользуясь, в том числе, сторонними программными средствами, совместимыми с используемой базой данных.

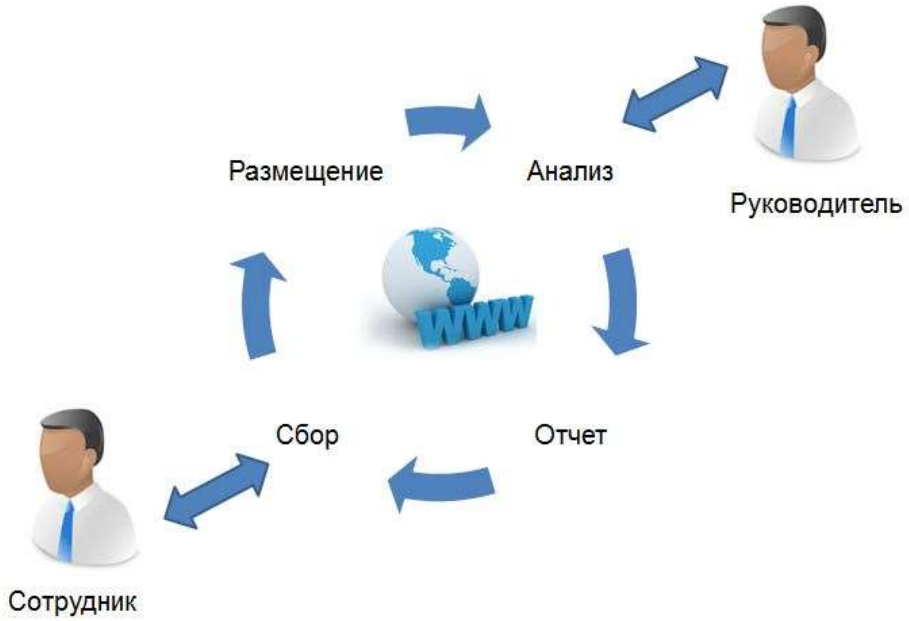


Рис. 2. Концепция системы

Всемирная сеть объединяет людей и корпорации, сегодня большая часть информационных потоков проходит в электронном виде, в том числе через интернет, который позволяет объединять удаленных друга от друга людей, предоставляя различные способы обмена информацией между ними.

С учетом всех факторов, доминирующей архитектурой в области программного обеспечения стала трехуровневая «клиент-серверная» архитектура.

Такой подход к организации приложения означает наличие трех основных элементов системы:

- клиентский уровень;
- уровень сервера приложений;
- уровень данных.

Клиентский уровень предоставляет интерфейс для взаимодействия пользователя и приложения. Он отвечает за представление данных, что означает предоставление функционала для отправки пользователем запросов к следующему уровню приложения и предоставления полученных от него данных.

Уровень сервера приложений реализует бизнес-логику, получая и обрабатывая запросы клиента, производит дополнительную необходимую обработку данных и осуществляет передачу информации между уровнем данных и клиентским.

Уровень данных, который реализуется сервером баз данных, представляет функции хранения данных, их извлечение и передачу на обработку по запросу от сервера приложений. Самодостаточные СУБД, обеспечивающие контроль целостности баз данных и безопасности, благодаря механизму транзакций и разграничения доступа сыграли важную роль в формировании этой архитектуры [1, 2].

Так как программа разрабатывается в первую очередь для возможности использования государственными органами, то она должна иметь возможность работать как на Windowsплатформе, так и на Linux. Использование форматов «xlsx» и «xls» обусловлено не только тем, что это один из самых распространенных форматов таблиц общего пользования, но и тем, что нет необходимости переобучать персонал под новую систему работы с таблицами. В качестве СУБД используется PostgreSQL, так как существует российский проект ее доработки PostgresPro. Также эта СУБД работает не только с реляционной моделью данных, но и позволяет использовать подход NoSQL. Это упрощает работу с пользовательскими таблицами, так как использование формата JSON для хранения данных в базе упрощает создание модели данных в том ключе, что не нужно строить сложную реляционную модель. Формат JSON позволяет поместить данные в базу так же, как они находятся в таблице, тогда как сложная реляционная

модель может потребовать прослеживать связи для правильного распределения данных по таблицам.

У реляционной модели есть важные преимущества в том, что это более привычная модель взаимодействия с данными, позволяющая пользоваться привычными сторонними аналитическими программами, которые могут подключаться к базе, и анализировать информацию.

Информационная система разрабатывается на языке программирования Java с использованием framework Spring. Для работы с excel файлами и загрузки файлов с web сайта на сервер используются соответствующие библиотеки apache. Динамическое содержимое web страницы выводится с помощью JSP/JSTL. Первоначально настройка импорта данных из табличного документа в базу, и генерация отчета настраивается в xml файлах, но планируется некоторый веб интерфейс для различных настроек. Работа с базой данных приложения организована с помощью ORM решения для java − Hibernate.

Список используемых источников

1. Исаев Е. А., Тарасов П. А., Корнилов В. В., Детков Г. В. Использование трехзвенной архитектуры «клиент-сервер» в современных системах обработки информации // Известия института инженерной физики. 2015. N 37, С. 38–43.

2. Мартин Фаулер, Дейвид Райс, Мэттью Фоммел, Эдвард Хайет, Роберт Ми, Рэнди Стаффорд. Шаблоны корпоративных приложений. М. : Вильямс, 2010. 544 с.

3. Иванова А. С. Проблема выбора СЭД в управленческих структурах // Времен связующая нить. Документационное обеспечение управления и архивное дело: от истории к современности. Саратов. : ФГБОУ ВПО «РЭУ им. Г. В. Плеханова», 2015. 156 с.

УДК 327.5:355.48(47:510)"1969"

М. Н. Халилов (студент группы ИКТО-31, СПбГУТ)

СОВЕТСКО-КИТАЙСКИЙ ПОГРАНИЧНЫЙ КОНФЛИКТ 1969 г. ИЗ-ЗА о. ДАМАНСКИЙ: ПРЕДПОСЫЛКИ И УРЕГУЛИРОВАНИЕ

В представляемой работе произведено рассмотрение приграничных столкновений между советской и китайской сторонами на реке Уссури в 1969 г. Цель работы заключается в анализе предпосылок, которые были причиной столкновений на границе, освещении самого хода этих событий, а также оценке последствий произошедшего конфликта для обеих стран после завершения боевых действий.

приграничные столкновения, советско-китайские отношения, остров Даманский.

Роль Китайской Народной Республики в мировой политике и экономике в последние годы значительно возросла. Невозможно говорить о дальнейшей эволюции политики Российской Федерации, не рассматривая вопроса двусторонних отношений между Россией и Китаем. Не всегда отношения между двумя странами развивались мирным путём. Одной из таких страниц, не самой приятной, были приграничные столкновения между советской и китайской сторонами на реке Уссури в 1969 г.

Цель работы заключается в рассмотрении предпосылок, которые были причиной столкновений на границе, освещении самого хода этих событий, а также оценить последствия произошедшего конфликта для обеих стран после завершения боевых действий.

В 2010 г. французская газета «Le Figaro» опубликовала несколько статей, со ссылкой на приложение к газете «Жэньминь жибао», утверждающих, что СССР готовил ядерный удар по КНР в августе-октябре 1969 г. Согласно этим статьям, США отказались сохранять нейтралитет в случае нанесения ядерного удара по КНР и 15 октября пригрозили атакой на 130 советских городов. «Спустя пять дней Москва отменила все планы ядерного удара, и в Пекине начались переговоры: кризис завершился», пишет газета [1].

Так как же развивались события тех лет на самом деле?

Как известно, в 1949 г. была образована Китайская Народная Республика (КНР), руководителем, который стал Мао Цзэдун. Новое государство придерживалось коммунистической идеологии. В 1950 г. в Москве был подписан договор о дружбе, союзе и взаимной помощи. Первые несколько лет КНР, которую и поддерживал в приходе к власти СССР, тесно сотрудничала со страной Советов, получая помощь в восстановлении народного хозяйства, оснащении армии [2, с. 658].

Коммунистическая Партия Китая (КПК) взяла курс на развитие общества, аналогичное периоду нахождения у власти И. В. Сталина в Советском Союзе. В телеграмме, Сталину в связи с первой годовщиной подписания договора, Мао Цзэдун писал: «Подписание Договора о дружбе, союзе и взаимной помощи <…> является мощной гарантией в борьбе против агрессии и за сохранение мира и безопасности на Дальнем Востоке и во всём мире» [3].

Однако, после смерти И. В. Сталина в 1953 г., и последующим развенчанием культа личности на XX съезде КПСС в 1956 г., отношения между СССР и КНР осложнились, поскольку китайское руководство осудило политику десталинализации в Советском Союзе. Вскоре председатель Центрального народного правительства Китая Мао Цзэдун объявил о плане за 3 года обогнать советских конкурентов в деле построения коммунизма. Мао пошёл ва-банк: он сделал ставку на «большой скачок», поскольку экономической базы для такого форсированного роста у Китая не было. В итоге, в конце 1950-х Китай пережил голод. Часть партийных

руководителей обвинила руководителя в авантюризме, за что в годы «культурной революции» многие из них поплатились, например, Лю Шаоци [4].

Так, в 1963 г. в статье «К вопросу о Сталине» Мао Цзэдун выступил с резкой критикой советского политического руководства, возглавившего страну после смерти И. В. Сталина: «Так называемая «борьба против культа личности» развёрнутая руководством КПСС, вовсе не имела своей целью восстановление «ленинских норм партийной жизни и принципов руководства», как они сами рекламируют это. Наоборот, эта «борьба» означает отход от учения Ленина о взаимоотношениях между вождями, партией, классом и массами, отход от принципа демократического централизма в партии» [5].

Началом «культурной революции» исследователи считают 1966 год. Главная её цель – укрепление лидерства Мао Цзэдуна в Партии. Начавшись вполне безобидно, как бунт молодёжи, недовольной западным влиянием на культурную жизнь Китая, очень быстро на улицах появились отряды «хунвейбинов» (борцов с антимаоистами), которые, например, могли отрезать длинные косы, раздирали слишком узкую одежду и т. д. Происходил грабёж населения и дискриминация интеллигенции. Очень умело в «горячие» головы вкладывалась и мысль о том, что Советский Союз – отнюдь не дружеская страна.

В официальном письме Председателя Совета Министров СССР А. Н. Косыгина Премьеру Госсовета КНР Чжоу Эньлаю от 2 февраля 1967 г. подробно описывалась ситуация: «У советского посольства днем и ночью происходят сборища, организуются демонстрации и шествия, носящие резко выраженный злобный антисоветский характер. Демонстрации сопровождаются грубой бранью в адрес Советского Союза и советского народа…» [6, с. 158].

На следующий год власти страны при помощи армии разделались с распоясавшейся молодёжью: свою задачу по физическому и моральному подавлению оппозиции они выполнили. «Ввысь в горы, вниз в сёла» – под этим лозунгом проходил следующий этап «культурной революции». Он включал в себя «переобучение» интеллигенции и чиновничества по плану, предполагавшему трудовое обучение и полезный физический труд [7].

В 1981 г. ЦК КПК пришёл к следующему заключению: «Культурная революция не была и не может быть революцией или социальным прогрессом в каком бы то ни было смысле. Она была смутой, вызванной сверху по вине руководителя и использованной контрреволюционными группировками, смутой, которая принесла серьезные бедствия партии, государству и всему многонациональному народу» [7].

На фоне этих событий стремительно ухудшались отношения Китая и СССР. В 1964 г. Н. С. Хрущёв был смещён со своей должности. Новое руководство СССР было склонно к мнению, что ухудшение отношений

с КНР вызвано только личным конфликтом между руководителями государств [8, с. 237]. Потому сразу после смещения Хрущёва на празднование очередной октябрьской годовщины в Москву прибыла китайская делегация во главе с премьером Чжоу Эньлаем. Китайская сторона выдвинула ряд условий, одно из которых заключалось в отказе СССР от провозглашения принципа мирного сосуществования между социализмом и капитализмом, что было неприемлемо [8, с. 237]. Однако неудачу переговоров советское руководство объясняло инцидентом во время приёма в Кремле, когда министр обороны маршал Р. Я. Малиновский, обращаясь к Чжоу Эньлаю и министру обороны КНР маршалу Пэн Дэхуаю, предложил им по советскому образцу сместить Мао Цзэдуна [8, с. 237]. Сохранялись иллюзии, что совместная помощь Северному Вьетнаму, ставшему жертвой американской агрессии, сблизит СССР и КНР. Лишь в итоге поездки Косыгина в Ханой и Пекин в феврале 1965 г. был сделан вывод о невозможности восстановления советско-китайской дружбы [8, с. 238].

Во второй половине 1960-х гг. резко обострились пограничные споры между странами. Китайская сторона утверждала, что, хотя, согласно результатам «исторических исследований», царская Россия захватила у Китая 1,54 млн км^2 территорий, однако КНР не претендует на их возвращение, настаивая лишь на «уточнении границы» [8, с. 238]. «Уточнение» сводилось к передаче Китаю территорий общей площадью 35 тыс. км^2 (для сравнения: площадь Бельгии – 30,5 тыс. км^2, Курской области – 29,8 тыс. км^2) [8, с. 238].

Конфликты на границе перерастали в вооруженные стычки. Крупнейшей из них стали бои на острове Даманский (или Чжэньбаодао) на реке Уссури. Утром 2 марта 1969 г. здесь китайскими пограничниками были обстреляны 55 советских пограничников, во главе с начальником погранзаставы «Нижне-Михайловка» старшим лейтенантом Стрельниковым. В бою с превосходящими силами китайцев погибли 31 советский пограничник, но прорваться китайцам не удалось [9].

15 марта китайской стороной была предпринята новая попытка захватить Даманский, которая также была отбита. Теперь в бою с обеих сторон принимали участие не только пограничники, но и регулярные войска, были задействованы артиллерия, танки, ракетные установки. Даманский стал первым боевым испытанием систем залпового огня «Град». Всего в этом конфликте с советской стороны погибли 58 человек, были ранены 94. Потери китайцев составили порядка тысячи человек, что и заставило их прекратить посягательство на территорию СССР [9].

Поначалу казалось, что именно китайское фанатичное руководство провоцировало стычки. Однако, как вспоминал Генри Киссинджер (американский дипломат, советник по Национальной безопасности США в 1969–1975 гг., Госсекретарь США в 1973–1977 гг.; инициатор и исполнитель «разрядки» в отношениях с СССР) «советские дипломаты стали предо-

ставлять детальные свидетельства советской версии событий в Вашингтон и заодно спрашивать, как Америка отнесется к тому, если произойдет эскалация этих столкновений» [10, с. 595]. Подозрения американцев подтверждались и данными разведки – стычки всегда происходили неподалёку от крупных советских баз военного снабжения и вдали от китайских военных центров. Кроме того, вдоль советско-китайской границы за короткий срок было сосредоточено почти 42 советские дивизии (более одного миллиона человек) [11, с. 240]. Советское военное вторжение в Китай означало бы самую серьезную угрозу глобальному соотношению сил со времен Кубинского ракетного кризиса. Распространение «доктрины Брежнева» на Китай предполагало бы, что Москва попытается сделать пекинское правительство столь же смиренным, каким в предшествующем году стало не по своей воле правительство Чехословакии [10, с. 595].

В то же время, все эти свидетельства, несмотря на ошибочность анализа, привели к правильному выводу. Ошибка заключалась в том, что инцидент на Даманском развязал действительно Китай, как и утверждал посол СССР Добрынин: китайцы устроили западню, вследствие чего советский пограничный наряд понёс большие потери [12, с. 23–24].

Концепция наступательного сдерживания, которую применил Китай, подразумевавшая не столько военное поражение противника, сколько психологический удар по нему, возымела фактически обратный эффект – Советский Союз усилил давление по периметру границы: на границе в Сяньцзяне был уничтожен китайский батальон [11, с. 240].

В сентябре 1969 г. на переговорах между А. Н. Косыгиным и Чжоу Эньлаем была достигнута договоренность о сохранении существующего положения советско-китайской границы. Но ожидавшееся подписание документа по возвращении Косыгина в Москву так и не состоялось. [11, с. 243] Провокации на границе продолжались в течение всех 1970-х гг. Позднее, в 1976 г., смерть Мао Цзэдуна несколько ослабила остроту конфликта, но улучшения отношений не произошло.

Причиной этого служило то, что между Соединёнными Штатами и Китаем оформилось взаимопонимание де-факто по части противодействия попыткам Советского Союза установления господства над Азией. Эти тезисы были оформлены в 1973 г. в Шанхайском коммюнике. И всё же, администрацию Никсона нельзя обвинить в попытках изолировать СССР, во враждебном настрое. Американское сближение с Китаем преследовало две цели: тщательный анализ собственных национальных интересов и соблюдение стратегического равновесия в мире. [10, с. 602]

Первые попытки наладить отношения с Китаем начались в начале 1980-х гг. – Советский Союз во главе с Л. И. Брежневым уже не мог выдерживать конфронтацию на два фронта (США и Китай). Три условия предъявлялись Пекином для восстановления отношений: вывод вьетнамских войск из Камбоджи, советских – из Афганистана и Монголии [14,

с. 12]. Курс на выполнение этих условий был взят и уже в 1986 г. был подписан Консульский договор. А по итогам переговоров М. С. Горбачёва с Дэн Сяопином в 1989 г. (после вывода советских войск из Афганистана) было подписано Совместное коммюнике. Документ зафиксировал следующие принципы дальнейшего построения отношений: взаимное уважение суверенитета и территориальной целостности, ненападение, невмешательство во внутренние дела друг друга, равенство и взаимная выгода, мирное сосуществование [14, с. 15].

Уже в процессе фактического распада СССР, 19 мая 1991 г. остров Даманский, который стал местом вооружённого конфликта двух стран соцлагеря отошёл под юрисдикцию КНР [14, с. 141]. На этом противостояние между соседними странами осталось в прошлом и началось постепенное развитие двусторонних отношений в русле партнёрства и взаимовыгодного сотрудничества в широком спектре отраслей экономики.

«Китай идет вперед, глядя назад» [15], – этот афоризм, по мнению академика Титаренко, отражает стратегию китайского руководства. Будущая история представляется китайцам как синтез прошлого и настоящего. Находить гармонию во взаимоисключающих вещах – «гармонию многообразного и несходного» – учил своих соотечественников древний философ Конфуций, живший в 551–479 гг. до н. э. [16]. И дальнейшее развитие событий, после кризисных лет соперничества, показало, что именно этим принципам и продолжают придерживаться руководители Китайской Народной Республики – этого крупного игрока на международной арене.

Список используемых источников

1. Как Никсон спас Китай от советской ядерной бомбы / пер. с фр. изданием InoPressa. URL: http://www.inopressa.ru/ article/13May2010/lefigaro/china.html (дата обращения 22.04.2016).

2. Аварин В. Я. Борьба за Тихий океан. М. : Госполитиздат, 1952. 672 с.

3. «Известия», 14 февраля 1951 г.

4. «Культурная революция» в Китае // Материал взят из книги В. Н. Усов. «Культурная революция в Китае». Китай: история в лицах и событиях. М., 1991. URL: http://china.kulichki.net/ history/CulturalRevolution/ (дата обращения 22.04.2016).

5. К вопросу о Сталине. Вторая статья по поводу открытого письма ЦК КПСС (13 сентября 1963 г.). URL: http://www.shapovalov.org/news/2011-02-09-1199/ (дата обращения 21.04.2016).

6. Окороков А. Секретные войны Советского Союза / Неизвестные войны XX века. М. : Эксмо, 2008. 736 с.

7. Мао Цзэдун и Культурная революция в Китае / Дилетант. Исторический журнал для всех: [сайт]. URL: http://diletant.media/articles/25397227/ (дата обращения 22.04.2016).

8. История России, 1945–2008 гг. : кн. для учителя / Филиппов А. В., Уткин А. И., Алексеев С. В. [и др.]. 2-е изд., дораб. и доп. М. : Просвещение, 2008. 528 с.

9. Конфликт на острове Даманский / Хронос: [сайт]. URL: http://www.hrono.ru/ sobyt/1900sob/1969damanski.php (дата обращения 21.04.2016).

10. Киссинджер Г. Дипломатия / пер. с англ. В. Львова. М. : Ладомир, 1997. 848 с.

11. Киссинджер Г. О Китае / пер. с англ. В. Н. Верченко. М. : Аст, 2014. 635 с.
12. Об этом инциденте см. аналитическое исследование Michael S. Gerson, The Sino-Soviet Border Conflict: Deterrence, Escalation, and the Threat of Nuclear War in 1969 (Alexandria, Va.: Center for Naval Analyses, 2010).
13. Обращение Ричардсона «Внешняя политика администрации Никсона, ее цели и стратегия». Т. LXI. № 1578 (22 сентября 1969 г.).
14. Ларин В. Л. В тени проснувшегося дракона: Российско-китайские отношения на рубеже XX–XXI веков. Владивосток: Дальнаука, 2006. 424 с.
15. Максимова О. О. Становление и развитие института Председателя Китайской Народной Республики (конституционно-правовое исследование) // Политика и право. Ученые записки. Благовещенск: УКЦ «Юрист». 2008. № 8. С. 67–76.
16. Максимова О. О., Кичигин С. А. Советские государствоведы о Конституциях Китайской Народной Республики // Сборник по материалам международной конференции «Приамурье – форпост России в АТР». ГУ Амурский областной «Государственный архив Амурской области». Благовещенск. 2008. С. 225–234.

Статья представлена научным руководителем,
аспирантом Гехтом А. Б.

УДК 659.182/.187

А. Е. Яскина (студентка группы РСО-21, СПбГУТ)

НЕЗАКОННАЯ РЕКЛАМА В ИНТЕРНЕТЕ И СПОСОБЫ ЕЁ КОНТРОЛЯ

Выбранная тема актуальна в первую очередь из-за своей универсальной специфики и относительной новизны слияния проблематики незаконной рекламы и её существования в интернет-пространстве. Объектом изучения выбранной темы является незаконная реклама, а предметом – незаконная реклама конкретно в сети Интернет.

интернет-реклама, Интернет, неправомерные действия.

Основными СМК в современном обществе, являются СМИ – это газеты, радио, телевидение. Информационная революция изменила их, а также формы и содержание медиа продукции и медиа среды, способствовала появлению принципиально нового канала коммуникации – Интернета. По мере стремительного развития технологий, носители рекламы приобретают новые, электронные формы. Происходит это настолько динамично, что нововведения не успевают фиксировать. Такие средства коммуникации, как интернет-газеты, интернет-телевидение, интернет-радио, уже не в новинку и получили широкое распространение. Реклама в интернете – не исключение.

Основные достоинства интернет-рекламы:

1) Гибкость замены данных (или иначе, обновления).

2) Мультимедиа – объединение базовых аспектов: визуальный, звуковой, печатный, видеоматериалы [1].

3) Персонализация – доставка необходимой информации может быть обеспечена согласно предпочтениям пользователей через содержание, многообразие средств влияния на целевую аудиторию.

4) Интерактивность. Интернет предполагает наличие моментальной обратной связи, которая отсутствует у традиционных СМИ.

5) Добровольность. Пользователь самостоятельно выбирает узконаправленные источники информации.

6) Трансграничность.

Получатели информации не привязаны к конкретному местоположению и могут находиться в любой точке земного шара

1) Доступность и оперативность.

В отличие от телевидения, к примеру, время передачи информации не ограничено.

2) Экономия расходов на содержание медианосителей.

Технологическое развитие электронных СМИ создает пустую нишу для контроля органов власти, которые и так в какой-то степени потеряли монополизм на распространение и производство информации. Технологии развиваются, а нормы до сих пор остаются неизменными [2].

Реклама, распространяемая в Интернете, попадает род действие Российского законодательства о рекламе. Но, в силу специфики рекламы в Интернете, далеко не все общие требования законодательства к ней применимы.

К примеру, временные ограничения рекламы разрешенного гражданского оружия, пива и азартных игр в полной мере соблюдать невозможно из-за большого количества часовых поясов в стране. Допустим, на сайт одновременно заходят два посетителя, один «кликает» в разрешенное время, а другой – нет, ведь место расположения сервера не может разделиться. Отслеживание часового пояса по IP затруднительно, так как адрес легко поменять на другой.

Существуют две точки зрения относительно того, распространяется ли действующее законодательство на интернет-рекламу в целом.

- Российское законодательство вообще не регламентирует рекламу в Интернете.
- Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» регулирует различные виды интернет-рекламы, но не учитывает её специфику.

Верно, в Законе о рекламе не найти нормативов, регулирующих конкретно «интернет-рекламу», однако если обратиться к статье 18 вышеуказанного закона, можно выделить, что он устанавливает особенности правового регулирования рекламы, распространяемой по сетям электросвязи.

Отталкиваясь от определения электросвязи согласно статье 2 Федерального закона от 07.07.2003 № 126-ФЗ: «любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам», интернет можно определить именно как электросвязь.

На настоящий момент, основным документом, регулирующим рекламу в интернете, является Федеральный закон «О рекламе». Согласно ст. 4 Федерального закона "О рекламе", законодатель признает приоритет данного Закона по сравнению с другими нормативными актами, регламентирующими порядок регулирования рекламной деятельности [3]. Законом определено, что отношения, возникающие в процессе производства, размещения и распространения рекламы могут регулироваться также нормативными правовыми актами Президента Российской Федерации и нормативными правовыми актами Правительства Российской Федерации.

Контроль и надзор в сфере законодательства в сфере рекламы выполняет ФАС (Федеральная антимонопольная служба). В случае выявления в сети Интернет рекламы, которая не отвечает требованиям законодательства, виновные лица привлекаются к ответственности антимонопольными органами.

При поступлении же запросов о персонализированном рекламном обращении, по ФИО, дело направляется в РОСКОМНАДЗОР, а конкретно – в отдел персональных данных.

В условиях прямого обмена между администраторами сайта и получателями информации, реклама никак не контролируется в виду отсутствия посредника, что налагает ответственность владельцев за содержание сайта.

Также, при определении лица, подлежащего привлечению к административной ответственности за ненадлежащую рекламу, непроизвольно возникает вопрос. Кому должны выдаваться предписания о нарушении законодательства о рекламе: непосредственно владельцу сайта, или все же рекламодателю? Частично ответ на этот вопрос можно найти в 3 пункте статьи 17 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4], владелец сайта может быть освобожден от гражданско-правовой ответственности в случае незнания о незаконности размещаемой информации и своей непричастности к генерации и последующему изменению информации.

Такое явление интернета, как анонимность затрудняет контроль информации в сети. Если антимонопольный орган не в силах определить собственника ресурса, он в праве обратиться в правоохранительные органы с целью установления личности.

Итак, предположим, реклама в интернете в России урегулирована нормами права, и распространяется на доменные имена с окончанием «ru». Но как действовать относительно узлов «com» и «org»? Получается, если

доменное имя зарегистрировано за пределами Российского сегмента киберпространства, то закон о рекламе не распространяется на информацию, содержащуюся на сайте.

Очевидно, что в эпоху расцвета интернет-технологий, регулирование отношений вышло далеко за пределы государства, что требует проработки универсального международного акта в сфере глобальной рекламы, по каждому отдельному виду рекламы в интернете и мерам наказания за неправомерные действия.

Список используемых источников

1. Россошанский А. В. Современные тенденции развития средств массовой коммуникации // Известия Саратовского университета. 2009. Сер. Социология. Политология. Т. 9. Вып. 1. С. 105–108.

2. Кирилловых А. А. Реклама и рекламная деятельность: проблемы правового регулирования. М. : Деловой двор, 2013. 224 с.

3. О рекламе (с изм. и доп., вступ. в силу с 01.10.2015): федер. закон Рос. Федерации от 13 марта 2006 N 38-Ф (ред. от 08.03.2015); принят Государственной Думой Федер. Собр. Рос. Федерации 22 февраля 2006 г.; одобрен Советом Федерации Федер. Собр. Рос. Федерации 3 марта 2006 г.

4. Об информации, информационных технологиях и о защите информации (с изм. и доп., вступ. в силу с 10.01.2016): федер. закон от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015); принят Государственной Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.; одобрен Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г.

Статья представлена научным руководителем,
старшим преподавателем Андрияновой-Качеишвили Л. Т.

СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

УДК 621.391

Г. В. Адамович (студент группы ИКТВ-33, СПбГУТ)
Л. А. Гречихин (студент группы ИКТВ-33, СПбГУТ)
Е. М Мелихов (студент группы ИКТВ-33, СПбГУТ)
П. А. Чагин (студент группы ИКТВ-33, СПбГУТ)

СОВЕРШЕНСТВОВАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ «МОДЕЛИРОВАНИЕ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ» ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ ИНСТИТУТА ВОЕННОГО ОБРАЗОВАНИЯ

Для изучения мультисервисных сетей связи специального назначения требуется профессиональная и легко осваиваемая учебная база, которую необходимо постоянно поддерживать и обновлять. Данный модернизированный лабораторный стенд даёт новые возможности по изучению проводных сетей связи, а также их составных частей.

модернизация узла связи, мультисервисные сети связи специального назначения, оборудование синхронного мультиплексирования, цифровые системы передач.

В институте военного образования развернут лабораторный стенд, который предназначен для изучения мультисервисных сетей связи специального назначения (СССН) построенных на оборудовании синхронного мультиплексирования комбинированное – ОСМ-К (SDH-NGN) и их составных частей. В настоящее время, возникла необходимость его модернизации из-за замены устаревшего оборудования.

Перед студентами Института Военного Образования, стояла задача в модернизации учебного лабораторного стенда. При этом, данная установка, должна отвечать следующим требованиям:

- поддержка современные технологий передачи данных с коммутацией цифровых сигналов плезиохронной цифровой иерархии (ПЦИ) Е1 до сигналов синхронной цифровой иерархии STM-1/STM-4;
- подключение периферийного (оконечного) оборудования специальной связи;
- возможность моделирования различных сетей связи.

Реализовать мультисервисную сеть, с поддержкой современных технологий передачи данных удалось, используя следующее оборудование транспортных сетей связи и оборудование сетей доступа:

Оборудование транспортных сетей связи представлено синхронным мультиплексором (ОСМ-К). Оборудование синхронного мультиплексирования комбинированное (ОСМ-К) предназначено для использования на сетях связи СЦИ в качестве мультиплексора ввода/вывода, терминального мультиплексора, кросс-коммутатора, линейного регенератора.

Мультиплексор ОСМ-К включает в себя следующие блоки (табл. 1):

ТАБЛИЦА 1. Список блоков, включенных в ОСМ-К

Название блока	**Технические характеристики и функции**
Блок ввода питания (ВП):	● ввод входного питания; ● резервирование входного питания (при установке двух блоков).
Блок коммутации и синхронизации (КС):	● коммутацию нагрузки на уровне VC12, VC3, VC4 в 112 потоках STM-1: [16STM-1 x 4 (блока CTM-16) + 4STM-1 x 2 x 6 (блоков CTM-4)]; ● синхронизацию ОСМ-К от источников: внутреннего, внешнего, агрегатных и компонентных сигналов; ● два независимых порта внешней синхронизации; ● «горячее» резервирование матрицы коммутации и узлов синхронизации
Блок управления, контроля и служебной связи (УКС):	● контроль и управление ОСМ-К по протоколу SNMP (интерфейс 10/100 Base-T) посредством ПО «Супертел-NMS»; ● организацию служебной связи; ● контроль до 4-х внешних датчиков (токовая петля); ● управление до 4-х исполнительных устройств («сухие» контакты реле).
Блок CTM-1:	● количество интерфейсов STM-1 – 4шт.; ● тип интерфейса – электрический G.703 или оптический G.957, G.692; ● исполнение интерфейсов – сменные SFP модули; ● тип оптических разъемов – LC.
Блок CTM-4:	● количество интерфейсов STM-4 – 2 шт.; ● тип интерфейса – оптический G.957, G.692 (CWDM); ● исполнение интерфейсов – сменные SFP модули; ● тип оптических разъемов – LC.
Блок 21E1:	● количество интерфейсов E1 – 21 шт.; ● соответствие G.703; ● поддерживает функцию «Retiming» для каждого E1.
Блок Eth 1000:	● количество интерфейсов Ethernet 1000: один оптический 1000 BASE-LX/1000 BASE-ZX или один электрический 1000 BASE-T.

Оборудование сетей доступа представлено коммутатором цифровых сигналов (КЦС) и первичным мультиплексором (МП).

КЦС предназначен для кросс-коммутации канальных интервалов КИ (64 кбит/с), а также для ввода/вывода сигналов абонентских интерфейсов.

МП представляет собой многофункциональное каналообразующее оборудование со скоростью передачи сигнала 2 048 кбит/с с возможностью гибкого конфигурирования и предназначен для применения в качестве оборудования абонентского доступа на сетях связи различного назначения.

МП и КЦС включает в себя следующие блоки (табл. 2).

ТАБЛИЦА 2. Список блоков, включенных в КЦС и в МП

Название блока	Технические характеристики и функции
Блок БП (Г):	● ввод входного питания; ● формирование вызывного сигнала для блоков абонентского окончания.
Блок КУ-S:	● управление режимами работы оборудования и установленных блоков; ● сбор информации о состоянии блоков в оборудовании; ● связь с системой управления.
Блок ТЧ:	● обеспечивает ввод/вывод четырех сигналов ТЧ, ИКМ преобразование сигналов ТЧ в цифровые сигналы со скоростью 64 кбит/с и передачу их в четырех канальных интервалах (КИ) первичного группового сигнала (ПГС Е1).
Блок АК МБ:	● ввод/вывод двух сигналов ТЧ, ИКМ преобразование сигналов ТЧ в цифровые сигналы 64 кбит/с и передачу их в двух канальных интервалах КИ сигнала Е1.
Блок SDSL-2:	● осуществляют прямое и обратное преобразование цифрового сигнала *nx*64 кбит/с в сигналы интерфейса SDSL.
Блок КЛС:	● на основе MAC-адресов осуществляет коммутацию пакетов между четырьмя портами Ethernet 10/100 и двумя портами WAN, сигналы которых коммутируются: на внутреннюю шину со скоростями *n*x64 кбит/с для дальнейшей передачи в структуре сигнала Е1.
Блок МП-1:	● обеспечивает прием/передачу одного сигнала Е1. Формирует первичный групповой сигнал Е1 из основных цифровых каналов (ОЦК) 64 кбит/с.
Блок ТК (МП):	● обеспечивает передачу восьми независимых телеграфных каналов ТК со скоростью до 800 бод – каждый телеграфный канал передается в своем бите канального интервала группового сигнала Е1.
Блок ЦК (КЦС):	● обеспечивает коммутацию КИ сигналов Е1 128 направлений (4096×4096 КИ); ● синхронизация КЦС, т. е. формирование набор рабочих частот и импульс начала цикла; ● выделение и запись в сигналы Е1 канала ТО (биты национального использования S1–S5); ● управление резервированием сигналов Е1 и сигналов линейных интерфейсов по типу 1+1 и резервирование тактовой частоты синхронизации.
Блок 8*E*1 (КЦС):	● ввод/вывод 8 сигналов Е1.
Блок МК-8 (МП):	● обеспечивает ввод/вывод абонентских интерфейсов с двух внутренних направлений до 62 каналов 64 кбит/с; ● осуществляет кроссовую коммутацию цифровых каналов 64 кбит/с в пределах десяти направлений передачи (8 Е1, 2 ЛИ).

При развёртывании лабораторного стенда была учтена его потребляемая мощность (для КЦС и МП - 70Вт, требования по напряжению к источнику питания от 19,2 до 33 В или от 38,4 до 72 В, для ОСМ-К 150 Вт, требования по напряжению к источнику питания от 19,2 до 72 В). Обеспечить необходимое питание мы смогли благодаря использованию блока питания УЭП-2К.

Представленный лабораторный стенд состоит из двух узлов связи, разнесенных по двум аудиториям. Для их взаимодействия была выбрана

пассивная оптическая сеть. Каждый узел связи – оснащен выделенным физическим коммутационным полем.

Для передачи данных по оптической среде, используется ОСМ-К. Данное оборудование, включая также МП и КЦС, было установлено в серверный шкаф.

Как и полевой узел связи, лабораторный стенд имеет телефонный центр, который представлен полевым коммутатором П-193м2 с имитацией каналов ТЧ прибором П-321м. Также, к учебной установке подключен телеграфный комплекс, который состоит из телеграфного аппарата П-115 и устройства низкоскоростных цифровых каналов АТ-3126-1.

Обучающийся на одном рабочем месте способен проектировать сети связи благодаря разработанному программному обеспечению компании «Супертел-NMSv2» и использованию, отдельно выведенного, физического коммутационного поля, которое позволяет коммутировать цифровые сигналы плезиохронной цифровой иерархии (ПЦИ) Е1 до сигналов синхронной цифровой иерархии (СЦИ) STM-1/STM-4.

Для вывода коммутационного поля нам понадобились специальные кабели, имеющие коннекторы, соответствующие разъемам блоков.

Блоки МК-8 и 8Е1 имеют по одной вилке формата D-Sub 44 Pin. Используемые нами розетки D-Sub имеют 44 контакта (рис. 2.).

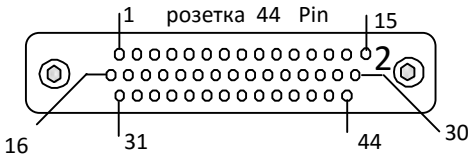


Рис. 2. Вид розетки D-Sub 44 Pin

На каждый сигнал Е1 приходится 4 контакта (2 на тракт приема и 2 на тракт передачи). Таким образом для вывода 8 сигналов Е1 с блоков МК-8 и 8Е1 на коммутационное поле, нам необходимо 32 контакта, к каждому из которых, припаивается 1 жила кабеля типа «витая пара».

Так как, используемый нами кабель «витая пара» содержит 8 жил, то для вывода 8 сигналов Е1 нам потребовалось 4 кабеля по 2 метра.

Блоки т2р и 21Е1 имеют по 3 розетки формата D-Sub 44 Pin. Таким образом для вывода 21 сигнала *Е1* с одного блока *т2р/21Е1* нам потребовалось 3 вилки D-Sub 44 Pin. Из 44 контактов на каждой вилке задействованы по 28 контактов (7 сигналов Е1 на вилку по 2 жилы на тракт приема и по 2 на тракт передачи). На каждую вилку требуется так же 4 кабеля, но в данном случае в каждом 4-ом кабеле задействованы только 4 жилы из 8. В сумме на блок т2р/21Е1 потребовалось 12 кабелей «витая пара» по 2,5 м каждый.

Распайка производилась паяльником «Светозар» мощностью 40 Вт, при пайке использовался спирто-канифольный флюс и припой ПОС-61

с процентным содержанием олова – 61 % и свинца – 41 %. После распайки кабелей на D-Sub розетки, нами была произведена промежуточная проверка соединений с помощью цифрового мультиметра.

Для организации кроссировки каналов, группы кабелей, идущих от оконечной аппаратуры, были объединены в жгуты и аккуратно проложены до коммутационного поля. На одном конце такой жгут имеет разъём D-SUB 44pin для блоков: 21E1 типа «вилка», для 8E1 и МК-8 типа «розетка». Все коннекторы были распаяны по схемам, приведенным в руководстве по эксплуатации для каждого из блоков. На другом конце, группа кабелей была заправлена в плинты, которые имеют по 5 пар гнёзд приём/передача. Заправка проводов в коммутационное поле производилась при помощи специального ножа. Далее, плинты были закреплены на специальные штанги.

Окончательная проверка работоспособности учебного лабораторного стенда была произведена уже после полной установки коммутационного поля. Для блоков МК-8 и 8E1 тестирование проходило при помощи физического замыкания тракта приема сигналов E1 на его тракт передачи. Проверка коммутации на блоках МК-8 и 8E1 определялась отсутствием светодиодной индикации замыкаемого канала, а для блока 21E1 окончательная проверка производилась с помощью портативного анализатора ИКМ потоков БЕРКУТ-E1.

В итоге, для организации коммутационного поля на одном лабораторном стенде нам потребовалось следующие ресурсы, представленные в таблице 3.

ТАБЛИЦА 3. Расходуемые материалы для создания коммутационного поля

Наименование	Величина	Количество
Вилка D-Sub 44 pin	шт.	3
Розетка D-Sub 44 pin	шт.	4
Кабель «витая пара»	м	62
Плинты	шт.	14

Таким образом, модернизированный лабораторный стенд позволяет проводить подготовку специалистов на современном уровне.

Список используемых источников

1. НТЦ ВСП "Супертел-ДАЛС": [портал]. URL: http://supertel-dals.ru/

Статься представлена научным руководителем,
доцентом, подполковником Стахеевым И. Г.

004.056.53

А. В. Александрова (студентка группы ИКТВ-44, СПбГУТ)
С. А. Марунич (студент группы ИКТВ-32, СПбГУТ)
Д. М. Пономарев (студент группы ИКТВ-31, СПбГУТ)

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В настоящей статье решается задача разработки наиболее оптимальной защиты информации от несанкционированного доступа к данным и хакерским атакам в сетях связи специального назначения с использованием сертифицированных средств защиты информации, на основе фрагмента корпоративной сети СПбГУТ, обеспечивающей подключение ЛВС Института Военного Образования.

сети связи специального назначения, защита информации, несанкционированный доступ.

Использование компьютеров и автоматизированных технологий в сетях связи специального назначения (СССН) усложняет задачу по обеспечению защиты от несанкционированных действий (НСД). Компьютеры, объединенные в инфокоммуникационную сеть, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому возникает необходимость обеспечения безопасности информации и снижении или исключении рисков, связанных с предоставлением прав доступа пользователей сети к конфиденциальным, персональным или другим критическим данным.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Защита информации от НСД включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

На рисунке 1 представлена типовая сеть передачи данных. Данная сеть предоставляет возможность файлового обмена информацией, а так же все виды высокотехнологичных услуг связи.

Для достижения цели нашей работы, мы рассмотрим данную сеть на предмет уязвимостей к несанкционированному доступу к информационным ресурсам сети.

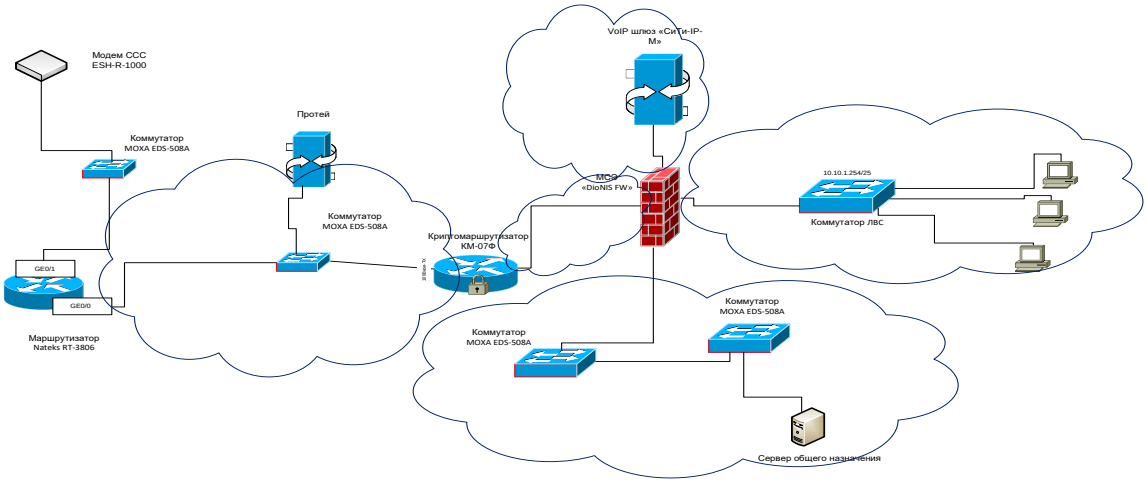


Рис. 1. Типовая архитектура построения сети передачи данных

Такое типовое построение сети имеет ряд существенных недостатков:

- Информационные ресурсы сети хранятся на компьютерах пользователей.
- Отсутствует единая система идентификации и аутентификации пользователей.
- Отсутствует контроль за подключением периферийных устройств.
- Отсутствует контроль за интернет трафиком.
- Отсутствует единая антивирусная защита.
- Нет разграничения допуска пользователей к файлам различной степени секретности.
- Отсутствует контроль за информацией, выводимой на печать.
- Не ведётся журнал событий СПД.
- Отсутствует возможность создания замкнутой программной среды.
- Не ведется контроль над аппаратной составляющей рабочих станций.

Целью нашей научной работы является разработка сетевой защиты от НСД которая позволит существенно снизить уязвимость обрабатываемой информации от несанкционированных действий пользователей.

В ходе анализа существующих методов защиты информации от НСД был выбран метод построения защиты от НСД, построенный с применением аппаратно-программного комплекса, включающего в себя (рис. 2):

- Контроллер домена Active Directory.
- Сервер Secret Net и Zlock RV.
- Сервер антивирусной защиты.

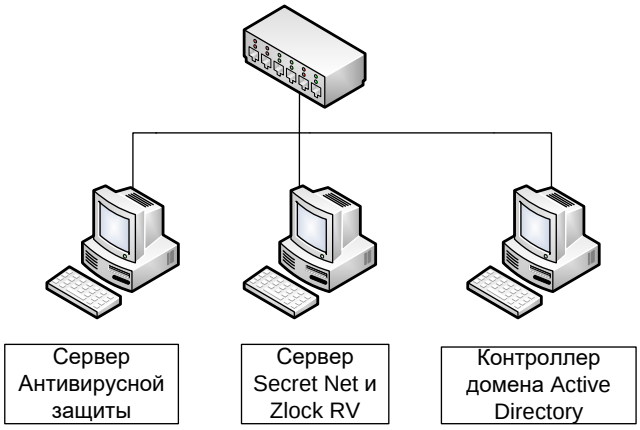


Рис. 2. Метод построения защиты информации от НСД, построенный с применением аппаратно-программного комплекса

Active Directory («Активный каталог», AD) – данное программное средство будет использовано, в первую очередь, для создания единой системы авторизации и контроля за учётными записями пользователей, а так же для управления возможностями пользователей, посредством групповых политик, помимо этого посредством AD возможен контроль за программным обеспечением пользователей, его установкой или удалением.

Secret Net – Специальное программное обеспечение (СПО), которое является средством защиты информации (СЗИ) от НСД. СПО предназначено для разграничения доступа к защищаемым информационным ресурсам СССН, обеспечения контроля их целостности, а также регистрации и учета фактов НСД.

Zlock RV – СПО, предназначеное для разграничения доступа к аппаратным ресурсам сети, а также контроля действий пользователей сети с файлами на флеш- и USB-запоминающих устройствах, а так же печати документов.

Сервер антивирусной защиты – Представляет собой комплекс СПО, состоящий из СПО серверной части – Kaspersky Security Center и СПО клиентской части – Kaspersky Endpoint Security Center который предназначен для защиты от вирусных угроз в СССН.

Центр хранения и обработки данных (ЦХОД) – является серверной машиной, доступ к данным на которой предоставляется только авторизированным пользователям, согласно их уровню допуска.

Использование ЦХОДа позволяет централизовать доступ пользователей к охраняемым информационным ресурсам сети, при введении системы двойной авторизации степень защищённости данных, имеющих уровень доступа значительно возрастает. Хранение данных таким образом значительно упрощает защиту от НСД.

Вариант построения СПД с интегрированным модулем защиты от НСД и централизованной системой хранения данных (ЦСХД) реализо-

ван и опробован на фрагменте корпоративной сети СПБГУТ, обеспечивающей подключение ЛВС Института военного образования. Вариант построения СПД с интегрированным модулем защиты от НСД и ЦСХД представлен на рисунке 3.

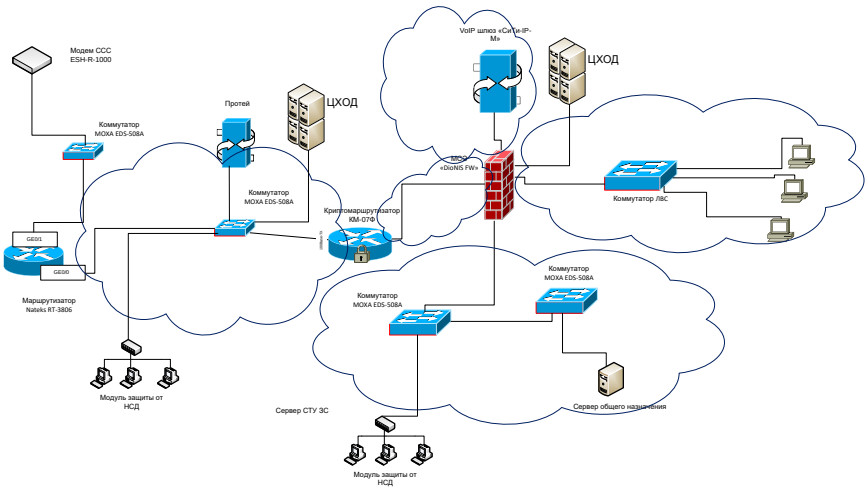


Рис. 3. Сеть передачи данных Института военного образования интегрированным модулем защиты информации

Список используемых источников

1. Спецификация и возможности поставляемого ПО [Электронный ресурс] / kaspersky.ru: [сайт]. URL: http://www.kaspersky.ru/security-center

2. Спецификация и возможности поставляемого ПО [Электронный ресурс] / securitycode.ru: [сайт]. URL: http://www.securitycode.ru/products/secret_net/

3. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114.

Статья представлена научным руководителем,
полковником В. А. Александровым

УДК 621.391

А. С. Безбородова (студентка группы ИКТВ-34, СПбГУТ)
К. И. Стахеев (студент группы ИКТВ-33, СПбГУТ)

ВАРИАНТЫ ПРИМЕНЕНИЕ АТМОСФЕРНО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ НА ОБЪЕКТАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В статье представлена история развития АОЛС, а также варианты и способы установки оборудования АОЛС на объектах специального назначения. Представлены достоинства и недостатки АОЛС. Предложены варианты применения АОЛС на объектах специального назначения.

атмосферная оптическая линия связи, объекты специального назначения,

В 1880 г. Белл запатентовал фототелефон, в котором солнечный луч, отражённый от зеркальца, модулировался голосом, передавался через атмосферное пространство и поступал на твёрдотельный детектор. Так появился прототип современных атмосферных оптических линий связи (АОЛС). Коэффициент готовности такой линии в среднем за год не мог быть более 50 %, так как после захода солнца связь обрывалась.

В настоящее время системы передачи информации подразделяются на проводные и беспроводные. Проводная линия связи обладает огромной пропускной способностью, но в больших городах строительство кабельных систем затруднительно, так как прокладка кабеля в канализационных коммуникация между двумя точками может потребовать больших затрат. Это обстоятельство приводит к широкому развитию беспроводных систем в городских условиях, которые не уступают проводным линиям связи по надежности и скорости передачи информации.

Атмосферная оптическая линия связи (АОЛС) – вид связи, позволяющий передавать информацию между объектами в атмосфере, имея оптическое соединение без использования оптоволокна или радио эфира. Импульс светового излучения при прохождении в атмосфере практически не испытывает дисперсионных искажений фронтов, характерных практически для всех оптических волокон.

В настоящее время технология обеспечивает передачу цифровых потоков до 10 Гбит/с. Современное состояние атмосферных оптических линий связи позволяет создавать надежные каналы связи на расстояниях от 100 до 1 500–2 000 м в условиях атмосферы и до 100 000 км в открытом космосе.

АОЛС для двух объектов осуществляется только посредством соединения типа «точка-точка». Технология основывается на передаче данных модулированным излучением в инфракрасной части спектра через атмосферу. На принимающей стороне оптическая система фокусирует оптиче-

ский сигнал на высокочувствительный фотодиод (или лавинный фотодиод), который преобразует оптический пучок в электрический сигнал. При этом, чем выше частота (до 1,5 ГГц), тем больше объём передаваемой информации. Далее сигнал демодулируется и преобразуется в сигналы выходного интерфейса.

Длина волны в большинстве реализованных систем варьируется в пределах 700–950 или 1 550 нм, в зависимости от применяемого лазерного диода.

АОЛС позволяют сверхоперативно организовать беспроводный оптический канал связи (мобильные системы с автонаведением обеспечивают установление связи за 10–15 мин) при незначительных затратах. Также АОЛС целесообразно применять на объектах специального назначения.

Согласно *приказу правительства РФ от 10.03.2001 г. № 221 объектами специального назначения являются:*

- предприятия военно-промышленного комплекса;
- учреждения уголовно-исполнительной системы;
- объекты военной инфраструктуры;
- здания и сооружения, предназначенные для управления войсками;
- здания и сооружения для размещения и хранения военной техники;
- здания и сооружения для хранения военного имущества и оборудования;
- здания и сооружения для испытаний вооружения;
- военные городки;
- производственные предприятия;
- общественные здания и сооружения.

Применение системы АОЛС на объектах специального назначение связанно с тем, что она имеет значительное преимущество – защищенность канала связи от несанкционированного доступа. По этому критерию данная технология является уникальной. Во всех остальных случаях (волоконные и медные кабели, радиолинии) для защиты информации требуется использование специальных кодов.

В открытой оптической линии защита обеспечивается за счет узкой диаграммы направленности излучения. С помощью внешних ИК-приборов можно обнаружить наличие канала связи, но для перехвата информации необходимо установить приемник непосредственно в канал связи, что практически неосуществимо.

Многие производители отмечают в качестве достоинства АОЛС быстроту организации линии связи. Действительно, кроме общих временных затрат, связанных с оформлением аренды мест установки аппаратуры, время на инсталляцию канала при отработанной технологии исчисляется часами.

Рис. 1. Организация АОЛС при ограничения природного характера

Использование АОЛС очень удобно, так как не требуется сложный и дорогостоящий монтаж (рис. 1). Поэтому существует множество вариантов использования АОЛС, среди которых можно отметить:

- создание локальной сети нескольких зданий;
- построение «последней мили» в сетях широкополосного доступа;
- соединение телефонных станций;
- соединение центров обработки данных для передачи информации;
- соединение серверов с автоматически управляемыми производственными комплексами на предприятиях;
- соединение серверов видеонаблюдения с конечной видеоаппаратурой (в т. ч. HDTV);
- соединение базовых станций в сетях мобильной связи и т. д.

Процессы, проходящие в приемо-передающих устройствах АОЛС можно представить в виде следующего описания. Передаваемые данные поступают в приемопередающий модуль, где происходит кодирование информации, фокусировка оптической системой в узкий лазерный луч и непосредственно передача. На другой части линии связи стоит принимающая оптическая система, которая фокусирует оптический сигнал на высокочувствительный фотодиод и преобразовывает его в электрический сигнал.

К преимуществам технологии АОЛС можно отнести:

- использование частот, не требующих лицензирования;
- оптические системы не чувствительны к электромагнитному шуму;
- системы не создают помех для радиооборудования (поэтому для их построения не нужно разрешений и согласований с уже установленным оборудованием);
- не создают помех друг для друга (благодаря чему их можно использовать в густонаселенных районах устанавливая оборудование в непосредственной близости друг от друга);
- простота реализации (монтажа) и небольшие габариты оборудования (единственный важный момент в том, что крепиться оборудование

должно к неподвижным, прочным опорам – многоэтажки, сварные стальные конструкции и т. п.;

- высокая скорость передачи данных;
- сохранение инвестиционных вложений в сеть связи при переезде (оборудование снимается и монтируется в новом месте);
- нет необходимости в инфраструктуре (сеть можно развернуть там, где нет возможности проведения кабельных сетей);
- высокий уровень безопасности передачи информации (подключиться к сети практически невозможно, поскольку согнал передается при помощи лазера, а не отправляется в радиоэфир).

Недостатками технологии АОЛС являются:

- зависимость от погодных условий (тумана, снегопадов и т. д.);
- строгий лимит по расстоянию между передатчиком и приемником;
- дороговизна оборудования;
- прочное крепление оборудования, поскольку смещение (ветер, механические нагрузки и проч.) передатчика или приемника ухудшает качество связи;
- недостаточная осведомленность пользователей о данной технологии, из-за чего отрасль развивается недостаточно быстро.

И в заключение еще немного о достоинствах АОЛС. Беспроводная оптика без труда преодолевает водные и транспортные магистрали, железнодорожные пути и линии электропередач (ЛЭП). Она вне конкуренции в случае сжатых сроков построения, т. к. запуск канала занимает всего несколько часов. Системы могут применяться только на соединениях «точка-точка» и оперируют очень низкой диаграммной направленности излучения, поэтому можно создать почти неограниченное количество каналов в непосредственной близости друг от друга. Системы АОЛС нечувствительны к электромагнитному шуму и не производят его, у них лучшая чем у радио, защищенность.

Поскольку системы АОЛС обычно устанавливают на крышах, то нарушителю нужно преодолеть физическую преграды и попасть на крышу. Да еже нужно перехватить луч света и постараться при этом не прерывать передачу данных. У многих производителей систем АОЛС простые модели точек доступа очень похожи на камеры слежения, что является сдерживающим фактором для потенциальных вредителей.

Список используемых источников

1. Гумбинас А. Ю., Милютин Е. Р. Статистическая теория атмосферного канала оптических информационных систем. М. : Радио и связь, 2002. 210 с.

Статья представлена научным руководителем
Загорельским В. В.

УДК: 004.738.5

А. Ю. Березин (студент группы РА-31, СПбГУТ)

ПОДГОТОВКА К ВЕДЕНИЮ ВОЙН В КИБЕРПРОСТРАНСТВЕ

В статье ведется речь о таких понятиях, как киберпространство, кибервойна, анализ степени подготовки различных стран к войне в киберпространстве, так же приведены исторические выкладки на эту тему.

кибервойна, Stuxnet, кибератаки на АЭС, КиберСВ США, МАГАТЭ.

Для начала хотелось бы поближе познакомить вас с тем, что же такое киберпространство и кибервойны.

Киберпространство – это метафорическая абстракция используемая в компьютерных технологиях, является виртуальной реальностью. Это как мир внутри компьютерных сетей.

Кибервойна – информационное противостояние в киберпространстве, в том числе компьютерное противостояние в Интернете, одна из разновидностей информационной войны.

Основные цели данных войн – дестабилизация компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на интернет в повседневной жизни. Если подробнее, то это использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической, информационной безопасности и суверенитету другого государства.

Существуют несколько типов таких войн

- Вандализм – использование хакерами интернета для порчи интернет-страниц, замены содержания оскорбительными или пропагандистскими картинками.
- Пропаганда – рассылка обращений пропагандистского характера или вставка пропаганды в содержание других интернет-страниц.
- Сбор информации – взлом частных страниц или серверов для сбора секретной информации или её замены на фальшивую, полезную другому государству.
- Отказ сервиса – атаки с разных компьютеров для предотвращения функционирования сайтов или компьютерных систем.
- Вмешательства в работу оборудования – атаки на компьютеры, которые занимаются контролем над работой гражданского или военного оборудования, что приводит к его отключению или поломке.

- Атаки на пункты инфраструктуры – атаки на компьютеры, обеспечивающие жизнедеятельность городов, их инфраструктуры, таких как телефонные системы, водоснабжения, электроэнергии, пожарной охраны, транспорта и т. д. [2].

Далее хочу вас познакомить инцидентом, названным «первая известная кибервойна в истории». В июне 2010 г. Иран стал жертвой кибератаки. в компьютерную сеть исследовательского ядерного центра в Натанзе был занесён вирус Stuxnet. Этот вирус вывел из строя примерно 1 000 ядерных центрифуг. Из-за этого происшествия атомная программа Тегерана была отброшена по крайней мере на два года назад. А ведь для этого всего хватило обычной USB-флешки. Так же с помощью этого вируса была произведена атака на газету New York Times. Целью злоумышленников было похищение паролей и личных данных журналистов газеты. Stuxnet стал первым компьютерным червем, нанесшим вред физическим объектам. Мишенью Stuxnet были любые устройства, связывающие компьютеры с машинами. Такой же вирус или червь можно использовать для нападения на заводы, электроэнергетические системы, светофоры и даже железнодорожные стрелки.

Перейдем к основной теме. Как мы знаем, страна США является развитой страной первого эшелона, и будет взята, как пример. Итак, в недавно принятом документе Пентагона «Стратегия действий МО США в киберне-тическом пространстве» отмечается рост зависимости эффективности проводимых операций вооруженными силами как в мирное, так и в военное время от защищенности информационных систем. При этом угрозы, исходящие из киберпространства, стали рассматриваться как наиболее серьезные и превосходящие по своей значимости международный терроризм и распространение оружия массового поражения. В настоящее время для успешного ведения боевых действий в киберпространстве и противодействия угрозам, исходящим из него, киберкомандование объединенного стратегического командования (в дальнейшем ОСК) активно создает киберсилы, формирует нормативно-правовую базу их применения, совершенствует инфраструктуру. Так, по планам Пентагона, к 2019 г. должно быть завершено создание трех оперативных формирований (ОФ):

- стратегических операций в киберпространстве;
- оперативно-стратегических операций в киберпространстве;
- формирование киберзащиты.

В состав ОФ войдут 133 кибергруппы общей численностью 6 200 человек.

Командование боевых действий сухопутных войск США в киберпространстве (киберкомандование СВ) отвечает за создание в будущем 41 кибергруппы, в том числе стратегических и оперативно-стратегических операций в киберпространстве, обеспечения, киберзащиты и других.

Предполагается, что полной оперативной готовности штаб командования СВ достигнет к 2019 г., его численность составит 600 человек (военнослужащих и гражданского персонала).

В интересах создания единого информационного пространства Пентагона киберкомандование СВ проводит мероприятия по стандартизации своих информационных сетей и обеспечению их кибербезопасности. Произошло слияние ранее существовавших зональных центров сетевых операций и обеспечения безопасности СВ с региональными группами реагирования на чрезвычайные ситуации в компьютерных сетях. На данной базе сформированы центры проведения кибероперацій в зонах, на которые возложено решение следующих задач:

- приведение разнородных сетей к единому стандарту;
- ведение разведки в сетях противника;
- защита соответствующих зональных участков интегрированной телекоммуникационной инфраструктуры СВ;
- обеспечение ситуационной осведомленности об обстановке в сетях.

Киберкомандование СВ провело также ряд мероприятий по совершенствованию системы подготовки кадров. В апреле 2014 г. на базе учебного центра войск связи СВ командования учебного и научных исследований по строительству сухопутных войск был образован учебный центр боевых действий в киберпространстве. Он включает два отделения

- подготовки специалистов войск связи;
- операторов кибероперацій.

На данный центр возложены следующие задачи:

- разработка стратегии действий СВ в киберпространстве;
- подготовка по ведению боевых действий в киберпространстве;
- согласование и объединение разнообразных учебных программ подготовки киберспециалистов.

В настоящее время киберкомандование ОСК испытывает острую нехватку в наборе необходимого количества личного состава, обладающего соответствующими знаниями. В целом киберкомандование СВ планирует к 2020 г. набрать 3 800 специалистов для работы в данной области. Для привлечения и удержания на службе личного состава (как военнослужащих, так и гражданского персонала) предлагается использовать разнообразные финансовые инструменты, такие как целевое назначение денежных надбавок специалистам этих подразделений, денежные надбавки при выполнении специальных заданий, а также премиальные бонусы для тех, кто проходит службу на оперативных должностях и пр. Так же предлагается оплачивать учебу студентов гражданских вузов с обязательным последующим их распределением на кибердолжности в МО. При этом особое внимание киберкомандование СВ уделяет приведению учебных программ

к единому стандарту, что должно позволить готовить киберспециалистов не только в интересах СВ, но и для единых сил.

Согласно проекту бюджета Пентагона, на 2016 г. на нужды киберкомандования СВ предусматривается выделение 1,02 млрд долларов, в том числе 90 млн на создание учебного центра боевых действий в киберпространстве [1].

Какие же еще могут быть угрозы? В декабре 2014 г. произошел взлом южнокорейского оператора АЭС Hydro and Nuclear Power Co Ltd. Хакер разослал 5 986 содержащих вредоносный код электронных писем более чем 3 тыс. сотрудников компании и в итоге получил доступ в ее внутреннюю сеть. Затем злоумышленник потребовал заглушить три реактора АЭС, угрожая их разрушением. Тогда в сеть попала закрытая информация, такая как чертежи и спецификации атомных реакторов, а также личные данные сотрудников компании-оператора АЭС. Власти Южной Кореи обвинили во взломе Северную Корею. Из чего следует, что не только США готовится к кибервойнам.

Еще один известный инцидент с АЭС «Дэвис-Бесс» в Огайо произошел в 2003 г., когда обслуживающая АЭС компания была заражена червем Slammer, который привел к отказу серверов корпоративной сети. Оператор совершил ошибку и в ходе расследования инцидента подключил корпоративную сеть к внутренней компьютерной сети станции, и вирус распространился дальше, что сделало невозможным использование компьютеров сотрудниками самой АЭС, которые потеряли связь друг с другом. Также на шесть часов была выведена из строя система отображения параметров безопасности, которая показывает операторам, как работает оборудование и насколько оно исправно [3].

Обеспечение соответствия общим стандартам безопасности, в том числе в рамках концепции физической ядерной безопасности на атомных объектах, помимо национальных операторов осуществляет Международное агентство по атомной энергии (МАГАТЭ). Данная организация уже давно обращает внимание на компьютерную безопасность АЭС, и публикует соответствующие технические руководства. В 2015 г. состоялась первая конференция МАГАТЭ по компьютерной безопасности на атомных объектах. МАГАТЭ собрала представительные делегации, в том числе и от России в составе представителей «Росатома» и МИД России. Такие конференции теперь будут проходить каждый год, и на них будут представляться доклады, например, по результатам моделирования возможной комплексной кибератаки на АЭС

Таким образом кибервойны стали чрезмерно важной проблемой. Кибератаки могут представлять огромную угрозу даже простому гражданскому населению. И в данный момент все страны ведут укрепления своих военных «киберсил», как и различные организации ведут укрепление за-

щиты своих сетей. Эта подготовка началась уже первых дней существования интернета и компьютерных сетей.

Список используемых источников

1. Подполковник А. Белый Подготовка Сухопутных войск США к ведению боевых действий в киберпространстве // Зарубежное военное обозрение. 2015. № 11. С. 47–50.

2. Киселёв В., Костенко А. Кибервойна как основа гибридной операции // Армейский сборник. 2015. № 11.

3. Алексей Короткин, Владимир Тодоров Могут ли хакеры устроить аварии на ядерных объектах // Газета.ru: [сайт]. 2015. Октябрь. URL: https://www.gazeta.ru/tech/2015/10/05/7796681/nuclear-security-threats.shtml

Статья представлена научным руководителем,
кандидатом исторических наук, доцентом Мосеевым В. И.

УДК 621.396

Березянская В. М. (студент группы ИКТВ-43, СПбГУТ)
Мартынов А. А. (студент группы ИКТВ-43, СПбГУТ)
Савинский С. И. (студент группы ИКТВ-43, СПбГУТ)

ИСТОРИЯ РАЗВИТИЯ ОТЕЧЕСТВЕННОЙ СПУТНИКОВОЙ СВЯЗИ

Статья посвящена истории развития отечественной спутниковой связи, идею которой впервые предложил Артур Кларк в 1945 г. В статье будет рассмотрен первый искусственный спутник земли, его запуск и усовершенствование, создание различных систем спутниковой связи, а также полет первого человека в космос.

Артур Кларк, спутник, спутниковая связь, радиоретранслятор

Впервые идею спутниковой связи представил в 1945 г. англичанин Артур Кларк.

В радиотехническом журнале он опубликовал статью о перспективах ракет, подобных «Фау-2», для запуска спутников Земли в научных и практических целях.

Знаменателен последний абзац этой статьи: «Искусственный спутник на определенном расстоянии от Земли будет совершать один оборот за 24 ч. Он будет оставаться неподвижным над определенным местом и в пределах оптической видимости почти с половины земной поверхности. Три ретранслятора, размещенные на правильно выбранной орбите с угловым разнесением на 120°, смогут покрыть телевидением и УКВ радиовещанием

всю планету; я боюсь, что те, кто планирует послевоенные работы, не сочтут это дело простым, но я считаю именно этот путь окончательным решением проблемы».

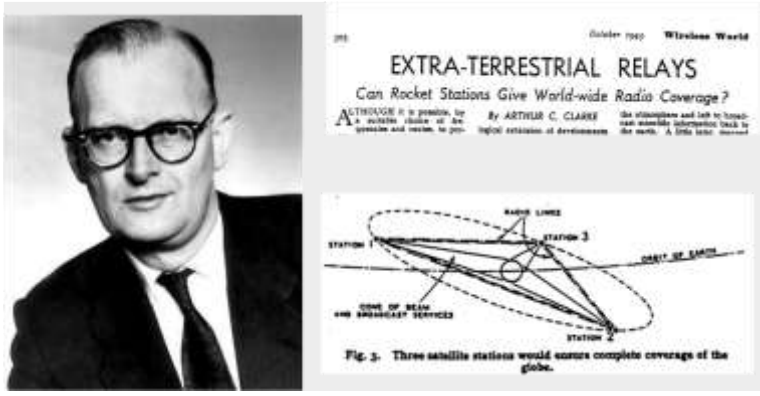


Рис. 1. Артур Кларк

Далее рассмотрим основные этапы становления систем спутниковой связи.

4 октября 1957 г. в СССР был осуществлен запуск первого в мире искусственного спутника Земли, первого космического объекта, сигналы которого принимались на Земле. Излучаемые спутником сигналы использовались не только для пеленгации, но и для передачи информации о процессах на спутнике.

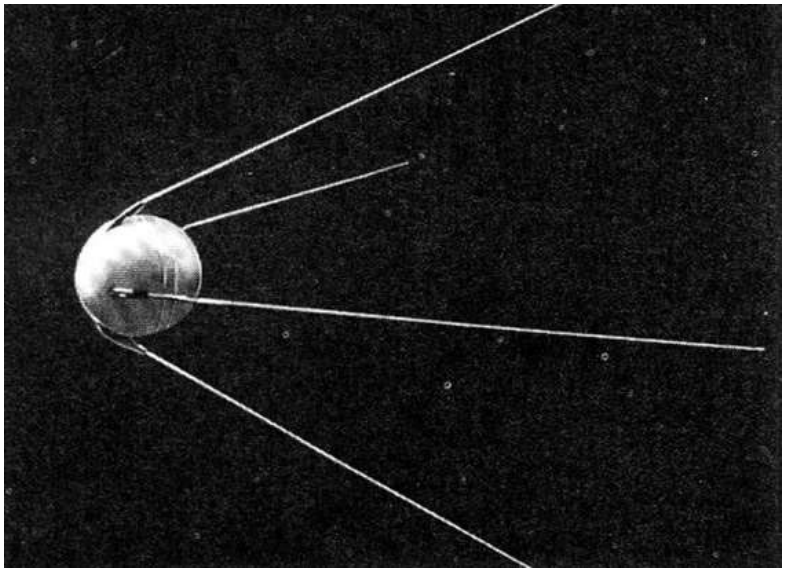


Рис. 2. Первый искусственный спутник Земли

12 апреля 1961 г. в Советском Союзе впервые в истории человечества осуществлен полет человека в космическое пространство. Космический корабль «Восток» с летчиком-космонавтом Ю. А. Гагариным на борту был выведен на орбиту спутника Земли.

Для пеленгации корабля и передачи телеметрической информации использовалась радиосистема «Сигнал», работавшая на частоте 19,955 МГц. Двусторонняя связь космонавта с Землей обеспечивалась радиотелефонной системой, работавшей в диапазонах коротких (19,019 и 20,006 МГц) и ультракоротких (143,625 МГц) волн.

В конце 50-х гг. прошлого века в СССР и США начали проводиться экспериментальные исследования возможностей использования искусственных спутников Земли в качестве радиоретрансляторов (активных и пассивных) в наземных системах связи.

Первый активный радиоретранслятор «Score» был запущен 18 декабря 1958 г. на наклонную эллиптическую орбиту с высотой апогея 1 481 км, перигея 177 км. Аппаратура спутника состояла из двух приемопередатчиков, (132,435 и 132,095 МГц). Продолжительность связи составляла приблизительно 4 мин за 1 оборот спутника. Спутник сгорел при входе в атмосферу 21 января 1959 г.

Второй активный радиоретранслятор «Курьер» был запущен 4 октября 1960 г. на наклонную эллиптическую орбиту (высотой апогея 1 270 км и перигея 970 км). Аппаратура спутника состояла из 4 приемопередатчиков (частота 150 МГц для передачи команд и 1 900 МГц для связи), устройства магнитной памяти и источников питания – солнечных элементов и химических батарей. Продолжительность сеанса связи составляла 5 мин за один оборот спутника. Срок службы спутника составил 1 год.

10 июля 1962 г. на наклонную эллиптическую орбиту с апогеем 5 600 км и перигеем 950 км был запущен активный ретранслятор «Телстар». Одновременно он ретранслировал или 600 симплексных телефонных каналов, или 12 дуплексных телефонных каналов, или один телевизионный канал. Продолжительность сеанса связи на линии США – Европа через этот спутник составляла около 2 часов в сутки.

14 февраля 1963 г. был запущен первый синхронный спутник системы «Синком» с параметрами орбиты: высота апогея 37 022 км, высота перигея 3 4185, период обращения 1 426,6 мин. Рабочая частота на линии Земля – спутник равна 7 360 МГц, на линии спутник – Земля 1 820 МГц. В качестве первичного источника питания на спутнике использовались солнечные элементы.

23 апреля 1965 г. в СССР был запущен первый спутник связи «Молния-1». С запуском второго спутника связи «Молния-2» 14 октября 1965 г. была создана и введена в эксплуатацию система спутниковой связи "Молния-1", по названию спутника. Эта система позволила организовать связь Москвы с районами Дальнего Востока, Сибири, Средней Азии.

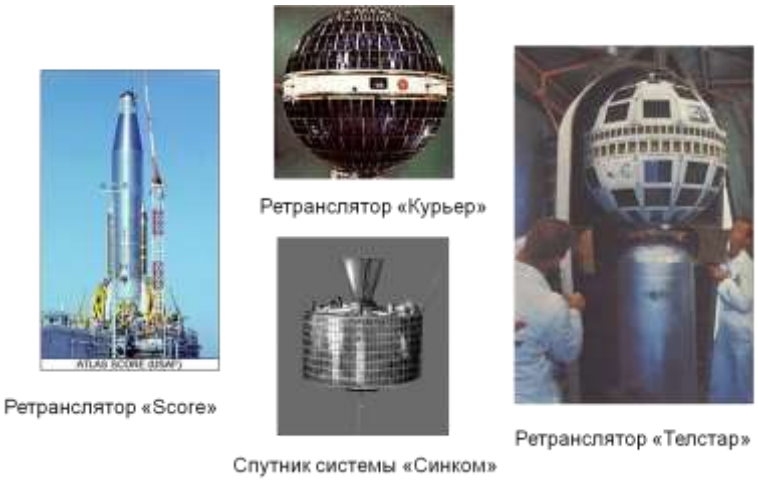


Рис. 3. Активные радиоретрансляторы

В системе "Молния-1" передавались программы телевизионного (ТВ) и радиовещания (РВ), полосы газет, а также осуществлялись телефонные и телеграфные связи с указанными районами. К концу 1967 г. в стране были введены еще 20 станций, которые с имеющимися станциями образовали первую в мире систему распределения телевидения "Орбита".

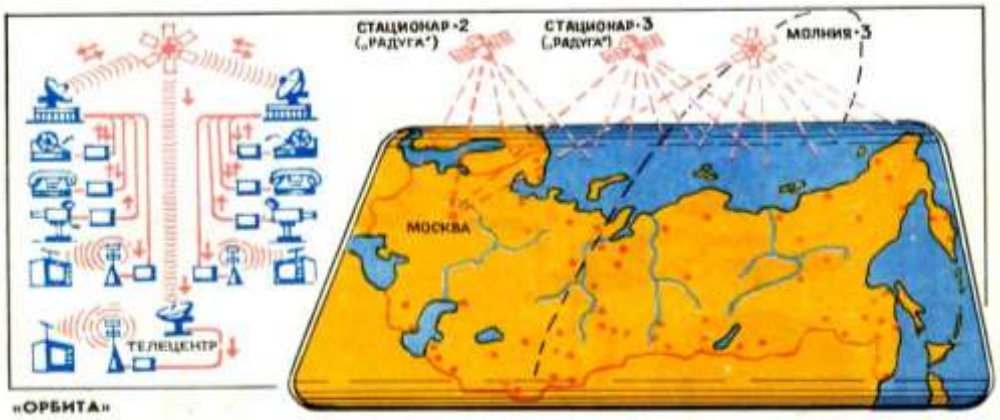


Рис. 4. Система спутниковой связи «Орбита»

В 1973 г. создана перевозимая и самолетная станции "Контакт" для телефонной связи во время визитов и перелетов руководства страны.

Также, в 1974 г., была создана перевозимая станция МАРС для передачи ТВ изображения и звука в реальном масштабе времени из районов, где не было стационарных станций спутниковой связи. Она использовалась для трансляции ТВ репортажей во время стартов космических кораблей или показа других важных событий, происходящих как в стране, так и за рубежом.

В середине 1973 г. был введен в эксплуатацию трехствольный ретранслятор на спутнике "Молния-3", имеющий также высокоэллиптическую орбиту. Такие высокие орбиты (в апогее около 40 тыс. км) очень удобны для организации связи на территории нашей страны, так как зона

радиовидимости с такого спутника охватывает всю территорию Советского Союза и всю северную полярную область Земли. Получить такую же зону радиовидимости со спутников, находящихся на геостационарной орбите в любых точках над экватором, невозможно.

С вводом в эксплуатацию многоствольного спутника "Горизонт", выведенного на геостационарную орбиту в 1975 г., завершилось создание новой системы спутниковой связи в нашей стране. Система была названа по имени спутника – "Горизонт". Первые спутники системы были расположены в точках стояния над экватором 14° з. д.; 35° и 80° в. д. На каждом из них было по шесть стволов, работающих в диапазоне 4/6 ГГц, и один ствол в диапазоне 11/14 ГГц.

В 1976 г. был выведен на геостационарную орбиту спутник "Экран" с точкой стояния над экватором 99° в. д., который позволил создать зону непосредственного телевизионного вещания в районах Урала и Западной Сибири.

В 1965 г. начала действовать самая крупная международная организация спутниковой связи ИНТЕЛСАТ. С помощью этой системы в 1987 г. обеспечивалось около двух третей международных каналов спутниковой связи, а в настоящее время - около одной трети.

В 1980-е гг. началось развитие персональной спутниковой связи. При этой связи спутниковый телефон непосредственно соединяется со спутником, находящимся на околоземной орбите.

В настоящее время в общем балансе связи на спутниковые системы пока приходится примерно 3 % мирового трафика. Но потребности в спутниковых линиях продолжают расти, поскольку при дальности свыше 800 км спутниковые каналы становятся экономически более выгодными по сравнению с другими видами дальней связи.

Список используемых источников

1. Украинцев Ю. Д., Цветов М. А. История связи и перспективы развития телекоммуникаций: учебное пособие. Ульяновск : УлГТУ, 2009. 128 с.

2. Танетов В. Н. От "внеземной ретрансляции" к первым спутникам связи // Электросвязь. 1998. № 11.

3. Сворень Р. Щедрая звезда «Экрана»: Заметки с международной выставки «Связь-81» // Наука и жизнь. 1981. № 12, С. 22–24, С. 2–3 вкл.

Статья представлена научным руководителем,
кандидатом технических наук, капитаном Сагдеевым А.

УДК 654.026

И. В. Бодров (слушатель, ВАС)
Ю. Г. Гаврилов (слушатель, ВАС)
К. С. Чубарев (кандидат военных наук, профессор, ВАС)

ЭФФЕКТИВНОСТЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ СВЯЗЬЮ

В работе представлена методика расчета эффективности функционирования систем управления связью. Методика учитывает оценку системы управления возможную через оценку ее элементов, а именно – пунктов управления, органов управления, технической основы системы управления. Более подробно рассмотрен один из показателей оценки устойчивости технической основы системы управления узла связи, которым является коэффициент исправного действия направлений служебной связи. При этом учитывается, что по каналам (линиям) служебной связи осуществляется как речевой обмен информацией между должностными лицами системы управления узла связи, так и сбор (передача) технологической информации о состоянии (на изменение состояния) контролируемых объектов.

управление узлом связи, система управления, требования к системе управления, оценка системы управления, устойчивость управления.

Оценка эффективности функционирования системы управления любым военным объектом связи, в том числе и узлом связи подвижного пункта управления, должна осуществляться по показателям наиболее существенных свойств, которыми обладает конкретная система управления.

В руководящих документах по вопросам специальной связи свойства (требования) системы управления узла связи, как и системы управления связи в целом не определены.

В учебной литературе, в некоторых материалах научных исследований существуют различные подходы к описанию требований (и их оценке по соответствующим показателям) к системам управления различного назначения. В основном взгляды сводятся к тому, что систему управления каким-либо объектом связи необходимо оценивать по показателям, характеризующим свойства самого объекта, в состав которого входит данная система управления [1].

Так, систему управления связью предлагается оценивать по показателям, характеризующим пропускную способность, устойчивость, мобильность и другие свойства системы связи.

Аналогично, в данных работах, систему управления узлом связи пункта управления предлагается оценивать по показателям, характеризующим свойства самого узла связи пункта управления (обладать постоянной готовностью к приёму и немедленной передаче всех видов информации, высокой живучестью и надёжностью; обеспечивать максимальные

удобства пользования средствами связи и автоматизации управления должностным лицам органов управления; удовлетворять требованиям электромагнитной совместимости всех развёртываемых на узле связи радиоэлектронных средств; иметь возможность манёвра средствами, каналами, видами и услугами связи и др.).

Данный подход, на наш взгляд, не совсем адекватно отражает процесс функционирования самой системы управления связью (узлом связи).

Одним из возможных вариантов оценки эффективности системы управления связью (узлом связи) может быть ее оценка по показателям, характеризующим свойства не системы, а процесса управления, то есть, по показателям устойчивости, непрерывности, оперативности и скрытности управления [1].

При этом, например, оперативность управления узлом связи определяется временным показателем цикла управления $t_{цу}$:

$$t_{цу} = t_{сб} + t_{обр} + t_{реш} + t_{пз},$$

где $t_{сб}$ – время сбора информации; $t_{обр}$ – время обработки информации; $t_{реш}$ – время принятия решения; $t_{пз}$ – время постановки задач

Более детальная оценка системы управления возможна через оценку ее элементов, а именно – пунктов управления, органов управления, технической основы системы управления [2].

При данном подходе свои особенности имеет оценка эффективности работы органов управления. Органы управления в различных структурах, в том числе в системах управления связью, системах управления узлов связи, оцениваются по численному составу, а также по показателям, характеризующим квалификацию, опыт работы и другие персональные «качественные» характеристики должностных лиц.

Показателями оценки пунктов управления могут быть их оснащенность средствами управления (средствами связи и автоматизации) и производительность пункта управления, которая определяется объемом работы (в единицу времени), выполненной должностными лицами, размещенными на пункте управления и производительностью соответствующих средств управления, в том числе возможностями программного обеспечения.

Техническая составляющая системы управления, в основной своей части, может быть оценена с помощью методик, применяемых для оценки соответствующих свойств системы связи (узла связи).

Под технической основой системы управления узла связи следует понимать сеть служебной связи, систему сбора информации о состоянии объектов управления, а также технические средства управления.

Наиболее существенным свойством технической основы системы управления узла связи, является, на наш взгляд, устойчивость ее функционирования при различных возможных воздействиях [1].

Одним из показателей оценки устойчивости технической основы системы управления узла связи может быть коэффициент исправного действия направлений служебной связи. При этом учитывается, что по каналам (линиям) служебной связи осуществляется как речевой обмен информацией между должностными лицами системы управления узла связи, так и сбор (передача) технологической информации о состоянии (на изменение состояния) контролируемых объектов. Кроме устойчивости каналов (линий) служебной связи необходимо учитывать надежность работы технических средств сбора, обработки, хранения, отображения и передачи служебной информации.

Таким образом, под устойчивостью сети служебной связи следует понимать ее способность обеспечить управление узлом связи в условиях воздействия на ее элементы различных внешних факторов, сохраняя значения показателей надежности средств управления в заданных пределах.

Средства управления и линии служебной связи, составляющие структуру сети служебной связи, могут выходить из строя под воздействием различных факторов, т. е. обладают конечной (не абсолютной) устойчивостью. Их устойчивость зависит как от применяемого рода связи (проводная или радио линия и др.), так и от условий функционирования объекта управления.

Нарушение процесса передачи информации в системе управления узлом связи может происходить в результате поражения элементов узла связи огневыми средствами, нарушения условий электромагнитной совместимости радиоэлектронных средств (ЭМС РЭС), преднамеренных и непреднамеренных помех, выхода из строя средств управления по технико-эксплуатационным причинам [3].

Количественными показателями, характеризующими устойчивость системы управления узла связи, приняты коэффициент исправного действия ($K_{и}$) и среднее время простоя ее работы ($t_{п}$), которые могут быть отнесены и к элементам системы – к направлению, линии и каналу служебной связи. Для существующих систем управления устойчивость сети служебной связи складывается из устойчивости отдельных направлений служебной связи. Поэтому количественные показатели устойчивости направлений служебной связи ($K_{и\ нсс}$, $t_{п\ нсс}$) используются в качестве основных при оценке устойчивости системы управления узла связи в целом.

Критерием оценки устойчивости направлений служебной связи служат выражения $K_{и\ нсс} \geq K_{и\ нсс\ тр}$, $t_{п\ нсс} \leq t_{п\ нсс\ тр.}$, т. е. коэффициент исправного действия и среднее время простоя направления служебной связи должны быть не хуже требуемых.

Так как требования по устойчивости системы управления узла связи нигде не определены, то будем исходить из требований по устойчивости направлений связи, по которым обеспечиваются оперативные связи от данного узла связи пункта управления. При этом, на наш взгляд, коэффи-

циент исправного действия системы управления узла связи (на всех направлениях служебной связи) должен быть не ниже, чем коэффициент исправного действия для направлений оперативных связей первой группы важности, т. е. $K_{и\ тр.} \geq 0{,}95$. Данное утверждение обусловлено тем, что срыв управления любым элементом узла связи (любым объектом управления) в ходе выполнения задач по обеспечению связи может привести к снижению устойчивости функционирования узла связи в целом и направлений связи первой группы важности, в частности. В то же время, в ходе развертывания (свертывания, перемещения) узла связи, когда не обеспечивается выполнение задач по связи, требования к устойчивости системы управления узла связи могут быть снижены до уровня, обеспечивающего управление элементами узла связи хотя бы по одному любому каналу (линии) служебной связи.

Список используемых источников

1) Теоретические основы построения систем военной связи в объединениях и соединениях: учебник. Часть 2. Научно-практические основы построения организационно-технических систем военной связи / под общей ред. Ю. А. Пирогова. – СПб. : ВАС, 2007. 540 с.

2) ГОСТ РВ 5819-104-2007. Объединенная автоматизированная цифровая система связи Вооруженных Сил Российской Федерации. Общие требования к сетям доступа. М. : НИИ «Эталон», 2007.

УДК 654.026

Ю. Г. Воробьев (слушатель, ВАС)
Ю. Г. Гаврилов (слушатель, ВАС)
С. А. Падишин (кандидат военных наук, профессор, ВАС)

МЕТОДИКА ОЦЕНКИ СИСТЕМ МОНИТОРИНГА СИСТЕМЫ И СЕТЕЙ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В работе представлена методика оценки систем мониторинга сетей специального назначения. Сети специального назначения имеют свои особенности по причине выполняемых ими задач, структуры сетей, системы управления, применяемых технологий. В методике представлены основные показатели оценки системы мониторинга, которые, на взгляд авторов, позволяют ее оценить с учетом особенностей функционирования сетей связи специального назначения.

методика оценки, показатели оценки, критерии оценки, место системы мониторинга.

В настоящее время бурное развитие получили системы, позволяющие проводить контроль работы современных инфокоммуникационных сетей связи, при этом необходимо отметить, что в методологическом плане данный вопрос является недостаточно разработанным. Для сетей связи специального назначения он является актуальным еще и по той причине, что на сетях связи используется телекоммуникационное оборудование, работающее как на принципах коммутации каналов, так и на принципах коммутации пакетов.

Под методикой оценки систем мониторинга системы и сетей связи будет понимать совокупность форм, процедур, способов и приемов, применяемых в определенной логической последовательности, позволяющей провести оценку эффективности системы мониторинга сетей связи как на этапе разработки, так и на этапе ее эксплуатации.

Вопросы оценивания (квалиметрии) сложных информационных систем, а система мониторинга, как одна из ключевых элементов системы управления связью, таковой несомненно является, достаточно подробно рассмотрены в теоретическом плане.

Проведенный анализ научной литературы по квалиметрии информационных систем, показывает, что процесс измерения и оценки реализуется, как правило, в два этапа:

1 этап – измерение характеристик информационной системы, в данном случае системы мониторинга;

2 этап – формирование решения по принятым критериям выделенных существенных свойств (своевременности, результативности, ресурсопотребления) [1, 2].

В соответствии с требованиями и свойствами системы мониторинга определим показатели оценки системы мониторинга:

- допустимое время на доведение информации;
- полнота оценки всех элементов системы связи;
- допустимое время на обнаружении ошибки в системе;
- периодичность опроса элементов системы связи об их состоянии;
- наглядность отображения информации;
- ресурсопотребление (экономичность).

На рисунке 1 показано место системы мониторинга в общей системе связи специального назначения. Из него видно, что система мониторинга в современных условиях играет ключевую роль в технической основе системы управления связью.

Так как основным функциональным предназначением системы мониторинга является своевременное доведение до ДЛ по связи информации о несоответствии параметров предоставляемых услуг связи, состояния аппаратуры и линий первичной и вторичных сетей связи, то в качестве одного из основных существенных свойств исследуемой системы определена своевременность.

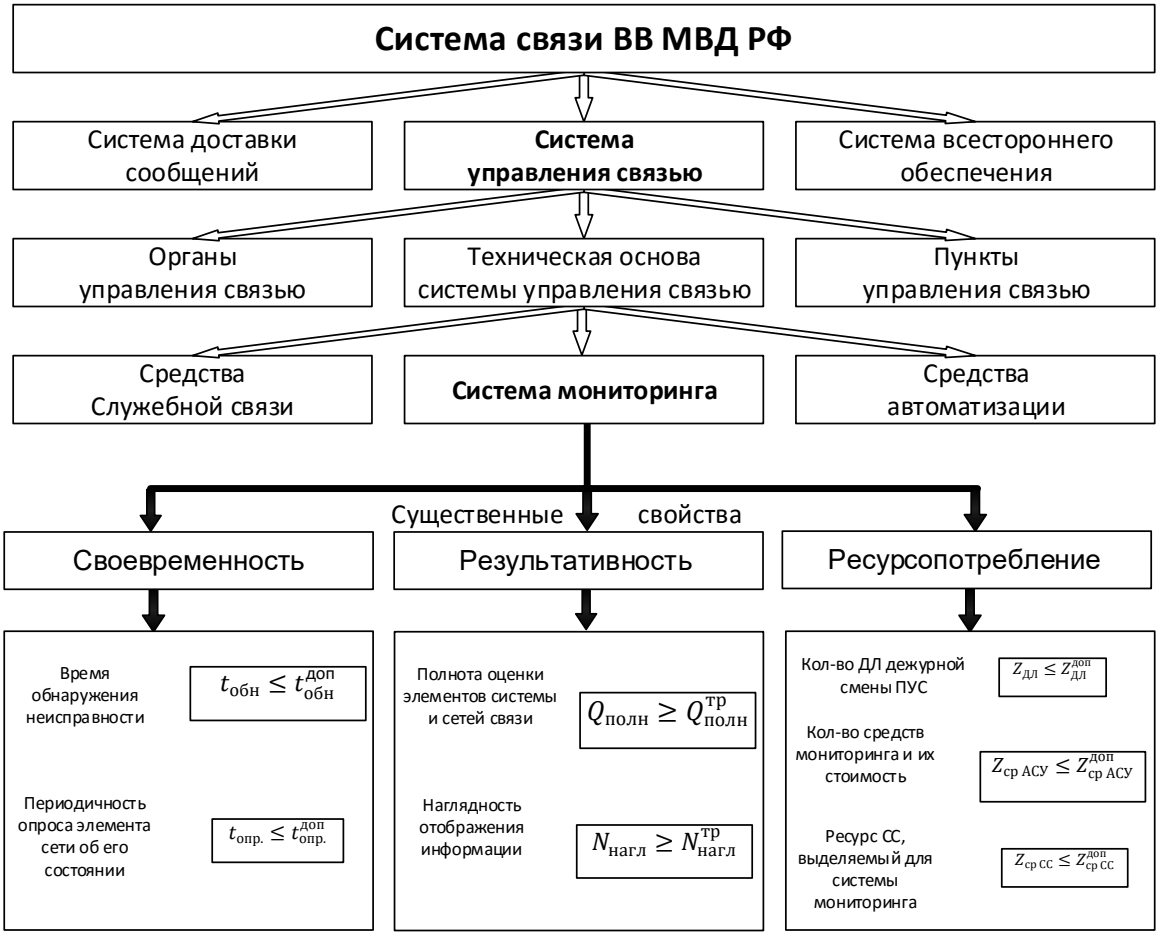


Рис. 1. Место системы мониторинга системе связи специального назначения

Для оценки своевременности предлагается использовать следующие показатели:

- время обнаружения неисправности ($t_{обн}$);
- время доведения информации обнаруженной неисправности до ДЛ по связи ($t_{дов.}$).
- периодичность опроса элемента сети об его состоянии ($t_{опроса.}$).

Критериев оценки своевременности в руководящих документах на сегодня нет, поэтому в исследовательских целях определяем следующие правила оценивания:

$$t_{обн.} \le t_{обн}^{доп} \to \min.$$

$$t_{дов.} \le t_{дов}^{доп} \to \min.$$

$$T_{опроса.} \le t_{опроса}^{доп} \to \min.$$

В каждом конкретном случае, допустимое время обнаружение неисправности на сети будет определяться исходя из имеющихся технических и оперативных возможностей системы мониторинга и выделенного для ее работы ресурса сетей связи.

Для оценки своевременности работы систем мониторинга в качестве одного из основных показателей определен показатель периодичности опроса элемента сети об его состоянии ($t_{опроса.}$). Данный показатель является составной часть показателя, характеризующего время доведения до должностного лица информации об обнаружения неисправности.

Если мы считаем, что линии связи, по которым передается информация состояния об объекте контроля, всегда исправны, пропускной способности выделенного ресурса сети достаточно для передачи необходимых объемов информации, то мы может констатировать следующий факт, что время передачи информации по каналам связи является в сотни и тысячи раз меньше, чем время, через которое производится опрос элементов системы об ее состоянии. То есть, мы может сказать, что: $t_{опроса} \approx t_{дов}$.

Практика применения современных систем мониторинга подтверждает данный факт, время доведения является ничтожно малой величиной по сравнению с периодичностью опроса сети.

Соответственно, своевременность работы систем мониторинга возможно оценивать именно по показателю периодичности опроса сети. При этом, должностное лицо, которое определяет требуемую периодичность опроса должно помнить, что высокая частота опроса может создать на сети связи такой прецедент, когда объемы информации состояния о сети связи будут занимать большой процент ресурса пропускной способности необходимый для передачи оперативной информации и тем самым препятствовать нормальной работе сетей.

Практический опыт работы операторов связи показывает, что как правило, они поддерживаются следующего правила: объем информации управления сетями связи не должен быть более 10 % от пропускной способности линии связи.

Также в качестве существенного свойства в работе определяется результативность работы системы мониторинга, данное свойство является комплексным и включает две составляющих:

- полноту оценки элементов системы связи – $Q_{полн.}$;
- наглядность отображения информации – $N_{нагл.}$.

Критериев оценки, характеризующих полноту оценки элементов системы связи и наглядность отображения информации в руководящих документах на сегодня нет, поэтому в исследовательских целях определяем следующие правила оценивания:

$$Q_{полн.} \geq Q_{полн}{}^{тр} \rightarrow \max$$

$$N_{нагл.} \geq N_{нагл}{}^{тр} \rightarrow \max.$$

Ресурсопотребление, выделяемый для обеспечения работы системы мониторинга, на наш взгляд, целесообразно разделить на три основных со-

ставляющих, которые необходимо учитывать, как на этапе разработки системы, так и на этапе ее эксплуатации, а именно:

- количество личного состава, привлекаемого для обеспечения работы системы мониторинга и уровень его подготовленности – ($Z_{ДЛ}$);
- количество необходимых технических средств для обеспечения работы системы мониторинга и соответственно стоимость закупки, монтажа и эксплуатации оборудования – ($Z_{срАСУ}$);
- ресурс системы связи, который необходимо выделить для обеспечения работы системы мониторинга – ($Z_{срСС}$).

В качестве критериев оценивания соответственно определяем:

$$Z_{ДЛ} \leq Z_{ДЛ}^{доп} \rightarrow \min.$$

$$Z_{срАСУ} \leq Z_{срАСУ}^{доп} \rightarrow \min$$

$$Z_{срСС} \leq Z_{срСС}^{доп} \rightarrow \min.$$

Методика оценки системы мониторинга выступает в роли математического аппарата вычисления целевой функции $Ц = f_{Ц}(G)$, необходимой для возможности сравнения различных систем мониторинга в процессе поиска их оптимальной структуры.

С точки зрения причинно-следственных связей, система мониторинга непосредственно влияет на качество функционирования самой системы связи, которое происходит с временной задержкой, определяемой показателями своевременности работы системы мониторинга.

Определив совокупность показателей и критериев существенных свойств, характеризующих параметры работы систем мониторинга системы и сетей связи общую постановку задачу разработки методики f_Q оценки системы мониторинга формализовано можно представить в следующем виде:

$$Q = f_0\left(\boldsymbol{P}_{ОП}\right)G,R,Y;\ \boldsymbol{P}_{ОП} = \left\{\boldsymbol{T}_{о}, \boldsymbol{P}_{б}, \boldsymbol{U}\right\}, \quad (1)$$

где Q – результаты оценки системы мониторинга; $P_{оп}$ – оцениваемые показатели своевременности и результативности (качества обмена управляющей информации в системе мониторинга); G – параметры структуры системы мониторинга; R – параметры используемых ресурсов для построения и эксплуатации системы мониторинга; Y – параметры дестабилизирующих воздействий на систему мониторинга; $T_о$ – показатели своевременности работы системы мониторинга; $P_б$ – показатели безопасности обмена информацией в системе мониторинга; U – показатели достоверности обмена информацией в системе мониторинга.

Под результатами оценки системы мониторинга будем понимать рассчитанные (в соответствии с методикой) значения частных и обобщенных показателей, а также результаты их сравнения с требуемыми значениями.

На основании известных методов оценки сложных многомерных систем (в том числе систем управления) в состав разработанной общей методики оценка возможно включить модели оценки частных показателей качества системы мониторинга:

1) С выделением доминирующего показателя своевременности доставки управляющей информации с контролем выполнения требований к достоверности и безопасности.

2) С оценкой показателей, характеризующих результативность работы системы мониторинга, а именно: полнота оценки элементов системы и сетей связи, наглядность отображения информации управления системой и сетями связи.

3) С обобщением различных показателей качества системы мониторинга с учетом ресурсопотребления.

Таким образом, в данной статье показаны общие подходы к решению задачи по оценки системы мониторинга системы и сетей связи специального назначения.

Список используемых источников

1. Вознюк М. А. Теоретические основы квалиметрии высшей военной школы. СПб. : ВАС, 1997. 141 с.

2. Вознюк М. А., Мусаев А. А. Елшин А. В. Теоретические основы квалиметрии информационных систем. СПб. : ВАС, 1999. 108 с.

3. Попов А. А., Телушкин И. М., Бушуев С. Н. Общая теория систем. Часть 1. СПб. : ВАС, 1992. 247 с.

4. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. СПб. : ВАС, 2006. 460 с.

УДК 621.396.67

К. С. Голованов (студент группы ИКТВ-42, СПбГУТ)
А. А. Миловидов (студент группы ИКТВ-42, СПбГУТ)
С. О. Широков (студент группы ИКТВ-42, СПбГУТ)

ОСОБЕННОСТИ РАБОТЫ И СПОСОБЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПОДЗЕМНЫХ АНТЕНН

В работе проведен анализ функционирования подземных антенн для воздушных радиолиний. Указана область их применения в системах связи специального и гражданского назначения. Исследованы факторы, влияющие на снижение эффективности

подземных антенн по сравнения с мачтовыми. Приведены современные способы и технологии построения подземных антенн.

подземная антенна, эффективность.

Основной областью применения подземных антенн являются пункты управления в оборудованных фортификационных сооружениях и районах гражданской обороны, а также для радиоуправления в системах инженерных заграждений, радиоразведке, радиопеленгации.

Подземная антенна (ПА) – это антенное устройство, расположенное под поверхностью земли и предназначенное для излучения или приема радиоволн (рис. 1).

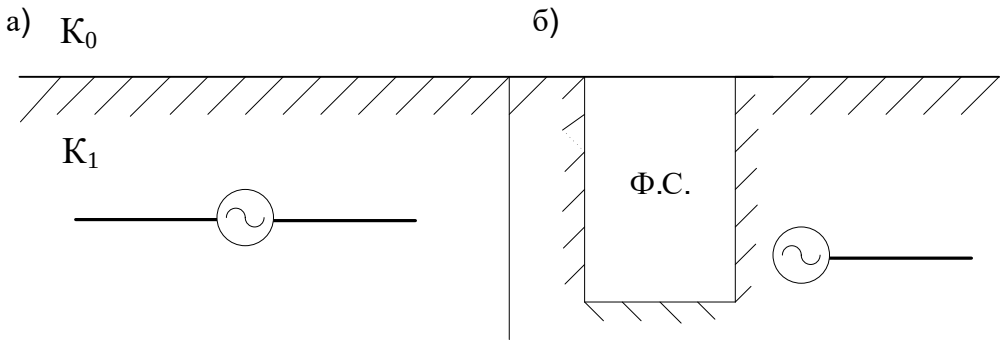


Рис. 1. Подземная антенна:
а) – симметричная; *б*) – несимметричная

В сравнении с мачтовыми ПА обладают рядом достоинств. Основными из них являются:

- разведзащищенность, то есть ее неуязвимость при визуальном осмотре, аэрокосмической и агентурной разведке. Данное обстоятельство позволяет применять ПА в особо сложных и опасных районах расположения подразделений;
- физическая защищенность, а именно, при использование вероятным противником оружия массового поражения (ядерного оружия) у ПА, в отличие от ее аналогов, например, мачтовых антенн, существует шанс продолжить работу в осложнившейся боевой обстановке, это объясняется тем, что обычные мачтовые антенны разрушаются при избыточном давлении ударной волны 0,1–0,2 кг/см^2, в то время как ПА сохраняют свою работоспособность при действии всех поражающих факторах ядерного взрыва, равных 20–30 кг/см^2;
- долговечность, которая определяется техническими решениями, применяемыми материалами и изделиями, режимом работы и качеством изготовления антенны. Срок службы антенны может составлять более 10 лет, что обусловлено отсутствием возможности проведения плановых работ на подземных антеннах.

Вышеприведенные достоинства в большей степени обусловлены их использованием в системах связи специального назначения.

В гражданской сфере использование данного типа антенн экономически оправдано в климатически неблагоприятных и экстремальных условиях. ПА, в отличие от мачтовых, обладают более высокой надежностью. Это объясняется тем, что ПА могут быть выполнены из кинематически гибких конструкций, обеспечивающих защиту от действия сжатия и сдвигов грунта. Именно поэтому в таких районах как Курилы, Сахалин, Камчатка или Тыва целесообразнее использовать ПА в связи с повышенной сейсмической опасностью данных районов.

В процессе использования подземных антенн можно выделить особенности их функционирования. Несмотря на то, что ПА находится в диссипативной среде она должна обладать энергетическими характеристиками близкими к антеннам, находящимся в воздушном пространстве. Для достижения таких же свойств необходимо рассмотреть факторы, влияющие на эффективность ПА.

В качестве подземных антенн применяются горизонтальные (расположенные параллельно поверхности земли) провода. Это объясняется тем, что при переходе через границу раздела земля-воздух горизонтальная составляющая напряженности электрического поля превышает вертикальную.

Коэффициент усиления горизонтального вибратора в земле, выполненного из изолированного провода, существенно меньше, чем коэффициент усиления аналогичного вибратора в воздухе.

Причины низкой эффективности такого излучателя заключается в том, что большие потери в ближней зоне полупроводящей среды, где напряженность поля E велика, ток быстро затухает, и *действующая* длина оказывается малой, так как плотность тока ($\vec{j} = \sigma\vec{E}$) определяет мощность тепловых потерь:

$$P_\sigma = \frac{1}{2}\int \sigma(E)^2 dv,$$

то из данной формулы следует: чем больше плотность тока, тем больше мощность потерь.

В связи с тем, что ПА находится в диссипативной среде, энергия электромагнитной волны имеет неблагоприятное распределение, это связано с тем, что, доходя до границы раздела двух сред, диссипативной и воздушной, большая часть энергии отражается от границы земля-воздух (рис. 2), вследствие чего лишь малая часть энергии переходит через границу раздела, данное явление обусловлено большой разницей макроскопических параметров среды. Стоит заметить, что снижение эффективности подземных

антенн увеличивается по мере увеличения длины волны и проводимости грунта.

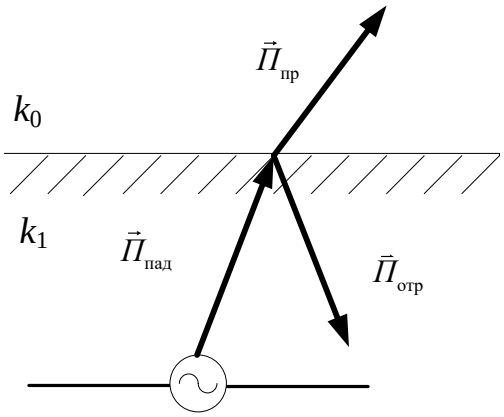


Рис. 2. К вопросу об эффективности ПА

При установке ПА следует учитывать, что энергия передаваемого сигнала будет убывать в зависимости от глубины установки антенны и от выбора грунта, в котором мы устанавливаем антенну. Именно поэтому глубину установки антенны следует выбирать такую, чтобы обеспечить требуемую энергетику радиолинии, но в то же время сохранить защищенность антенны.

Вследствие распространения, значительное затухание волны в диссипативной среде от антенны до поверхности земли в слое толщиной h осуществляется по экспоненциальному закону:

$$E(h) = E(0) \cdot e^{-\alpha h},$$

где α - коэффициент затухания радиоволн в земле, возрастающий с увеличением ее проводимости и частоты, h - глубина заложения антенны.

Для снижения воздействия факторов, влияющих на эффективность подземных антенн , разработаны специальные технологии построение подземных антенн:

1) Увеличение диаметра проводника ПА (рис. 3). Антенну изготавливают из металлических труб большого диаметра, широких пластин и многопроводных полотен из параллельных или расходящихся проводов. При этом уменьшается плотность тока и, соответственно, концентрация поля в ближней зоне антенны, что уменьшает тепловые потери.

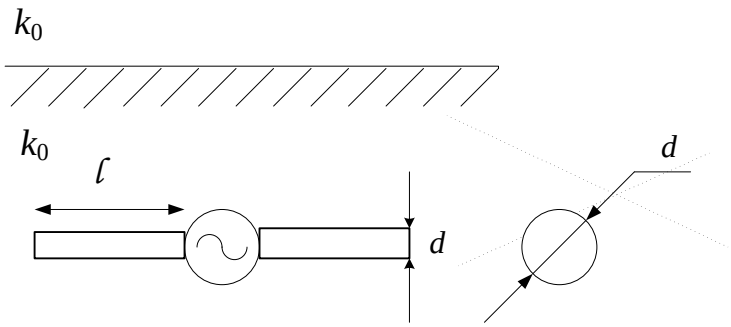


Рис. 3. Трубчатая ПА

2) Экранирование нижнего полупространства. Для этого следует под антенной расположить металлический экран (рис. 4), препятствующий распространению волн вглубь грунта.

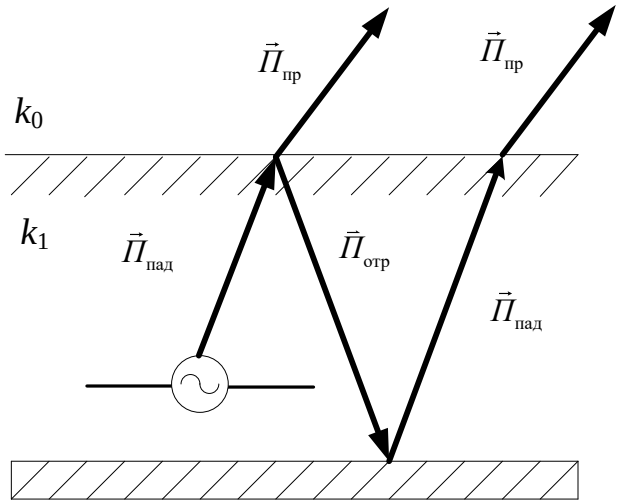


Рис. 4. ПА однонаправленного излучения

3. Снижение проводимости среды в области, непосредственно окружающей проводник. Для этого провод покрывается слоем изоляции (рис. 6) или располагается в воздушной полости (рис. 5). В этом случае область, где концентрируется максимальное поле, оказывается заполненной диэлектриком без потерь, из-за чего уменьшается затухание тока по проводу и увеличивается действующая длина антенны. Для получения существенного выигрыша толщина изоляции должна в несколько раз превышать диаметр провода антенн.

В работе проведен анализ функционирования подземных антенн для воздушных радиолиний. Рассмотрены варианты применения подземных антенн в системах радиосвязи специального и гражданского назначения, а также исследованы факторы, влияющие на эффективность подземных антенн по сравнению с мачтовыми и способы ее повышения.

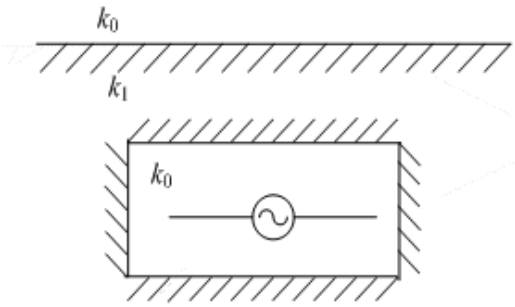


Рис. 5. Туннельная ПА

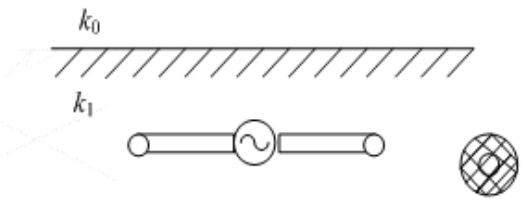


Рис. 6. Кабельная ПА

Список используемых источников

1. Каменев В. В., Сосунов Б. В., Проценко М. С., Щербаков Д. С. Распространение радиоволн и антенно-фидерные устройства / под ред. Каменева В. В. СПб. : ВАС, 2007. 260 с.

2. Б. В. Сосунов, В. В. Филиппов. Основы расчета подземных антенн. Л. : ВАС, 1990, 82 с.

3. Лавров Г. А., Князев А. С. Приземные и ПА. Теория и практика антенн, размещенных вблизи поверхности земли. М. : Советское радио, 1965. 474 с.

4. Кинг Р., Смит Г. Антенны в материальных средах / пер. с англ. М. : Мир, 1984. 824 с.

Статья представлена научным руководителем,
кандидатом технических наук Проценко М. С.

УДК 621.391

А. А. Гулидов (соискатель, ВАС)

ПРЕДЛОЖЕНИЯ ПО ОЦЕНКЕ ЭФФЕКТИВНОСТИ РАДИОПОДАВЛЕНИЯ КАНАЛОВ СПУТНИКОВОЙ СВЯЗИ

Данная статья посвящена вопросам разработки методического аппарата для радиоподавления каналов спутниковой связи. В частности, рассматривается эффективность постановки помех несанкционированным абонентам спутниковой системы связи.

спутниковые системы связи, оценка эффективности, радиоподавление, помехи.

Введение

Для систем радиоконтроля актуальной задачей является оценка эффективности радиоподавления несанкционированных абонентов спутниковых систем связи (ССС) [1]. Традиционный подход, основанный на энергетическом превосходстве, предполагает достаточное число комплексов активного мониторинга, что сложно обеспечить на практике [2].

В жестких экономических условиях прагматичным является, так называемое, интеллектуальное подавление абонентов ССС [3], при котором поражаются отдельные элементы сигнала, приводящие к нарушению связи. При таком подходе происходит рациональное использование энергетического потенциала, но его реализация не возможна без процедур оценки эффективности. Особенно остро этот вопрос стоит при подготовке специалистов, когда физическое подавление абонентов невозможно, ввиду юридических аспектов. Вопросам разработки методического аппарата для такого подхода и посвящена настоящая статья.

Предложения по оценке эффективности блокирования каналов

Интересным является решение, предложенное в [4], предусматривающее возможность контроля при подавлении абонентов через спутник-ретранслятор. Несомненным достоинство такого подхода является возможность контролировать результаты подавления по вынесенному тракту приема. Это позволяет дополнительное использование процедур распознавания реализованных в [5, 6], что существенно расширяет возможности контроля и позволяет оценить величину частотной расстройки помехи и сигнала на длительности каждого тактового интервала, возникающей в результате неточности измерений по каналу приема или недостаточных навыков операторов пунктов активного мониторинга.

$$\Delta_{\text{сп}} = \left| f_{\text{п}} - f_{\text{с}} \right|, \tag{1}$$

где $f_{\text{п}}$ – значение частоты помехи; $f_{\text{п}}$ – значение частоты сигнала.

Расстройка (1) может рассматриваться в качестве контролируемого параметра при определении эффективности. Другим параметром контроля выступает расстройка допустимого превышения мощности помехи над сигналом, при котором обеспечивается блокирование абонентов ССС. Для разработки методического аппарата рассмотрим условия постановки помех в каналах частотной манипуляцией (ЧМ) и относительной фазовой манипуляцией (ОФМ) вероятности ошибки будет определяться следующим образом:

$$P_{\text{ош}} = \begin{cases} \dfrac{1}{2}\exp\left(-0{,}5\cdot\dfrac{P_{\text{с}}}{P_{\text{ш}}+P_{\text{п}}}\right) = \dfrac{1}{2}\exp\left(-\dfrac{0{,}5}{\dfrac{P_{\text{ш}}}{P_{\text{с}}}+\dfrac{P_{\text{п}}}{P_{\text{с}}}}\right) = \dfrac{1}{2}\exp\left(-\dfrac{0{,}5}{\dfrac{1}{h^2}+\hbar^2}\right) \\ \text{для ЧМ сигнала;} \\ \dfrac{1}{2}\exp\left(-\dfrac{P_{\text{с}}}{P_{\text{ш}}+P_{\text{п}}}\right) = \dfrac{1}{2}\exp\left(-\dfrac{1}{\dfrac{P_{\text{ш}}}{P_{\text{с}}}+\dfrac{P_{\text{п}}}{P_{\text{с}}}}\right) == \dfrac{1}{2}\exp\left(-\dfrac{1}{\dfrac{1}{h^2}+\hbar^2}\right) \\ \text{для ОФМ сигнала.} \end{cases} \tag{2}$$

В формуле (2) $h^2 = P_с / P_ш$ – отношение мощностей сигнала $P_с$ и шума $P_ш$ (ОСШ), а $\hbar^2 = P_п / P_с$ – отношение мощностей помехи $P_п$ и сигнала $P_с$ (ОПС). На рисунке 1 показаны графические зависимости $P_{ош} = f(P_п / P_с) = f(\hbar^2)$ для сигналов с ЧМ и ОФМ, с учетом значения $h^2 =$ 20 дБ в канале.

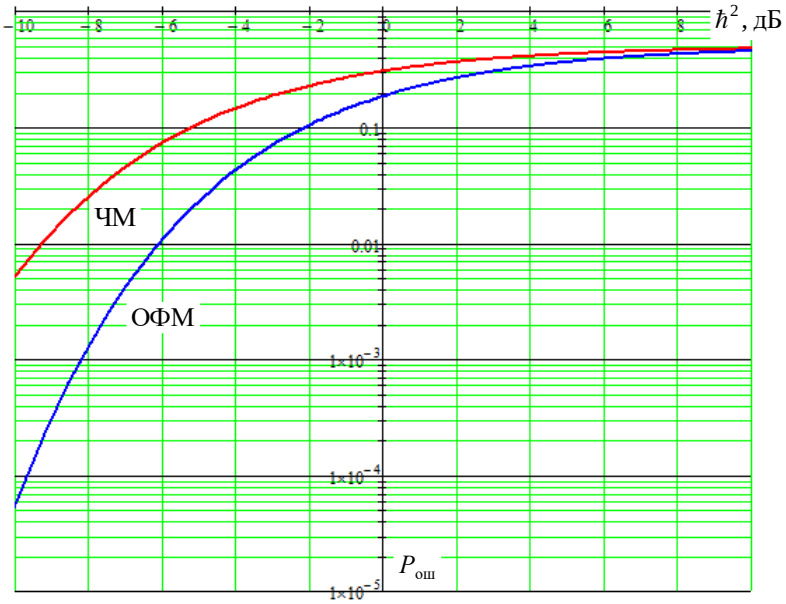


Рис. 1. Вероятность ошибки в канале от значения ОПС
для сигналов частотной и относительной фазовой манипуляции

Анализ полученных зависимостей показывает, что при больших значениях ОПС $\hbar^2$ (когда $P_{ош} \geq 0{,}1$) влияние шумовых составляющих на величину $P_{ош}$ незначительное, что позволяет ими пренебречь. Существенным фактором, определяющим достоверность $P_{ош}$, является неточность в определении потребного значения Δ при выборе ОПС. С учетом Δ, получим:

$$P_{ош} = \begin{cases} \dfrac{1}{2}\exp\left(-0{,}5 \cdot \dfrac{P_с}{P_ш + P_п}\right) = \dfrac{1}{2}\exp\left(-\dfrac{0{,}5}{\dfrac{1}{h^2} + \hbar^2 \pm \Delta}\right) \\ \text{для ЧМ сигнала;} \\ \dfrac{1}{2}\exp\left(-\dfrac{P_с}{P_ш + P_п}\right) = \dfrac{1}{2}\exp\left(-\dfrac{1}{\dfrac{1}{h^2} + \hbar^2 \pm \Delta}\right) \\ \text{для ОФМ сигнала.} \end{cases} \quad (3)$$

На рис. 2 показаны графические зависимости вероятности ошибки от погрешности определения ОПС Δ для значения $\hbar^2 = 1$. Здесь показаны линии, ограничивающие область изменения вероятности ошибки при постановке прямошумовой помехи сигналам ЧМ (вверху) и линии, ограничивающие область при постановке прямошумовой помехи сигналам ОФМ (внизу).

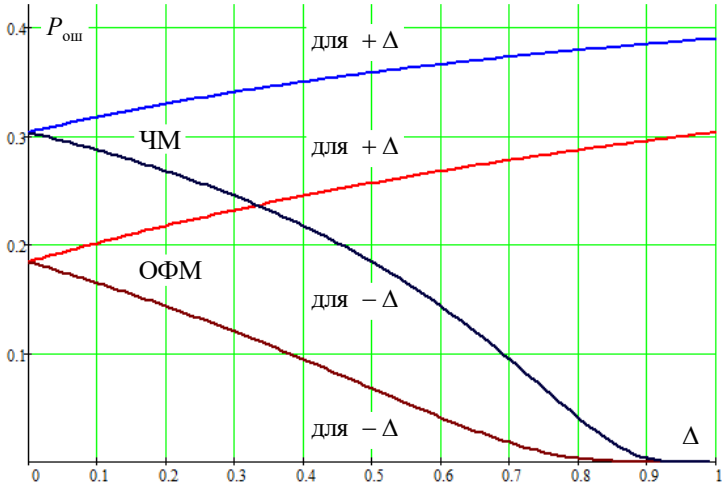


Рис. 2. Зависимость вероятности ошибки в канале
от ошибки определения искомого значения ОПС
для сигналов частотной и относительной фазовой манипуляции

Восходящие кривые на рисунке 2 соответствуют погрешностям со знаком плюс, а снисходящие – со знаком минус.

Анализ полученных результатов показывает, что вероятность ошибки с возрастанием погрешности ОПС увеличивается или уменьшается, в зависимости от знака (возрастает, если знак плюс, и убывает, если знак минус).

Отклонение вероятности ошибки от истинного значения, при погрешности со знаком плюс может достигать: 35 % при постановке помех сигналам ЧМ, и 24 % при постановке помех сигналам ОФМ. Если погрешности имеют знак минус, то, соответственно получаем значения 97 и 100 % при подавлении сигналов ЧМ и ОФМ. Анализ учета предложенного значения в (3) можно обеспечить на основе использования различных методов обнаружения, в частности, разработанных в [7, 8, 9], которые позволят измерить амплитудные различия, характеризующие величину Δ.

Заключение

Предложенный методический аппарат позволяет оценивать эффективность постановки помех несанкционированным абонентам ССС на основе расчёта ошибки в выборе требуемого значения ОПС. Следовательно, открывается возможность подобрать наименьший уровень помехи, при ко-

тором обеспечивается решение задачи блокирования при минимальных энергетических затратах.

При постановке помех в режиме обучения личного состава предлагается формировать помеху под уровнем шумов, а на приеме посредством процедур корреляции получать отклик по величине, которой и проводить последующие измерения. Такой подход позволит исключить нарушение юридических прав легитимных абонентов ССС и, в тоже время, предоставит возможность личному составу получить требуемый навык.

Направление дальнейшего исследования видится в совместной оценке частотной расстройки и энергетической погрешности при постановке помех, а также использования метода совместного оценивания сигналов, представленного в [10].

Список используемых источников

1. Дворников С. В. Проблема поиска сигналов источников информации при радиомониторинге. Мобильные системы. 2007. № 4. С. 33–35.

2. Радзиевский В. Г. Современная радиоэлектронная борьба. Вопросы методологии. М. : Радиотехника, 2006. 424 с.

3. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. М. : Вузовская книга, 2011. 800 с.

4. Ю. М. Урличич, В. А. Поповкин и др. Способ оценки эффективности радиоподавления сигнала спутниковой связи путем воздействия помехами на приемные системы ретрансляторов и устройство для его реализации: пат. РФ на изобретение № 2420760 по заявке № 2009143758/09 от 26.11.2009;

5. Аладинский В. А., Дворников С. В., Сауков А. М., Симонов А. Н. Способ распознавания радиосигналов: пат. на изобретение RUS 2261476 26.01.2004.

6. Дворников С. В., Дворников А. С., Желнин С. Р., Оков И. Н., Сауков А. М., Симонов А. Н., Яхеев А. Ф. Способ распознавания радиосигналов: пат. на изобретение RUS 2356064 24.04.2007.

7. Дворников С. В. Метод обнаружения на основе посимвольного перемножения реализаций спектра наблюдаемого процесса с автоматическим расчетом порога принятия решения // Научное приборостроение. 2004. Т. 14. № 4. С. 92–97.

8. Дворников С. В., Железняк В. К., Комарович В. Ф., Храмов Р. Н. Метод обнаружения радиосигналов на основе обработки их частотно-временных распределений плотности энергии. Информация и космос. 2005. № 4. С. 13–16.

9. Дворников С. В. Метод обнаружения сигналов диапазона вч на основе двухэтапного алгоритма принятия решения // Научное приборостроение. 2005. Т. 15. № 3. С. 114–119.

10. Алексеев А. А., Аладинский В. А., Железняк В. К., Комарович В. Ф., Дворников С. В. Применение методов частотно-временной обработки акустических сигналов для анализа параметров реверберации // Научное приборостроение. 2001. Т. 11. № 1. С. 65–76.

Статья представлена научным руководителем,
доктором технических наук, профессором Дворниковым С. В.

УДК 621.391

С. С. Дворников (лаборант, ВАС)

ПРЕДЛОЖЕНИЯ ПО ФОРМИРОВАНИЮ СИГНАЛОВ МЕТОДОМ ПОСЛЕДОВАТЕЛЬНОЙ КОНКАТЕНАЦИИ ВЕЙВЛЕТ-ФУНКЦИЙ

В работе представлены результаты исследования возможности использования в системах радиосвязи сигналов, формируемых в базисе вейвлет-функций (БВФ). Сигналы, сформированные в БВФ, наделяются свойством структурной скрытности по отношению к базисам гармонических функций. Представленные результаты моделирования подтверждают данное заключение. В статье обоснован подход к синтезу сигналом методом последовательной конкатенации вейвлетов различной структуры, соответствующих информационным символам.

базисные функции, манипуляционные форматы, вейвлет-функции, фазоманипулированные сигналы, помехоустойчивость, скрытность сигналов.

Вейвлеты все чаще применяются для синтеза на их основе различных видов сигналов. В частности, в [1, 2] предложен синтез различных форм фазоманипулированных сигналов на основе вейвлетов. Таким образом, открываются новые направления практического применения вейвлетов для формирования на их основе радиосигналов.

Действительно, принцип передачи информации базируется на физические различия радиосигналов, соответствующих различным компонентам информационного алфавита. При амплитудной модуляции указанные различия наблюдаются в изменении амплитуды, при частотной модуляции – в номиналах несущих частот, а при фазовой модуляции – соответственно в позициях фазы [3]. В настоящее время одним из наиболее помехоустойчивых видов манипуляционных форматов является двойная фазовая манипуляция (ФМн-2). Принцип ее реализации состоит в инверсии фазы при смене информационных символов. Так на рисунке 1 показана временная диаграмма тестового сигнала ФМн-2 длительностью в 312 дискретных отчета (здесь и далее верхний индекс указывает на базис формирования сигнала, на рисунке 1 символ Г обозначает гармонический базис формирования).

Анализ структуры сигнала ФМн-2 показывает, что он представляет собой результат конкатенации радиоимпульсов, начальная фаза которых определяется информационным значением битовой посылки. Следовательно, синтез сигналов ФМн-2 можно осуществлять посредством ключевой схемы, представленной на рисунке 2, в которой битовая последовательность регулирует подачу радиоимпульсов в канал. При таком подходе длительность посылок будет определяться скоростью манипуляции ключа.

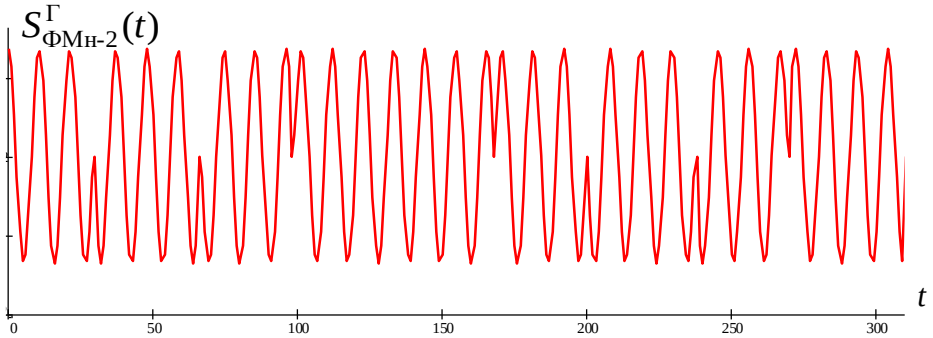


Рис. 1. Временная развертка тестового сигнала ФМн-2 на основе гармоник

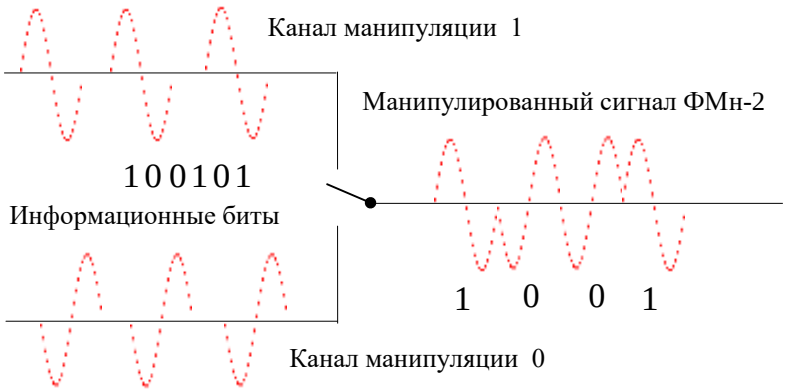


Рис. 2. Принцип формирования сигналов ФМн-2
на основе последовательной конкатенации радиоимпульсов

Рассмотренный подход открывает возможности по синтезу ФМн-2 сигналов на основе вейвлетов, если в качестве формирующих радиоимпульсов определить инверсные формы вейвлетов. В результате получим вейвлет-фазоманипулированное (ВФМ) колебание.

Предлагается в качестве формирующего использовать вейвлет Гаусса первого порядка $\psi(t)$, представляющий производную от функции Гаусса.

$$\psi_m(t) = (-1)^m \partial_t^m \left[\exp(-t^2/2) \right]. \quad (1)$$

Аналитически вейвлет Гаусса 1-го порядка имеет следующий вид [1]:

$$\psi(t) = -t \exp(-t^2/2). \quad (2)$$

Анализ выражения (2) указывает на локализованный характер функции. Следовательно, синтез непрерывного колебания на его основе в принципе невозможен. Однако вейвлет Гаусса может быть в качестве формирующего колебания в ключевой схеме (см. рис. 2). Так, на рисунке 3 представлены формирующие сигналы $\psi_1(t)$ и $\psi_0(t)$, синтезированные на основе прямой и обратной формы вейвлета Гаусса.

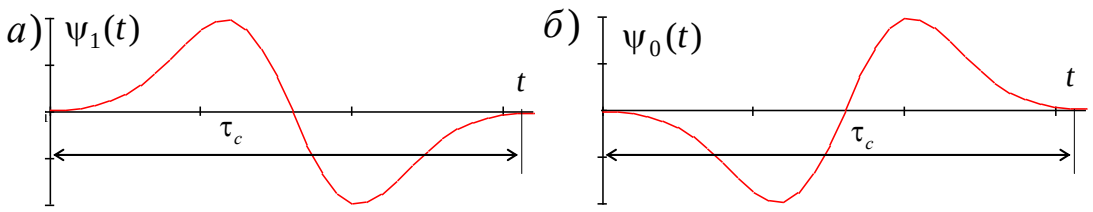


Рис. 3. Формирующие элементы для синтеза ВФМ сигнала:
а – логической единицы; *б* – логического нуля

Отметим, что свойства локализации вейвлета и его двусторонняя временная структура в полной мере отвечает свойствам формирующих колебаний в соответствии с рассмотренным выше подходом.

На рисунке 4 показаны фрагменты фазоманипулированных сигналов, сформированных на основе элементов синусоид и на основе вейвлетов.

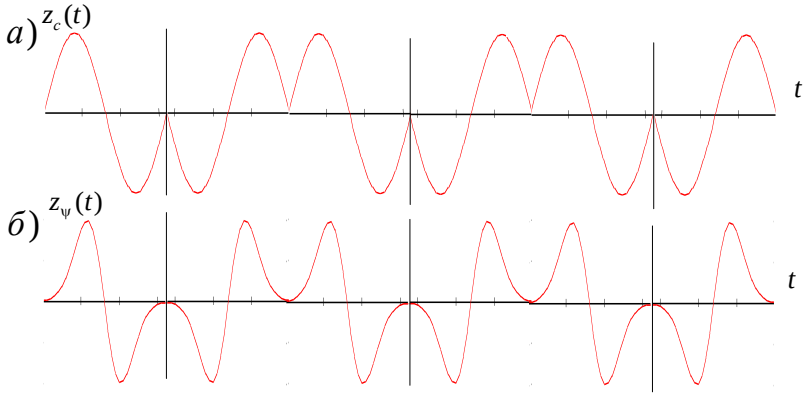


Рис. 4. Сигнал фазовой манипуляции, синтезированный
на основе фрагментов: *а* – синусоид; *б* – вейвлетов

Таким образом, подход к синтезу ФМн-2 сигналов на основе последовательной конкатенации фрагментов радиоимпульсов, позволил разработать метод формирования ВФМ сигналов, в основе которых лежат вейвлеты прямой и инверсной структуры.

Важной особенностью предлагаемых сигналов является их структурная скрытность по отношению к системам мониторинга [4], обрабатывающих радиоизлучения в базисах гармонических функций. Это объясняется структурой ВФМ сигналов, в основе которых лежат вейвлеты Гаусса.

Так, на рисунке 5*а* представлены фрагменты формирующих сигналов на основе синусоиды $s_0(t)$ и вейвлета Гаусса 1-го порядка $\psi_1(t)$ равной энергии, а на рис. 5*б*, соответствующие им модули спектров $|F_0(f)|$ и $|V_1(f)|$.

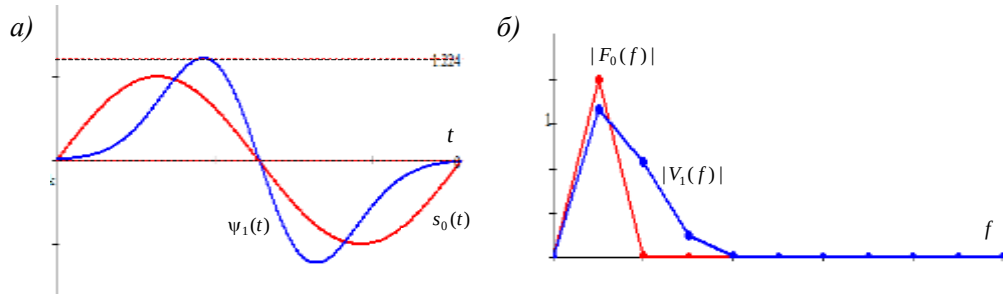


Рис. 5. Формирующие сигналы на основе синусоиды и вейвлета Гаусса:
а – временное представление; *б* – частотное представление

На рисунке 6 приведено распределение энергии формирующих сигналов в частотном пространстве.

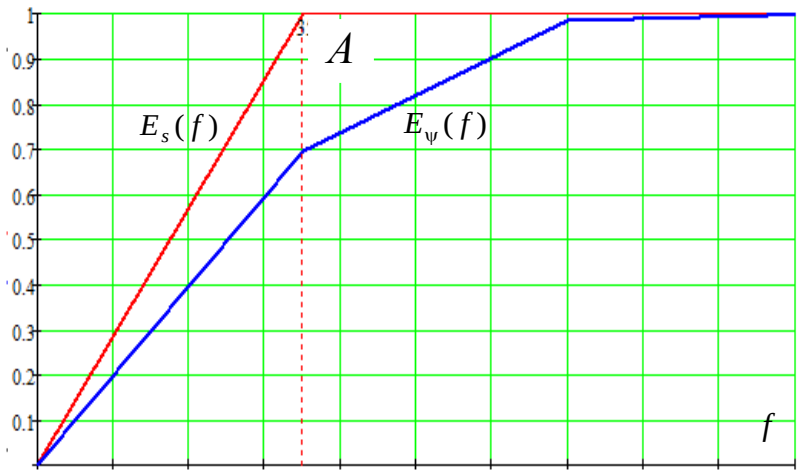


Рис. 6. Распределение энергии формирующих сигналов
на основе синусоиды и вейвлета Гаусса в частотном пространстве

Анализ полученных результатов позволяет сделать следующее заключение. Обработка вейвлет-сигналов в базисе функций Фурье является неоптимальной и эквивалентна снижению энергии на 30 % (см. рис. 5). Аналитически это равносильно добавлению в формуле вероятностной оценки помехоустойчивости коэффициента 0,7 [3]:

$$P_{B\text{ФМн}} = Q\left(\sqrt{\frac{2E_b}{N_0}} \times 0{,}7\right). \qquad (3)$$

Полученный результат можно интерпретировать как снижения помехоустойчивости вследствие структурного несоответствия гармоник и вейвлетов в частотно-временном пространстве. Указанные различия определим, как структурную скрытность, характеризуемую показателем увеличения вероятности ошибки на бит (см. рис. 7).

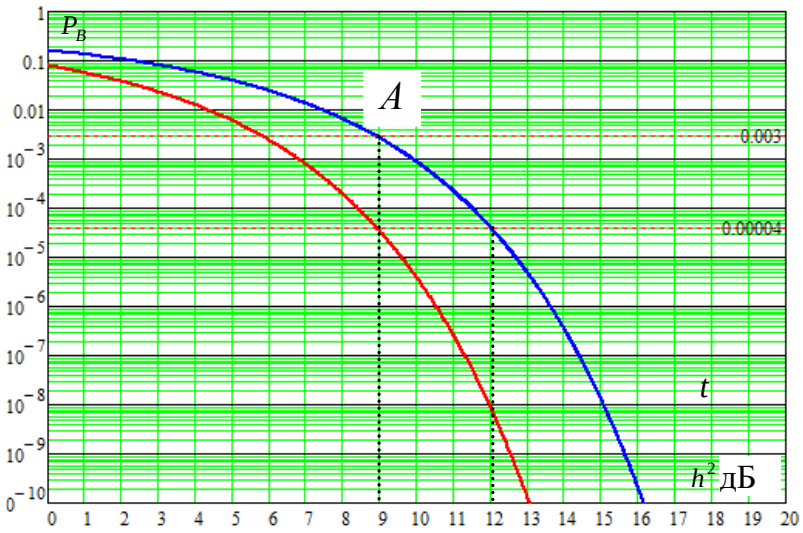


Рис. 7. Оценка эффективности процедур структурной скрытности по показателю вероятности ошибки на бит: – для сигналов ФМн-2

Анализ полученных результатов позволяет сделать следующее заключение. При отсутствии априорной информации о базисе формирования сигнала, система мониторинга будет проводить анализ в эффективной полосе приема, включающей не менее 90–95 % спектральной энергии в соответствии со скоростью передачи сообщений, в базисе гармонических функций. В этом случае, в полосе, оптимальной для обработки, будет сосредоточено менее 70 % спектральной энергии ВФМ сигналов, в основе которых лежат вейвлеты Гаусса 1-го порядка. Это ведет к увеличению вероятности ошибки более чем на два порядка, что равносильно снижению отношения сигнал шум в канале более чем на 3 дБ

Предполагается, что указанный эффект может быть усилен при увеличении числа различных видов, используемых вейвлетов, применяемых для синтеза ВФМ сигналов. Поскольку в этом случае возрастает сложность обработки таких конструкций, обусловленная отсутствием априорной информации о базисах их формирования.

Дальнейшие исследования видятся в разработке эффективных методов демодуляции вейвлет-сигналов. А также решения задачи распознавания ВФМ на основе подхода, предложенного в [5], основу которого составляют процедуры вейвлет-преобразований обрабатываемых излучений.

Список используемых источников

1. Дворников С. В., Дворников С. С., Манаенко С.С., Погорелов А.А. Синтез фазоманипулированных вейвлет-сигналов // Информационные технологии. 2015. № 2. С. 140–143.

2. Дворников С. В., Манаенко С. С. Помехоустойчивость фазоманипулированных сигналов на основе вейвлетов Гаусса // Вестник Воронежского государственного технического университета. 2015. Т. 11. № 3. С. 123–125.

3. Прокис Дж. Цифровая связь / пер. с англ.; под ред. Д. Д. Кловского. М. : Радио и связь. 2000. 800 с.

4. Дворников С. В., Дворников С. С., Манаенко С. С., Пшеничников А. В. Спектрально-эффективные сигналы с непрерывной фазой // Вестник Воронежского государственного технического университета. 2016. Т. 12. № 2. С. 87–93.

5. Устинов А. А., Дворников С. В., Дворников С. С., Коноплев М. А., Сухаруков Г. А., Осадчий А. И. Способ распознавания радиосигналов. Пат. на изобретение RUS 2430417 25.05.2010.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Пшеничниковым А. В.

УДК 621.391

С. С. Дворников (лаборант, ВАС)

ВЕЙВЛЕТ-СИГНАЛЫ ДЛЯ СИСТЕМ РАДИОСВЯЗИ

В данной работе представлены результаты исследования возможности использования сигналов, формируемых в базисе вейвлет-функций (БВФ). БВФ предлагается формировать из производных различных порядков от функции Гаусса. Применение БВФ позволяет получать сигналы с новыми свойствами. Сигналы, формируемые в БВФ, обладают структурной скрытностью по отношению к системам мониторинга, использующих для анализа базисы гармонических функций Фурье. Представлены результаты оценки помехоустойчивости системы с сигналами, формируемыми в БВФ. Предложены варианты новых сигнальных конструкций для систем радиосвязи.

базисные функции, манипуляционные форматы, вейвлет-функции, фазоманипулированные сигналы, помехоустойчивость, скрытность сигналов.

Введение

Широкое практическое применение в радиотехнике методы вейвлет-преобразований получили благодаря работам А. Гроссмана и Ж. Морле, применительно к обработке сейсмических и акустических сигналов [1].

В настоящее время различные алгоритмы на основе вейвлет-функций (далее вейвлеты) успешно используются при распознавании образов, исследовании нестационарных колебаний, синтезе речевых сигналов и других задачах анализа сигналов [2, 3, 4, 5, 6].

Между тем, вейвлеты все чаще применяются для прямого численного моделирования как иерархический базис, адаптированный для описания динамики сложных нелинейных процессов. В том числе и для синтеза на их основе различных видов сигналов, что обусловлено возможностью

создания с их помощью ортогональных конструкций для манипуляционных форматов.

В частности, в [6] предложен синтез фазоманипулированных сигналов, обладающих свойствами повышенной помехоустойчивости по отношению к их классическим формам на основе гармонических функций.

Таким образом, открываются новые направления применения вейвлетов в качестве сигналов для систем радиосвязи. Именно исследованию данного вопроса посвящена настоящая статья.

Теоретические основы для формирования сигналов на основе вейвлетов

В общем случае, вейвлеты $\psi(t)$, согласно [3], представляют собой базисные функции, обеспечивающие с помощью целочисленного масштабирования исходного материнского вейвлета реконструкцию пространства $L^2(\mathbf{R})$, в котором они заданы.

Между тем в [2] обосновано, что аналогом частоты для вейвлетов является следующее представление $\psi(2^k t-\tau)$, здесь τ и k – целые числа $(\tau, k \in \mathbf{I})$. Следовательно, посредством масштабных преобразований $(1/2^k)$ и временных сдвигов $(\tau/2^k)$ можно описать любое функциональное пространство, при этом используя единственный базисный материнский вейвлет $\psi(t)$.

Поскольку норма вейвлет-базиса, согласно [3], представляется как

$$\| \psi(2^k t-\tau) \|_2 = 2^{-k/2} \| \psi(t) \|_2 , \tag{1}$$

то при условии, что материнский вейвлет $\psi(t) \in L^2(\mathbf{R})$ имеет единичную норму, все функции базиса $\{\psi_{\tau k}\}$ вида

$$\psi_{\tau k}(t) = 2^{k/2}\psi(2^k t-\tau), \quad \tau, k \in \mathbf{I}, \tag{2}$$

также нормированы к единице, т. е. $\| \psi_{\tau k} \|_2 = \| \psi \|_2 = 1$.

Таким образом, любой вейвлет из рассматриваемого пространства $\psi \in L^2(\mathbf{R})$ будет ортогональным, если определенное соотношением (2) семейство $\{\psi_{\tau k}\}$ представляет собой ортонормированный базис этого функционального пространства $L^2(\mathbf{R})$, т. е.

$$\left\langle \psi_{\tau k}, \psi_{l m} \right\rangle = \delta_{\tau k}\delta_{l m}, \tag{3}$$

и каждая функция f указанного пространства, т. е. $f \in L^2(\mathbf{R})$, может быть представлена в виде ряда

$$f(t) = \sum_{k,\tau=-\infty}^{\infty} c_{k\tau}\, \psi_{k\tau}(t). \tag{4}$$

В общем случае, согласно [2], условий (3) и (4) недостаточно для определения вейвлета в качестве базисной функции. Строгость выполнения этого условия предполагает существование обратных преобразований. Однако на практике достаточно выполнения свойств устойчивости и, в соответствии с [3], «приблизительной» ортогональности системы разложения.

С указанных позиций для базиса (2) в качестве таких условий выступают свойства адекватности расширения и сдвига исходного вейвлета $(1/2^k, \tau/2^k), k, \tau \in \mathbf{I}$ и возможность обратной реконструкции с точностью до постоянного множителя, ограничивающего класс возможных базисных функций. В частности, Фурье образ для базисных вейвлетов должен быть равен нулю в начале координат [1].

Вейвлет, используемый для реконструкций (в дальнейшем для синтеза сигналов), должен удовлетворять условиям базиса Рисса. Согласно которым всегда существуют такие две константы A и B, где $0 < A \le B < \infty$, для которых соотношение [3]

$$A \| \{c_{k\tau}\} \|_2^2 \le \left\| \sum_{k=-\infty}^{\infty} \sum_{\tau=-\infty}^{\infty} c_{k\tau}\, \psi_{k\tau} \right\|_2^2 \le B \| \{c_{k\tau}\} \|_2^2, \tag{5}$$

выполняется при любой ограниченной и дважды квадратично суммируемой последовательности $\{c_{k\tau}\}$:

$$\| \{c_{k\tau}\} \|_2^2 = \sum_{k=-\infty}^{\infty} \sum_{\tau=-\infty}^{\infty} |c_{k\tau}\, \psi_{k\tau}|^2 < \infty. \tag{6}$$

В большинстве практических приложений достаточно выполнение свойств полуортогональности для вейвлета, предусматривающего равенство нулю условия (3). В общем случае, условиям существования вейвлета соответствуют производные высоких порядков от функции Гаусса [3, 5]

$$\psi_m(t) = (-1)^m \partial_t^m \left[\exp(-t^2/2) \right]. \tag{7}$$

Здесь $\partial_t^m = \partial^m[\ldots]/\partial t^m, \quad m \ge 1$.

Таким образом, функции, синтезируемые на основе выражения (7), являясь вейвлетами, удовлетворяют условиях формирования на их основе базисов. Методология вейвлетов наиболее широкое применение нашла в различных областях обработки сигналов, связанных с решением вопросов фильтрации, анализа, распознавания [1, 2, 3, 4]. Однако она не исключает применения вейвлетов и в интересах передачи информации [5, 6].

Предложения по синтезу сигналов на основе вейвлетов

Возможность формирования на основе вейвлетов функциональных базисов (2), открывает широкие возможности, в частности, по синтезу сигналов с принципиально новыми свойствами [6]. Действительно, принцип передачи информации базируется на физические различия радиосигналов соответствующих различным компонентам информационного алфавита. Так при амплитудной модуляции указанные различия наблюдаются в изменении амплитуды. При частотной модуляции – в номиналах несущих частот, а при фазовой модуляции – соответственно в позициях фазы [7].

Под модуляционным форматом в дальнейшем будем понимать совокупность вида модуляции (манипуляции) и скорости передачи сигнала [8].

Очевидно, что аналогичным образом в процессе модуляции можно использовать вместо несущих колебаний и вейвлеты. При этом следует учитывать, что в отличие от гармоник вейвлеты локализованы не только в частотном, но и во временном пространстве, следовательно, их применение оправдано в манипуляционных системах, в которых четко локализован единичный элемент сигнала, передающий информацию.

В первую очередь к таковым следует отнести дискретные частотные и фазовые манипуляционные форматы, когда при каждой смене позиций можно в качестве несущего колебания использовать новый вид вейвлета [5].

В частности, для двухпозиционных форматов (когда для передачи бинарной информации используют две градации изменения параметра) возможно применение в качестве второго несущего колебания инверсную форму вейвлета и т. д.

Таким образом, вейвлеты, способные формировать функциональные базисы, вполне могут быть использованы для синтеза сигналов частотной и фазовой манипуляции.

В настоящее время одним из наиболее помехоустойчивых видов манипуляционных форматов является двойная фазовая манипуляция (ФМн-2) [7]. Принцип ее реализации состоит в инверсии фазы при смене позиции.

Так на рисунке 1 показана временная диаграмма тестового сигнала ФМн-2 длительностью в 312 дискретных отчета (здесь и далее верхний индекс указывает на базис формирования сигнала, на рисунке 1 символ Г обозначает гармонический базис формирования).

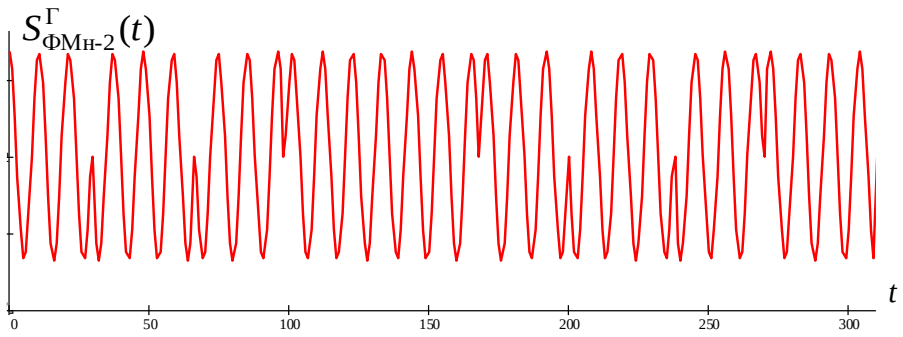


Рис. 1. Временная развертка тестового сигнала ФМн-2 на основе гармоник

Между тем, анализ структуры сигнала ФМн-2 показывает, что он представляет собой совокупность повторяющихся радиоимпульсов с одинаковой частотой заполнения, но различным значением начальной фазы. Таким образом, искомый радиосигнал ФМн-2 представляет собой результат конкатенации радиоимпульсов, начальная фаза которых определяется информационным значением битовой посылки.

В соответствии с рассмотренным подходом систему синтеза сигнала ФМн-2 можно представить ключевой схемой, представленной на рисунке 2, в которой битовая последовательность регулирует подачу радиоимпульсов в канал. При таком подходе длительность посылок будет определяться скоростью манипуляции ключа.

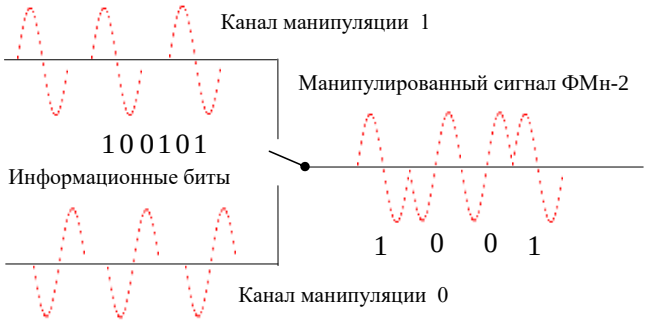


Рис. 2. Синтез сигналов ФМн-2
на основе последовательной коммутации радиоимпульсов

Рассмотрим основные процедуры указанного синтеза. Поскольку при фазовой манипуляции скорость передачи определяется минимальной длительностью элемента сигнала τ_c, в пределах которого его фаза остается постоянной, то для модели, состоящей из совокупности повторяющихся радиоимпульсов, начальные фазы которых соответствуют значениям логических нулей и единиц, предлагается вначале определить их длительности.

Затем на первом этапе формируются непосредственно элементы сигнала $s_1(t)$ и $s_0(t)$, соответствующие логическим единице и нулю (см. рис. 3).

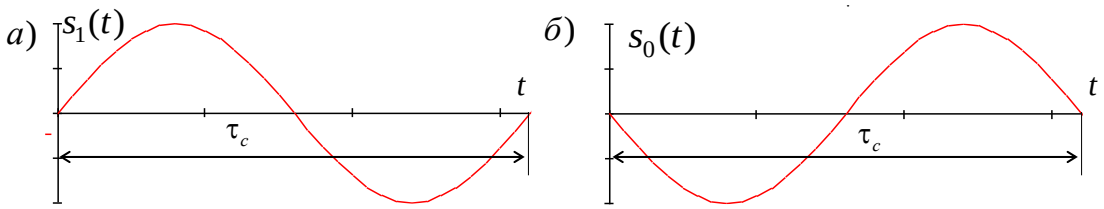


Рис. 3. Элементы сигнала ФМн-2, соответствующие:
а – логической единице; *б* – логическому нулю

На втором этапе, согласно информационной последовательности, из сформированных элементов сигнала $s_1(t)$ и $s_0(t)$ синтезируется требуемая модуляционная конструкция (результирующий ФМн сигнал).

Элементы сигнала, представленные на рисунке 3, подобраны таким образом, что на длительности посылки укладывается строго один период колебания. Отметим, что результирующий сигнал, сформированный указанным выше образом, по своим свойствам ничем не будет отличаться от сигнала, синтез которого сводится к инверсии фазы высокочастотного колебания.

Рассмотренный подход открывает возможности по синтезу ФМн-2 сигналов на основе импульсных фрагментов произвольного наполнения, в частности, вейвлетов. Действительно, если в качестве элементов сигнала $s_1(t)$ и $s_0(t)$ определить соответствующие структуры вейвлетов, то в результате получится вейвлет-фазоманипулированное (ВФМ) колебание.

В качестве формирующего предлагается определить, так называемый вейвлет Гаусса первого порядка $\psi(t)$, представляющий первую производную от функции Гаусса (7) [3]. Аналитически вейвлет Гаусса первого порядка будет описываться следующим выражением:

$$\psi(t) = -t\exp(-t^2/2). \tag{8}$$

Анализ выражения (8) указывает на локализованный характер функции, т. е. синтез непрерывного колебания на его основе в принципе невозможен. Однако вейвлет Гаусса может быть использован в качестве фрагмента для синтеза манипулированного (формирующего) колебания, в соответствии с рассмотренным выше подходом.

Так, на рисунке 4 представлены формирующие сигналы $\psi_1(t)$ и $\psi_0(t)$, синтезированные на основе вейвлета Гаусса.

Отметим, что свойства локализации вейвлета и его двусторонняя временная структура в полной мере отвечает свойствам формирующих колебаний в соответствии с рассмотренным выше подходом.

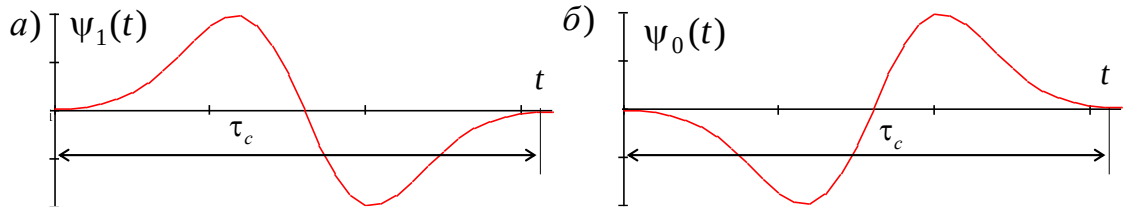


Рис. 4. Формирующие элементы для синтеза вейвлет-фазоманипулироанного сигнала: *а* – логической единицы; *б* – логического нуля

На рисунке 5 показаны фрагменты фазоманипулированных сигналов, сформированных на основе элементов синусоид и на основе вейвлетов.

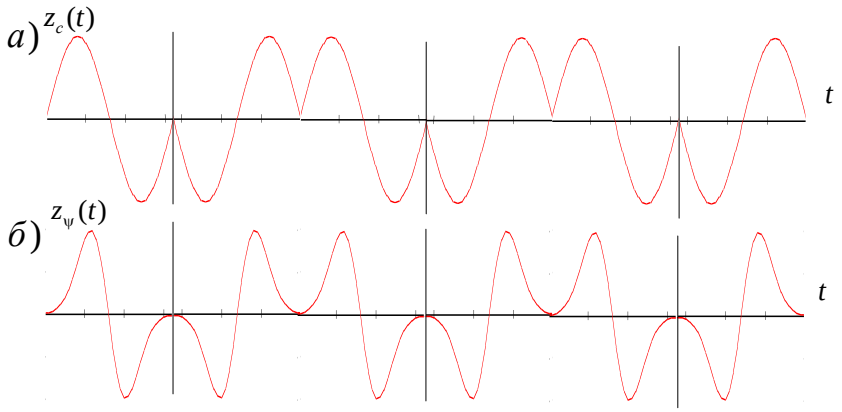


Рис. 5. Сигнал фазовой манипуляции, синтезированный на основе фрагментов: *а* – синусоид; *б* – вейвлетов

Таким образом, подход к синтезу фазоманипулированных сигналов на основе последовательной конкатенации фрагментов радиоимпульсов с соответствующей начальной фазой, позволил разработать ВФМ сигналы, в основе которых лежат вейвлеты прямой и инверсной структуры [5]. В общем случае, ключевая схема, представленная на рисунке 5, может быть расширена до любого числа градаций фаз. В этом случае потребуются пары вейвлетов различных порядков. Например, для синтеза ВФМ-4 сигналов необходимо будет задействовать вейвлеты Гаусса 1-го и 2-го порядка и их инверсные формы.

В радиотехнике, наряду с фазоманипулированными сигналами широко используются и сигналы частотной манипуляции. Прежде всего, это объясняется относительно простотой реализацией процедур их синтеза и обработки, а также не критичностью к системам синхронизации. При этом наибольшее распространение получила двойная частотная манипуляция (ЧМн-2).

Сущность систем передачи с частотной манипуляцией состоит в спектральном различии манипулированных колебаний передающих информационные биты на равных тактовых интервалах [8].

В частности, на рис. 6*а* показана временная диаграмма двух колебаний, формирующих сигнал ЧМн-2. Очевидно, что для сигналов ЧМн-2 помехоустойчивость определяется, в том числе, и частотным разносом между несущими $\Delta F = f_1 - f_0$ (рис. 6*б*).

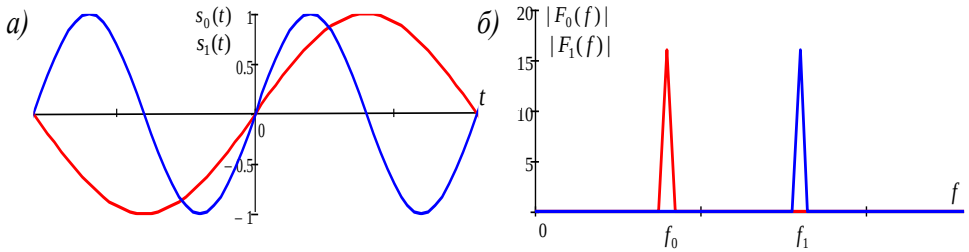


Рис. 6. Компоненты сигнала ЧМ-2 на основе гармонических колебаний:
а – временные; *б* – частотные

Между тем, аналогичные различия в частотных и временных параметрах можно обеспечить и для фрагментов вейвлетов, являющихся производными функции Гаусса (7).

В частности, на рисунке 7*а* показана временная диаграмма двух колебаний, формирующих сигнал ЧМн-2, на основе 1-й и 5-й производных функции Гаусса (7), а на рисунке 7*б* показаны их спектры.

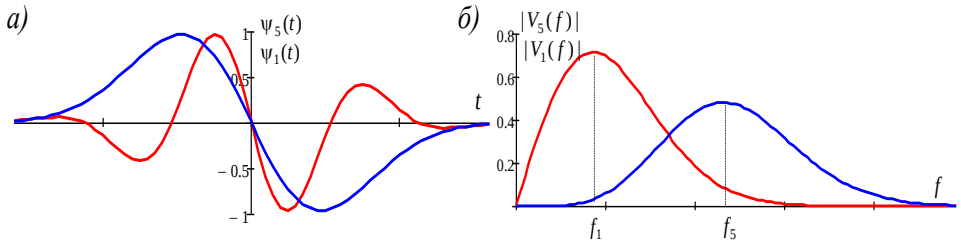


Рис. 7. Компоненты сигнала ЧМн-2 на основе вейвлетов Гаусса 1-го
и 5-го порядков: временные – *а)*; частотные – *б)*

Следует отметить, что по своей природе сигналы ЧМн-2 представляют собой колебания, частота которых изменяется в зависимости от информационных битов. С другой стороны, частотно-манипулированные сигналы можно рассматривать как упорядоченную последовательность импульсов с различной частотой, соединенных между собой путем конкатенации, т. е. по аналогии с рассмотренным синтезом фазоманипулированных сигналов [5].

В этом случае формирование сигналов ЧМн-2 можно реализовать в соответствии со схемой, аналогичной на рисунке 2, только в этом случае в качестве формирующих будут выступать радиоимпульсы с различным частотным наполнением (рис. 8). Действительно, для синтеза вейвлет-сигналов достаточно в схеме на рисунке 8 в каналах манипуляции разме-

стить фрагменты производных от функции Гаусса (см. рис. 2*а*). В результате получается вейвлет-сигнал (см. рис. 9*а*), аналогичный по своим свойствам и информативности сигналу ЧМн-2 (см. рис. 4*б*).

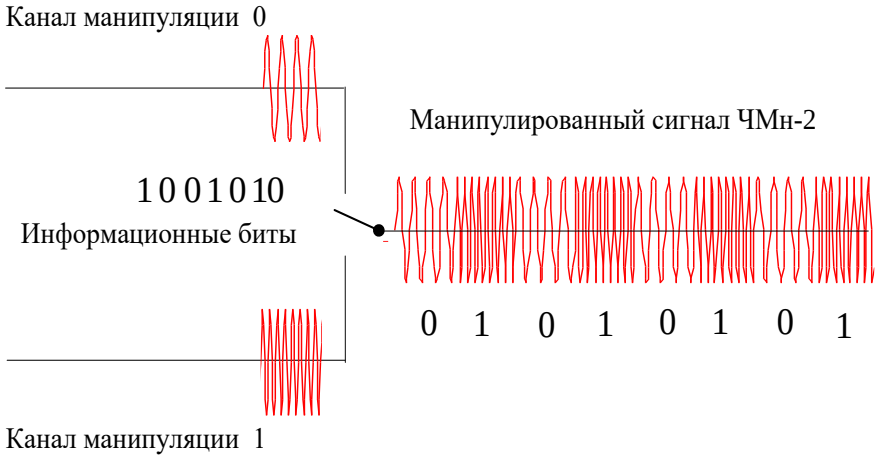


Рис. 8. Принцип формирования сигналов ЧМн-2 коммутацией радиоимпульсов

В общем случае, в качестве исходных формирующих фрагментов для синтеза вейвлет-сигналов ЧМн-2, которые определим как вейвлет частотно-манипулированные (ВЧМ) колебания могут выступать функции, рассчитываемые согласно выражению (7) при различных значениях m.

Необходимо отметить, что такой подход использован в [6], где формируемые подобный образом сигналы рассматривались в качестве альтернативы фазоманипулированным сигналам. Однако для ВФМ сигналов целесообразно использовать инверсные формы исходных вейвлетов.

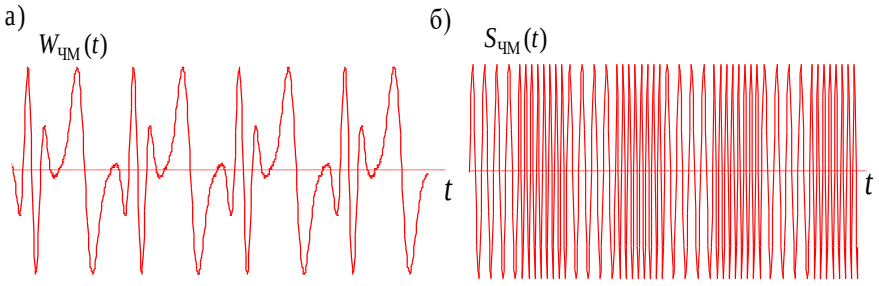


Рис. 9. Временная развертка частотно-манипулированных сигналов на основе: *а* – вейвлетов; *б* – гармонических колебаний

Проведенный анализ спектров вейвлетов Гаусса различных порядков, синтезированных на основе выражения (7) показывает, что увеличение порядка дифференцирования функции Гаусса, т. е. увеличение значения m, ведет к смещению максимума спектральной плотности на частотной оси при сохранении значимой полосы частот, необходимой для отображения вейвлета. Так на рисунке 10 показаны функции огибающих спектров

вейвлетов, полученных на основе формулы (7) при различных значениях m.

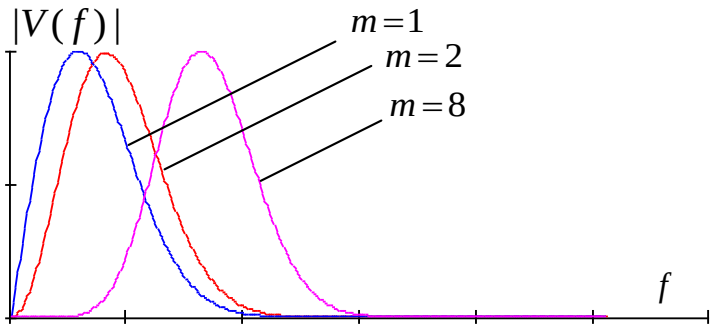


Рис. 10. Функции огибающих спектров вейвлетов при различных значениях m

Полученный результат обусловлен следующим. Неизменность ширины значимой полосы частот объясняется сохранением значимой длительности формируемой функции при различных значениях m [7]. В тоже время, повышение степени дифференцирования ведет к увеличению числа осцилляций в синтезируемом вейвлете, что равносильно увеличению частоты заполнения одиночного импульса. Именно этот факт и выступает в качестве основного аргумента при определении вида манипуляции как частотной для нового класса вейвлет-сигналов.

Таким образом, чем больше разница в значениях m формирующих вейвлетов, тем шире занимаемая полоса частот, и, следовательно, больше база. В качестве примера на рис. 11 показан фрагмент сигнала ВЧМ-2, синтезированного на основе вейвлетов при m = 1 и m = 8.

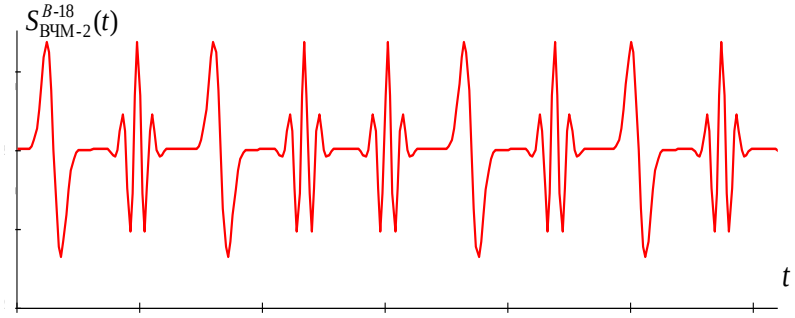


Рис. 11. Временная развертка тестового сигнала ВЧМ-2 на основе вейвлетов1-го и 8-го порядков

В ходе моделирования было установлено, что использование базисов вейвлетов при m = 1 и m = 8 для синтеза тестового сигнала ВЧМ-2 ведет к увеличению базы в 4,9 раза по отношению к гармоническому базису и в 1,4 раза по отношению к вейвлет-базису при m = 2. На рисунке 12 показаны спектры сигнала ЧМн-2 (удвоенное значение частоты между подне-

сущими) и ВЧМ-2 сигналов, сформированного на основе производных функции Гаусса 1-го и 5-го порядков (с увеличением порядка ширина спектра возрастает).

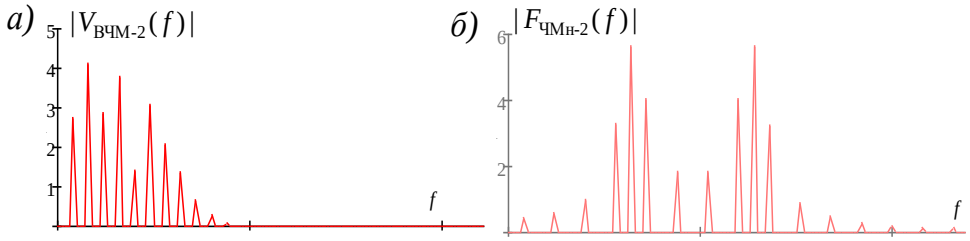


Рис. 12. Спектры сигнала ВЧМ-2 на основе:
а – вейвлетов; *б* – гармонических колебаний

Таким образом, представление синтеза частотно-манипулированных сигналов как последовательной конкатенации фрагментов радиоимпульсов позволил разработать модель формирования вейвлет-частотно-манипулированных сигналов с заданными свойствами.

Оценка эффективности разработанных подходов по показателю структурной скрытности сигналов

Важной особенностью предлагаемых сигналов является их структурная скрытность по отношению к системам мониторинга, обрабатывающих радиоизлучения в базисах экспоненциальных функций.

Прежде всего, это объясняется структурой ВФМ и ВЧМ сигналов, в основе которых лежат вейвлеты Гаусса различных порядков.

Так, на рисунке 13*а* представлены фрагменты формирующих сигналов на основе синусоиды $s_0(t)$ и вейвлета Гаусса 1-го порядка $\psi_1(t)$ равной энергии, а на рисунке 13*б*, соответствующие им модули спектров $|F_0(f)|$ и $|V_1(f)|$.

Анализ представленных результатов позволяет сделать следующий вывод: при равной временной длительности, синусоида имеет более компактный спектр по отношению к гауссиану. В случае наличия шумов канала визуальный анализ не позволит однозначно определить вид формирующего сигнала [8]. Поэтому, при отсутствии априорной информации о базисе формирования сигнала, система мониторинга будет проводить анализ в эффективной полосе приема, включающей не менее 90–95 % спектральной энергии в соответствии со скоростью передачи сообщений, в базисе экспоненциальных функций. В этом случае, в полосе, оптимальной для обработки будет сосредоточено менее 70 % спектральной энергии формирующих сигналов, в основе которых лежат вейвлеты Гаусса 1-го порядка (рис. 14).

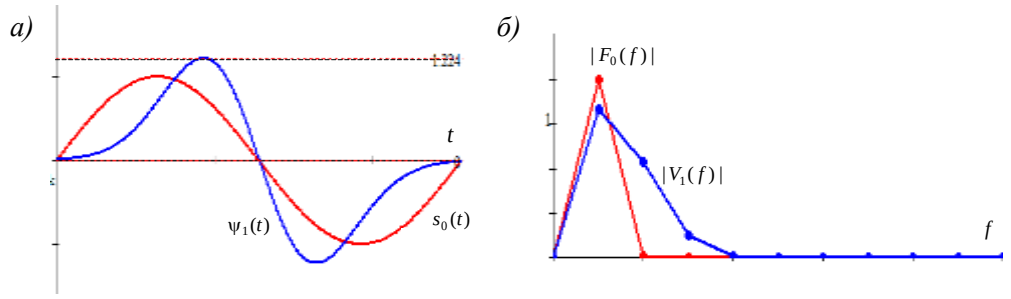


Рис. 13. Формирующие сигналы на основе синусоиды и вейвлета Гаусса:
а – временное представление; *б* – частотное представление

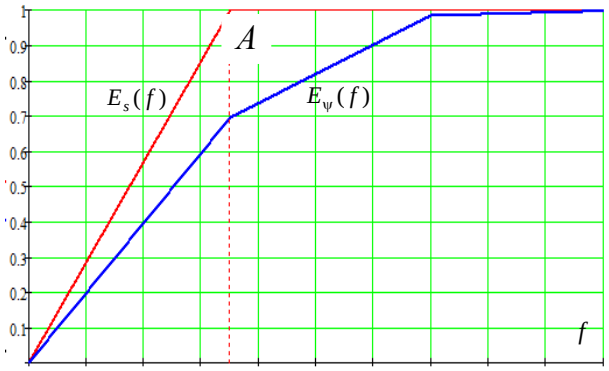


Рис. 14. Распределение энергии формирующих сигналов
на основе синусоиды и вейвлета Гаусса в частотном пространстве

Графики на рисунке 14 строились в соответствии с формулами:

$$E_s(f) = \sum_s F_0^2(f), \tag{9}$$

$$E_\psi(f) = \sum_f V_1^2(f). \tag{10}$$

Между тем, близость временной структуры формирующих сигналов при различных законах распределения энергии, определяет структурную скрытность сигналов, которая, согласно [9], характеризует свойство сигналов, затрудняющее эффективную реализацию процедур их обнаружения и измерения параметров, с целью последующего извлечения вложенной информации. Именно благодаря структурной скрытности, не исключено, что обработка сигналов, сформированных в базисе вейвлетов, будет осуществляться в традиционном базисе функций Фурье [10]. Урон, определяемый структурной скрытностью, можно определить по значению вероятности битовой ошибки, возникающей из-за ошибочного выбора базиса обработки.

Так, значение вероятности ошибки на бит для сигналов двойной фазовой манипуляции может быть рассчитано по формуле:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \tag{11}$$

где E_b – энергия, приходящаяся на бит; N_0 – спектральная плотность мощности шума. В формуле (11) $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty}\exp(-t^2/2)\,\mathrm{d}t$ – функция плотности распределения вероятности.

В тоже время, учитывая, что обработка вейвлет-сигналов в базисе функций Фурье приведет к снижению энергии на 30 % (см. рис. 14), что равносильно преобразования формулы (11) к виду:

$$P_{B\text{ФМн}} = Q\left(\sqrt{\frac{2E_b}{N_0}} \times 0{,}7\right). \tag{12}$$

Аналогичные рассуждения приводят к соответствующему выражению и для сигналов частотной манипуляции

$$P_{B\ \text{ЧМн}} = Q\left(\sqrt{\frac{E_b}{N_0}} \times 0{,}7\right). \tag{13}$$

В результате получим следующие графики оценки структурной скрытности по критерию увеличения вероятности ошибки на бит, представленные на рисунке 15.

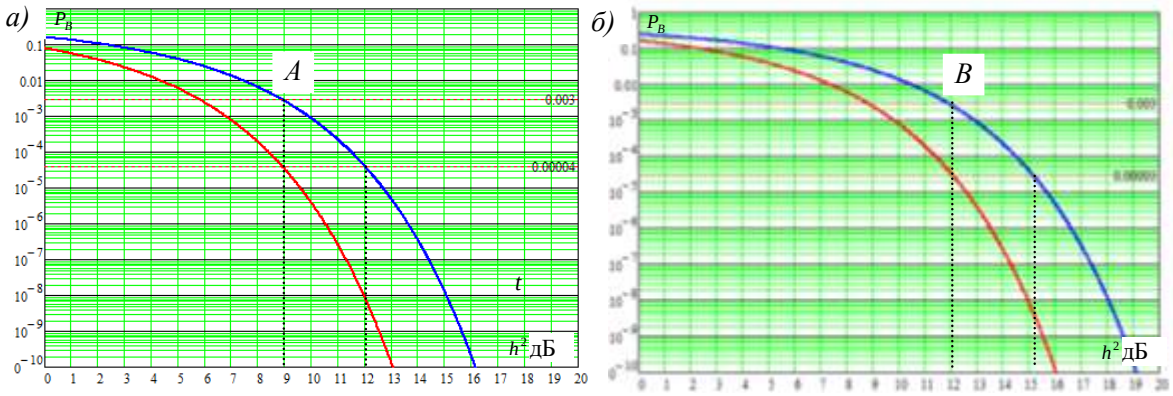


Рис. 15. Оценка эффективности процедур структурной скрытности по показателю вероятности ошибки на бит: *а* – для сигналов ФМн-2; *б* – для сигналов ЧМн-2

Анализ полученных результатов позволяет сделать следующее заключение. При прочих равных условиях, структурная скрытность нового класса сигналов, сформированных на в базисе вейвлетов, обеспечивает увеличение вероятности ошибки более чем на два порядка, что равносильно по-

вышению требований к каналу передачи данных более чем на 3 дБ (соответственно точка *A* на рисунке 15*а* и точка *B* на рисунке 15*б*).

Заключение

Таким образом, полученные результаты позволяют сделать следующее заключение. Синтез сигналов на основе фрагментов вейвлетов позволяет получить модулированные колебания, которые за счет структурной скрытности обеспечат повышение вероятности ошибки в канале более чем на два порядка, что равносильно снижению помехоустойчивости на 3 дБ.

Предполагается, что указанный эффект может быть усилен при увеличении числа различных используемых вейвлетов, применяемых для синтеза сигналов, поскольку в этом случае возрастает сложность обработки таких конструкций, обусловливается отсутствием априорной информации о базисах их формирования.

Дальнейшие исследования видятся в разработке эффективных методов демодуляции вейвлет-сигналов.

Список используемых источников

1. Wavelets (Eds J.M. Combes, A. Grossmann, P. Tchamitchian) (Berlin: Springer-Verlag, 1989).

2. Rioul O., Vetterli M. Wavelets and signal processing // IEEE Trans. Signal Processing. Oct. 1991. Vol. 10. P. 14−38.

3. Астафьева Н. М. Вейвлет-анализ: Основы теории и примеры применения // Успехи физических наук, 1996. Т. 166. № 11. С. 1145–1170.

4. Дворников С. В., Оков И. Н., Устинов А. А., Умбиталиев А. А. Способ сжатия графических файлов методами вейвлет-преобразования // Вопросы радиоэлектроники. Серия: Техника телевидения. 2015. № 3 (21). С. 100−106.

5. Дворников С. В., Дворников С. С., Манаенко С. С., Погорелов А. А. Синтез фазоманипулированных вейвлет-сигналов // Информационные технологии. 2015. № 2. С. 140−143.

6. Дворников С. В., Манаенко С. С. Помехоустойчивость фазоманипулированных сигналов на основе вейвлетов Гаусса // Вестник Воронежского государственного технического университета. 2015. Т. 11. № 3. С. 123−125.

7. Прокис Дж. Цифровая связь / пер. с англ.; под ред. Д. Д. Кловского. М. : Радио и связь. 2000. 800 с.

8. Дворников С. В., Дворников А. С., Желнин С. Р., Оков И. Н., Сауков А. М., Симонов А. Н., Яхеев А. Ф. Способ распознавания радиосигналов. Патент на изобретение RUS 2356064, 24.04.2007.

9. Каневский З. М., Литвиненко В. П. Теория скрытности. Воронеж : ВГУ, 1991. 144 с.

10. Цыцулин А. К., Зубакин И. А. Множественность решений уравнений связи для непрерывной системы // Вопросы радиоэлектроники. Серия: Техника телевидения. 2013. № 2. С. 47−59.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Пшеничниковым А. В.

УДК 654.1

А. А. Долгомер (студент группы ИКТВ-52, СПбГУТ)

ОРГАНИЗАЦИЯ СВЯЗИ ПРИ ВЫПОЛНЕНИИ БОЕВЫХ ЗАДАЧ СОВЕТСКИХ РАЗВЕДЧИКОВ В ТЫЛУ ПРОТИВНИКА В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Великая отечественная война – «кровавый рубец» в истории нашей страны: тысячи жизней были прерваны в ходе истребления фашистской орды, ликвидации нацистского режима. Силами всех родов войск удалость остановить геноцид русского народа и народов, проживавших на территории СССР. Огромную роль в этой освободительной операции сыграла военная связь. Она была разной: связь во время боя, связь между подразделениями… В данной работе особое внимание уделено организации связи во время разведывательной деятельности. Ведь именно разведка поставляла такие необходимые данные для Победы.

военная связь, военная разведка, виды связи.

Лязг оружия, топот конских копыт, свист пуль и зарево от залпового огня… Разве можно представить человечество без войн? Сквозь призму времени все они сливаются в единую киноленту: вот, древние греки воюют с персами, а вот, крестоносцы покоряют новые земли, и «рядом с ними» французы сражаются с русскими при Бородине... Ценой миллионов жизней вершится история, перекраивается мир. Роберт Рождественский писал:

На Земле
безжалостно маленькой
жил да был человек маленький.
У него была служба маленькая.
И маленький очень портфель.
Получал он зарплату маленькую...
И однажды —
прекрасным утром —
постучалась к нему в окошко
небольшая,
казалось,
война...

Сотни лет подряд «стучится» война в мирную жизнь, всякое поколение вынуждено брать в руки оружие и вставать на защиту родного дома и родной земли. Однако невозможно воевать, не зная силы и планы противника. Для этого существует *военная разведка.*

Военная разведка проводится с целью выяснения военно-политического и военно-экономического потенциала вероятного или действующего противника. Она организуется командованием и штабами всех

степеней, ведётся в любой обстановке. По масштабам, предназначению и задачам военная разведка делится на *стратегическую, оперативную и тактическую.*

Стратегическая разведка является высшей формой разведывательной деятельности и ведётся непрерывно с целью установить состав, состояние и дислокацию вооружённых сил противника; выявить его взгляды на характер и способы ведения войны. Примером стратегической разведки может служить деятельность советских спецслужб в период Великой Отечественной войны. Так, ГРУ и ИНО НКВД располагали мощнейшей агентурной сетью, имевшей доступ к высшим эшелонам власти вермахта.

Оперативная разведка во многом схожа со стратегической, однако имеет меньшие масштабы и более конкретную установку. Если *стратегическая* разведка определяет планы и задачи командования на межгосударственном уровне, то *оперативная разведка* ведётся в целях получения разведывательных данных для подготовки и проведения текущих операций. Она состоит из двух компонентов: войскового и агентурного.

Тактическая разведка необходима для организации и успешного ведения боя. Она является исключительно войсковой и имеет гораздо меньшие масштабы, нежели стратегическая или оперативная виды разведки.

Тактическая и оперативная виды разведки являются самыми опасными в разведывательной службе, так как они требуют не только работы под огнем, но и также работы в окопах противника или непосредственно за ними. Эти виды разведки в условиях Великой отечественной войны довольно тесно соприкасались с партизанской разведкой. Она велась на оккупированной фашистами территории и занимала одно из главных мест в успешном отражении натиска врага.

Очевидно, что передача информации, добытой в ходе разведки, очень важна; как и важна связь между разведчиками и штабом. В данной работе я рассмотрю организацию военной связи при выполнении боевых задач советских разведчиков в тылу противника в годы Великой отечественной войны.

Военная связь заключается в передаче и приёме информации в системах управления войсками и оружием; она является основным средством обеспечения управления войсками.

В зависимости от используемых линейных средств и среды распространения сигналов военная связь делится на *проводную, радиосвязь, радиорелейную, тропосферную, спутниковую, волоконно-оптическую, сигнальную и связь подвижными средствами.*

Предназначение, достоинства и недостатки основных видов связи рассмотрены в таблице 1.

ТАБЛИЦА 1. Виды военной связи: достоинства и недостатки.

Вид связи	Предназначение	Достоинства	Недостатки
Радиосвязь	Применяется во всех звеньях управления для передачи команд и распоряжений	● связь с объектами, местоположение которых неизвестно; ● связь через территорию, занятую противником; ● связь через непроходимые и зараженные участки местности; ● передача информации неограниченному числу корреспондентов.	● подверженность радиолиний средствам радиоподавления противника; ● зависимость качества связи от условий прохождения радиоволн.
Радиорелейная связь	Обеспечение высококачественной многоканальной связи	● мало зависит от состояния атмосферы.	● зависимость от рельефа местности; ● малая дальность связи; ● невозможность работы в движении; ● громоздкость; ● высокая вероятность перехвата данных противником.
Проводная связь	Применяется во всех звеньях управления (от взвода (роты) и выше). Осуществляется посредством электрических сигналов по проводам и кабелям связи.	● высокое качество связи; ● простота организации; ● большая скрытность; ● не подвержена воздействию радиопомех противника.	● большая уязвимость от всех видов вооружения противника; ● малая скорость работ по прокладке; ● значительные трудозатраты при эксплуатации.
Связь подвижными средствами	Обеспечение фельдъегерско-почтовой связи; используется для доставки боевых документов, секретный и почтовых отправлений	● абсолютная достоверность связи.	● значительное время, требующееся для доставки документов; ● возможность перехвата информации противником.
Тропосферная связь	Используется для передачи больших объёмов информации на значительные расстояния	● повышенная дальность связи; ● большая пропускная способность; ● не зависит от рельефа местности.	● необходимость преодоления больших затуханий в пространстве; ● необходимость использования антенн с высоким коэффициентом усиления.

Из всех перечисленных видов связи самой качественной является *проводная связь.* Высокая пропускная способность, простота организации и неподверженность воздействию радиопомех противника определяют её востребованность на фронте среди всех звеньев управления. Однако возможно ли её использование в тылу противника? Очевидно, нет. Прокладка проводов перед носом врага, по меньшей мере, обречена на провал и потери среди личного состава, посланного на выполнение работ, а также на обнаружение местонахождения разведывательного отряда. Кроме того, разведывательная деятельность предполагает постоянное перемещение, а проводная связь едва ли может удовлетворить этой потребности – носить за собой катушку с проводами и при этом оставаться незамеченными практически невозможно. Вследствие всего вышеперечисленного использование проводной связи разведчиками в тылу врага не представляется возможным.

Тропосферная связь могла бы стать отличной альтернативой проводной, но учитывая специфику статьи, а именно, организация связи советских разведчиков в тылу врага в годы Великой Отечественной войны и то, что тропосферная связь появилась в конце 50-х гг., этот вариант также отпадает.

Радиорелейная связь осуществляется между стационарными объектами, а это, как уже было замечено, не подходит для разведывательной деятельности.

Остаётся *радиосвязь.* В силу несравнимо большей мобильности и доступности по сравнению с проводной и тропосферной видами связи, а также благодаря возможности передачи информации через территории, занятые противником, она является основным средством связи в разведке. Преимущественно радиосвязь использовалась разведчиками, в частности, партизанами в период Великой Отечественной войны. В книге А. Н. Асмолова «Фронт в тылу вермахта» читаем:

«Вооружённые партизанские силы Ленинградской области в начальный период войны были более многочисленны и лучше оснащены, чем отряды многих других областей. Они раньше других стали получать и необходимую партизанскую технику для диверсий. Некоторые отряды, формировавшиеся в Ленинграде, получали даже радиостанции – редкое явление в начале войны…»

Таким образом, радиостанции были очень необходимы для связи разведчиков в тылу врага, но в начальный период войны их катастрофически не хватало.

Примеры радиостанций, использовавшихся в период Великой отечественной войны:

1) А-7: советская переносная ультракоротковолновая радиостанция военного назначения. Производство началось в конце 1942 – начале 1943 г.

Радиостанция предназначалась, прежде всего, для связи в радиосетях стрелковых полков и артиллерийских дивизионов.

2) «Север»: советская переносная коротковолновая радиостанция. Была разработана в 1939–1940 гг. и усовершенствована в 1942 г. Радиостанция до конца войны использовалась в войсках, разведывательных группах, партизанских отрядах.

Также разведывательными группами использовались трофейные радиостанции, то есть радиостанции, добытые непосредственно в бою. Они предназначались в основном для создания радиопомех противнику в ходе радио-электронной борьбы (РЭБ).

Необходимость связи в разведывательных группах очевидна. Связь в данном случае – это не только передача руководству ценной информации о планах и расстановке сил противника, но и возможность управлять разведывательными группами, возможность организовать их структуру изнутри.

Рассмотрим подробнее деятельность советских разведчиков в годы Великой отечественной войны.

Стратегическая разведка

В предвоенный период советская стратегическая разведка расширяла агентурную сеть на территории Германии и оккупированных ею государств. Её деятельность носила в основном информационный характер, а аналитическая работа фактически не велась. И всё же высшее политическое руководство страны своевременно получало предупреждения о готовящемся нападении Германии на СССР.

Советский разведчик Рихард Зорге с 1936 г. работал в Японии – возглавлял организацию антифашистов-интернационалистов. По поручению немецкого командования он добывал секретную информацию, связанную с политикой Японии в отношении Германии и США. Именно Рихард Зорге, один из первых, сообщил в Москву данные о составе нацистских сил вторжения, дате нападения на СССР, общую схему военного плана вермахта. Главной целью Рихарда Зорге было предотвращение войны между СССР и Японией.

К июню 1941 г. советская стратегическая разведка не имела централизованного контроля над всеми агентурными сетями. После начала боевых действий добытые сведения стали доставляться в Центр не с курьерами и дипломатической почтой, а с помощью подпольных радиопередач.

В 1941–1943 гг. гестапо и Абверу удалось разгромить многие наши резидентуры в Германии и на оккупированных ею странах, а также в Швейцарии. Серьёзно пострадали резидентуры в Смоленске, Киеве, Одессе, Херсоне, Николаеве и других крупных городах, находившихся в зоне немецкой оккупации.

После провалов в 1941–1943 гг. были значительно усилены антифашистская и интернациональная базы. Совершенствовались методы работы разведорганов, улучшались координация и взаимодействие между разными видами разведки.

В 1943 г. в военной контрразведке был создан самостоятельный отдел, который занимался заброской в тыл противника агентурных и диверсионных групп.

Агентурная разведка внесла большой вклад в развитие боевых действий на фронтах; предоставляемая агентами информация имела решающее значение на передовых.

Оперативная и тактическая виды разведки. Партизанская борьба

В ходе оперативной разведки большое значение приобретала информация, поступавшая от партизанских соединений.

Однако партизанская разведка стала эффективной далеко не сразу. В 1941–1942 гг. практически все партизанские отряды вели разведку в своих интересах, и лишь сравнительно небольшое количество партизанских отрядов и групп вело разведку для армии. Этот период помимо развития и роста партизанского движения характерен ошибками в организации.

Постепенно связь с партизанами налаживалась. В книге «Фронт в тылу вермахта» А. Н. Асмолова читаем:

«Налаженная через линию фронта связь позволяла командованию, а также партийным органам не только управлять партизанскими силами, но и активно вести политическую борьбу среди партизан и населения, оказавшегося на оккупированной территории, быть в курсе событий и дел, происходивших в тылу немецко-фашистской армии».

Ближе к середине войны Верховное Главнокомандование Красной Армии и штабы фронтов получали от советских партизан систематическую информацию стратегического значения.

Центральный штаб партизанского движения, добывавший из тыла посредством более 400 радиостанций огромную разведывательную информацию, выпускал ежедневно на её основе сводку большого объема и отправлял в Ставку Верховного Главнокомандования, Генштаб, штабы фронтов и в Разведывательное управление.

Партизанская разведка охватывала все виды деятельности вражеской армии, все военные, политические и экономические мероприятия оккупационных германских властей. Она часто раскрывала замыслы противника в самом зародыше и оказывала тем самым неоценимую услугу Родине.

А советская разведка в целом в годы войны прошла трудный, но славный путь, и сохранила многие тысячи жизней наших солдат. Комплексное использование всех видов и средств разведки сыграло важную роль в обеспечении победоносного исхода последних операций войны.

Организация связи в разведывательной деятельности происходит в зависимости от конкретного вида разведки.

Связь с агентурными источниками в тылу противника

Агентурная связь может быть личной и безличной.

Личная связь осуществляется путем личного общения разведчиков агентурной разведки с командиром разведывательной группы с целью решения задач разведки. Она осуществляется с соблюдением мер конспирации по заранее разработанным условиям.

Достоинства личной связи:

- личное воздействие;
- получение подробного разъяснения разведывательной задачи, а также способов её выполнения;
- выявление и уточнение положения разведчика;
- изучение и проверка завербованных агентов.

Недостатки личной связи:

- уязвимость, повышенные требования к соблюдению мер конспирации, безопасности и организации проведения;
- невысокая оперативность.

Основными формами личной агентурной связи являются:

1) очередная встреча,
2) экстренная встреча,
3) контрольная встреча,
4) "случайная" встреча,
5) встреча по условиям явки.

Безличная связь осуществляется без непосредственного личного общения и контактов между сотрудниками разведки.

Достоинства безличной связи:

- конспиративность и безопасность работы, т. к. она позволяет поддерживать связь без личных контактов;
- возможность осуществления связь между различными категориями сотрудников разведки, независимо от их общественного положения, личных особенностей и даже знания языка противника.

Формами безличной связи являются:

1) связь через тайники;
2) радиосвязь;
3) связь с использованием почты, телеграфа, телефона, интернета и прессы;
4) связь с использованием сигнализации.

Основные трудности проведения связи с агентурными источниками в период Великой Отечественной войны заключались в следующем. Аппаратура была громоздкой, часто ломалась. Радиус её действия не превышал

1 000 км, следовательно, связь поддерживалась с городами западного СССР, такими как: Киев, Минск, Львов, Житомир, Брест. С большинством из них связь была прервана в первый месяц войны. К сентябрю 1941-го г. передать какую-либо информацию в центр стало невозможно.

Также одной из главных проблем была немецкая контрразведка, которая особенно активизировалась после начала войны. Они использовали радиопеленгацию – определение направления на источник радиоизлучения. В городе, где предположительно находилась резидентура, появлялись несколько грузовиков с радиопеленгационным оборудованием, патрулируя улицы, они могли с точностью до дома определить местонахождение радиоаппаратуры. В результате влияния всех этих факторов, внешней разведке пришлось практически заново восстанавливать свою работу в оккупированных странах.

Связь с партизанскими отрядами в тылу противника

В начале войны связь в партизанском отряде была одним из самых уязвимых мест. А. Н. Асмолов в книге «Фронт в тылу вермахта» так описывает сложившуюся ситуацию:

«Связь с отрядом у нас до сих пор является самым слабым местом. Связь у нас только живая. Радиосредств нет. В условиях большой отдалённости отрядов в тылу противника (до 300 км) живая связь ни в коей степени не обеспечивает руководства отрядами. Отсутствие радиосредств для связи с отрядами самым серьёзным образом срывает руководство партизанским движением. Наличие радиосвязи с отрядами своевременно обеспечивало бы также командование фронта ценными разведывательными данными о противнике в его тылу».

В течение 1942 г. многим партизанским отрядам были сброшены на парашютах полевые радиостанции, а также обученные радисты. Некоторые партизанские отряды радиооборудование получали от партийных комитетов.

Разведывательные данные, собираемые разведчиками, в отряды поступали обычно через связных. Но эта система, как мы видим, была пригодна только для сбора местной разведывательной информации. Для получения же указаний из руководящих центров небольшие группы время от времени проходили пешком значительные расстояния. В Крыму различные партизанские отряды первоначально поддерживали связь друг с другом по телефону.

В основном же пользовались радио, которое было для партизан практически единственным средством связи с органами за линией фронта.

Кроме радиостанций, партизаны часто пользовались также портативными радиопередатчиками. Партизаны, которых перебрасывали на оккупированную немцами территорию для выполнения специальных заданий, всегда имели такие передатчики. Иногда партизан сбрасывали на пара-

шютах с самолетов, некоторые переправлялись в лодках или просто переходили линию фронта пешком. В каждой такой партии было не менее одного опытного радиста, который обычно поддерживал связь непосредственно с тем органом, который их послал; если же это не удавалось, он старался наладить связь с ближайшим партизанским отрядом.

Если бы партизаны не имели радиосвязи, их действия, вне всякого сомнения, были бы менее эффективными.

Подводя итоги всему вышесказанному, хочется заметить, что только комплексное использование разных видов разведки и средств связи обеспечивало наиболее полное представление советского командования о силах и планах противника. Именно взаимодействие разных видов разведки и средств связи, а также своевременная передача ценной и достоверной информации способствовали победе русского народа в Великой отечественной войне.

Список используемых источников

1. Военный энциклопедический словарь / Пред. гл. ред. в 63 комиссии Н. В. Огарков. – М. : Воениздат, 1984. 863 с.

2. Асмолов А. Н. Фронт в тылу вермахта. 2-е изд., доп. М. : Политиздат, 1983. 302 с.

3. Коваленя А., Краснова М., Лемешонок В., Новиков С. Великая Отечественная война советского народа (в контексте Второй мировой войны). М. : Белорусская наука, 2008. 350 с.

Статья предоставлена научным руководителем,
старшим преподавателем Груздевым Д. А.

УДК 623.746

В. В. Звонарев (начальник лаборатории, ВКА им. А. Ф. Можайского)
И. Ю. Парамонов (докторант, ВКА им. А. Ф. Можайского)
И. С. Петрова (научный сотрудник, ВКА им. А. Ф. Можайского)
А. С. Попов (старший научный сотрудник, ВКА им. А. Ф. Можайского)

АЛГОРИТМ УПРАВЛЕНИЯ РЕЖИМАМИ РАБОТЫ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА В СИСТЕМЕ ПЕРЕДАЧИ ИНФОРМАЦИИ

В статье представлен алгоритм автоматического управления режимами передачи информации при заданном значении вероятности безобрывной связи. Использование предлагаемого алгоритма позволяет формировать режимы управления с учетом динамических характеристик процесса замираний.

замирания сигнала, канал управления, вероятность правильного приёма сообщения, интервал корреляции.

В радиоканалах с низко расположенными антеннами, кроме прямых трасс распространения радиоволн в пределах прямой видимости между беспилотным летательным аппаратом (БЛА) и наземным пунктом управления (НПУ), возникает многолучевое распространение, обусловленное как отражением от окружающих объектов, так и постановкой специального вида помех противником. Многолучевое распространение радиоволн наиболее характерно для городских условий, где стены зданий и дорожное покрытие обладают высокой отражательной способностью. В результате принимаемый сигнал состоит из нескольких компонентов с разными амплитудами, фазами и направлениями прихода.

Таким образом, одним из следствий распространения радиоволн в условиях многолучёвости и неоднородности в атмосфере является появление замираний сигнала (изменение уровня сигнала).

Замирания сигнала в радиоканале передачи информации от БЛА к НПУ приводят к существенному ухудшению характеристик канала и, соответственно, качества связи. Количественно качество связи может характеризоваться вероятностью правильного приёма сообщения или пакета – $P_{бо}$. Приближённой, но технически осуществимой, оценкой вероятности правильного приёма сообщения является отношение числа правильно принятых сообщений (пакетов) к общему числу переданных сообщений, что возможно определить в тестовом режиме передачи сообщений известной структуры. Оценка оказывается тем точнее, чем больше временной интервал тестирования цифрового радиоканала.

Первым недостатком последнего варианта оценки является отсутствие передачи полезной информации по радиоканалу во время его тестирования. Вторым недостатком является невозможность определить причину снижения качества связи, кроме общего понимания того, что, скорее всего, качество связи в цифровом канале ухудшилось вследствие возникновения замираний на физическом уровне радиоканала. И, не в последнюю очередь, не зная параметров случайного процесса замираний, например, интервала корреляции – τ_0, нельзя спрогнозировать, как количественно изменится качество канала при изменении режимов работы радиолинии. Эту задачу в таком случае можно решить лишь экспериментально, опытным путём, пошагово изменяя режимы передачи, например, длительность сообщения, избыточность кода и т. д.

Режимы передачи информации могут быть установлены следующими мерами:

- изменение мощности передаваемого сообщения;
- изменением (увеличением) избыточности помехоустойчивого кода;
- уменьшением скорости информационного потока сообщений;

- изменением длительности сообщения;
- изменением вида и параметров модуляции несущего колебания цифрового сообщения;
- изменением частоты несущего колебания и коэффициентов усиления передающей и приёмной антенн и т. д.

Структурная схема автоматического управления режимами передачи информации по первому варианту, т. е. с использованием методик расчёта, разработанных в [2, 3], представлена на рисунке 1.

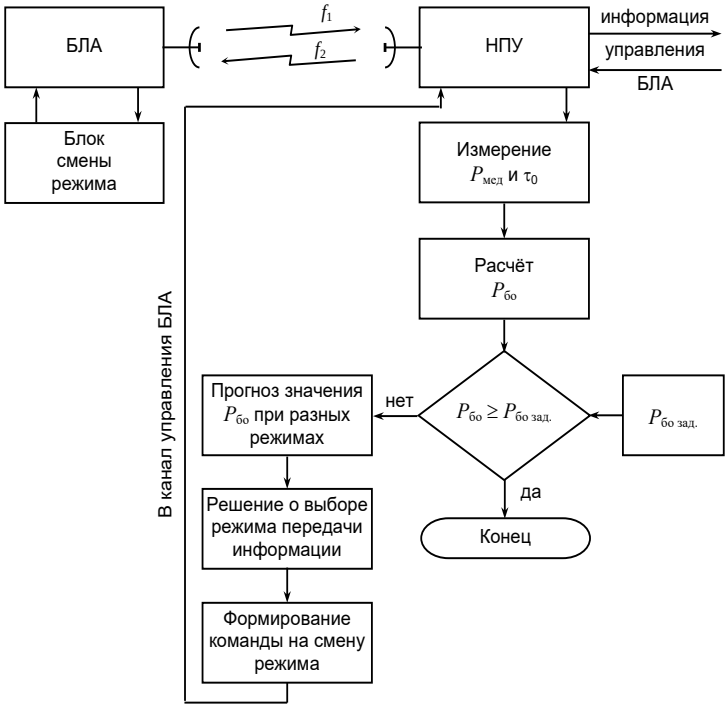


Рис. 1. Структурная схема автоматического управления режимами передачи информации при заданном значении вероятности безобрывной связи $P_{бо}$

Последовательность работы схемы следующая. Информационные сообщения определённой длительности передаются по каналу f_1 от БЛА к НПУ. Вероятностная модель замираний в виде многомерной плотности вероятности задана с точностью до характеристик модели, например, дисперсии флуктуации и интервала корреляции – τ_0. В блоке измерения медианного значения мощности приёмника НПУ – $P_{мед}$ и интервала корреляции проводятся накопление статистики и оценка этих характеристик для использования при расчёте значения показателя качества связи – вероятности правильного приёма сообщения – $P_{бо}$. В блоке сравнения измеренное значение $P_{бо}$ сравнивается с его заданным (требуемым) по техническим характеристикам – $P_{бо\ зад}$. При $P_{бо} \geq P_{бо\ зад}$ никаких действий не производится. В случае $P_{бо} < P_{бо\ зад}$ в блоке прогнозирования осуществляется расчёт прогноза значений $P_{бо}$ при различных режимах передачи, таких, например, как

уменьшение длительности сообщения, изменение скорости передачи за счёт увеличения длительности элементарной посылки, или увеличения избыточности кода, а также напрямую изменение мощности передачи сообщения на минимально возможное значение приращения. В следующем блоке принимается решение о выборе конкретного режима передачи информации. Например, уменьшить длительность сообщения в 1,5 раза, увеличить избыточность помехоустойчивого кода с эффектом увеличения эквивалентной мощности на 4 дБ, увеличить мощность передачи сообщения на 2 дБ и т. д. В следующем блоке формируется структура команды на изменение режима, соответствующее выбранному. Команда кодируется на выделенных позициях служебной информации сообщения (пакета) управления БЛА с НПУ и передаётся от НПУ к БЛА по радиоканалу f_2. Принимаемая команда расшифровывается в блоке смены режима и осуществляет изменение режима передачи в БЛА.

При недостижении условия $P_{бо} \geq P_{бо\ зад}$ процедура повторяется до положительного эффекта. Затем весь цикл повторяется через заданный техническим заданием интервал времени.

Таким образом, достигается сохранение (поддержание) требуемого качества передачи информации в радиоканале с БЛА.

Структурная схема автоматического управления режимами передачи информации с использованием счётчика принятых сообщений, представлена на рисунке 2.

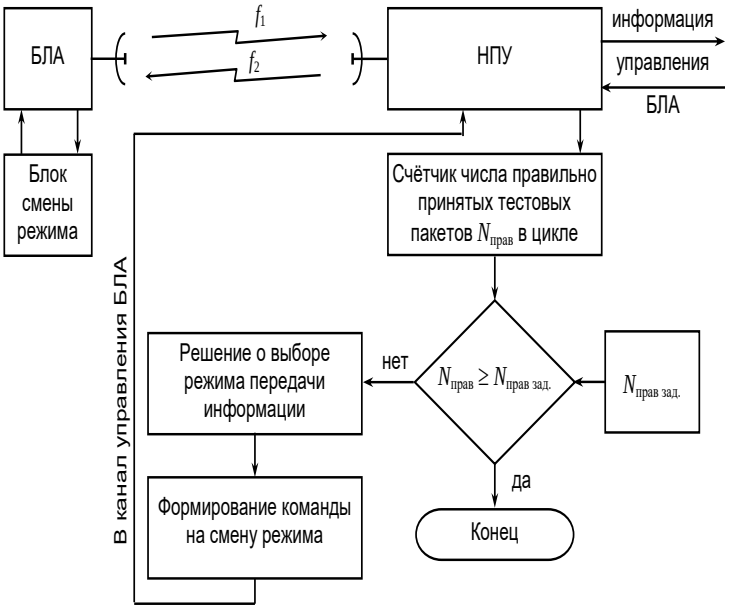


Рис. 2. Структурная схема автоматического управления режимами передачи информации с использованием счётчика принятых сообщений

В данном случае течение заданного времени передаются тестовые сообщения полностью известной структуры. На стороне НПУ тестовые сообщения после демодуляции с декодирования сравниваются с их копиями

и осуществляется подсчёт числа правильно принятых тестовых пакетов в цикле с полным числом переданных пакетов. В блоке сравнения число правильно принятых пакетов – $N_{прав}$ сравнивается с заданным (требуемым) числом правильно принятых пакетов – $N_{прав.\ зад}$ в цикле. Если $N_{прав} \geq N_{прав\ зад.}$, то никаких действий по смене режима передачи не осуществляется. И новый подсчёт $N_{прав}$ проводится через заданный техническими условиями интервалы времени. Если же фиксируется отношение $N_{прав} < N_{прав\ зад.}$, то в следующем блоке принимается решение о необходимости смены режима передачи. И в последующем блоке осуществляется выбор режима передачи сигналов управления на смену режима. Для достижения требуемого качества канала в данном случае может осуществляться только выбор некоторых фиксированных режимов с небольшим числом вариантов и без прогнозирования, поскольку на уровне цифрового канала причины ухудшения качества канала неизвестны и прогнозирование невозможно. Кроме того, повторное тестирование канала может привести к существенной потере пропускной способности канала, именно вследствие применения режима тестирования.

Таким образом, использование предлагаемого показателя качества – вероятности правильного приёма сообщения заданной (конечной) длительности в канале передачи информации БЛА – НПУ и предлагаемого режима передачи позволяет без искусственной потери пропускной способности канала обеспечить с высокой точностью поддержание требуемого качества канала в текущем (реальном) времени.

Применение в тестовом режиме известной процедуры подсчёта числа правильно принятых сообщений (пакетов) в цифровом канале (после демодуляции и декодирования) не обеспечивает достаточно эффективного поддержания качества канала передачи информации между БЛА и НПУ, что может привести к невыполнению БЛА задач функционального назначения, потере управления и потере самого БЛА.

При расчётах вероятностей группирования ошибок в сообщении на основе искусственных моделей канала Гильберта, Гильберта – Эллиота, Фричмана и др. можно определить вероятность правильного приёма сообщений при назначенных (теоретически) статистических характеристиках группирования ошибок. По предлагаемой в работе методике может быть рассчитана вероятность правильного приёма сообщения в физическом радиоканале при известных статистических характеристиках процесса замираний сигнала.

Сопоставление этих результатов позволяет выявить зависимость статистических характеристик в моделях Гильберта и др. от статистических характеристик процесса замираний сигнала в физическом канале, характеристики которых определяются в моделях группирования ошибок из принятой в данной работе многомерной вероятностной модели случайного процесса замираний сигнала с использованием предлагаемых методик.

Список используемых источников

1. Печаткин А. В. Системы мобильной связи. Часть 1. Принципы организации, функционирования и частотного планирования систем мобильной связи: учеб. пособие. Рыбинск : РГАТА, 2008. 122 с.
2. Звонарёв В. В., Попов А. С., Пряхин В. А. Методика расчёта коэффициента запаса по мощности для обеспечения заданной вероятности непрерывания передачи информации в канале с замираниями сигнала // Вестник ВКО. 2015. С 47–51.
3. Звонарев В. В., Попов А. С., Филиппов А. А., Залозний Д. А. Вероятность безобрывной связи как вероятность передачи сообщения в канале с замираниями // Вестник войсковой ПВО: тематический сборник, Смоленск, 22–23 мая 2014 г. С. : ВА ВПВО ВС РФ, 2014. С. 55–60.

УДК 62.03

Г. Н. Иванов (студент группы ИКТ-405, СПбГУТ)

РАЗВИТИЕ БЕСПРОВОДНОЙ СВЯЗИ

В статье рассматривается история развития беспроводной связи (радиосвязи) в России, представлено изобретение российского ученого А. С. Попова, повлиявшее на ход истории в области радиосвязи.

беспроводная связь, радиосвязь, изобретение радио.

Изобретение радио является одним из величайших достижений человеческой культуры конца XIX столетия. Появление этой новой отрасли техники не было случайностью – она подготавливалась предшествующим развитием науки и отвечала требованиям эпохи. Как правило, первые шаги во вновь зарождающихся областях техники неизбежно бывают связаны с предыдущими научными и техническими достижениями. Однако, в каждой новой технической области всегда можно найти определенную физическую основу. Такой физической основой для возможности появления радиотехники послужило электромагнитное поле [1].

Учение об этом поле, до того, как оно нашло себе техническое применение, разрабатывалось многими выдающимися учеными на протяжении почто полстолетия. В 1867 г. английский физик Джеймс Клерк Максвелл, на основании открытия Майклом Фарадеем и исходя из предположения о неразрывности тока, теоретически доказал, что в диэлектрике может существовать особый вид тока, связанный с перемещением силовых линий электрического поля. Этот ток Максвелл назвал током смещения, который подобно току проводимости, порождает вокруг себя электромагнитное поле. Также он доказал, что электромагнитные волны распространяются

в пространстве со скоростью света и хорошо проходят через вещество, непроводящее ток. Теория Максвелла было очень большим шагом в науке, и носила новаторский характер [2, с. 13].

Спустя девять лет после смерти Максвелла существование электромагнитных волн экспериментально доказал молодой немецкий физик – Генрих Герц. В 1888 г. Герц доложил Берлинской академии наук результаты своей работы «О лучах электрической силы», в ходе которой было произведено множество экспериментов, позволяющие получить опытным путем электромагнитные волны и исследовать их свойства. Одним из первых изобретений Герца в области электромагнитных волн было изобретение вибратора, которое позже получило название «Вибратор Герца». С помощью него Герцу удалось получить электромагнитные волны и исследовать их свойства в разных состояниях. Начало было положено. Дальнейшим исследованием электромагнитных волн занимались такие ученые как Н. Теслу, О. Лоджа, М. Минчин, Э. Резефорд, Д. Бозе, П. Н. Лебедев, И. Томсон, О. Д. Хвольсон [3].

Наши ученые не оставались в стороне от исследований. А. С. Попов, как сотрудник военно-морского технического учебного заведения понимал необходимость беспроводной связи между суднами, а также связь кораблей с землёй. Он изучал и плотно занимался поисками технических решений для создания беспроводной связи.

В начале 1895 г. Попов сконструировал переносной прибор, для обнаружения и регистрирования электрических колебаний. Это прибор был первым техническим средством индикации электромагнитных волн, практически пригодным для целей связи. Продолжая работу со своим учеником Рыбкиным для увеличения чувствительности обнаружения электромагнитных волн была присоединена антенна, состоявшая из простого куска проволоки. Усовершенствовав модель, уже 25 апреля 1895 г. подробно рассказал о результатах своей работы и своих экспериментов на заседании Русского физико-химического общества, а также продемонстрировал работу радиоприемника для обнаружения и регистрирования электромагнитных волн. Впервые радиоприемник применили в области метеорологии. А. С. Попов переделав его для регистрации гроз, показал на Всероссийской промышленной выставке и был награжден дипломом II степени, в дальнейшем передал устройство метеорологической службе. Устройство получило название «грозоотметчик» [4].

7 мая 1895 г. А. С. Попов представил доклад «Об отношении металлических порошков к электрическим колебаниям».

Параллельно изучением электромагнитных волн занимался молодой итальянский ученый Гульельмо Маркони. О его работах стало известно только в 1896 г. И уже в сентябре этого же года в газетах стало сообщаться о беспроводной передачи сигналов на расстояние 7 км, осуществимым Маркони. 2 марта 1897 г. Маркони получает патент на «усовершенствова-

ние в передаче электрических импульсов и сигналов на расстояние». И наконец, к середине весны 1897 г. Маркони удаётся передать сигнал без провода на расстояние 16 км.

В 1898 г. Морское Министерство организовало производство своих приборов в мастерских лейтенанта Колбасьева и у парижского механика Дюкрете, который в дальнейшем стал главным поставщиком его приборов.

В ноябре 1899 г. у острова Гогланд сел на мель броненосец «Генерал-адмирал Апраксин», и по поручению Морского Министерства А. С. Попов организовал первую в мире практическую радиосвязь. Между г. Котка и броненосцем на расстоянии около 50 км в течение трех месяцев было передано свыше 400 радиограмм.

После успешной работы радиолинии Гогланд-Котка Морское Министерство первым в мире приняло решение о вооружении всех судов русского Военно-Морского Флота радиотелеграфом как средством постоянного вооружения.

Днем принятия решения о введение в эксплуатацию радиосредств в Вооруженные Силы Российского Флота считается 8 марта 1900 г. В связи с прекрасными результатами использования радиосвязи, начинается активное исследование этих средств. Появляется первая радиомастерская – Кронштадская. Дата точного ее создания до сих пор никому неизвестна. По одной из версий она была создана 2 сентября 1900 г., по второй 20 июля этого ж года и по третьей версии 24 июля 1900 г. Все эти даты верны и предполагают основание радиомастерской. Но ведь самое главное это труды мастерской. В радиомастерской собирали радиооборудование для Военно-Морского Флота. Здесь осуществлялось разработка, проектирование, тестирование, обслуживание и ремонт радиосредств. Основными деятелями стоит отметить А. С. Попова и Е. Л. Коринфского. В июне 1910 г. радиомастерская была переведена в Санкт-Петербург. За время существования радиомастерской 1900–1910 г. было создано, а также установлено более 65 радиостанций, ремонт техники и обслуживание было четко налажено. Реализация и использование беспроводной связи были достигнуты.

В борьбе за власть Советов с первых часов Великой Октябрьской социалистической революции связь играла важнейшую роль. Великий вождь мирового пролетариата В. И. Ленин придавал огромное значение связи. Незадолго до начала вооруженного восстания он говорил: «мы должны… занять сразу телеграф и телефон, поместить наш штаб восстания у центральной телефонной станции, связать с ним по телефоны все заводы, все полки, все пункты вооруженной борьбы и т. д. …» И уже к 30 октября 1917 г. была передана радиограмма, подписанная В. И. Ленином, а 9 ноября этого же года передана им же сообщение: «Радио всем…» [5]. В 1921 г. под руководством А. И. Коваленкова была создана первая советская передающая радиотелефонная станция АК-23. Активно начали производить ар-

тиллерийские радиостанции (Гора-1, Гора-2, Гора-3). К концу 20-х годов были разработаны и поступили на вооружение 17 кавалерийских и авиационных радиостанций, такие как 1ВФ, 2Д и др. Но самый активный ход работы начался в конце 30-х годов. Были созданы радиостанции для танков (71-ТК, 71-ТК1, 71-ТК2, 71-ТК3, 72-ТК и др.) и даже для самолетов (5-СУ, 11-СК,14-СК и др.) [6].

Огромную роль в продвижении и росте радиосвязи сыграла Великая Отечественная Война. Очень известная радиостанция РСИ-4, которая устанавливалась и на истребителях, и на штурмовиках типа И-16, ЯК-1, ЯК-7 и множество других известных самолетах. Появились множество модернизированных переносимых радиостанций (РРС). После войны работа над радиосвязью не прекращалась. Были созданы носимые радиостанции, работающие на УКВ для ротных радиосетей, для спец-войск и других подразделений [2, с. 173].

В настоящее время радиосвязь используется не только в военной промышленности, но и в гражданской. Радио стало не только средством общения и связи между объектами, но и средством массовой информации, стала носить также и развлекательный характер и научный. Несомненно, основной задачей для инженеров остается мощность защиты радиосети или определенной частоты, а также помехоустойчивость и качество.

Список используемых источников

1. Борисов В. Г., Юный Радиолюбитель. 3-е изд. М.-Л. : Ленэнерго, 1959.
2. Родионов В. М. Зарождение радиотехники. М. : Наука, 1985. С. 13, С. 173.
3. Статья для Берлинской энциклопедии «Электричество в элементарном разложении», 1890.
4. Рогозинский П. А. Сообщение об изобретении А. С. Поповым особого переносного прибора, о его докладе в Физическом отделении РФХО // Кронштадский вестник. 1895. 30 апреля (12 мая) (№ 51).
5. Ленин В. И. Полн. собр. соч.: в 55 т. Т. 34. М. : Издательство политической литературы, 247 с.
6. Лодж О. и Говард Д. О первых радиограммах // Из предыстории радио: сборник оригинальных статей и материалов / под ред. Л. И. Мандельштама. Вып. 1. М.-Л.: изд-во АН СССР, 1948. с. 375.

Статья представлена научным руководителем,
кандидатом военных наук, доцентом, полковником Мальцевой О. Л.

УДК 621.391

Р. В. Иванов (соискатель, ВАС)

ПРЕДЛОЖЕНИЯ ПО ОЦЕНКЕ ЗАЩИЩЕННОСТИ РАДИОКАНАЛОВ ОТ СТРУКТУРНЫХ ПОМЕХ

Рассматриваются предложения по оценке защищенности радиоканалов с частотной модуляцией от структурных помех. Представляются результаты по расчету вероятности ошибки имитонавязывания. Даются предложения по практическому использованию результатов.

радиоканал с частотной модуляцией, структурные помехи, вероятностная оценка защищенности, имитоустойчивость.

Введение

В настоящее время радиоканалы широко используются для управления роботизированными системами, в том числе беспилотными летательными аппаратами, поэтому вопросы оценки их защищенности от структурных помех являются актуальными.

В настоящей работе рассмотрен радиоканал с частотной модуляцией, как обеспечивающий наибольшую дальность при использовании его в интересах управления [1]. Однако, простата указанного модуляционного формата, используемого при передаче дискретной информации, делает радиоканал доступным для воздействия на него структурными помехами.

В дальнейшем определим воздействие структурных помех, направленных на формирование неверных команд в решающем устройстве, как процедуру имитонавязывания. А имитоустойчивость (имитостойкость) – как способность противостояния имитонавязыванию.

Таким образом, постановку структурных помех, приводящих к имитонавязыванию, можно отнести к одному из наиболее опасных видов деструктивного воздействия на радиоканалы управления.

Проблема имитонавязывания уже рассматривалась в различных работах [2, 3, 4], что подчеркивает актуальность рассматриваемой проблематики. Настоящая статья посвящена исследованию вопросов оценки имитоустойчивости радиоканалов с частотной модуляцией.

Оценка имитостойкости радиоканалов с частотной модуляцией

Процедуры имитонавязывания предполагают использование помех близких по своей частотно-временной структуре подавляемым сигналам [3]. При этом сущность имитонавязывания заключаться в подмене истинного сигнала помехой, приводящей к неверному принятию решения при демодуляции [5]. Фактически при имитонавязывании в радиоканалах с ча-

стотной модуляцией происходит формирование помехой на входе демодулятора символа, противоположного информационному, т.е. на решающем элементе создается ситуация неопределенности в принятии решения. В результате чего, выходная последовательность символов будет носить случайный характер.

Учитывая указанные обстоятельства, рассмотрим особенности демодуляции сигналов с частотной модуляцией. Поскольку управление роботизированными системами, как правило, осуществляется в движении, то на практике используется некогерентное детектирование, которое согласно [6] обеспечивает вероятность битовой ошибки равное

$$P_B = \frac{1}{2}\exp\left(-\frac{E_B}{2N_0}\right), \tag{1}$$

где E_B – энергия символа (для бинарных передач); N_0 – спектральная плотность мощности шума (в рассматриваемой ситуации – спектральная плотность мощности структурной помехи).

В [3] показано, что одной из проблем эффективной постановки структурной помехи является обеспечение их тактовой синхронизации с имитируемым сигналом. Согласно [7], это обусловлено различными причинами, такими как различия дистанций связи и подавления, наличие априорных знаний о битовой структуре команды, возможностей методов измерения и оценивания параметров сигналов и т. д.

Для учета особенностей приводящих к рассинхронизации помехи и сигнала введем понятие коэффициента временного несовпадения структурной помехи и сигнала на входе демодулятора ρ, который, с учетом его вероятностной природы, будет лежать в пределах $\rho \in [0;1]$.

Тогда $\rho = 1$ будет соответствовать условиям передачи помехой символа противоположного передаваемого сигналом управления в пределах тактового интервала, т. е. условиям, при которых решающее устройство работает случайным образом. А $\rho = 0$ будет соответствовать ситуации, когда структура помехи соответствует структуре сигнала и полностью совпадает с ним по такту, т. е. способствует его достоверному приему.

Для условий скрытного радиоэлектронного подавления наилучшая ситуация наступит в случае равенства энергий структурной помехи $E_{\text{П}}$ и сигнала, приходящаяся на бит E_B, и обеспечению условия $\rho = 1$.

$$E_{\text{П}} = E_B. \tag{2}$$

Действительно, выполнение равенства (2) должно приводить к полной неопределенности на входе решающего устройство демодулятора.

С учетом указанных замечаний, выражение (1) можно преобразовать к следующему виду, таким образом, чтобы в нем учитывалось тактовое несовпадение структурной помехи и сигнала, т.е. результирующая формула полностью характеризовала процесс имитонавязывания:

$$P_B = \frac{1}{2}\exp\left(-\frac{E_B + (1-2\rho)E_{\Pi}}{2N_0}\right). \qquad (3)$$

Полученная формула (3) представляет собой модель оценки вероятности ошибки в канале с частотной модуляцией в условиях имитонавязывания, т. е. воздействия оптимальной по структуре и энергии имитационной помехи.

Действительно, эффективность имитонавязывания обусловлена только вопросами тактовой синхронизации с имитируемым сигналом, которая в модели (3) учитываются посредством параметра ρ.

При $\rho = 1$ имеем $P_B = 0{,}5$, что характеризует полную неопределенность на решающем устройстве демодулятора.

Напротив, при $\rho = 0$ происходит суммирования энергии сигнала и помехи, приводящее к повышению достоверности принятия правильного решения. На рисунке 1 представлены результаты зависимости вероятности битовой ошибки P_B от ОСШ при различных значениях параметра ρ.

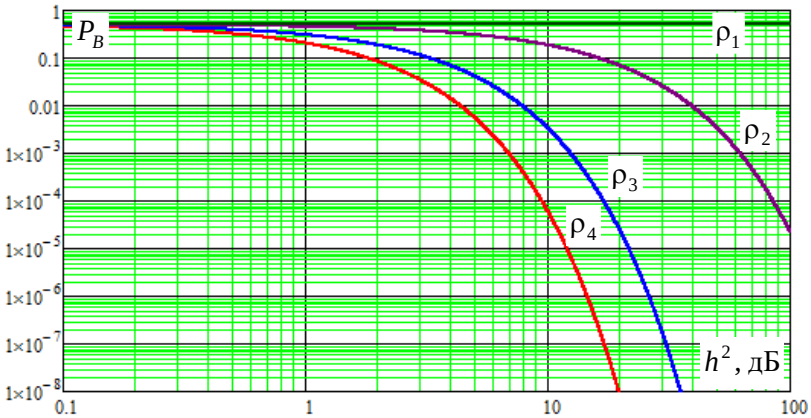


Рис. 1. Зависимость вероятности битовой ошибки от ОСШ при различных значениях коэффициента временного несовпадения

Так, на рисунке 1 показана зависимость вероятности битовой ошибки при $\rho_1 = 1$; $\rho_2 = 0{,}9$; $\rho_3 = 0{,}5$ и $\rho_4 = 0{,}1$. Таким образом, выражение (3) можно рассматривать в качестве модели оценки эффективности процедур имитонавязывания. Ее практическая реализация будет заключаться в измерении длительности тактового интервала несовпадения помехи с имитируемым сигналом в приемном тракте роботизированной системы. Полученное

вероятностное значение позволит осуществлять планирование мероприятий как по имитонавязыванию, так и по имитозащите.

Заключение

Проведенные исследования показали, что реализация процедур эффективного имитонавязывания связана с определенными сложностями не только по формированию помех заданной частотно-временной структуры, но и обеспечению их согласованности по уровню и тактовой синхронизации с имитируемыми сигналами.

Продуктивной мерой, позволяющей избежать имитонавязывание, является установка на входе демодулятора индикатора уровня принимаемого сигнала. При его превышении значения, определяемого допустимым дисперсионным разбросом, необходимо роботизированную систему автоматически переводить в автономный режим.

Кроме того, целесообразно для управления использовать сигналы с различным тактовым интервалом на длительности команды, изменяемым случайным образом, или же использовать сигналы сложных конструкций [8].

Направление дальнейшего исследования связано с оперативным решением вопросов обнаружения [9] самого факта деструктивного воздействия структурных помех на радиоканалы.

Список используемых источников

1. Точилов Л. Системы управления БЛА [Электронный ресурс] / ISPL.ru: [сайт]. URL: http://www.ispl.ru/Sistemy_upravleniya-BLA.html, свободный.

2. Орощук И. М. Оценка имитостойкости радиоканала с замираниями при использовании сигналов с частотной манипуляцией // Радиотехника. 2004. № 11. С. 12–18.

3. Дворников С. В., Погорелов А. А., Вознюк М. А., Иванов Р. В. Оценка имитостойкости каналов управления с частотной модуляцией // Информация и космос. 2016. № 1. С. 32–35.

4. Дворников С. В., Кузнецов Д. А., Кожевников Д. А., Пшеничников А. В., Манаенко С. С. Теоретическое обоснование синтеза ансамбля биортогональных сигналов с повышенной помехоустойчивостью // Вопросы радиоэлектроники. Серия: Техника телевидения. 2015. № 5 (22). С. 16–20.

5. Дворников С. В., Устинов А. А., Пшеничников А. В., Борисов В. В., Москалец А. Г., Бурыкин Д. А. Демодуляция сигналов ОФТ на основе адаптивного порога // Вопросы радиоэлектроники. Серия: Техника телевидения. 2013. № 2. С. 90–97.

6. Зюко А. Г. Помехоустойчивость и эффективность систем связи. М. : Связь, 1972. 360 с.

7. Дворников С. В. Проблема поиска сигналов источников информации при радиомониторинге // Мобильные системы. 2007. № 4. С. 33–35.

8. Агиевич С. Н., Дворников С. В., Гусельников А. С. Описание сигналов в базисах функций сплайн-Виленкина – Кристенсона // Контроль. Диагностика. 2009. № 3. С. 52–57.

9. Дворников С. В. Метод обнаружения на основе посимвольного перемножения реализаций спектра наблюдаемого процесса с автоматическим расчетом порога принятия решения // Научное приборостроение. 2004. Т. 14. № 4. С. 92–97.

Статья представлена научным руководителем,
доктором технических наук, профессором Дворниковым С. В.

УДК 004.4

М. С. Корчагин (студент группы ИКТВ-33, СПбГУТ)
Ю. А. Фролова (студент группы ИКТВ-33, СПбГУТ)

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ РЕАЛИЗАЦИИ ВНЕДРЕНИЯ ЛОЖНОГО DNS-СЕРВЕРА

Внедрение ложного DNS-сервера. Межсегментное внедрение ложного DNS-сервера. В статье представлены обе реализации с помощью модели Петри-Маркова.

моделирование сетевых атак, внедрение ложного DNS-сервера.

Внедрение ложного DNS-сервера

Целью данной сетевой атаки является перехват злоумышленником запроса атакуемого хоста к настоящему DNS-серверу. С помощью этого он подбирает номер порта, с которого отправляет запрос. Ему необходимо определить идентификатор запроса, который, как правило, либо равен единице, либо имеет близкий порядок. Отправив ответы с разными идентификаторами, злоумышленник может достичь успеха в атаке.

Смоделировать данную атаку можно с помощью сети Петри-Маркова.

Обозначения элементов данной сети: s_i – позиции, t_i – переходы.

s_1 – злоумышленник готов к проведению атаки; s_2 – атакуемый хост готов; t_1 – ожидание передачи запроса атакуемого хоста к DNS-серверу; s_3 – требуемый запрос перехвачен; t_2 – анализ запроса и формирование ответа; s_4 – необходимый ответ сформирован; t_3 – отправка ответа атакуемому хосту; s_5 – ответ отправлен; t_4 – прием атакуемым хостом ложного ответа и изменение его таблицы имен; s_6 – соединение атакуемого хоста с ложным сервером осуществлено.

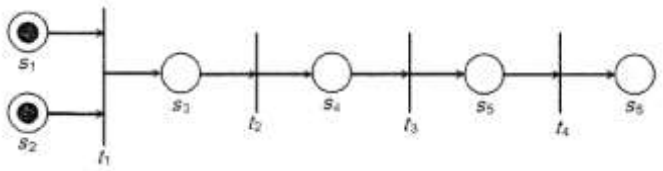


Рис. 1. Вид сети Петри-Маркова процесса реализации внутри-сегментного внедрения ложного DNS-сервера

Вероятности перемещения из позиций этой сети равны единице, так как они не имеют инцидентные дуги.

Элементы матрицы определяющие логические функции срабатывания сети, могут быть записаны (без учета направленности) следующим образом:

$$V_{s_1 t_4} = \begin{array}{c|cccc} & t_1 & t_2 & t_3 & t_4 \\ \hline s_1 & 1 & 0 & 0 & 0 \\ s_2 & 1 & 0 & 0 & 0 \\ s_3 & s_1 t_1 \cap s_2 t_1 & 1 & 0 & 0 \\ s_4 & 0 & 1 & 1 & 0 \\ s_5 & 0 & 0 & 1 & 1 \\ s_6 & 0 & 0 & 0 & 1 \end{array}.$$

Для данной сети Петри-Маркова существует система интегро-дифференциальных уравнений:

$$\Phi s_1 t_1(t) = \pi 11 \int_0^t f s_1 t_1(\tau)\, d\tau$$

$$\Phi s_2 t_2(t) = \pi 22 \int_0^t f s_2 t_1(\tau)\, d\tau$$

$$\Phi_1(t) = \int_0^t f s_1 t_1(\tau) \Phi s_2 t_1(\tau) + f s_2 t_1(\tau) \Phi s_1 t_1(\tau)\, d\tau$$

$$\Phi s_3 t_2(t) = \pi 32 \int_0^t f s_3 t_2(\tau) \Phi s_1 t_1(t-\tau)\, d\tau,$$

$$\Phi s_4 t_3(t) = \pi 43 \int_0^t f s_4 t_3(\tau) \Phi s_3 t_2(t-\tau)\, d\tau,$$

$$\Phi s_5 t_4(t) = \pi 54 \int_0^t f s_5 t_4(\tau) \Phi s_4 t_3(t-\tau)\, d\tau,$$

Применяя пуассоновское приближение, получаем среднее время перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения:

$$\tau 1 = \frac{\tau 11^2 + \tau 11 \tau 21 + \tau 21^2}{\tau 11 + \tau 21};$$

$$\tau = \tau 1 + \tau 32 + \tau 43 + \tau 54 + \tau 65 + \tau 75;$$

$$\tau 1 = \frac{\tau 11^2 + \tau 11 \tau 21 + \tau 21^2}{\tau 11 + \tau 21} + \tau 32 + \tau 43 + \tau 54 + \tau 65 + \tau 75;$$

Исходные параметры атаки принимают следующие значения: $\tau 21 = 15{,}5$ с – среднее время запуска и настройки программы для реализации атаки, $\tau 21 = \tau 23 = 0{,}1$ с, $\tau 23 = 0{,}2$ с – средние времена соответственно пересылки и обработки пакетов.

Среднее время перехода по всей сети $\tau = 16{,}25$ с, зависимость реализации атаки от времени представлена на рисунке 2.

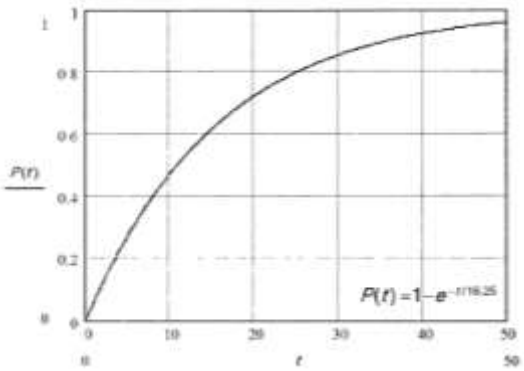


Рис. 2. Зависимость вероятности реализации внутрисегментного внедрения ложного DNS-сервера от времени

Межсегментное внедрение ложного DNS-сервера.

При данной атаки злоумышленник не может перехватить зарос атакуемого хоста к настоящему DNS-серверу. Появляется задача, определить номер порта, с которого был отправлен запрос и идентификатор запроса. В большинстве систем этот идентификатор равен единице или имеет близкий порядок. Поэтому, при отправке нескольких ответов с разными идентификаторами и номерами порта, злоумышленник может рассчитывать на успех атаки.

Возможно смоделировать данную атаку с помощью сети Петри-Маркова.

Обозначения элементов сети: s_i – позиции, t_i – переходы.

s_1 – атакуемый хост готов; t_1 – ожидание передачи запроса атакуемого хоста к DNS-серверу; s_2 – атакуемый хост отправил запрос к DNS-серверу и ожидает ответа; s_3 – злоумышленник сформировал и отправляет атакуемому хосту ложные DNS-ответы; t_2 – прием атакуемым хостом ложного ответа и изменение его таблицы имен; s_4 – соединение атакуемого хоста с ложным сервером осуществлено.

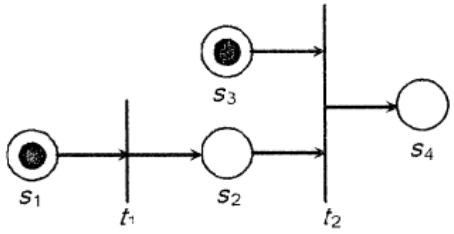


Рис. 3. Вид сети Петри-Маркова процесса реализации межсегментного внедрения ложного DNS-сервера

Ниже представлены матрицы, определяющие логические функции срабатывания сети, могут быть записаны (без учета направленности дуг графа) следующим образом:

$$V_{s_1 t_4} = \begin{array}{c|cc} & t_1 & t_2 \\ \hline s_1 & 0 & 1 \\ s_2 & 1 & 0 \\ s_3 & 1 & 1 \\ s_4 & 0 & s_2 t_2 \cap s_3 t_2 \end{array}.$$

Для данной сети Петри-Маркова запишем следующую систем интегро-дифференциальных уравнений.

$$\Phi s_1 t_1(t) = \pi 11 \int_0^t f s_1 t_1(\tau) d\tau;$$

$$\Phi s_2 t_2(t) = \pi 22 \int_0^t f s_2 t_2(\tau) d\tau;$$

$$\Phi s_3 t_2(t) = \pi 32 \int_0^t f s_3 t_2(\tau) \Phi s_1 t_1(t-\tau) d\tau;$$

$$\Phi_1(t) = \int_0^t f s_2 t_2(\tau) \Phi s_3 t_2(\tau) + f s_3 t_2(\tau) \Phi s_2 t_2(\tau) d\tau.$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями.

Применяя пуассоновское приближение, можно получить среднее время перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения:

$$\tau 1 = \tau 11 + \tau 32;$$

$$\tau = \frac{\tau 1^2 + \tau 1 * \tau 22 + \tau 22^2}{\tau 1 + \tau 22};$$

$$\tau = \frac{(n*T+\tau 11)^2 + (n*T+\tau 11)*\tau 22 + \tau 22^2}{(n*T+\tau 11)+\tau 22}.$$

Исходные параметры атаки принимают следующие значения: $\tau 21$=15,4 с – среднее время запуска и настройки злоумышленником программы для реализации атаки, $\tau 11 = \tau 22 = 0{,}2$ с , $\tau 32 = 1$ с – средние времена соответственно пересылки и обработки пакетов.

Таким образом $\tau = 17{,}53$ с – среднее время перехода по всей сети и зависимость вероятности реализации этапа от времени имеет вид.

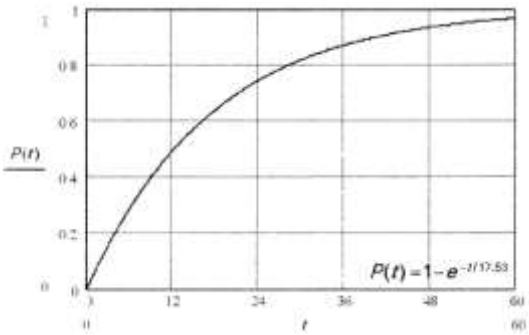


Рис. 4. Зависимость вероятности реализации межсегментного внедрения ложного DNS-сервера от времени

Список используемых источников

1. Радько Н. М. Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М. : Радио Софт, 2010. 232 с. ISBN 978-5-93274-019-4.

Статья представлена научным руководителем,
кандидатом технических наук, старшим преподавателем, капитаном Сагдеевым А. К.

УДК 654.026

О. И. Кривошей (курсант, ВАС)
С. П. Кривцов (старший преподаватель, ВАС)
Н. С. Микина (курсант, ВАС)
В. И. Чеботарёв (доцент, ВАС)

ПОСТРОЕНИЕ ИМИТАЦИОННОЙ МОДЕЛИ ЛИНИЙ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ПЕРЕДАТЧИКАМИ РАДИОЦЕНТРА СТАЦИОНАРНОГО УЗЛА СВЯЗИ С ПОМОЩЬЮ СИМУЛЯТОРА ЛОКАЛЬНОЙ СЕТИ

В работе рассмотрена имитационная модель линий дистанционного управления передатчиками радиоцентра стационарного узла связи построенная в симуляторе локальной сети GNS3. В статье описан порядок построения имитационной модели, состав основного оборудования линий дистанционного управления передатчиками, составлена таблица маршрутизации внутренних локальных сетей, и внешних телекоммуникационных связей между элементами радиоцентра.

имитационная модель, стационарный узел связи, радиоцентр, локальная сеть, линии дистанционного управления передатчиками, маршрутизатор, таблица маршрутизации, симулятор локальной сети.

В Вооруженных Силах РФ проходит активный процесс реформирования, в том числе и в Войсках связи. При этом основой будет выступать глобальная (пространственно-разнесенная) информационная сеть, создаваемая на базе имеющихся и перспективных сетей связи и передачи данных на основе применения современных телекоммуникационных технологий и обладающая высокими оперативно-техническими характеристиками. Такая сеть должна обеспечить непрерывный и единообразный обмен информацией для всех систем и средств, используемых в мирное время и при ведении боевых действий.

Организационно-техническая структура перспективных узлов связи реализуется на основе телекоммуникационной архитектуры, предполагающей построение базовой сети связи на основе стека протоколов TCP/IP. В основу построения архитектуры узлов связи пунктов управления специального назначения положен принцип создания защищенной мультисервисной сети связи на базе интегрированной IP-платформы с поддержкой качества обслуживания на всех уровнях [1].

Наряду с основной частью стационарного узла связи (СУС) претерпевают значительные изменения и вынесенные элементы СУС, а в частности отделение передающих радиоустройств (ОПРУ) и отделение приёмных радиоустройств (ОПрРУ). В настоящее время в зависимости от состава и группировки войск, дислокации на его территории соединений и частей,

от узла связи обеспечивается функционирование от 5 до 20 радионаправлений к узлам связи выше стоящего штаба, так и к узлам связи подчинённых соединений и воинских частей.

Все средства радиосвязи СУС организационно и технически объединяются в ОПРУ, ОПрРУ и радиобюро. В ходе анализа стало ясно, что элементы радиоцентра могут обеспечить следующие основные возможности:

Радиобюро – принимать и обеспечивать дежурство в 3–5 радионаправлениях или радиосетях с возможностью записи переговоров.

Отделение передающих радиоустройств – организовать передачу в 1–3 радионаправлениях или радиосетях на радиостанциях большой мощности, в 3–20 радионаправлениях или радиосетях на радиостанциях средней мощности; обеспечить работу 60 телефонных каналов, для линий дистанционного управления (ЛДУ) передатчиками, служебной и оперативной связи и 48 каналов тонального телеграфирования и низкоскоростных каналов передачи данных.

Отделение приемных радиоустройств – организовать работу в 30–50 радионаправлениях или радиосетях, обеспечить работу по 60 телефонным каналами и по 48 каналам тонального телеграфирования и низкоскоростных каналов передачи данных.

Линии дистанционного управления передатчиками состоят из аппаратуры аналогового каналообразования работающей по магистральным медным кабелям связи и в качестве резервных линий используются аналоговые радиорелейные станции.

В итоге на основе данного анализа приходим к выводу, что радиоцентр может обеспечить только аналоговую связь, которая не всегда соответствует требованиям современной системы связи.

Для совершенствования ЛДУ передатчиками радиоцентра СУС предлагается использовать современные телекоммуникационные средства и фрагмент внутренней телекоммуникационной сети узла связи, состоящей из:

1) Комплекта телекоммуникационных средств основной части узла связи (находиться в радиобюро) в состав которого входит:

- магистральная оптическая линия связи от основной части узла связи к ОПРУ с резервной цифровой радиорелейной линией;
- магистральная оптическая линия связи от основной части узла связи к ОПрРУ с резервной цифровой радиорелейной линией;
- пограничный маршрутизатор узла;
- коммутатор локальной вычислительной сети 3 уровня;
- VoIP шлюз для преобразования голосовой информации в IP пакеты;
- IP шлюз для преобразования телеграфной информации в IP пакеты;
- абонентская локальная вычислительная сеть радиобюро.

2) Комплекта телекоммуникационной аппаратуры связи ОПРУ в состав которого входит:

- магистральная оптическая линия связи от ОПРУ к ОПрРУ с резервной цифровой радиорелейной линией;
- пограничный маршрутизатор узла;
- коммутатор локальной вычислительной сети 3 уровня;
- VoIP шлюз для преобразования голосовой информации в IP пакеты;
- IP шлюз для преобразования телеграфной информации в IP пакеты;
- абонентская локальная вычислительная сеть ОПрРУ.

3) Комплекта аппаратуры связи ОПрРУ, в состав которого входит:

- оборудование магистральной оптической линии связи с резервными цифровыми радиорелейными линиями;
- пограничный маршрутизатор узла;
- - коммутатор локальной вычислительной сети 3 уровня;
- VoIP шлюз для преобразования голосовой информации в IP пакеты;
- IP шлюз для преобразования телеграфной информации в IP пакеты;
- абонентская локальная вычислительная сеть ОПрРУ.

Использование телекоммуникационных средств предоставляет пользователю оптимальное сочетание скорости передачи, высокой энергетики радиолинии и широкого набора функциональных возможностей.

Введение этого оборудования позволит обеспечить цифровую связь между основной частью узла связи и удаленными элементами узла связи. Наличие локальной компьютерной сети между основной частью и удаленными элементами узла связи позволит организовать новые услуги связи, такие как [2]: видеоконференцсвязь, электронную почту, систему видеонаблюдения, открытую IP-телефонию, передачу файлов и данных.

Для исследования процессов передачи информации по ЛДУ передатчиками была разработана имитационная модель в программной среде GNS3, в состав которой вошли элементы радиоцентра и техника описанные выше. Имитационная модель ЛДУ передатчиками на СУС будет иметь вид, представленный на рисунке 1.

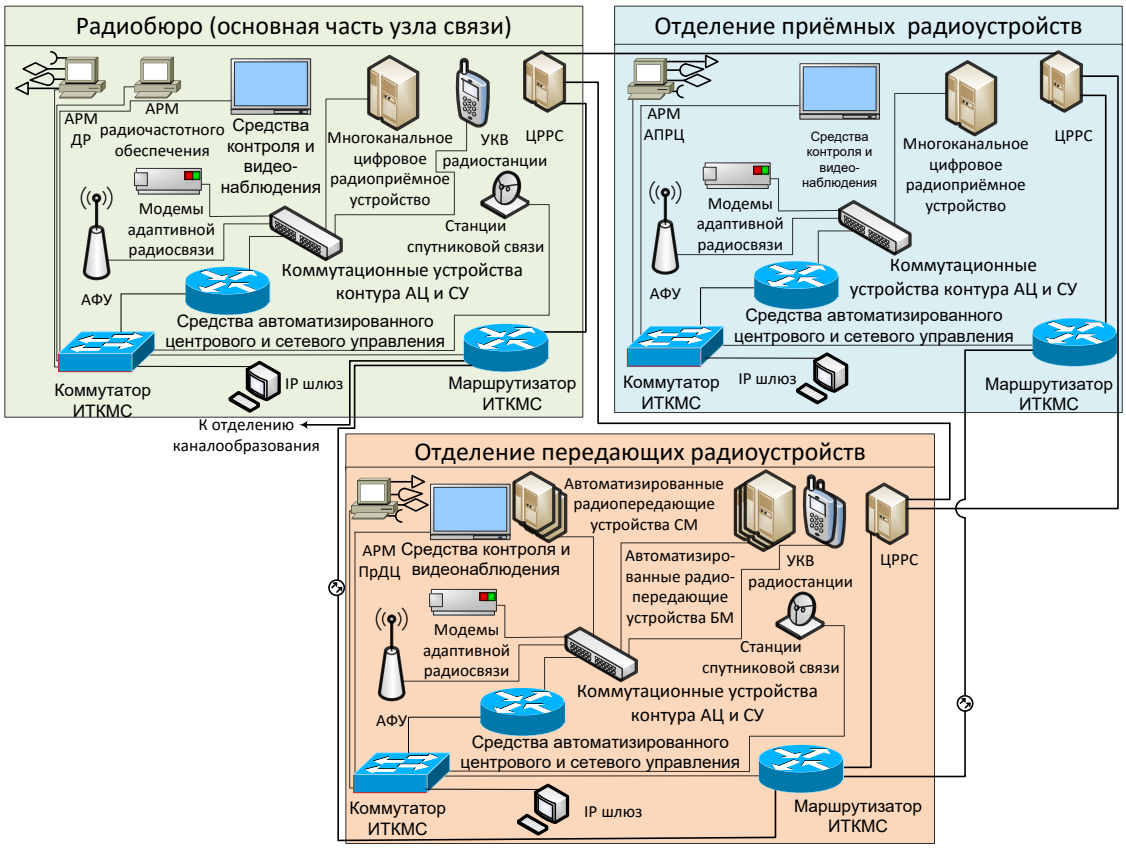


Рис. 1. Схема радиоцентра стационарного узла связи

Согласно схемы радиоцентра стационарного узла связи производиться расчёт локальных вычислительных сетей и сетей связи между элементами радиоцентра. Схема маршрутизации представлена в таблице 1.

ТАБЛИЦА 1. Схема маршрутизации

№ п/п	Маршрутизатор и его порт	Адрес и маска марш-рутизатора	Маршрутизатор корреспондента и его порт	Адрес и маска маршрутиза-тора корре-спондента	Маршрути-затор корре-спондента
Радиоцентр					
Радиобюро					
1.	routerРБ Gig0/0	10.120.1.1/30	routerОПРРУ Gig0/0	10.120.1.5/30	ОПРРУ
2.	routerРБ Gig0/1	10.120.1.2/30	routerОПРДРУ Gig0/0	10.120.1.9/30	ОПРДРУ
3.	routerРБ Gig1/0	10.120.2.1/26	switchРБ Gig7	10.120.2.2/26	РБ
Отделение приемных радиосредств					
4.	routerОПРРУ Gig0/0	10.120.1.5/30	routerРБ Gig0/0	10.120.1.1/30	РБ
5.	routerОПРРУ Gig0/1	10.120.1.6/30	routerОПРДРУ Gig0/1	10.120.1.10/30	ОПРДРУ
6.	routerОПРРУ Gig1/0	10.120.2.65/26	switchОПРРУ Gig7	10.120.2.66/26	ОПРРУ
Отделение передающих радиосредств					
7.	routerОПРДРУ Gig0/0	10.120.1.9/30	routerРБGig0/1	10.120.1.2/30	РБ

№ п/п	Маршрутизатор и его порт	Адрес и маска маршрутизатора	Маршрутизатор корреспондента и его порт	Адрес и маска маршрутизатора корреспондента	Маршрутизатор корреспондента
8.	routerОПРДРУ Gig0/1	10.120.1.10/30	routerОПРРУ Gig0/1	10.120.1.6/30	ОПРРУ
9.	routerОПРДРУ Gig1/0	10.120.2.129/26	switchОПРДРУGig7	10.120.2.130/26	ОПРДРУ

В результате в симуляторе локальной сети имитационная модель радиоцентра СУС будет иметь вид представленный на рисунке 2.

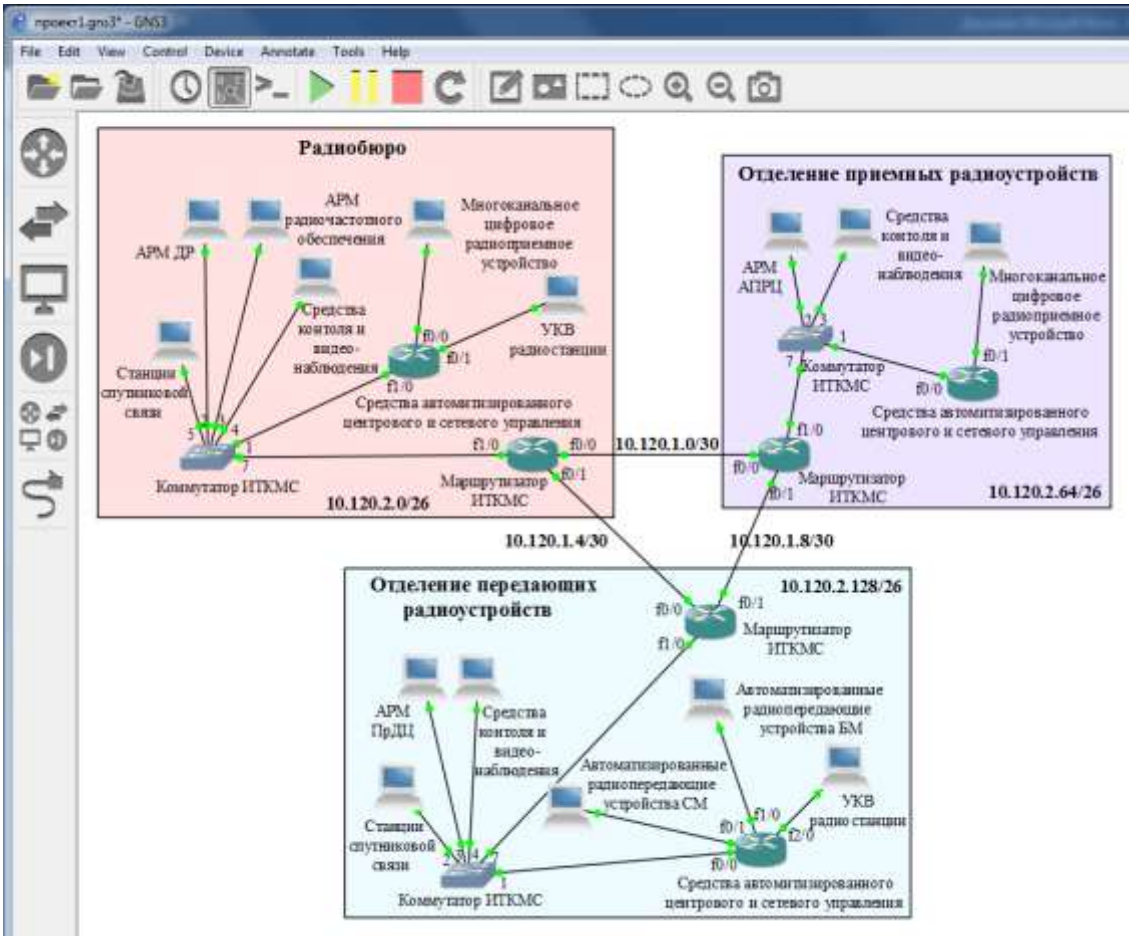


Рис. 2. Имитационная модель радиоцентра стационарного узла связи.

В результате предложений по усовершенствованию радиоцентра был оптимизирован состав техники связи, которой оснащается радиоцентр, была кардинально пересмотрена система управления радиоцентром, были введены новые виды и услуги связи. С введением цифрового оборудования появилась возможность передачи каналов АТС, которые позволяют довести до удаленных объектов прямые городские номера, а также телефоны внутренней связи, появилась возможность доведения до узла связи прямых телефонов, введение которых позволяет отказаться от ручного коммутатора дальней связи, в результате чего сокращается состав дежурной смены и из ее состава исключается дежурный телефонист коммутатора дальней

связи, также появляется возможность довести до удаленных элементов радиоцентра телефонные номера АТС-IP-телефонии, что позволяет осуществить звонки практически во все части телекоммуникационной сети МО РФ.

Введение телефонов АТС позволяет обеспечить факсимильную связь, как между абонентами узла связи, так и с выходом в междугороднюю сеть, что в разы ускоряет оперативность работы радиоцентра.

Описанные принципы построения линий дистанционного управления стационарного узла связи легли в основу построения имитационной модели стационарного узла.

Список используемых источников

1. Лобанов С. Н., Тевс О. П., Черенков В. Е. Формирование структуры перспективных узлов связи пунктов управления специального назначения [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. Т. 2. / под ред. С. В. Бачевского. СПб. : СПбГУТ, 2015. С. 1332–1338. URL: http://www.sut.ru/doci/nauka/4.apino.2015.sut.pdf

2. Иванов В. Г., Панихидников С. А., Тевс О. П. Организационно-технические аспекты построения перспективных узлов связи центров управления специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. Т. 2. / под ред. С. В. Бачевского. СПб. : СПбГУТ, 2015. С. 1255–1260. URL: http://www.sut.ru/doci/nauka/4.apino.2015.sut.pdf

Статья представлена научным руководителем,
доктором технических наук, профессором Мякотиным А. В.

УДК 621.396

Д. А. Кузнецов (студент группы ИКТВ-31, СПбГУТ)
П. О. Митрошина (студентка группы ИКТВ-31, СПбГУТ)
А. А. Сёмин (студент группы ИКТВ-31, СПбГУТ)

ОСОБЕННОСТИ ПОСТРОЕНИЯ РАДИОКАНАЛА С БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ

В данной статье описаны особенности построения радиолинии с беспилотным летательным аппаратом. Проведен анализ, выявлены требования, \ и рассмотрены потери при распространении сигнала. Проведен анализ бюджета канала связи, рассмотрены различные виды модуляции сигнала. И предложена борьба с частотно-спектральными искажениями.

радиоканал, беспилотные летательные аппараты, канал связи.

В последнее время уделяется особое внимание использованию беспилотных летательных аппаратов (БПЛА) как в гражданской, так и в военной среде. Эффективность использования во многом определяет «чистота» канала связи между наземным пунктом управления (НПУ) и БПЛА. Значит всплывает вопрос об оптимизации радиоканала передачи данных.

Радиолиния НПУ-ЛА представляет собой узкополосный канал связи, т. к. объём передаваемой информации мал. Необходимая скорость передачи информации в этом канале порядка десятка Кбит/сек.

Радиолиния ЛА-НПУ должна иметь большую пропускную способность. Конкретное значение требуемой скорости передачи определяется полезной нагрузкой конкретного аппарата.

Требования к системам связи с БПЛА

Тип канала связи	Передача командно-телеметрических данных	Передача данных полезной нагрузки
Вероятность битовой ошибки	Не более 10^{-6}	Не более 10^{-3}
Скорость передачи данных	Не более 56 Кбит/с	1–20 Мбит/с (зависит от назначения аппарата и типа полезной нагрузки)

Анализ канала связи с БПЛА

Канал радиосвязи между БПЛА и наземным пунктом управления относится к авиационному каналу, который описывается многолучевой моделью с явлениями переотражения, рассеивания и дифракции.

Отражение имеет место, когда электромагнитная волна сталкивается с препятствием, размеры которого значительно превышают длину волны.

Дифракция происходит, когда трасса распространения между передатчиком и приемником перекрыта плотным препятствием с размерами большими по отношению к длине волны сигнала, что приводит к формированию позади препятствия вторичных волн.

Рассеивание происходит, когда распространяющийся сигнал наталкивается на объект, размеры которого порядка длины волны сигнала или менее, это приводит к переизлучению энергии сигнала по всем направлениям.

Эти три эффекта образуют общую картину замираний в канале, достаточно полно представляемую как замираниями крупного масштаба и мелкомасштабными замираниями.

В большинстве случаев БПЛА гражданского назначения работают в пределах прямой видимости НПУ. При наличии преобладающего по ам-

плитуде прямого луча распределение мгновенных значений огибающей сигнала описывается законом Райса:

$$p(x) = \frac{x}{\sigma_x^2} \cdot e^{-\frac{x^2}{\sigma_x^2}} \cdot e^{-K} \cdot I_0\left(\frac{x}{\sigma_x}\sqrt{2K}\right),$$

где $I_0(z)$ – модифицированная функция Бесселя первого рода нулевого порядка; K – параметр, определяемый как отношение мощности зеркального компонента к мощности многолучевого сигнала; x – компонент мелкомасштабного замирания; σ_x^2– средняя мощность многолучевого сигнала до детектирования.

Потери при распространении сигнала

Крупномасштабные замирания представляют собой среднее ослабление мощности сигнала или потери на трассе при прохождении трасс большой протяженности. Два основных механизма, приводящие к эффектам замираний крупного масштаба – потери на трассе и затенение.

Средние потери радиосигнала на трассе определяются по формуле

$$L(d)[\text{дБ}] = L(d_0)[\text{дБ}] + 10\gamma \cdot \lg\left({}^{d}/_{d_0}\right) + X_\sigma, \qquad (1)$$

где $L(d_0)$ – средние потери на трассе прямой видимости при эталонном расстоянии d_0 в свободном пространстве; d – это расстояние между передатчиком и приемником; γ – экспонента потери на трассе, которая зависит от окружающей среды; X_σ – логарифмически нормальное замирание вследствие затенения.

В БПЛА системах эталонное расстояние d_0выбирается равным рабочей высоте.

Средние потери $L(d_0)$ при распространении в свободном пространстве рассчитываются по формуле

$$L(d_0)[\text{дБ}] = 10\lg\left({}^{4\pi d_0}/_{\lambda}\right)^2, \qquad (2)$$

где λ – длина волны сигнала.

Если расстояние d_0 и частота f ($f = \left({}^{c}/_{\lambda}\right)$, c – скорость света) измеряются в километрах и МГц соответственно, то из формул (1) и (2), получаем следующее (при $X_\sigma = 0$)

$$L(d)[\text{дБ}] = 10\gamma \cdot \lg(d) + (20 - 10\gamma)\lg(d_0) + 20\lg(f) + 32{,}45. \qquad (3)$$

Рассчитаем потери на трассе в зависимости от расстояния между БПЛА и НКУ для разных частот (0,9; 2,4; 5,8 ГГц).

Из рисунка 1 видно, что при расстоянии 30 км между НКУ и БПЛА затухания сигнала в свободном пространстве в диапазонах 0,9; 2,4 и 5,8 ГГц равны 121, 130 и 136 дБ соответственно. В худших условиях распространения (γ = 3) затухание сигнала сильно увеличивается. Для компенсации такого ослабления сигнала можно использовать такие способы как повышение коэффициента усиления антенн, использование энергетически выгодных видов модуляции, повышение выходной мощности передачиков.

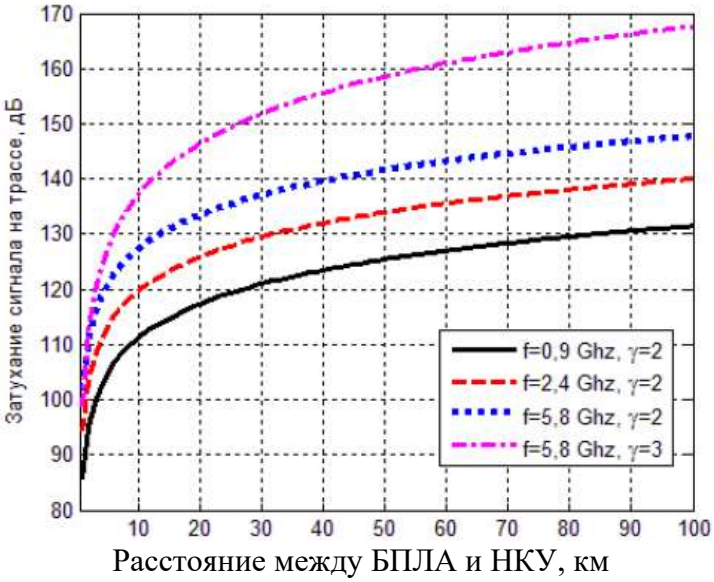


Рис. 1. Затухание сигнала на трассе в зависимости от расстояния между БПЛА и НКУ

Анализ бюджета канала связи с БПЛА

Для цифровой связи вероятность ошибки зависит от отношения энергии бита (E_b) к спектральной плотности мощности шума (N_0) в приемнике, определяемого выражением (4):

$$\frac{E_b}{N_0} = \frac{P_R}{N}\left(\frac{W}{R}\right),$$

где P_R – мощность принятого сигнала, N_0 – мощность шума, W – ширина полосы пропускания, R – скорость передачи бита.

Важнейшим показателем качества канала является зависимость вероятности появления ошибочного бита P_b от E_b/N_0. Разность между реаль-

ным (принятым) и требуемым отношениями E_b/N_0 дает энергетический резерв линии связи (это и называют бюджетом связи канала).

$$M(\text{дБ}) = E_b/N_0\ \text{прин}(\text{дБ}) - E_b/N_0\ \text{треб}(\text{дБ}). \quad (5)$$

Принятая антенной мощность определяется по формуле:

$$P_R(d)(\text{дБ}) = P_T(\text{дБ}) + G_R(\text{дБ}) + G_T(\text{дБ}) - L_S(\text{дБ}) - L_0(\text{дБ}), \quad (6)$$

где G_Rи G_T – коэффициенты усиления передающей и приемной антенн; P_T – переданная мощность; L_0 – коэффициент потерь системы, не связанных с распространением (потери в фидере и разъемах НКУ и БПЛА, поляризационное рассогласование антенн).

Из уравнений (4), (5) и (6), получаем:

$$M(\text{дБ}) = P_T(\text{дБм}) + G_R(\text{дБ}) + G_T(\text{дБ}) - L_S(\text{дБ}) - L_0(\text{дБ}) - P_S(\text{дБм}),$$

где P_S – чувствительность приемника, дБм.

Выбор вида модуляции

Основным требованием при создании системы связи с БПЛА является обеспечение возможности передачи данных с заданной скоростью и вероятностью ошибки при больших расстояниях между ЛА и НКУ. Для сравнения энергетической эффективности, на рисунке 2 показано некоторых видов модуляции по каналу с гаусовским шумом.

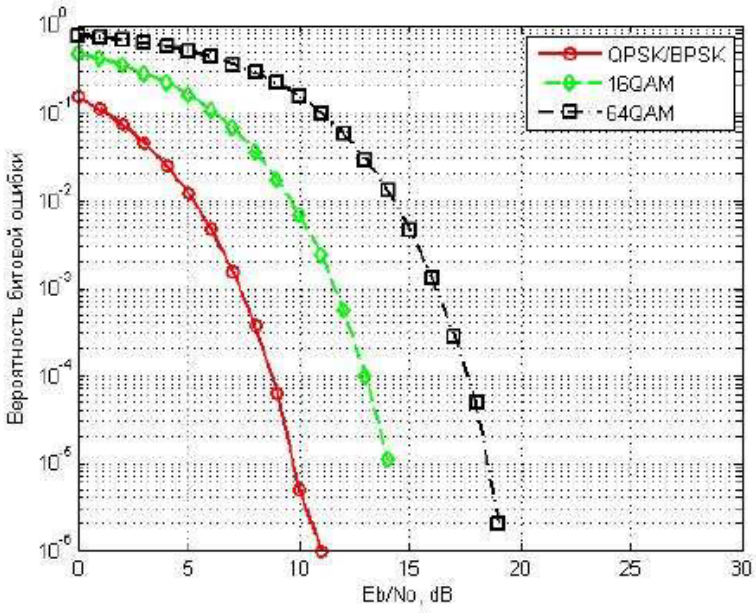


Рис. 2. Вероятность битовой ошибки для различных видов модуляции

Из рисунка 2 следует, что с увеличением позиционности модуляции вероятность битовой ошибки увеличивается, т. е. для поддержания заданного уровня битовой ошибки необходимо увеличивать отношение сигнал/шум (ОСШ) на входе приемника. Поэтому целесообразным является использование многопозиционной модуляции только при малых расстояниях между БПЛА и НКУ для передачи большего объема информации без изменения ширины полосы частот. Для обеспечения максимальной дальности связи необходимо использовать энергетически наиболее выгодные виды модуляции – такие как двоичная фазовая манипуляция (BPSK) и квадратурная фазовая манипуляция (QPSK).

Как видно из рисунка 1, при изменении расстояния между ЛА и НКУ в широких пределах (500 м – 30 км) мощность сигнала с несущей 2,4 ГГц на входе приемника будет изменяться на порядке 35 дБ. Такой большой энергетический запас позволяет использовать различные виды модуляции для повышения скорости передачи данных с БПЛА на НКУ при поддержании вероятности битовой ошибки на заданном уровне. Реализация данного подхода требует создания алгоритмов адаптивногоизменения схемы модуляции и кодирования цифровой системы связи.

Борьба с частотно-селективными искажениями сигнала

Канал связи с БПЛА является частотно-селективным из-за многолучевости распространения сигналов. Для борьбы с многолучевостью сигналов быларазработана технология мультиплексирования с ортогональным частотным разделением каналов (OFDM), которая эффективно применяется в беспроводных сетях Wifi и WiMax.

Основная идея OFDM заключается в том, что полоса пропускания канала разделяется на группу узких полос (субканалов), каждая со своей поднесущей. На всех поднесущих сигнал передается одновременно, что позволяет обеспечить практически сколь угодно большую общую скорость передачи информации при небольшой скорости передачи в каждом отдельном субканале. Данная технология трансформирует широкополосный частотно-избирательный канал во множество параллельных неизбирательных по частоте узкополосных каналов. Такая схема успешно компенсирует влияние многолучевости.

Высокая спектральная эффективность OFDM модуляции обеспечивается достаточно близким расположением частот соседних поднесущих колебаний, которые генерируются совместно так, чтобы сигналы всех под несущих были ортогональны.

Как правило, чем больше число поднесущих, тем меньше влияние замираний сигнала, обусловленных многолучевым распространением. Однако это приводит к усложнению аппаратуры и к увеличению искажений сигнала за счет доплеровского эффекта. В некоторых случаях при большом доплеровском сдвиге OFDM теряет свои преимущества. Следовательно,

необходимо выбрать оптимальное количество поднесущих при применении OFDM для передачи данных с БПЛА.

Выводы

Изменение параметров работы систем связи с БПЛА, вызванное изменением взаимного расположения ЛА и НПУ и влиянием среды распространения сигнала, приводит к необходимости адаптивного изменения основных параметров системы (вид модуляции, кодирование, скорость передачи данных и др.) в зависимости от условий прохождения сигнала, которое позволяет более эффективно использовать энергетический ресурс канала связи и многократно повышать эффективность работы системы.

Дальность связи БПЛА зависит от многих факторов, в том числе высоты ЛА, мощности передатчика ЛА, чувствительности приемника НПУ, типов антенн на борту ЛА и на НПУ, вида модуляции и др. Для увеличения дальности действия малоразмерных БПЛА необходимо использование энергетически выгодных видов модуляции и наземной антенны с высоким коэффициентом усиления. Для передачи данных (фотоснимков, видеоизображений) с БПЛА на НПУ в реальном времени требуется большая скорость передачи. Одним из наиболее эффективных подходов к повышению скорости передачи данных с применение модуляции OFDM.

Список используемых источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение : пер. с англ. Изд. 2-е, испр. М. : Издательский дом «Вильямс», 2003. 1104 с
2. Richard V. N., Prasad R. OFDM wireless multimedia communication. Artech House Boston London. 2000. 260 p.
3. Дмитриков В. Ф., Сергеев В. В., Самыгин И. Н. Повышение эффективности преобразовательных. М. : Радио и связь, 2005. 423 с.

Статья представлена научным руководителем,
кандидатом технических наук Сагдеевым А. К.

УДК 621.396

Д. А. Кузнецов (студент группы ИКТВ-31, СПбГУТ)
А. О. Широков (студент группы ИКТВ-42, СПбГУТ)
С. О. Широков (студент группы ИКТВ-42, СПбГУТ)

АНАЛИЗ ПОМЕХОЗАЩИЩЕННОСТИ РАДИОКАНАЛА

В данной статье описан способ построения классической радиолинии. Рассмотрены возможные потери в радиоканале, выбор оптимальной модуляции в зависимости от поставленных задач. Представлен способ кодирования и свёрточный код.

радиолиния, кодирование, свёрточный код.

В настоящее время в мире преобладает техника с мобильными элементами управления. А это значит, что для реализации управления требуется радиоканал. Но в зависимости от поставленных задач и полезной нагрузки радиоканалы отличаются друг от друга: требуется разная пропускная способность радиолинии, а значит и разные типы модуляции, разная помехозащищенность, разное кодирование.

Рассмотри схему классической радиолинии на рисунке 1.

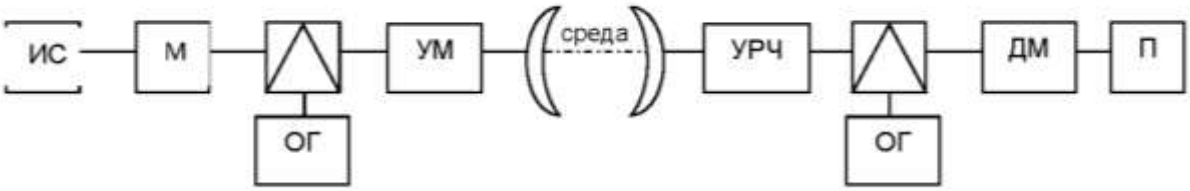


Рис. 1. Схема классической радиолинии

Источник сигнала (ИС) посылает аналоговый сигнал на вход модулятор (М), где при помощи определенного вида модуляции сигнал преобразуется и выходит промежуточная частота, после чего на смеситель, при помощи опорного генератора (ОГ), формируется нужный сигнал и усиливается на усилители мощности (УС), за чем идет антенна передатчика, которая посылает сигнал на антенну приёмника. Посылка сигнала идёт через среду распространения, которая характеризуется коэффициентом ослабления среды. На приёмной стороне при помощи усилителя радиочастот (УРЧ), смесителя, демодулятора осуществляется обратная операция, и сообщение доходит до приемника.

Что бы передать сообщение с наименьшими потерями, требуется подробно разобрать каждый участок схемы. В данной статье будут предъявлены лишь общие положения. Начиная с простого – среда передачи, которая характеризуется коэффициентом ослабления. Влияют, элементарно, даже погодные условия, например, влажность. С чем борются с помощью

усилителей мощности сигнала, и усилителем радиопомех. Но наиболее интересным встает вопрос о выборе вида модуляции.

Основным требованием при создании системы связи является обеспечение возможности передачи данных с заданной скоростью и вероятностью ошибки при больших расстояниях между. Для сравнения энергетической эффективности, на рисунке 2 показано некоторых видов модуляции по каналу с гаусовским шумом.

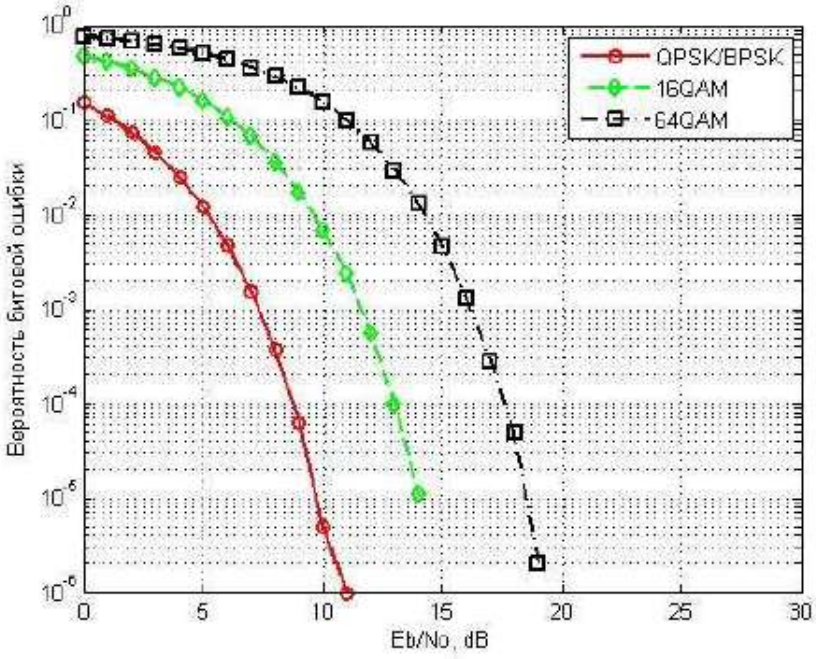


Рис. 2. Вероятность битовой ошибки для различных видов модуляции

Из рисунка 2 следует, что с увеличением позиционности модуляции вероятность битовой ошибки увеличивается, т. е. для поддержания заданного уровня битовой ошибки необходимо увеличивать отношение сигнал/шум (ОСШ) на входе приемника. Поэтому целесообразным является использование многопозиционной модуляции только при малых расстояниях между для передачи большего объема информации без изменения ширины полосы частот. Для обеспечения максимальной дальности связи необходимо использовать энергетически наиболее выгодные виды модуляции – такие как двоичная фазовая манипуляция (BPSK) и квадратурная фазовая манипуляция (QPSK).

Когда мы передаем сообщение от источника к приемнику, при передаче данных может произойти ошибка (помехи, неисправность оборудования и пр.). Чтобы обнаружить и исправить ошибку, применяют помехоустойчивое кодирование, т. е. кодируют сообщение таким образом, чтобы принимающая сторона знала, произошла ошибка или нет, и при могла исправить ошибки в случае их возникновения.

По сути, кодирование – это добавление к исходной информации дополнительной, проверочной, информации. Для кодирования на передающей стороне используются кодер, а на принимающей стороне – используют декодер для получения исходного сообщения.

Рассмотрим свёрточный кодер и алгоритм свёрточного декодирования Витерби на примере.

Пусть:
Сверточный кодер:
Параметры свёрточного кодера:
степень кодирования $k/n = 1/2$;
длину кодового ограничения $K = 3$;
векторы связи $\bar{g}_1 = 111$ $\bar{g}_2 = 101$;

Структурная схема кодера изображена на рисунке 3.

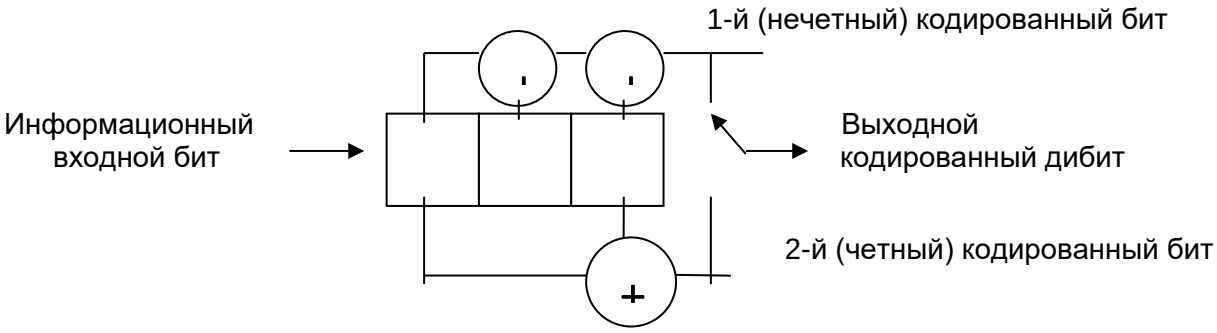


Рис. 3. Структура свёрточного кода

Для примера возьмём входную последовательность:
$m = 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0$.
Решеточная диаграмма свёрточного кодера:

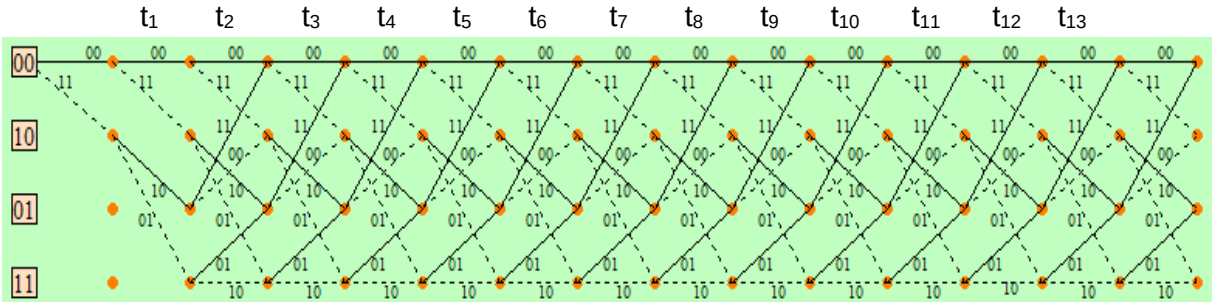


Рис. 4. Решеточная диаграмма свёрточного кодера

$B_{вх}$	1	0	1	1	0	1	0	1	0
$B_{вых}$	11	10	00	01	01	00	10	00	10

Согласно входной последовательности и параметрам кодера, получается выходная последовательность. Так же продемонстрирована работа кодера на решётчетой диаграмме (рис. 4).

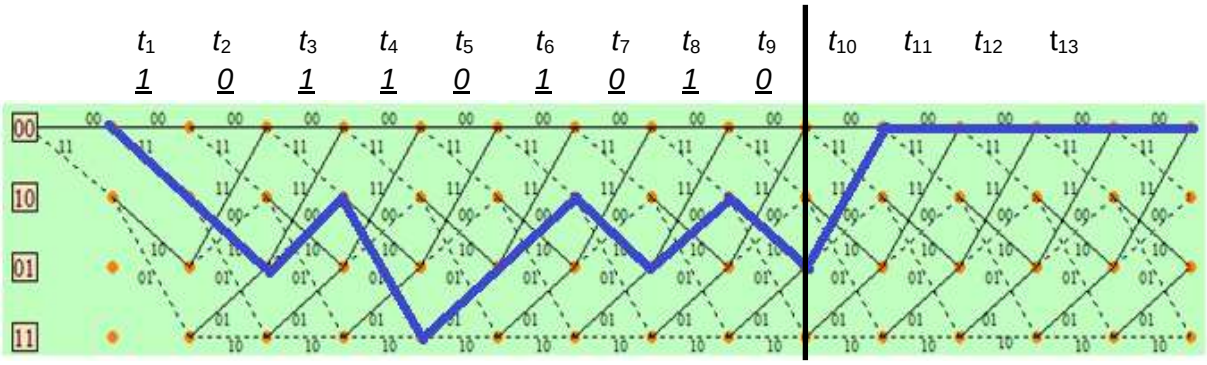


Рис. 4. Решеточная диаграмма свёрточного кодера

Выходная последовательность: u = 11 10 00 01 01 00 10 00 10. На стороне приёмника стоит декодер, который работает по алгоритму Витерби, рассмотрим принцип декодирования. Предположим, что в нашем сообщении произошла ошибка, и, например, во втором тактовом интервале произошла ошибка, тогда, на вход декодера поступает не наша последовательность u = 11 10 00 01 01 00 10 00 10 , а новая:

$$\bar{z} = 1\mathbf{0}\ 10|\ 00|01|01|00|10|00|10$$

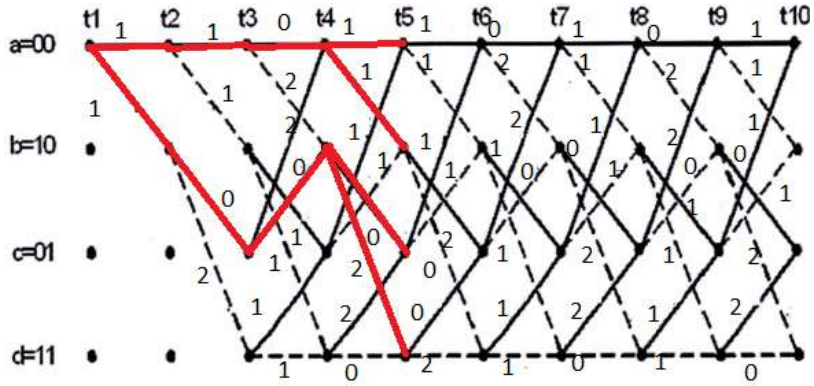
Для наглядности опять рассмотрим свёрточные диаграммы (рис. 5). Декодер рассматривает все пути развития, попутно сравнивая и отсевая пути с большим значением битовой ошибки.

По выжившему пути, перенесенному на решетчатую диаграмму кодера, определить соответствие информационным символам m, которые поступали на вход сверточного кодера, принятых кодовых символов с учетом исправленной ошибки.

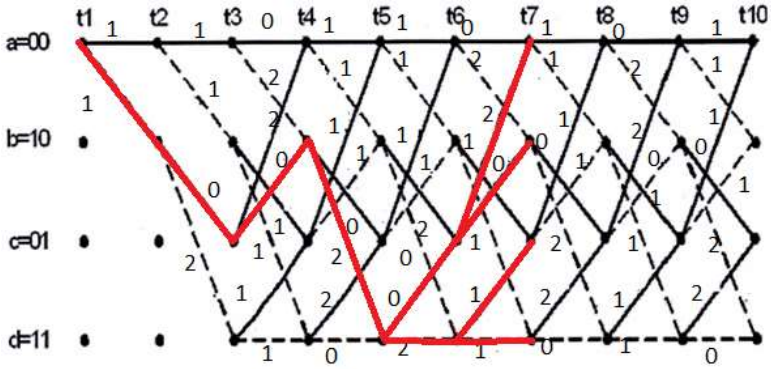
m = 101101010
u = 11 10 00 01 01 00 10 00 10
$\bar{Z}$= 10 10 00 01 01 00 10 00 10
W = 11 10 00 01 01 00 10 00 10

Ошибка исправлена.

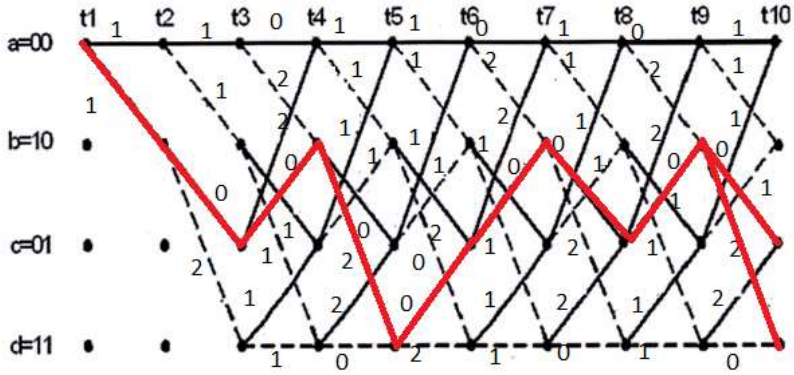
По полученным диаграммам декодера видно, что он раскодировал передаваемую последовательность дебит, причем умышленно внесенная однократная ошибка в позиции 2 была успешно исправлена. Это подтверждает его эффективную и практически значимую работу, следовательно, алгоритм декодирования на основе алгоритма Витерби можно успешно применять на практике.



а)



б)



в)

Рис. 5. Свёрточные диаграммы:
а) – диаграмма декодера на интервале $t_1 - t_5$;
б) –диаграмма декодера на интервале $t_1 - t_7$;
в) – диаграмма декодера на интервале $t_1 - t_{10}$

Таким образом, в данной статье была рассмотрена схема классической радиолинии, рассмотрены разные типы модуляций, выбрана модуляцияв зависимости от поставленных задач. Подробно описана работа свёрточного кодера и декодера по алгоритму Витерби.

Список используемых источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение : пер. с англ. Изд. 2-е, испр. М. : Издательский дом «Вильямс», 2003. 1104 с
2. Richard V. N., Prasad R. OFDM wireless multimedia communication. Artech House Boston London. 2000. 260 p.
3. Дмитриков В. Ф., Сергеев В. В., Самыгин И. Н. Повышение эффективности преобразовательных. М. : Радио и связь, 2005. 423 с.

Статья представлена научным руководителем,
кандидатом технических наук Сагдеевым А. К.

УДК 94

Д. В. Кылосов (студент группы РА-31, СПбГУТ)

ИСТОРИЯ РАЗВИТИЯ ИНСТИТУТА ВОЕННОЙ КАФЕДРЫ В РОССИИ

В работе проведен анализ развития института военной кафедры в России в период с 1926 г. по настоящее время. Работа актуальна в связи поиском методов и форм получения военной специальности студентами гражданских высших учебных заведений, а также с потребностью патриотического воспитания молодежи. Исследование носит обзорно-сравнительный характер, на основе исторических материалов и документов в области военного дела СССР и Российской Федерации.

военная кафедра, военная подготовка.

Высшим учебным заведениям всегда отводилась важная роль в подготовке мобилизационного запаса младших офицеров для Вооруженных сил. Необходимость в военных кафедрах в гражданских вузах была обусловлена созданием резерва младших офицеров на случай военных действий. Подготовка командиров обычно занимает больше времени, чем подготовка солдат и сержантов, поэтому командные кадры готовились в специальных учебных заведениях (училищах и академиях). Количество данных заведений было достаточным для войск мирного времени и увеличивать их число было бы экономически нерентабельно. Исходя из этого, руководство страны пыталось найти оптимальную форму подготовки командиров, которая бы не требовала дополнительных расходов и обеспечивала необходимое количество кадров. Решение было найдено в мировой практике – подготовка резерва в гражданских и средних специальных учебных заведениях.

История военной подготовки студентов высших учебных заведений берет начало 20 августа 1926 г. В этот день Постановлением ЦИК и СНК

СССР для учащихся вузов и техникумов была введена высшая допризывная военная подготовка (ВДВП). Предполагалось, что она станет первой ступенью подготовки средних командных кадров.

Подготовка проходила в 2 этапа. Первый этап – теоретическое обучение в объеме 180 академических часов. Студентами изучались: тактика, топография, огневая подготовка, специальная подготовка и строевая подготовка. Второй этап состоял из практической подготовки (сборов) во время летних каникул в воинских частях сроком 2 месяца. Военное обучение завершалось сдачей экзамена. После прохождения ВДВП и окончания ВУЗа или техникума студенты служили в Рабоче-крестьянской Красной армии (РККА) 9 месяцев или в Военно-Морских Силах Рабоче-крестьянской Красной армии (ВМС РККА) 12 месяцев. Обучающиеся, успешно сдавшие экзамены увольнялись в запас в качестве среднего комначсостава Союзных вооруженных сил. После окончания ВДВП студент, желающий поступить в военное училище или академию, зачислялся на сокращенный курс без вступительных экзаменов.

Одна из основных задач, которую решала высшая допризывная военная подготовка – освобождение будущих высококвалифицированных специалистов от призыва на действительную военную службу и использование их по специальности для нужд страны.

В начале 1926–27 учебного года начались занятия по военной подготовке при 135 ВУЗах и ССУЗах для 80 000 студентов. Одними из первых учебных заведений с ВДВП были МВТУ им. Н. Э. Баумана, МГУ им. М. В. Ломоносова, ВГУ и др.

Следующим этапом в развитии военных формирований в гражданских ВУЗах стало введение высшей вневойсковой подготовки (ВВП) вместо ВДВП в большинстве вузов. Об этом свидетельствует новая редакция постановления ЦИК и СНК СССР «О введении в действие закона об обязательной военной службе» 1930 г. Военная подготовка студентов приравнивалась к действительной военной службе. Это обстоятельство значительно повысило требования к военным кафедрам: раньше военные кафедры лишь подготавливали студентов к призыву в вооруженные силы, то теперь им следовало сделать из военной подготовки воинскую службу.

Как и ВДВП, ВВП делилась на теоретический курс, продолжительностью от 430 до 580 учебных часов, и на военные сборы, на которые отводилось 3–4 месяца на базе воинских частей.

Учебный процесс состоял из 4 периодов:

- 1 период – первые 20 дней после вступительных экзаменов и зачисления абитуриента в университет. Студенты обучались строевой подготовке, изучению личного оружия, освоению приемов его применения в одной из воинских частей или на учебном пункте военкомата – приобретались навыки и умения военнослужащего.

- 2 период – обучение в стенах вуза (1 год), а затем в войсках (2 месяца сборов). На протяжении данного периода студенты получали навыки, соответствующие требованиям к младшим командирам (командиры отделений, расчетов, экипажей).
- 3 период аналогичен второму периоду, только теперь подготовка студентов проходила на более высоком уровне, с учетом требований к средним командирам (командиры взводов).
- 4 период – год обучения в вузе. Повторялся пройденный материал и закреплялись полученные навыки. Подготовку проходили студенты мужского пола годные к действительной военной службе; остальные студенты, а также студентки, посещали занятия по противохимической обороне (ПВХО).

После успешного окончания вуза и полного курса ВВП, студентам присваивали воинское звание среднего начальствующего состава запаса.

По состоянию на 1932 г. подготовка средних командиров запаса осуществлялась в 162 вузах и 49 техникумах страны по 17 военно-учетным специальностям.

По приказу наркома обороны СССР № 0135 от 14 июля 1938 г. в гражданских вузах страны высшая вневойсковая подготовка была упразднена и на смену ей в 1939 г. пришла допризывная военная подготовка студентов. Она была обязательна для всех студентов, как мужчин, так и женщин. Общее руководство допризывной подготовкой студентов было возложено на Наркомат обороны СССР.

В рамках данного вида военной подготовки, студенты изучали программу курса молодого бойца. По очевидным причинам в случае начала войны вооруженные силы нуждались в медицинских кадрах, поэтому в медицинских вузах студенток готовили как помощников среднего медицинского персонала.

Кроме формы обучения поменялся и обучающий персонал. Если раньше это были высококвалифицированные специалисты, готовившие средних командиров, то теперь их использовать было нерентабельно. Они отправлялись на фронт, где могли применить свой опыт и знания, а вместо них набирались специалисты по одиночной подготовке бойца.

Начало Великой Отечественной войны, массовый призыв в действующую армию студентов, эвакуация высших учебных заведений подальше от линии фронта усложнили проведение допризывной подготовки в вузах.

17 сентября 1941 г. было принято постановление № 690 «О всеобщем обязательном обучении военному делу граждан СССР». С 1 октября 1941 г. вводилось обязательное военное обучение граждан СССР мужского пола в возрасте от 16 до 50 лет. Обучение проходило по 110-часовой программе, которая включала в себя строевую подготовку; овладение винтовкой, пулеметом, минометом, ручной гранатой; противохимическую защиту; рытье окопов и маскировку; тактическую подготовку одиночного бойца

и отделения. В качестве инструкторов привлекался средний командный и политический состав, младший начсостав запаса, с отсрочкой от призыва по мобилизации, а также наиболее подготовленный рядовой состав старших возрастов не призванный в армию.

В 1943 г. ситуация на фронте изменилась, численность офицерского состава действующей армии стабилизировалось, но возникла потребность в формировании мобилизационного запаса офицеров среднего звена. Правительство страны решило возобновить подготовку офицеров запаса для Вооруженных Сил в гражданских высших учебных заведениях. Наркомат обороны СССР начал разработку программ подготовки студентов согласно основным профилям вузов. К началу 1943–1944 учебного года были подготовлены программы по 14 профилям.

Окончательно военная подготовка студентов вновь была установлена Постановлением СНК СССР№ 413 от 13 апреля 1944 г. и приказом наркома обороны СССР № 75.

Подготовка была обязательна для всех студентов. Ее целью было воспитать патриотические чувства к Родине и советской власти; создать дисциплинированный, выносливый, физически крепкий и военно-обученный офицерский и сержантский запас Вооруженных сил; подготовить обучающихся, негодных к строевой службе, и девушек к несению тыловой и вспомогательной технической службе в армии.

Обеспечением военной подготовки кадрами, а также учебным оружием, патронами, образцами вооружения, программами, уставами, военно-учебными пособиями занимался Наркомат обороны, всем остальным снабжением занимались народные комиссариаты, в ведении которых состояли вузы. Направление военной подготовки в каждом вузе и программа также утверждались Наркоматом обороны и Комитетом по делам высшей школы при СНК СССР. Около 70 % офицеров, направленных на военные кафедры, были участники Великой Отечественной войны. Они заменили собой офицеров, не имеющих боевого опыта.

В 1967 г. вышел Закон СССР «О всеобщей воинской обязанности» в котором закреплялась отсрочка от военной службы на весь период обучения в вузе. Выпускники, закончившие обучение на военной кафедре, призывались на службы в ряды Вооруженных Сил по ежегодно устанавливаемым квотам сроком на 2 года. Обучение на военной кафедре было обязательно для всех студентов, годных по состоянию здоровья к службе в армии.

В марте 1993 г. был принят закон Российской Федерации «О воинской обязанности и военной службе». В данном законе впервые упоминается о заключении контракта между студентом и военной кафедрой. Таким образом, обучение на кафедре перестает быть обязательным. Также 20 июля 1993 г. выходит Постановление Правительства РФ №690, согласно которому ряд военных кафедр в ВУЗах подлежит расформированию.

С середины 90-х годов начинается реформирование Вооруженных Сил России, результатом которого стало масштабное сокращение числа военных кафедр в стране. По состоянию на 2008 год, в Российской Федерации осталось 35 военных кафедр.

С 2014–2015 учебного года подготовка офицеров запаса осуществляется по новой системе и новым программам, подготовленными Генштабом ВС России. Теперь военная подготовка осуществляется на базе межвузовских центров, созданных на основе действующих военных кафедр. Продолжительность подготовки зависит от военно-учетной специальности и составляет:

- 30 месяцев для офицера запаса
- 24 месяца для сержанта (старшины) запаса
- 18 месяцев для солдата (матроса) запаса.

С момента своего появления в 1926 г. военные кафедры прошли долгий путь развития от подготовки студентов к военной службе до института обучения средних командиров по определенной военно-учетной специальности. Они показали свою эффективность и необходимость в годы Великой Отечественной Войны. В послевоенный период благодаря военным кафедрам у студентов появилась возможность послужить на благо Родине и стать более квалифицированным специалистом по своему профилю обучения. Несмотря на сокращение числа кафедр в стране, они все еще остаются востребованы среди студентов. Появление межвузовских военных центров и новых форм обучения станет новым этапом развития военной подготовки в гражданских вузах.

Список используемых источников

1. Ростов Н. Д. Подготовка офицеров запаса в гражданских высших учебных заведениях Сибири в годы Великой Отечественной войны // Известия Алтайского государственного университета. Сер. История. Политология. 2008. № 4/3. С. 224–229.
2. Иовлев А. М. Деятельность КПСС по подготовке военных кадров. М. : Воениздат, 1976.
3. Русский архив: Великая Отечественная: Приказы народного комиссара обороны СССР. М., 1994. Т. 13 (2–1).
4. О всеобщей воинской обязанности: Закон СССР // Правда. 1939. 1–4 сент.

Статья представлена научным руководителем,
кандидатом исторических наук, доцентом Мосеевым В. И.

УДК 62-05

Е. Д. Лимарева (студентка группы ИКТ-406, СПбГУТ)

РОССИЙСКИЕ ИЗОБРЕТАТЕЛИ ТЕЛЕГРАФА П. Л. ШИЛЛИНГ И Б. С. ЯКОБИ

В статье рассматривается развитие телеграфной связи в России, даны биографические сведения и изобретения российских ученых П. Л. Шиллинга и Б. Я. Якоби, повлиявшие на ход истории в области телеграфии.

оптический телеграф, электромагнитный телеграф, П. Л. Шиллинг, Б. С. Якоби.

Электросвязь в России появилась и начала развиваться в царствование императора Николая I. Он был одним из немногих, кто сумел понять значение открытия принципиально нового вида связи. Он всегда интересовался техническими новинками. До наших дней дошли воспоминания его дочери, великой княжны Ольги Николаевны: «Папа, интересовавшийся всем, что касалось достижений науки, приказал докладывать ему обо всем» [2].

Событие, которое имело колоссальное значение для развития связи в России, а также и далеко за ее пределами, произошло 9 октября (21 октября по новому стилю) 1832 г. в Санкт-Петербурге. В этот день российский ученый Павел Львович Шиллинг устроил первую публичную демонстрацию изобретенного им электромагнитного телеграфа. Для того, чтобы продемонстрировать возможности нового средства связи, в одном крыле дома бы установлен передатчик (там собрались специально приглашенные гости), а приёмник был расположен в противоположном крыле (там находился кабинет П. Л. Шиллинга) на расстоянии около 100 м. Первая телеграмма из 10 слов была передана одним из гостей и практически моментально была принята П. Л. Шиллингом [4].

В дом российского ученого началось настоящее паломничество. Конечно же, самым важным из всех гостей для П. Л. Шиллинга стал император, посетивший его дом в 1835 г. Николай Павлович очень внимательно ознакомился с работой телеграфа, а затем, как и многие посетители дома изобретателя, отправил из одного конца дома в другой телеграмму на французском языке: «Я очарован, сделав визит господину Шиллингу».

Николай I был впечатлен и по достоинству оценил гениальное изобретение, которому в будущем предстояло невероятно ускорить передачу информации на расстояние. Но у П. Л. Шиллинга был только опытный образец, и никто (в том числе и изобретатель) не мог пообещать императору, что первый электромагнитный телеграф будет надежно и исправно работать. А надёжная и оперативная связь была нужна стране [1].

Многочисленные дела не давали П. Л. Шиллингу завершить свои исследования в области телеграфии, начатые еще в 1810 г. и возобновленные

им после 1825 г. Только в 1832 г. он смог завершить работу над телеграфным аппаратом, который быстрыми темпами начал встраиваться в жизнь страны.

Имеется описание изобретения П. Л. Шиллинга, сделанное самим автором примерно в 1837 г.: «Телеграф, мною изобретенный…основан на свойстве, открытом Ерстедом, что магнитная стрелка отклоняется от своего направления, когда поток сомкнутого вольтова столпа движется по самому направлению сей стрелки, …приступаю наконец, к описанию оного:

он состоит:

1ое. Из вольтова столбца.

2ое. Из проводников.

3е. Из умножителя и в соединении с оным находящимся коммутатором.

4ое. Из будильника».

Трудно переоценить заслуги П. Л. Шиллинга, который сумел творчески использовать открытия в области электромагнетизма, сделанные в предшествующие десятилетия. При этом он изучил как новейшие теоретические разработки в области магнетизма и электричества, так и практически все созданные к этому времени приборы. Именно П. Л. Шиллинг был первым ученым, кто смог осуществить передачу информации с помощью электромагнитного телеграфа.

Испытания первой линии электромагнитного телеграфа в России прошли успешно. Отмечалась, что часть линии, которая в течение пяти месяцев находилась под водой, работала бесперебойно. В мае 1837 г. Шиллингу было предложено соединить линией своего телеграфа Петербург с Кронштадтом. Однако произошла невосполнимая потеря, в июле Шиллинг умер, и устройство телеграфной линии было отложено на полтора десятка лет.

Незадолго до своей смерти, на одном из заседаний, которые рассматривали вопрос о телеграфном сообщении между Санкт-Петербургом и Кронштадтом, Шиллинг предложил вешать проволоку на столбах (до этого провода всегда прокладывались под землей). Это предложение было встречено с недоверием, но история подтвердила перспективы в этом направлении.

Академик Б. С. Якоби предложил пишущий телеграф, действовавший в течение трех лет (1839–1842 гг.) между Зимним дворцом и Главным штабом. В 1842 г. приборы академика Якоби были установлены на линии из Петербурга в Царское село и Александрию (недалеко от Петергофа). Вот что вспоминал Б. С. Якоби через два года после кончины императора: «Я счёл бы себя в высшей степени счастливым, если бы... мне было бы суждено иметь дело непосредственно и единственно с Государем императором, высокий ум которого имел лишь в виду будущность и общественную пользу от этого замечательного средства сообщения; который вполне

мог оценить новизну дела и трудности развития его; который с благородной снисходительностью извинял некоторые неизбежные не совершенства аппаратов, поощряя меня к дальнейшей деятельности на пути усовершенствований и соблюдая с мельчайшею точностью правила, установленные для пользования телеграфом».

Николай I вводит государственную регалию на телеграф и одновременно расширяет круг пользователей услугами государственного телеграфа [3].

Содержание телеграфной регалии на телеграф.

К почтам и железным дорогам как способам сообщения людей примыкает телеграф. Телеграф представляет собой скромнейшее, но в то же время и совершеннейшее средство сношений людей между собой, - скромнейшее потому, что дает возможность обмениваться только мыслями, тогда как почта и железные дороги доставляют вещи и даже людей; но вместе с тем и совершеннейшее, так как он, придавая невероятную быстроту передаче мыслей, уничтожает расстояние и делает человека почти вездесущим. Это последнее свойство придает телеграфу такое огромное значение в личном, семейном и особенно торговом и политическом отношениях, что захват его государством в регалию безусловно оправдывается и требуется общественными интересами.

В апреле 2016 г. Павлу Львовичу Шиллингу исполнилось 230 лет со дня рождения. Шиллинг первым в мире доказал возможность практического применения электромагнитных явлений для нужд связи и открыл путь для работ Морзе, Кука и Уитстона.

Рис. 1. П. Л. Шиллинг

Павел Львович Шиллинг – изобретатель, вошедший в историю благодаря работам в области электричества. Он родился в городе Таллинне в семье офицера русской армии в 1786 г. Учился в кадетском корпусе и после недолгой военной службы с 1803-го по 1812 г. работал переводчиком, а затем секретарем в русском посольстве в Мюнхене. Участвовал в сражениях Отечественной войны 1812 г. У Павла Львовича был довольно широ-

кий круг научных интересов, куда входили и «электроминная» техника, и телеграфия, и востоковедение, и криптография, и литография, и кабельная техника. После войны Павел Львович Шиллинг служил в Министерстве иностранных дел. Он изучил литографию и создал первую в России гражданскую литографию для печатания географических карт. После Шиллинг решил заставить электричество служить средством связи [4].

Рис. 2. Б. С. Якоби

В России работу над электромагнитным телеграфом продолжил Борис Семёнович Якоби, который родился в 1801 г. в Германии в Потсдаме, с 1835 г. на русской службе. Он тщательно изучил наследство Шиллинга и к 1839 г. создал несколько оригинальных систем телеграфных аппаратов. Самым важным из них был «пишущий телеграф».

В пишущем аппарате Якоби электромагнит при помощи системы рычагов приводил в движение карандаш. Запись сигналов производилась на фарфоровой доске, которая двигалась на каретке под действием часового механизма. Телеграфный аппарат Якоби в течение нескольких лет успешно работал на «царских» линиях: Зимний дворец – Главный штаб – Царское Село. Однако ученый не был доволен его работой. Зигзагообразные записи принятых депеш трудно поддавались расшифровке, мало удобным было также устройство каретки с экраном.

В течение многих лет Якоби продолжал совершенствование своего изобретения. В 1845 г. он создал абсолютно новую конструкцию стрелочного синхронного аппарата с горизонтальным циферблатом, электромагнитным приводом и прямой клавиатурой. Этот аппарат получил практическое применение в России, в Европе и стал основой для многих других синхронных телеграфных аппаратов. А в 1850 г. Якоби изобрел первый в мире буквопечатающий телеграфный аппарат, работающий по принципу синхронного движения. Это изобретение было одним из крупнейших достижений электротехники середины XIX в. В своем буквопечатающем аппарате изобретатель использовал все основные идеи, успешно реализованные им в стрелочном телеграфе. Это относится, прежде всего, к принципу

синфазности и синхронности, который был впоследствии положен в основу телеграфных аппаратов Д. Юза, В. Сименса и Э. Бодо. Этот принцип сохранил свое значение и для современных буквопечатающих аппаратов [5].

Однако правительство считало изобретение Якоби военным секретом и не разрешало ученому публиковать его описание. О нем даже в России знали немногие.

В 1844 г. Якоби приступает к решению задачи огромного по тем временам масштаба. Департамент железных дорог приглашает его для устройства линии вдоль Петербургско-Московской железной дороги. Якоби предполагал применить здесь ряд своих изобретений. В самый разгар работы Якоби над линией между Москвой и Петербургом министр путей сообщения Клейнмихель и подрядчики отдали прокладку линии иностранным концессионерам Сименсу и другим. К работе над телеграфом Якоби возвращался ещё не раз. В 1850 г. он создает буквопечатающий аппарат – прообраз аппаратов наших дней. Пробить своему изобретению дорогу в широкий мир Якоби не удалось [5].

Телеграфия способствовала объединению финансовых и товарных рынков, уменьшила стоимость передачи информации внутри и между предприятиями. Дальнейшее развитие и использование телеграфного аппарата позволило изменить подход к сбору информации. Сообщения и информация стали распространяться далеко и достаточно быстро. Конечно же, изобретение телеграфии в России – это очень важный этап развития в истории страны, который привел к коренным изменениям в самой телеграфной аппаратуре.

Список используемых источников

1. Тарасов Б. Н. Николай Первый и его время: документы, письма, дневники, мемуары, свидетельства современников и труды историков: в 2-х т. Т. l. М.,2000.
2. Сон юности. Воспоминания великой княжны Ольги Николаевны. 1825–1846 // Николай I: Муж. Отец. Император / Сост., предисл. Н. И. Азаровой. М., 2000.
3. Тимченко-Рубан Г. И. Очерк деятельности великого князя и императора Николая Павловича как руководителя военно-инженерною частью. Т.1: Инженерная организация и техника. СПб., 1912. 498 с.
4. Яроцкий А. В. Павел Львович Шиллинг. 1786–1837. М.: Наука, 1963. 186 с.
5. Яроцкий А. В. Борис Семенович Якоби. 1801–1874. М.: Наука, 1988. 240 с.

Статья представлена научным руководителем,
кандидатом военных наук, доцентом, полковником Мальцевой О. Л.

УДК 004.5

Н. А. Матвиенко (студент группы ИКТК-26, СПбГУТ)

ВОЕННЫЙ ИНТЕРНЕТ В АРМИЯХ РОССИИ И США

В статье рассматриваются, имеющиеся на данное время в вооруженных силах РФ и США, автоматизированные системы управления войсками (АСУВ), а также другое оборудование, использующееся для развертывания сети военного интернета, представлены сведения о новейших разработках современных средств связи для армий России и США.

военный интернет, военная паутина, автоматизированные системы управления войсками.

Армия России

«Военная паутина» объединяет соединения и воинские части от Калининграда до Нижнего Новгорода и от Североморска до Воронежа. Она была опробована в ходе учений войск связи Западного военного округа (ЗВО).

В настоящее время, помимо классических каналов связи, должностным лицам ЗВО доступны современные специализированные электронные коммуникационные сети (передачи данных), позволяющие осуществлять управление войсками в реальном масштабе времени, мгновенно передавать различные текстовые документы, а также фото и видеофайлы неограниченного объема. Кроме того, военный Интернет позволяет проводить видеосвязь командиров и начальников, находящихся в любой точке ЗВО, например, сеансы видеосвязи с экипажами кораблей, выполняющих задачи в Мировом океане. Военный интернет имеет высокую степень защиты от внешнего воздействия и позволяет проводить обмен информацией с гарантированной степенью ее защиты.

Еще одной из особенностей совершенствования Российских армейских систем связи является то, что постепенно в Минобороны переходят от аренды линий связи в Ростелекоме на создание и строительство специализированных линий связи с повышенной стойкостью к несанкционированному доступу. Причина в том, что отечественные операторы имеют тесные связи с зарубежными, что создает предпосылки для нарушения режима секретности, конфиденциальности и повышения вероятности утечки информации. Агрессия США в Югославии и на Ближнем Востоке показали, как интернет может отключаться по приказу силовых ведомств этой страны. В связи с этим весной этого года российские ведомства и силовые структуры имитировали отключение сети интернет и покрыли собственной тропосферной связью площадь, равную 57 Эстониям.

В ходе учений военными связистами округа создана автономная многоуровневая сеть узлов и постов связи, которая связала всеми видами открытой и закрытой связи соединения и воинские части сухопутной составляющей ЗВО, Балтийского и Северного флотов, а также авиационного командования. Для решения поставленных задач связистами округа только тропосферных линий связи было организовано на расстояния более 1,5 тысячи километров. В ходе маневров в режиме онлайн в едином информационном поле было организовано взаимодействие соединений и воинских частей, расположенных во всех уголках ЗВО. Новые подходы к организации систем связи, разработанных с использованием IT-технологий, предусматривают организацию устойчивой и непрерывной работы сетей управления даже в условиях непрерывных помех и возможного применения противником оружия массового поражения. В условиях внешнего противодействия и отключения обычных конечных пользователей интернета (в том числе и военных структур) в России разработан мобильный информационный пункт управления системы «Акация-М (МЭ)», производства концерна «Системпром» [3].

На вид комплекс похож на обычный КАМАЗ с кунгом, но в условиях необходимости этот мобильный пункт трансформируется в оконечный пункт распределения информацией, изменяясь по форме и назначению. Внутри комплекса находится модуль группы командования. Модуль с унифицированными рабочими местами начальников и офицеров родов войск и служб. Затем информация поступает к оконечным получателям информации (солдаты), на персональные терминалы или компьютеры, например, на ноутбуки серии Багет (УКШМ по российским ГОСТам).

Мониторы не имеют собственных вычислительных мощностей. Они подключены к выносным автоматизированным рабочим местам, выполненным на базе переносных защищенных ПЭВМ/ноутбуков. Компьютеры, используемые в комплексе, производятся в Корее, компанией Getac.

Для мобильных пользователей т. е. солдат и офицеров, находящихся в полевых условиях, разработан ряд переносных (планшетные компьютеры) терминалов, например, от производителя ОАО «МКБ «Компас». Командирский планшетник предназначен для решения задач управления и ориентирования в тактическом звене младшего командного состава. Он имеет встроенный СРНС ГЛОНАСС/GPS приемник, интегрированный модуль связи сети широкополосного доступа, интерфейсы: RS-232, RS-485, Ethernet и USB, цветной сенсорный дисплей с диагональю 10, слот для SD карты. Основой специализированных планшетников является материнская плата (и её модификации) МКВ COMPAS OP-8-001 собственной разработки.

Используются планшеты и других производителей, например, мобильный компьютер «Стрелец» от ОАО «Радиоавионика».

Компьютеры могут объединяться в сеть, и командир подразделения на экране своего монитора может следить за перемещениями подчиненных и принимать от них информацию, в том числе о противнике. Бойцу требуется нажать всего несколько кнопок, чтобы передать свои координаты, а также координаты и тип целей противника. Командир может накладывать эти данные как на электронную карту местности, так и на фотографию местности, полученную со спутника в режиме реального времени. В первую очередь такими комплектами будут оснащаться подразделения войсковой разведки России. Операционной системой военных компьютеров выбрана ОС МСВС 3.0. и её модификации.

Армия США

В США принято разделять автоматизированные системы управления войсками (АСУВ) на несколько классов в зависимости от выполняемых системами функций – Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (Команда, Контроль, Коммуникации, Компьютеры, Интеллект, Наблюдение и Разведка).

В настоящее время наиболее известной из всех существующих АСУВ тактического звена является американская система класса – «Force XXI Battle Command Brigade and Below» (FBCB2). Иначе «Система управления бригадой и подчиненными подразделениями в бою (битве) двадцать первого века» [1].

Предполагалось создать надежно функционирующую систему, которая объединяла бы не «перспективные боевые платформы», а уже имеющиеся в войсках средства ведения боевых действий. То есть танки М1 «Абрамс», БМП М2 и БРМ М3 «Бредли», а также БТР М-113. А также, многоцелевые автомобили HMMWV. И в разы повысить их боевую эффективность за счет сокращения цикла боевого управления и повышения ситуационной осведомленности.

На разработку АСУВ FBCB2 в 1996 г. было израсходовано около 47,6 млн долларов. А с 1997 по 2004 г. на доработку системы и устранение выявленных недостатков было потрачено, по различным оценкам, еще от 270 до 385 млн долларов. По некоторым данным общая сумма контрактов, связанных только с разработкой и совершенствованием системы с 1995 по 2010 г. оценивается в 800 млн долларов.

Серийное производство АСУ FBCB2 было налажено с 2002 г. В 2003 г. система получила «боевое крещение» в Ираке в составе 4 механизированной дивизии, получившей после оснащения комплектами FBCB2 прозвище «Digitized» («цифровая»). Все танки и БМП дивизии перед отправкой в зону боевых действий были оснащены соответствующими комплексами системы. Эта версия модернизации танков и БМП получила наименование «SEP» (программа расширения возможностей системы).

По плану до конца 2011 г. аппаратно-программными комплексами (АПК) системы FBCB2 должен быть оборудован каждый танк, БМП, САУ и все командирские автомобили бригад сухопутных войск (армии) США, а также корпуса морской пехоты (всего более 100 000 комплектов). До 2015 г. планируется оснастить носимыми комплексами системы каждого солдата специализированных боевых подразделений.

На декабрь 2011 г. в армию США и корпус морской пехоты уже поставлено около 85 000 комплектов автоматизированных рабочих мест для оснащения пунктов управления и отдельных боевых машин (транспортных средств).

Комплексы системы FBCB2 выпускаются в двух вариантах. Основной – машинное обеспечение на базе компьютера AN/UYK-128 Applique с сенсорными экранами (500МГц/4Гбайт/Windows 95/NT) в особо прочном корпусе), связанное с приемником системы NAVSTAR и цифровой радиостанцией и использующее программное обеспечение боевого управления. Второй вариант – программная версия для встроенных в системы оружия устройств обработки информации.

Оборудование FBCB2 стыкуется с другими бортовыми устройствами и системами боевой машины, (в т. ч. лазерным дальномером), для взаимного опознавания, автоматического формирования сообщений о целях противника и вызова огня.

Программно-аппаратный комплекс может взаимодействовать с различными средствами передачи данных (средствами связи различного диапазона). Обмен данными в «тактическом интернете» производится с использованием систем радиосвязи EPLRS и SINGARS, и системой подвижной спутниковой связи «Инмарсат» L-диапазона.

Такие комплекты являются едиными для всех уровней управления звена «бригада-отделение (танк)» и могут быть смонтированы (развернуты) на полевых пунктах управления бригады (здание, палатка, заглубленный, или защищенный пункт управления), на любом транспортном средстве типа автомобиль, на бронеобъекте (танк, БМП, БРМ, БТР), а также на вертолете [2].

Помимо системного блока, интерактивного дисплея и клавиатуры, которые смонтированы на транспортном средстве, в состав каждого аппаратно-программного комплекса FBCB2 входят еще несколько носимых устройств. Такие устройства получили наименование «FBCB2-Light Handheld». Для крепления выносных устройств непосредственно в машине, предусмотрены специальные гнезда и соответствующие разъемы для его подключения к остальным блокам, а также для подзарядки аккумуляторов.

Кроме навигатора, в состав каждого комплекта входит коммуникатор, позволяющий военнослужащему, находящемуся вне машины, получать (отправлять) короткие текстовые сообщения, принимать и отображать пе-

редаваемые другими комплектами данные о тактической обстановке, определять свое положение с привязкой к электронной карте, а также рассчитывать и отображать на электронной карте кратчайшие пути движения между точками, с учетом наличия дорожной сети.

По мнению американских военных, основными недостатками промежуточных вариантов коммуникаторов были их зависимость от GPS-приемника (они обязательно должны работать «в паре»), небольшая емкость аккумуляторов, а также невозможность для пользователя вносить изменения в тактическую обстановку.

Поэтому, в ходе дальнейшего совершенствования системы было разработано носимое устройство, лишенных таких недостатков. В модернизированном устройстве, коммуникатор совместили с GPS-навигатором, а также внесли в программное обеспечение возможность для пользователя не только получать данные об обстановке, но и самому формировать ее элементы и передавать их другим пользователям, также устройство получило дополнительный аккумулятор, который позволяет работать в течении 12 часов.

Список используемых источников

1. Системы управления, связи и разведки (C4I) Армии США [Электронный ресурс]. URL: http://defence.ru/article/892 (дата обращения 18.04.2016).

2. Автоматизированная система управления войсками в США [Электронный ресурс]. URL: http://vistrel-club.ru/node/242 (дата обращения 22.05.2016).

3. «Военный интернет» в ВС РФ [Электронный ресурс]. URL: http://4pda.ru/ 2012/ 09/21/ 72216 (дата обращения 03.05.2016).

Статья представлена научным руководителем,
кандидатом военных наук, доцентом полковником Мальцевой О. Л.

УДК 62-05

И. С. Першин (студент группы ИКТ-407, СПбГУТ)

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КОСМИЧЕСКИХ АППАРАТОВ В ПОСТРОЕНИИ СИСТЕМАХ СВЯЗИ

В статье рассматриваются основы построения систем спутниковой связи, особенности использование космических аппаратов на различных орбитах. Представлены сравнительные характеристики орбит и их назначение.

космические аппараты, спутниковые системы связи, орбита.

На сегодняшний день потребность в телекоммуникациях очень высока. Если бы современное человечество использовало только наземные средства связи чтобы передавать информацию, то коммутация двух удаленных устройств, потребовала бы значительных средств и развитие сложной инфраструктуры сети. Так же необходимо учитывать, что расстояния между ретрансляторами не могут превышать номинальных размеров, поэтому их расположение связанно не только с большими затратами на запуск и обслуживание, но и с техническими трудностями. Кроме того, такие системы не могут обеспечить качественный канал связи через океан, и труднодоступной местности. Все выше перечисленные минусы наземной связи являются неоспоримыми плюсами для спутниковых систем связи (ССС). Они ретранслируют сигнал прямиком с околоземной орбиты, что позволяет покрывать огромные территории. Благодаря очень высокой пропускной способности ССС обеспечивается бесперебойная связь, 24 часа в сутки 7 дней в неделю, а главное эксплуатация таких сетей экономически рентабельна и обоснована. ССС предлагают пользователям высокоскоростной обмен информацией, параллельную работу сразу нескольких помехозащищенных линий связи.

Впервые идея использования внеземных ретрансляторов связи была предложена в 1945 г. в статье «Внеземные ретрансляторы» английским учёным Артуром Кларком [1]. Но первые ретрансляторы были простыми пассивными отражателями радиосигнала. Они представляли из себя сферу металлическую или полимерную с металлическим напылением и не несли на борту никакого приемо-передающего обнародования. Современные же ССС являются активными. На космическом аппарате (КА) располагают ретранслирующую аппаратуру. За энергообеспечение аппаратуры на КА отвечают солнечные батареи, чего вполне достаточно т. к. перемещение спутника в пространстве-времени практически не требует энерго-затрат. Если космический аппарат расположен на весьма высокой орбите, то он может «покрыть» настолько обширную территорию, достигающую трети от поверхности Земли. Через такой ретранслятор могут связаться все наземные станции, находящийся в зоне покрытия данного спутника. Спутник связи по своей сути является ретранслирующим устройством в тракте передачи сигнала от передающей наземной стронции к оконечной.

Как известно космические аппараты перемещаются по орбитам. Орбиты делятся на 3 основных типа:

1) Полярная.
2) Экваториальная (Геостационарная).
3) Наклонная.

Рассмотрим особенности орбит.

Полярной называется орбита имеющая наклон её собственной плоскости к плоскости экватора. На сегодняшний день эти орбиты чаще всего используют военные и ученые. Военные спутники в основном применяются

для разведки, что же касается гражданско-исследовательских КА, то они служат для получения сведений о состоянии атмосферного слоя, общего изучения, и контроля поверхности Земли. Данный тип орбит имеет неприятную особенность. Так как параметры полета спутника постоянно меняются то для получения качественного сигнала требуется постоянная корректировка и подстройка приемного оборудования, что в разы удорожает такой подход [2].

Какие же орбиты относятся к Наклонным? Наклонными считаются все орбиты отличающийся от экваториальных и полярных, хотя следует отметить, что данный термин можно применить и к нестабильным геостационарным КА т. к. они в ходе своего движения откланяются от расчётной орбиты.

Наибольший интерес представляет геостационарная орбита. Занимающие ее КА имеют ряд преимуществ [3].

Рассмотрим подобрее что же она из себя представляет. Геостационарная орбита-это воображаемое круговое поле имеющее нулевой наклон орбиты, находящийся точно над экватором Земли. Спутник на данной траектории имеет угловую скорость вращения планеты вокруг оси. Его направление в горизонтальной системе координат не изменяется. При движении по этой орбите в восточном направлении совершает вокруг Земли 1 оборот ровно за одни звездные сутки (23 ч 56 мин 4 с) и это позволяет ему «висеть» в одной точке для наземного наблюдателя.

Ни при каких иных параметрах полета нельзя достичь неподвижности КА относительно определенной области на Земле. Данное явление существенно позволяет сэкономить на стоимости ССС. Антенны наземных передатчиков, использующих геостационарный спутник, не нуждаются в системах наведения и слежения за ним, а при необходимости для корректировки колебаний орбиты могут быть установлены специальные устройства.

Так же необходимо отметить что геостационарные системы около полюсов видны под очень острыми углами, а на самих полюсах вообще не видны. Из-за этой особенности на качество передачи влияют: рельеф местности, различные наземные радиосредства [4].

Подводя итог выделим преимущества и недостатки ССС с ретранслятором расположенном на КА с геостационарной орбитой.

Преимущества:

1) отсутствие следящего (сопровождающего) устройства;
2) стабильность и помехозащищенность сигнала в канале;
3) отсутствие эффекта Доплера;
4) организация связи не требует больших затрат.

К недостаткам такой системы можно отнести следующие факторы:

1) использование большого количества спутников на определенных участках орбиты;

2) невозможность покрытия полярных зон.

Список используемых источников

1. Ulybyshev Y. Geometric analysis of low-earth-orbit satellite communication systems: covering functions // Journal of Spacecraft and Rockets. 2000. V. 37. N 3. Pp. 385–391.

2. Аносов А. М., Смирнов А. А., Колосов А. В., Котов А. В. Системы низкоорбитальной спутниковой связи. // Технологии электронных коммуникаций. 1994. Т. 49. С. 6–47.

3. Чернявский Г. М., Бартенев В. А. Орбиты спутников связи. М. : Связь, 1978. 240 с.

4. Аболиц А. И. Информационная эффективность орбит спутников связи. Электросвязь 1996. N 7.

Статья представлена научным руководителем,
кандидатом военных наук, доцентом, полковником Мальцевой О. Л.

УДК 621.39

М. А. Суранова (студентка группы ИКТВ-32, СПбГУТ)

СПОСОБЫ ПОСТРОЕНИЯ ПРИЕМНОГО УСТРОЙСТВА, КАК МЕТОД ЗАЩИТЫ ОТ ПРЕДНАМЕРЕННЫХ ПОМЕХ ПРОТИВНИКА

При воздействии на радиоприемник интенсивных помех возникает перегрузка, вследствие которой приемник перестает реагировать на изменение сигнала. Перегрузки могут возникать: во входных и выходных усилительных каскадах, в УПЧ и демодуляторах.

помехи преднамеренные, усиление, шум, ограничение, амплитуда.

Одним из способов борьбы помехами является – автоматическая регулировка усиление (АРУ)

При работе РУ амплитуда напряжения на выходе УПЧ определяется при помощи детектора АРУ, на который подается еще и напряжение задержки $U_з$, усиливается и усредняется фильтром нижних частот (ФНЧ). Выходное регулирование напряжения $U_р$ управляет коэффициентом усиления УПЧ приемника $К_{упч} = К(U_р)$ с тем, чтобы поддерживать сигнал на выходе демодулятора на постоянном приемлемом уровне

$$U_{\text{вых}} = \text{К}(U_{\text{р}})U_{\text{вх}} \qquad \textit{при } U_{\text{вых}} \geq U_{\text{з}}$$

Таким образом, задержка срабатывания $U_{\text{з}}$ – это пороговый уровень входного сигнала, по превышении которого амплитудной сигнала срабатывает система АРУ.

АРУ «вперед». Данный метод эффективно использовать при защите от помех, которые имеют длительность больше, чем импульсы сигнала ($\tau_{\text{п}} > \tau_{\text{с}}$). Структурная схема такой системы АРУ показана на рисунке 1. Здесь постоянная времени $\tau_{\text{АРУ}} = \frac{1}{\Delta F_{\text{ф}}} > \tau_{\text{с}}$. В этот момент времени, когда приходит импульс сигнала длительностью $\tau_{\text{с}}$, коэффициент усиления видеоусилителя $\text{К}(E_2) = max$, а при приходе длинного импульса помехи ($\tau_{\text{п}} > \tau_{\text{с}}$).резко уменьшается и помеха на выходе ослабляется.

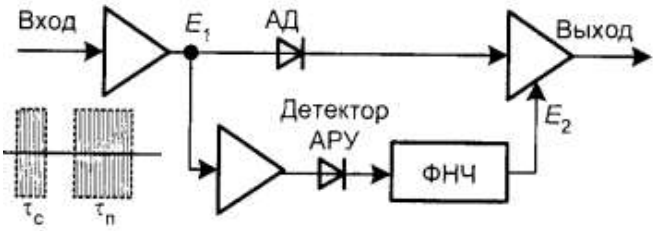


Рис. 1. АРУ «вперед»

АРУ «по ближним шумам». Это быстрая автоматическая регулировка усиления (БАРУ) по шумовой помехе, предшествующей появлению сигнала. Принцип действия БАРУ показан на осциллограмме рисунке 2.

В данном случае, если принят сильный сигнал $g = \frac{P_c}{P_{\text{п}}} > 1$, а усиление $\text{К}_{\text{р пм}}(P_{\text{ш}})$ установилось по шумовой помехе относительно более низкого уровня, сигнальный импульс пройдет на выход. Иначе, если в аналогичной ситуации принят слабый сигнал ($g < 1$), этот импульс будет практически подавлен, т. е. за счет работы схемы АРУ отрезок шумовой помехи, предшествующий и последующий импульсу сигнал, вырезается, подчеркивая при этом полезный сигнал $g > 1$.

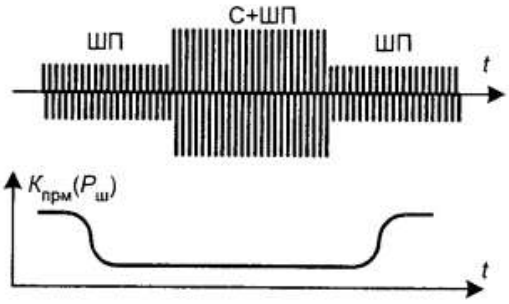


Рис. 2. АРУ по «ближним шумам»

Медлеиная АРУ (МАРУ) имеет постоянную составляющую времени $\tau_{\text{АРУ}} = \tau_c$. При таком условии импульс сигнала с меняющейся за время τ_c амплитудой $\text{E}_\text{c}(t_c), t \in [0, \tau_c]$ поддерживапется на выходе постоянным. Это защищает приемник от мощных импульсных помех. Схема работает и при $\tau_{\text{ПХ}} = \tau_c$, т. е. защищает приемник от длинных помеховых импульсов (например, создаваемых облаками дипольных отражателей).

АРУ с многократными стробами обеспечивает получение постоянного уровня выходного сигнала приемника $\text{E}_{\text{с вых}} = cons$ в широком диапазоне амплитуд входных сигналов от $\text{E}_{\text{с вых}\,min}$ до $\text{E}_{\text{с вых}\,max}$. Дя этого управляющий сигнал выбирают ступенчатым, $U_{\text{АРУ}} = k\Delta U_{\text{АРУ}}, k = var$, и регулировки усиления проводятся либо до прихода импульса сигнала, либо во время действия этого импульса, а так же на максимальной дальности работы РЛС.

Детектор с обратным смещением – это такой вариант АРУ, который обеспечивает постоянство амплитуды выходного сигнала приемника $\text{E}_{\text{с вых}} = cons$ при любом входном амплитудно-модулированном сигнале. Схема ослабляет импульсные помехи с большой длительностью, когда $\tau_\text{п} \gg \tau_\text{c}$ (помехи от облаков дипольных отражателей), вплоть до непрерывных шумовых помех.

Другой способ снижения риска перегрузок помехами – применение ограничителей.

Ограничитель сверху по уровню E_c такой способ используется для борьбы с импульсными помехами, у которых амплитуда значительно превышает амплитуду,$\text{E}_\text{п} \gg \text{E}_\text{c}$. При помощи преобразования суммы сигнала с помехой мощные импульсы на выход не проходят. Вследствие преобразования суммы сигнала с помехой мощные импульсы помехи на выход схемы ограничителя не проходят.

Двухпороговое ограничение применяется для помехозащиты канала обнаружения (рис. 3).

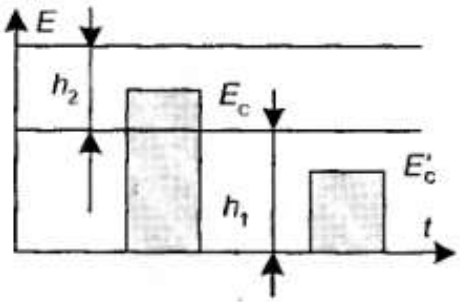


Рис. 3. Двухпороговое ограничения

Сначала работает каскад ограничителя с первым пороговым уровнем h_1. Такой селектор пропускает сигнал с амплитудой E_c и отсекает импульсы с $\text{E}_\text{c} < h_1$ и $\text{E}_\text{c} > h_1 + h_2$.

Ограничители снизу может применяться для подавления слабых помех. У ограничителей снизу (рис. 4) на выход проходят сигналы с $E_c > h_0$, а более слабые шумовые импульсные помехи $x < h_0$ подавляются.

Рис. 4. Ограничение снизу

Амплитудно-частотная селекция с помощью схем ФОФ или ШОУ. Схемы ФОФ (фильтр-ограничителей-фильтр) или ШОУ (широкополосная-ограничитель-узкополосная) Сущность данной схемы заключается в том, что для подавления импульсной помехи используется амплитудный ограничитель, который включается между двумя фильтрами (рис. 5)

Рис. 5. Схема с использованием амплитудного ограничителя между двумя фильтрами

Данная схема позволяет решить несколько задач:

Первое назначение – подавление мощных импульсных помех с сохранением удовлетворительной избирательности относительно узкополосных помех.

Первый из этих фильтров, называемый широкополосным, обеспечивает отсеивание сосредоточенных помех, расположенных на оси частот достаточно далеко от спектра сигнала, но имеет полосу пропускания $F_ш$более широкую, чем полоса частот F_y занимаемая сигналом (рис. 6).

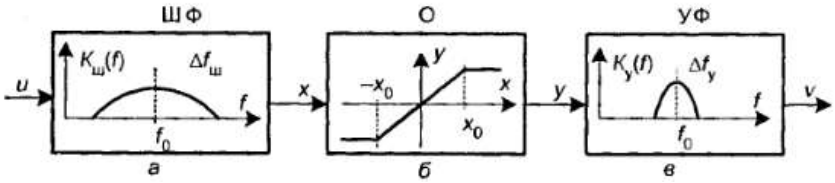


Рис. 6. Амплитудно-частотная селекция с помощью схем ФОФ или ШОУ

Сосредоточенные помехи попадают в полосу пропускания $F_ш$ с большей вероятностью, чем в полосу частот F_y. Однако вероятность того, что в полосе пропускания $F_ш$ будет много мощных сосредоточенных помех, которые на выходе ограничителя создадут комбинационные частоты,

попадающие в спектр сигнала, невелика, так как $F_ш$ не намного больше$F_у$. Все же помехи, которые прошли через широкополосный фильтр и ограничитель, не следует пропускать на решающую схему, поскольку они могут вызвать ошибки. Для этого служит узкополосный фильтр, с полосой пропускания $F_у$, завершающий функции частотной избирательности, в частности, узкополосный фильтр может быть согласован с сигналом

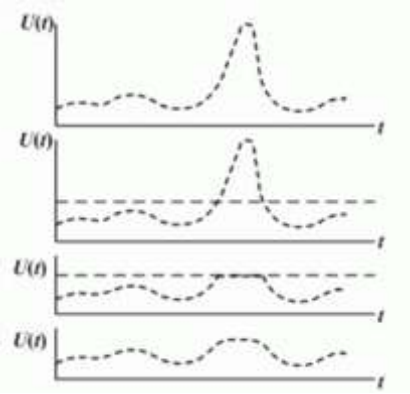


Рис. 7. Изменение огибающей импульса
в схеме ШОУ

В схеме ШОУ всегда предусматривается большой запас усиления после узкополосного фильтра. Это связано с тем, что иногда мощная помеха, прошедшая через широкополосный фильтр может при прохождении через ограничитель уменьшить мощность сигнала. Даже после подавления помехи в узкополосном фильтре, мощность сигнала окажется недостаточной для его нормального функционирования в дальнейшем

Для пояснения физического процесса подавления импульсной помехи в схеме ШОУ на рис. 8 показаны изменения огибающей импульса. На выходе широкополосного фильтра импульс имеет большую амплитуду, но относительно малую длительность. Ограничитель «срезает» амплитуду импульса и делает ее равной амплитуде сигнала, но не изменяет его длительности. В узкополосном фильтре длительность импульса увеличивается примерно в $\frac{F_ш}{F_у}$ раз и во столько же раз уменьшается его амплитуда. Благодаря этому амплитуда импульсной помехи на выходе схемы ШОУ оказывается приблизительно в $\frac{F_ш}{F_у}$ раз меньше амплитуды сигнала и не вызывает ошибок.

Второе назначение ФОФ – помехозащита приемников сигналов с угловой модуляцией от шумовых и других широкополосных помех.

Третье – стабилизация вероятности ложных помех $P_{лт}$ на выходе.

Среди нелинейных устройств подавления радиопомех широко распространены различные модификации приемников с логарифмическими амплитудными характеристиками усилителей промежуточной частоты

(рис. 8). Поскольку в области $U_{вх} < 1$ характеристика вида $y = log_a x$ при любом $a > 1$ нереализуема (при $(x \to 0, y \to \infty)$, для логарифмических усилителей выбирают характеристику, аппроксимируемую функцией $log_{10}(1 + x)$. Точка $x = 0$ на такой характеристике соответствует выходной сигнал $y = 0$.

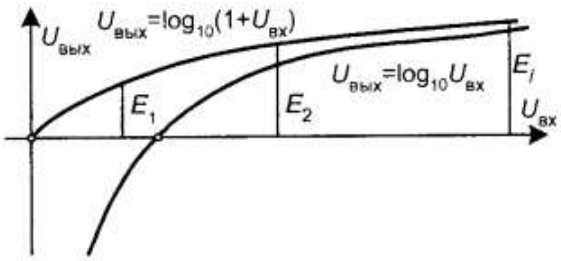


Рис. 8 Логарифмическая характеристика приемника

Список используемых источников

1. Тактико-специальная подготовка. Лекция 2: Связь как основное средство управления войсками. Основные задачи связи. Рода и виды связи [Электронный ресурс]. Военное образование в России: [сайт]. URL: http://voenobr.ru/uchmaterial/lections/133-tsp2.html?start=2

2. Составными частями радиоэлектронной борьбы являются радиоэлектронное поражение, радиоэлектронная защита и радиоэлектронно-информационное обеспечение [Электронный ресурс]. Студопедия – ваша школопедия: [сайт]. URL: http://studopedia.ru/1_54094_sostavnimi-chastyami-radioelektronnoy-borbi-yavlyayutsya-radioelektronnoe-porazhenie-radioelektronnaya-zashchita-i-radioelektronno-informatsionnoe-obespechenie.html

3. Орлов И. Я. Перспективные методы защиты информационных радиосистем от помех: учеб. метод. пособие. Н. Новгород : изд-во ННГУ, 2006. 126 с.

4. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: монография. СПб. : Свое издательство, 2013. 166 с.

5. Куприянов А. И., Сахаров А. В. Теоретические основы радиоэлектронной борьбы: учеб. пособие. М. : Вузовская книга, 2007. 356 с. ISBN 5-9502-0223-6.

Статья представлена научным руководителем Александровым В. А.

УДК 654.026

К. С. Чубарев (кандидат военных наук, профессор, ВАС)
В. Н. Щербаченко (слушатель, ВАС)

ПОВЫШЕНИЕ МОБИЛЬНОСТИ ПОЛЕВЫХ ПОДВИЖНЫХ УЗЛОВ СВЯЗИ

В работе представлена методика расчета времени развертывания пункта управления объединения построенного по модульному принципу. Методика учитывает тип аппаратных(станций) связи, их количество в составе узлов связи, укомплектованности экипажей, а также природно-климатические и метеорологических и других факторов.

мобильность, норматив, подвижный узел связи, трудозатраты на развертывание, системы специального назначения.

Обеспечение своевременности связи в системах управления специального назначения в значительной степени зависит от мобильности полевых подвижных узлов связи, под которой понимается способность данных узлов связи в установленные сроки развертываться, свертываться, перемещаться, изменять структуру.

Требуемое время выполнения задач подвижными узлами связи определяется конкретной обстановкой или утвержденными нормативами, содержание которых отражено в соответствующих сборниках для различных элементов системы связи.

Согласно сборнику нормативов, подвижный узел связи считается развернутым (свернутым) если выполнен определенный комплекс мероприятий [1].

Узел связи считается развёрнутым, если:

- все элементы узла связи развёрнуты и аппаратные соединены между собой линиями;
- линии дистанционного управления развернуты, отрегулированы образованные на них каналы и проверено управление передатчиками без выхода в эфир;
- проложены абонентские линии, установлены абонентские аппараты и проверено качество связи с телефонистом коммутатора на прохождение вызова и разговора;
- организована служебная связь на узле;
- развёрнута регламентно-техническая группа;
- установлена связь с элементами транспортной сети связи, от которых будет производится приём каналов;
- организовано выполнение мероприятий всестороннего обеспечения.

Узел связи считается свёрнутым, если:

- все элементы узла свернуты;
- вспомогательное имущество, оборудование и соединительные кабели уложены и находятся в готовности к применению;
- аппаратные (станции) находятся в колонне, автомобильная техника заправлена и готова к совершению марша;
- командно-штабные машины и личные радиостанции должностных лиц подготовлены к работе в движении;
- установлена связь управления узлом связи на марше;
- все важные документы в наличии;
- начальник узла связи доложил об окончании свёртывания узла и готовности к совершению марша.

Повышение мобильности узла связи, других элементов системы связи, достигается различными способами и мероприятиями, основными из которых являются: правильное уяснение полученных задач по связи и доведение их исполнителям; совершенствование способов действий подразделений связи; своевременное выдвижение и готовность подвижных объектов связи к наращиванию системы связи; оперативный маневр силами и средствами связи; механизация и автоматизация работ при развертывании (свертывании) узлов и линий связи; применение средств и комплексов связи на летно-подъемных средствах и в контейнерном исполнении; использование средств автоматизации при планировании, установлении и обеспечении связи; разработка типовых схем развертывания узлов связи и распределения (закрепления) каналов связи; сопрягаемость стационарных и полевых элементов систем связи различных уровней управления и др.

Наиболее эффективными, на наш взгляд, являются мероприятия по повышению мобильности узлов связи за счет тренировок экипажей аппаратных (станций) и подразделений связи в выполнении установленных нормативов.

Норматив – это величина времени, необходимого для выполнения в заданной последовательности действий и работ на технике связи при организации и обеспечении связи среднеподготовленным специалистом, аппаратной (станцией), центром или узлом связи в целом [1].

Нормативы по развертыванию подвижных объектов связи необходимы, в первую очередь, для контроля и, соответственно, повышения уровня подготовленности отдельных специалистов, экипажей, элементов узлов связи. Кроме того, наличие нормативов позволяет улучшить организацию взаимодействия между специалистами разных специальностей, между экипажами и подразделениями и, тем самым, добиться сокращения сроков и повышения качества выполнения комплексных задач. Немаловажным фактором также является то, что наличие нормативов позволяет в процессе планирования рассчитать сроки ввода в действие отдельных элементов си-

стемы связи и, на этой основе, принимать обоснованные решения, ставить исполнителям конкретные задачи.

По аналогии с сетями электросвязи специального назначения наличие нормативов по развертыванию подвижных объектов связи в сетях связи других категорий (сетях связи общего пользования, выделенных сетях связи, технологических и других сетях связи) также может способствовать более качественному выполнению задач при использовании мобильного компонента данных сетей [2].

В зависимости от типа аппаратных (станций) связи, их количества в составе узлов связи, укомплектованности экипажей, а также от физико-географических, метеорологических и других факторов рассчитываются конкретные нормативы на совершение марша и развертывание (свертывание) данных узлов связи или других элементов системы связи. Расчёт осуществляется через соответствующие трудозатраты (в человека-часах) на развертывание конкретного подвижного объекта связи.

В существующих сборниках имеются нормативы не на все ныне существующие средства и комплексы связи, поэтому предлагается следующий путь разработки отсутствующих нормативов.

1. Составляется и оптимизируется в процессе тренировок сетевой и линейный графы развертывания аппаратной.

Исходными данными для составления сетевого графа является состав экипажа, время выполнения отдельных первичных работ и последовательность их выполнения при развертывании аппаратной.

В качестве примера содержание и объем работ по развертыванию аппаратной А-1 представлены в таблице 1 (фрагмент), сетевой и линейный графы – на рисунке 1 (фрагмент).

ТАБЛИЦА 1. Содержание и объем работ по развертыванию аппаратной А-1

Код работ	**Содержание работ**	**Трудозатраты (чел.-мин)**
0	Начало развертывания	-
0 – 1	Установка аппаратной на место развертывания	6
1 – 2	Оборудование заземления и подключение его к аппаратной	4
1 – 3	Сборка антенны, установка и мачты	16
…	…	…
5 – 7	Прием кабельных линий от других аппаратных	4
…	…	…
6 – 8	Подготовка аппаратуры к работе и проверка «на себя»	10
…	…	…
19 – 21	Доклад о выполнении работ	2

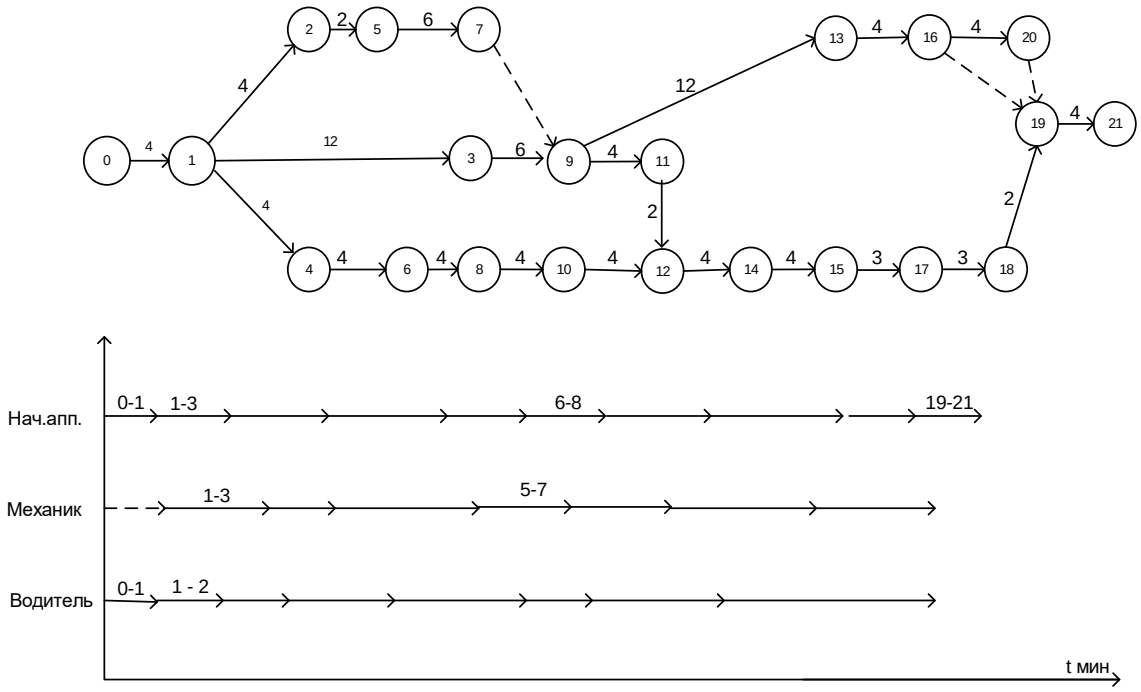


Рис. 1. Сетевой и линейный графы развертывания аппаратной А-1

2. Определяется математическое ожидание и среднее квадратичное отклонение времени развертывания аппаратной.

Исходными данными являются временные затраты на развертывание аппаратной по результатам не менее десяти замеров (развертываний).

3. Определяется объем трудозатрат (чел. мин.) на развертывание аппаратной, как сумма трудозатрат на выполнение отдельных работ.

Аналогичным образом рассчитываются трудозатраты для других подвижных аппаратных связи.

Объемы трудозатрат по каждой аппаратной связи является исходными данными для расчета времени развертывания всего узла связи, используя известные методики.

Список используемых источников

1. Градусов Р. А., Касанин С. Н. Организация и структура полевых узлов связи объединения: учебно-методическое пособие. Минск: БУИГР, 2012. 119 с.

2. О связи: федер. закон Рос. Федерации от 7 июля 2003 г. № 126–ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2006 г.

УДК 004.942, 621.39

Т. Р. Ялунина (студентка группы ИКТО-31, СПбГУТ)

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ НЕЛИНЕЙНЫХ ЭФФЕКТОВ В ОПТИЧЕСКИХ ВОЛОКНАХ

В связи с внедрением систем спектрального уплотнения и увеличением требуемой мощности передаваемого сигнала, достигающей уже 30 дБм, влияние нелинейностей оптических волокон становится существенным: их проявление на таких высоких мощностях вносят значительные искажения в передаваемый сигнал, тем самым, снижая достоверность и ограничивая длину регенерационного участка. Проводить экспериментальные исследования нелинейностей затруднительно, что обусловлено одновременным проявлением нескольких эффектов и необходимостью применения сложных и дорогостоящих приборов. Компьютерное моделирование упрощает процесс исследований, расширяя возможности исследования оптических систем связи.

компьютерное моделирование, оптическое волокно, нелинейные эффекты, четырехволновое смешение, DWDM.

Нелинейные эффекты являются одним из факторов, ограничивающих длину регенерационного участка и пропускную способность волоконно-оптических линий связи. Они обусловлены передачей достаточно большой мощности света. При малых мощностях взаимодействие света со средой представляет собой линейный эффект: оно пропорционально первой степени мощности света. Нелинейные же эффекты пропорциональны более высоким степеням мощности света и значительно увеличиваются с ее ростом [1].

Существует два свойства оптических волокон, обуславливающие высокую эффективность протекания в них нелинейных процессов: концентрация света на маленькой площади вблизи сердцевины волокна и сохранение высокой концентрация света на всей длине волокна.

Проявление нелинейных эффектов в системах связи может выражаться в изменении формы сигнала, вызванном фазовыми и амплитудными нелинейными искажениями, в появлении новых спектральных компонент и в нелинейном шуме – случайных отклонениях значений символа от его среднего значения.

Основные типы нелинейных эффектов можно разделить на неупругие и упругие взаимодействия. В данной работе проанализированы именно упругие взаимодействия. Они обусловлены зависимостью показателя преломления от интенсивности света (эффектом Керра). К ним относятся: четырехволновое смешение (FWM – *Four Wave Mixing*), фазовая самомодуляция волн (SPM – *Self-Phase Modulation*), модуляционная нестабильность (MI – *Modulation Instability*) и перекрестная фазовая модуляция (XPM – *Cross Phase Modulation*) [2].

Эти явления могут приводить к значительным изменениям ширины и формы импульсов, а также к появлению перекрестных помех, зависящих от количества каналов, которые используются в DWDM-системе [3].

При проведении исследования была использована программа OptiSystem, позволяющая моделировать нелинейные эффекты, протекающие как совместно, так и независимо друг от друга. Были рассмотрены все виды упругих взаимодействий, оценены зависимости нелинейностей от параметров системы и сделаны выводы о совпадении результатов, полученных с помощью программы, с ожиданиями, основанными на теоретических справках. В связи с однотипностью алгоритма исследования, рассмотрим моделирование на примере только одного из исследуемых нелинейных эффектов – четырехволновом смешении. Этот вид искажений возникает при нелинейном взаимодействии волн с близкими частотами. Некоторые из вновь генерируемых комбинационных частот попадают в спектральные каналы DWDM системы, что приводит к перекрестным помехам. Количество вновь появившихся паразитных волн быстро увеличивается с ростом числа спектральных каналов. Основной же вклад в перекрестные помехи дают соседние каналы, так как влияние удаленных каналов быстро уменьшается из-за нарушения фазового синхронизма. Схема моделирования четырехволнового смешения в программе OptiSystem представлена на рисунке 1.

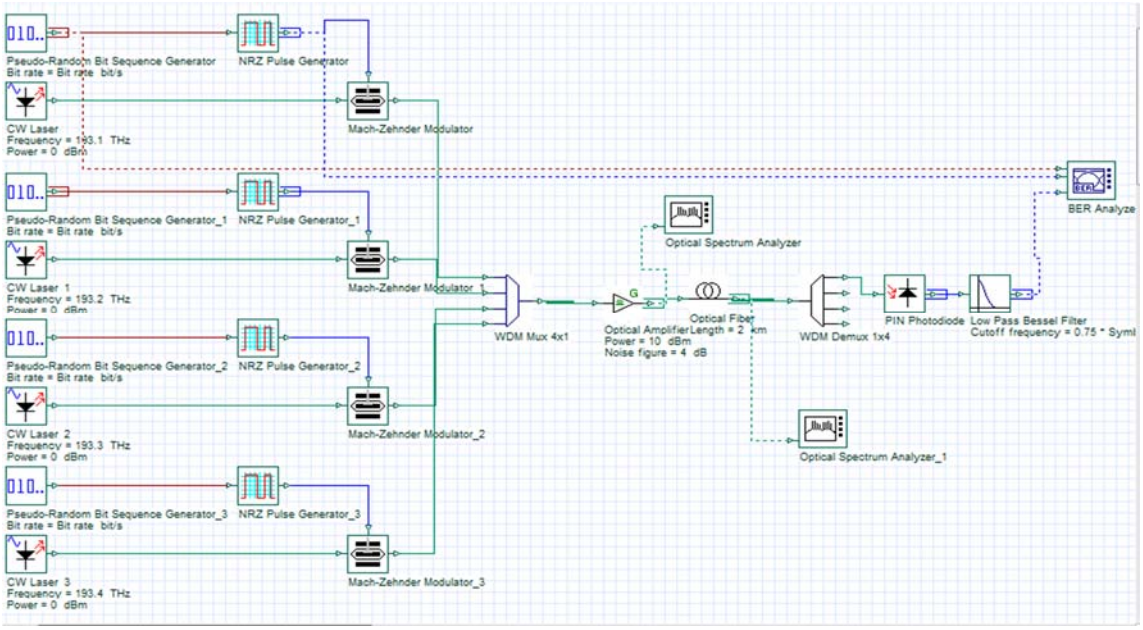


Рис. 1. Схема моделирования четырехволнового смешения

На схеме представлена четырехканальная DWDM-система с оптическим усилителем, изначально установленным на усиление по мощности до 10 дБм, 2 км оптического волокна, система преобразования оптического сигнала в электрический для одного канала,

спектральные анализаторы, установленные до и после прохождения сигнала по волокну, и BER Analyser для оценки качества связи.

В процессе проведения исследования были оценены зависимости вклада четырехволнового смешения от таких параметров системы, как: мощность передаваемого сигнала (10 дБм, 15 дБм, 20 дБм), коэффициент хроматической дисперсии (16,75 пс/(нм·км), 1 пс/(нм·км)), площадь модового пятна (80 мкм^2, 55 мкм^2), длина волокна (2 км, 20 км).

На основании моделирования были сделаны выводы, что влияние четырехволнового смешения зависит от передаваемой мощности и от коэффициента хроматической дисперсии. На рисунках 2 и 3 приведены спектры сигналов после прохождения по волокну при разных условиях.

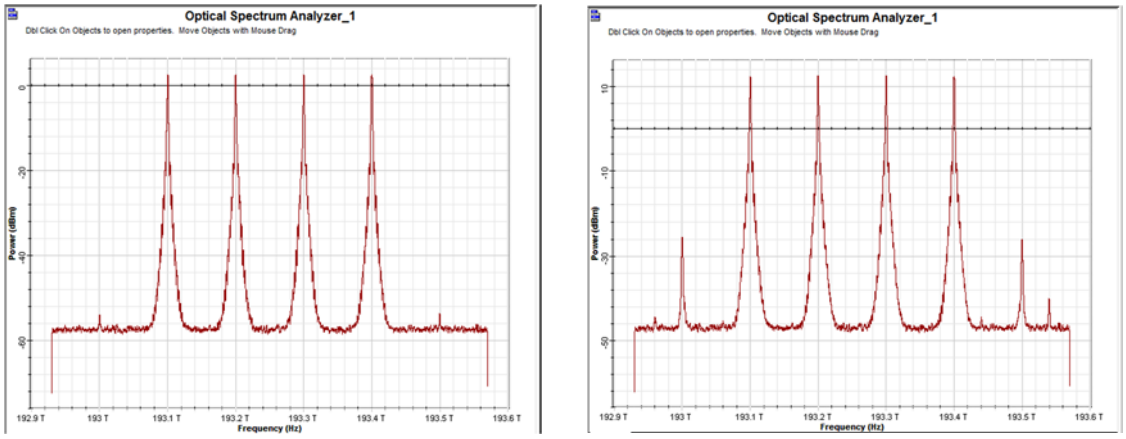


Рис. 2. Спектр сигнала после прохождения по волокну при 10 дБм и при 20 дБм

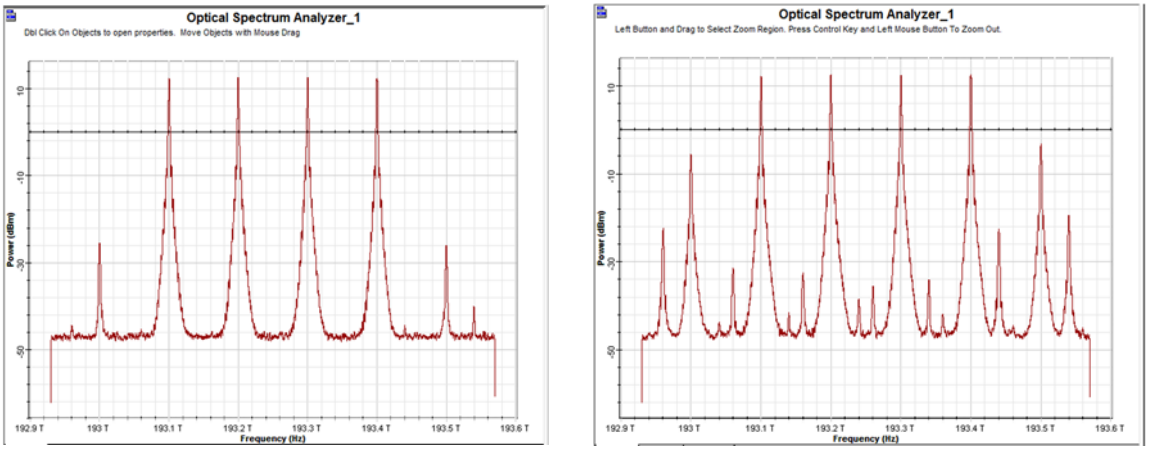


Рис. 3. Спектр сигнала после прохождения по волокну при хроматической дисперсии, равной 16,75 пс/(нм·км) и 1 пс/(нм·км) соответственно

На рисунке 4 приведены рассчитанные спектры сигналов при уменьшении площади модового пятна ($A_{эфф}$ = 80 мкм^2 и $A_{эфф}$ = 55 мкм^2). Увеличение эффектов четырехволнового смешения объясняются тем, что коэффициент нелинейности обратно пропорционален $A_{эфф}$:

$$\gamma = (2\pi/\lambda)\,(n_2/A_{эфф}).$$

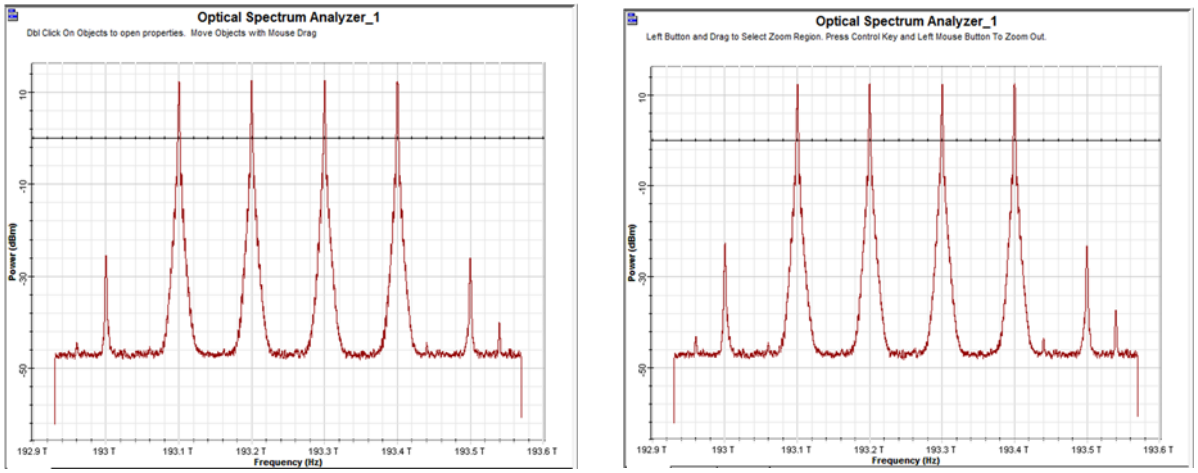


Рис. 4. Спектр сигнала после прохождения по волокну при площади модового пятна, равной $A_{эфф}$ = 80мкм^2 и $A_{эфф}$ = 55мкм^2 соответственно

По результатом моделирования также сделан вывод, что четырехволновое смешение практически не зависит от длины волокна. На рисунке 5 приведен спектр на выходе волокна, который не меняется от увеличения его длины с 2 км до 20 км соответственно.

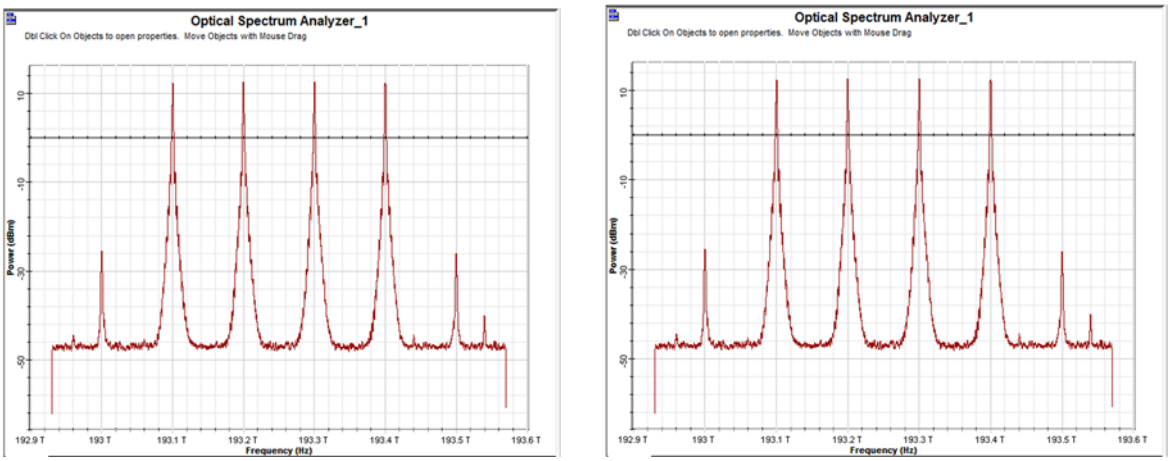


Рис. 5. Спектр сигнала на выходе волокна при длине волокна, равной 2 км и 20 км соответственно

Это связано с тем, что существует эффективная длина взаимодействия $L_{вз}$, характеризующая длину, в пределах которой проявляется четырехволновое смешение. Соответственно увеличение длины волокна не способствует его увеличению.

Результаты моделирования позволяют пронаблюдать логику появления новых спектральных составляющих. Количество паразитных спектральных составляющих определяется выражением: $K = N2(N-1)/2$, где N – число задействованных каналов системы передачи. Если смоделировать трехканальную систему, с частотами 193,1 ТГц; 193,2 ТГц; 193,4 ТГц, то количество вновь генерируемых компонент равно 9, а проявятся они

на комбинаторных частотах $f_i, \pm f_j \mp f_k$: 192 8 ТГц; 192 9 ТГц; 193 0 ТГц; 193 0 ТГц; 193 3 ТГц; 193 3 ТГц; 193 5 ТГц; 193 6 ТГц; 193 7 ТГц. На рисунке 6 представлен спектр сигнала до прохождения по волокну и после.

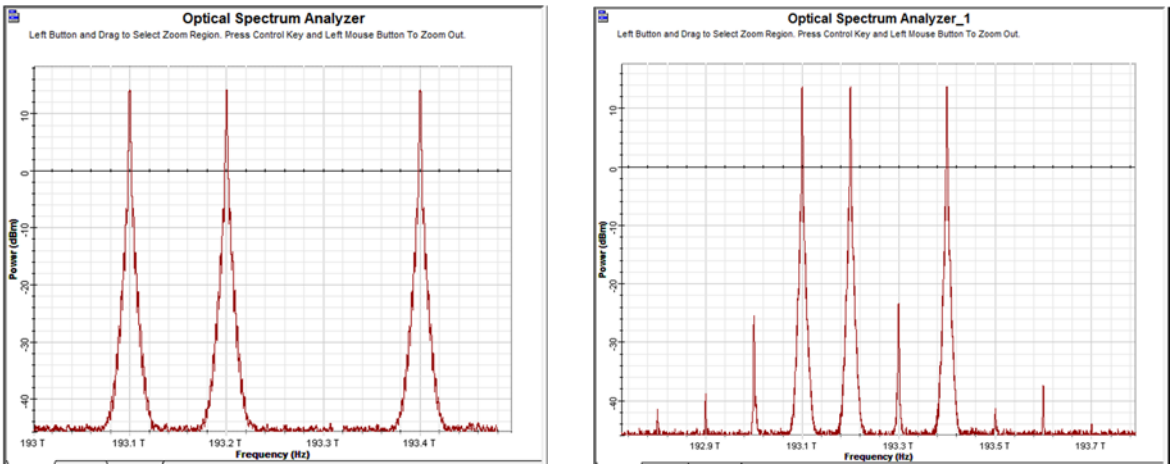


Рис. 6. Спектр сигнала трехканальной DWDM-системы
до и после прохождения по волокну

Таким образом, компьютерное моделирование позволяет проводить наблюдения за совершенно разными явлениями в системах связи, что было продемонстрировано на примере эффектов четырехволнового смешения. Существует возможность создавать системы с неограниченным разнообразием параметров, моделировать эффекты, протекающие совместно или независимо друг от друга. Это очень упрощает процесс исследования и экономит время.

Список используемых источников

1. Агравал Г. Нелинейная волоконная оптика: пер. с англ. / Под ред. П. В. Мамышева. М. : Мир, 1996. 324 с.

2. Листвин А. В., Листвин В. Н., ШвырковД. В. Оптические волокна для линий связи. М. : ЛЕСАРарт, 2003. 106 с. ISBN 5-902367-01-8.

3. Леонов А., Наний О., Трещиков В. Нелинейные искажения и нелинейный шум в когерентных сетях связи // Первая миля. 2014. № 4. С. 51–55.

Статья представлена научным руководителем,
кандидатом технических наук Дюбовым А. С.