ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича»

На правах рукописи

КУЛИК ВЯЧЕСЛАВ АНДРЕЕВИЧ

РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ КОМПЛЕКСНОГО ТЕСТИРОВАНИЯ СИСТЕМ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Специальность 05.12.13 — Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук
Киричек Руслан Валентинович

Санкт-Петербург — 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. В настоящее время активное развитие получила концепция, связанная с построением сетей нового поколения и называющаяся концепцией Интернета вещей (ИВ). Данная концепция связана с разработкой и внедрением встраиваемых вычислительных устройств, которые будут использоваться для автоматизации множества сфер человеческой жизнедеятельности, таких как медицина, логистика, управление городской инфраструктурой, беспилотный транспорт, автоматизация управления домашним хозяйством и другое. Предполагается, что устройства Интернета вещей станут внедряться повсеместно, десятками тысяч устройств на одного человека. Огромное количество устройств создаст повышенную нагрузку на существующее сетевое оборудование. В связи с этим предполагается, что существующая сетевая инфраструктура не сможет справиться с постоянно возрастающим количеством вычислительных устройств, подключенных к сетям связи общего пользования, поэтому концепция Интернета вещей также включает в себя вопросы разработки подходящей под новые требования сетевой инфраструктуры. В качестве такого решения была выбрана концепция сетей пятого поколения 5G/IMT-2020. В рамках сетей 5G/IMT-2020 предлагается ряд решений, позволяющих увеличить пропускную способность и скорость обработки сетевых пакетов для проводных и беспроводных каналов связи. Идея децентрализации сетей связи являлась одной из центральных тем при проектировании концепции 5G/IMT-2020. Новые возможности, предоставляемые сетями 5G/IMT-2020, дали новый виток развитию таких технологий, как облачные, граничные и облачные вычисления. Данные технологии предлагают пользователю выносить все сложные вычислительные операции за пределы оконечного терминала пользователя, что является оправданным решением в случае, когда задача является настолько сложной, что оконечное устройство, с учетом его вычислительных возможностей, не имеет

возможности решить ее за приемлемое время. Таким образом, в структуру сетей Интернета вещей включается ряд новых типов устройств — облачных, граничных и туманных серверов. Внедрение данных устройств в сетевую инфраструктуру открывает возможности по внедрению технологий Интернета вещей в новые области, такие как промышленная автоматизация. Технологии, реализованные на основе решений ИВ и используемые в сфере промышленной автоматизации, называются промышленным Интернетом вещей (ПИВ). Алгоритмы анализа данных, применяемые в облачных, граничных и туманных вычислениях, могут быть использованы для решения задач предупреждения отказов промышленного оборудования, проектирования новой продукции, моделирования логического распространения продукции и т. д.

Решения ПИВ имеют некоторые отличия от решений ИВ, в частности, данные системы имеют повышенные требования по отказоустойчивости, по поддержке работы устройств и приложений в режиме реального времени. Также стоит отметить, что системы, используемые для организации локальных сетей промышленных предприятий, имеют множество специальных отраслевых технологических решений и стандартов, которые применяются для автоматизации сбора данных и управления оконечным промышленным оборудованием. Тем не менее, вопрос устойчивости сетевой инфраструктуры промышленного предприятия, в связи с предполагаемым отличием трафика ПИВ от ИВ, является открытым, так как не существует каких-либо моделей, позволяющих оценить влияние трафика, генерируемого устройствами ПИВ, на существующую сетевую инфраструктуру. Подобная модель могла бы позволить как оценить внедрение данных решений в существующую сетевую инфраструктуру, так и разработать специальную комплексную методику тестирования, позволяющую провести тестирование реальной инфраструктуры промышленного предприятия.

Интеграция решений ИВ в промышленную сетевую инфраструктуру сопряжена с проблемами конвертации протоколов и форматов полезных данных между собой в промышленных системах и протоколов, используемых в сетях связи

общего пользования (ССОП). Решение данной проблемы может заключаться в реализации специального типа устройств, отвечающих за преобразование протоколов и форматов полезных данных между собой и называющихся семантическими гетерогенными шлюзами ПИВ. Данный класс устройств позволит реализовать процедуру семантического преобразования промышленных протоколов с протоколами, используемыми в ССОП.

Степень разработанности темы. В последние годы появилось довольно большое количество работ российских и зарубежных авторов, посвященных исследованию технологий промышленного Интернета вещей и характерных особенностей его трафика.

На сегодняшний день в научных школах, возглавляемых российскими и зарубежными учеными А. Е. Кучерявым, Е. А. Кучерявым, В. И. Карташевским, А. В. Росляковым, В. К. Сарьяном, А. М. Тюрликовым, Д. Е. Намиотом, Р. В. Киричком, A. Shahzad, Y. G. Kim, R. Narayanan, C.S. R. Murthy, H. Cho, J. Jeong и др., ведутся работы по исследованию решений промышленного Интернета вещей. В частности, были выявлены проблемы, возникающие при внедрении промышленных протоколов с технологиями передачи данных через сети связи общего пользования на основе протокола IP, и было предложено множество решений для преобразования технологий физического, канального и сетевого уровней. Несмотря на то, что в целом указанная область исследуется довольно активно, ряд вопросов остается нерешенным. Необходимо отметить объективно малое количество работ, посвященных комплексному тестированию систем ПИВ и методам преобразования протоколов прикладного уровня.

Объект исследования — системы промышленного Интернета вещей.

Предмет исследования — параметры функционирования систем промышленного Интернета вещей в условиях имитации функциональной нагрузки.

Цель работы и задачи исследования. Целью диссертационной работы является разработка моделей и методики для проведения комплексного тестирования систем промышленного Интернета вещей.

Для достижения поставленной цели решаются следующие задачи:

- проанализировать и выявить области применения технологий ПИВ в рамках задач автоматизации работы промышленных предприятий;
- разработать модельную сеть для исследования характеристик трафика ПИВ от различных устройств;
- разработать модель фрагмента сети ПИВ для оценки пропускной способности канала связи в локальной сети и провести имитационное моделирование ее работы;
- разработать структуру семантического гетерогенного шлюза ПИВ;
- разработать метод построения семантических гетерогенных шлюзов ПИВ для реализации процедур преобразования сообщений в рамках сетей ПИВ;
- разработать модельную сеть для проведения исследования времени преобразования протоколов ПИВ между собой и провести симуляцию работы семантического гетерогенного шлюза для оценки времени преобразования протоколов ПИВ и их форматов полезных данных между собой;
- разработать методику комплексного тестирования сетей ПИВ для оценки производительности существующей инфраструктуры промышленных предприятий.

Научная новизна результатов исследования

1. Разработаны имитационная и аналитические модели фрагментов сети промышленного Интернета вещей, которые отличаются от известных тем, что данные модели построены с учетом гетерогенного характера трафика, полученного на основе экспериментальных исследований и последующего анализа.

2. Разработан метод построения семантического гетерогенного шлюза промышленного Интернета вещей, который отличается от известных тем, что учитывает модели конвертации прикладных протоколов ПИВ и промышленных технологий и позволяет сократить время преобразования прикладных протоколов

по сравнению с ранее существующими методами.

3. Разработана методика комплексного тестирования систем промышленного Интернета вещей, которая отличается от известных тем, что описывает процедуру и спецификации тестирования, учитывает гетерогенный характер трафика промышленного Интернета вещей, при имитации трафика от различных источников.

Теоретическая и практическая значимость работы

Теоретическая значимость диссертационной работы состоит в том, что предложенные модели фрагмента сети промышленного Интернета вещей могут быть использованы как для исследования характеристик трафика промышленного Интернета вещей, так и для выявления порогового уровня функционирования всей сети при повышенных уровнях функциональной нагрузки. Разработанный метод построения семантических гетерогенных шлюзов промышленного Интернета вещей может быть использован для исследования функционирования семантических гетерогенных шлюзов промышленного Интернета вещей, а также для исследования процедур преобразования прикладных протоколов и форматов передаваемых полезных данных. Разработанная методика комплексного тестирования систем промышленного Интернета вещей может быть использована при исследованиях работы как физических систем промышленного Интернета вещей, так и виртуальных сущностей таких систем.

Практическая значимость диссертационной работы состоит в том, что предложенные имитационная и аналитические модели фрагмента сети промышленного Интернета вещей могут быть использованы для разработки систем комплексного тестирования сетевой инфраструктуры в условиях имитации повышенной функциональной нагрузки. Предложенный метод построения семантического гетерогенного шлюза промышленного Интернета вещей может быть использован для разработки и отладки семантических гетерогенных шлюзов промышленного Интернета вещей. Разработанная методика комплексного тестирования систем промышленного Интернета вещей, включающая алгоритмы

генерации трафика и требования к тестированию, может быть использована для создания программно-аппаратных комплексов для тестирования систем промышленного Интернета вещей.

Методология и методы исследования. Проводимые исследования базируются на теории массового обслуживания, математической статистике, методах моделирования и натурных экспериментах. Моделирование фрагмента сети промышленного Интернета вещей и семантического гетерогенного шлюза промышленного Интернета вещей проведено на основе пакетов имитационного моделирования Anylogic и Python Ciw.

Положения, выносимые на защиту

1. Модели фрагмента сети промышленного Интернета вещей, позволяющие учитывать гетерогенный характер трафика.

2. Метод построения семантического шлюза промышленного Интернета вещей, уменьшающий длительность времени преобразования прикладных протоколов по сравнению с известными методами на 14 %.

3. Методика комплексного тестирования сетей промышленного Интернета вещей, обеспечивающая тестирование с учетом гетерогенного характера трафика.

Степень достоверности и апробация результатов

Достоверность полученных автором научных и практических результатов определяется обоснованным выбором исходных данных при постановке частных задач исследования, основных допущений и ограничений, принятых в процессе математического моделирования, соответствием расчетов с результатами экспериментальных исследований, проведенных лично автором, согласованностью с данными, полученными другими авторами и апробацией результатов исследований на международных, всероссийских и ведомственных научно-технических конференциях и конгрессах. Основные теоретические и практические результаты работы реализованы в учебном процессе кафедры Сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича при чтении лекций, проведении

практических занятий и лабораторных работ, а также при выполнении научно-исследовательских работ для ПАО «Ростелеком». Кроме того, научные результаты, полученные Куликом Вячеславом Андреевичем, были использованы при подготовке вкладов СПбГУТ в 11 и 20 исследовательских комиссий сектора стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т) и при разработке международного стандарта в 41 подкомитете совместного технического комитета №1 Международной организации по стандартизации и Международной электротехнической комиссии (ИСО/МЭК).

Апробация результатов исследования. Основные результаты диссертационной работы докладывались и обсуждались на таких конференциях, как 19th International conference on distributed computer and communication networks (DCCN-2016) (Москва, 2016), 18th International conference on advanced communication technology (ICACT-2016) (Пхёнчхан, 2016), 3-я Международная научно-техническая конференция студентов, аспирантов и молодых ученых «Интернет вещей и 5G» (INTHITEN 2017) (Санкт-Петербург, 2017), 10th International congress on ultra-modern telecommunications and control systems and workshops (ICUMT-2018) (Москва, 2018), 19th International conference on next generation teletraffic and wired/wireless advanced networks and systems (NEW2AN-2019) (Санкт-Петербург, 2019), 22nd International conference on distributed computer and communication networks (DCCN-2019) (Москва, 2019).

Публикации по теме диссертации. Всего соискателем по теме диссертации публиковано 24 работы, из них 6 статей в рецензируемых научных изданиях; 5 в изданиях, индексируемых в международных базах данных; 1 свидетельство о регистрации программного обеспечения; 12 в других изданиях и материалах конференций.

Соответствие специальности. Диссертационная работа соответствует пунктам 2, 3, 11, 14 паспорта специальности 05.12.13 «Системы, сети и устройства телекоммуникаций».

Личный вклад автора. Основные результаты теоретических

и экспериментальных исследований получены автором самостоятельно. В работах, опубликованных в соавторстве, соискателю принадлежит основная роль при постановке и решении задач, а также обобщении полученных результатов.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, выводов, списка используемых источников и двух приложений. Полный объем диссертации составляет 180 страниц, из них к основной части относится 157 страниц. Работа содержит 53 рисунка, 13 таблиц и список из 126 литературных источников.

Глава 1. АНАЛИЗ МЕТОДОВ ТЕСТИРОВАНИЯ УСТРОЙСТВ, СЕТЕЙ И СИСТЕМ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

1.1. Концепция промышленного Интернета вещей и перспективы ее развития

В настоящее время активно развивается концепция Интернета вещей, подразумевающая активное внедрение встраиваемых технологий в современные инфокоммуникационные сети связи. Данная концепция с каждым днем охватывает все большее число областей человеческой жизнедеятельности, таких как беспилотное управление транспортом, управление городской инфраструктурой, контроль проведения медицинских операций, автоматизация жилых помещений, офисов и др. [61–62]. С недавнего времени в рамках концепции Интернета вещей (далее ИВ) развивается новое направление — промышленный Интернет вещей (далее ПИВ) [82], которое затрагивает вопросы создания гетерогенной интеллектуальной системы автоматизации работы промышленных предприятий. Системы ПИВ находят свое применение в самых различных областях производства, таких как сельское хозяйство, производство электронного оборудования, машиностроение, производство станков, автоматизация сбора и учета данных с энергетических сетей, производство авиационной, космической и военной техники и т. д.

Согласно стандарту МСЭ-Т Y.4003 «Обзор умных производств в контексте промышленного Интернета вещей», промышленный Интернет вещей (Industrial Internet of Things) — это концепция преобразования промышленности, использующая для этого существующие и новые информационные и телекоммуникационные технологии и основанная на концепции Интернета вещей [16]. В рамках ПИВ планируется провести автоматизацию работы промышленного оборудования, расчетов экономических показателей, обеспечения безопасности работников и пр. Основным отличием систем данного типа является их тесное

взаимодействие с облачными и граничными технологиями и использование высокопроизводительных самообучающихся систем как для текущей оценки работы предприятия, так и для планирования его развития.

В настоящее время внедрение технологий, относящихся к промышленному Интернету вещей, сопряжено с проблемами как с интеграцией данных технологий с устаревшими решениями для промышленной автоматизации, так и с отсутствием какой-либо системы автоматизации на предприятии. Решение данных проблем заключается в разработке единых технологических стандартов для интеграции как систем промышленной автоматизации, так и оборудования, не имеющего цифровых интерфейсов управления, с системами ПИВ. В настоящее время идет активный процесс стандартизации технологий ПИВ в различных международных и отраслевых организациях, таких как МСЭ-Т, ИСО/МЭК, Industrial Internet Consortium и др.

1.2. Классификация сфер автоматизации работы промышленных предприятий

На промышленных предприятиях существует целый ряд направлений, работа которых подлежит автоматизации. Помимо очевидной автоматизации работы производственного оборудования (например, фрезерные станки, токарные станки, сварочное оборудование, промышленный манипулятор и др.), существует целый ряд направлений, подлежащих автоматизации в рамках предприятия и связанных с человеческой безопасностью и общественной деятельностью. В качестве основных сфер автоматизации следует выделить следующие направления:

- ✓ Автоматизация работы производственного оборудования [77, 91, 118]. Автоматизация работы данного оборудования позволит автоматизировать рутинные операции, в обратном случае производимые человеком, собирать данные о состоянии оборудования от встроенных в него датчиков, проводить анализ полученного трафика и на основе результатов анализа давать рекомендации по эксплуатации

данного оборудования. Для автоматизации его работы необходимо разработать и реализовать сценарии подключения различных типов оборудования к системам ПИВ, например:

- оборудования, не имеющего цифровых систем контроля его работы;
- оборудования, не имеющего встроенной поддержки сетевого взаимодействия со сторонними промышленными системами, такими как OPC UA, SCADA;
- оборудования поддерживающего взаимодействие с промышленными системами контроля работы оборудования.

✓ Автоматизация мониторинга и управления состояния продукции предприятия [75, 82, 121]. Мониторинг состояния продукции предприятия позволит оценить реальные эксплуатационные характеристики производимой продукции и позволит контролировать технический процесс ее производства, в зависимости от результатов анализа данных, полученных в ходе мониторинга.

✓ Автоматизация работы бизнес-приложений [81, 86], таких как системы планирования ресурсов предприятия (ERP), управления взаимодействия с клиентами (CRM), управления жизненным циклом продукта (PLM), исполнения производственных процессов (MES), управления человеческими ресурсами (HRM) и др. Сбор и отправка данных с бизнес-приложений в единую комплексную систему мониторинга и управления промышленным предприятием на основе технологий ПИВ позволят произвести комплексную оценку работы предприятия с точки зрения экономической рентабельности и выдать рекомендации по экономическому планированию и логистике.

✓ Автоматизация работы мультимедийных систем мониторинга безопасности промышленного предприятия [85, 90, 124]. Данные системы, чаще всего в форме камер видеомониторинга, используются для контроля соблюдения правил обеспечения безопасности

жизнедеятельности предприятия и контроля доступа на территорию предприятия. Интеграция данного типа оборудования с системами ПИВ позволит обеспечить надежную идентификацию, аутентификацию и авторизацию персонала предприятия и беспрерывный контроль соблюдения техники безопасности в производственных помещениях.

- ✓ Автоматизация работы систем локального и глобального позиционирования [89, 106, 111, 122]. Данные системы могут использоваться для сбора данных о местонахождении того или иного объекта на территории предприятия или за его пределами. Внедрение данных решений в системы ПИВ позволит отслеживать местонахождение и техническое состояние оборудования или производимой продукции и на основе полученной информации выдавать рекомендации по эксплуатации оборудования или продукта, а также рекомендации по производственному циклу продукции. Также данные системы могут использоваться для авторизации доступа к помещениям и контроля соблюдения техники безопасности сотрудниками предприятия.
- ✓ Автоматизация сбора и анализа данных с открытым доступом из сети Интернет [114-115, 120, 123]. Обрабатываемая информация может использоваться для решения задач глобального позиционирования промышленных систем, для взаимодействия с клиентами предприятия, для сбора статистики о функциональных качествах производимой продукции и др. Данная информация может быть использована при проектировании будущей продукции предприятия.

1.3. Обзор международной деятельности в области стандартизации концепции промышленного Интернета вещей

В настоящее время идет активная работа в области международной

стандартизации технологий промышленного Интернета вещей, в частности, данное направление наиболее активно развивается организацией Industrial Internet Consortium.

Консорциум промышленного Интернета вещей, или Industrial Internet Consortium (IIC) — это некоммерческая международная организация, объединяющая различные отраслевые организации и разрабатывающая стандарты и рекомендации по направлениям промышленной автоматизации и ПИВ, например «The Industrial Internet of Things Volume G1: Reference Architecture» [3], «The Industrial Internet of Things Volume G5: Connectivity Framework» [4], «The Industrial Internet of Things Volume T3: Analytics Framework» [5].

В отраслевом стандарте IIC «The Industrial Internet of Things Volume G1: Reference Architecture» описывается структура эталонной архитектуры ПИВ (ЭА ПИВ), включающей в себя архитектуру программной платформы для разработки решений ПИВ. ЭА ПИВ используется для разработки и определения основных проблем в реализации архитектуры решения ПИВ и их дальнейшего решения. Данная архитектура может быть использована в качестве шаблона для различных проектов ПИВ.

В отраслевом стандарте IIC «The Industrial Internet of Things Volume G5: Connectivity Framework» описывается структура набора программных инструментов для обеспечения связанности элементов систем ПИВ. Одной из основных проблем в ПИВ является обеспечение взаимодействия различных проприетарных технологий между собой. Набор программных инструментов для обеспечения связности, описанный в данном стандарте, предназначен для создания единого программного или сетевого интерфейса, позволяющего обеспечить взаимодействие решений ПИВ, совместимых с данным стандартом.

В отраслевом стандарте IIC «The Industrial Internet of Things Volume T3: Analytics Framework» описывается структура набора программных инструментов для анализа данных для решений ПИВ. В данном стандарте определяются типы систем анализа данных, которые могут использоваться в рамках ПИВ, а также

структура программных инструментов и интерфейсов, позволяющих разрабатывать данные системы, и аналитические модели, которые могут быть применены в ходе анализа данных.

Помимо стандартов IIC существует рекомендация МСЭ-Т Y.4003 «Обзор умных производств в контексте промышленного Интернета вещей» [16], разработанная 20-й исследовательской комиссией сектора стандартизации телекоммуникаций Международного союза электросвязи (МСЭ-Т). Данная рекомендация описывает рекомендованную архитектуру систем ПИВ в рамках «умных производств» и основные требования к решениям ПИВ.

Также в настоящее время разработкой стандартов и рекомендаций, связанных с системами ПИВ, занимаются такие организации, как ИСО/МЭК, OpenFog Consortium, Национальная ассоциация участников рынка промышленного интернета (НАПИ), Ассоциация Интернета вещей, Российская ассоциация Интернета вещей и др. Тем не менее, данные Стандарты и Рекомендации находятся на стадии рассмотрения.

1.4. Анализ систем промышленного Интернета вещей

1.4.1. Эталонные архитектуры систем промышленного Интернета вещей

Технологии ПИВ являются составной частью концепции Интернета вещей, и перед описанием существующих эталонных архитектур ПИВ следует рассмотреть более общую эталонную архитектуру ИВ, описанную в стандарте МСЭ-Т Y.4000/Y.2060 «Обзор Интернета вещей» [21], изображенную на рисунке 1.

Данная архитектура состоит из четырех функциональных и двух нефункциональных уровней. В число функциональных входят следующие уровни:

1. Уровень приложений, включающий в себя программное обеспечение оконечных устройств, серверов, шлюзов и других элементов сетей ИВ.
2. Уровень поддержки услуг и поддержки приложений, включающий в себя следующие элементы:

- Общие возможности поддержки, которые могут быть использованы

различным программным обеспечением ИВ, таким как системы управления базами данных или системы анализа данных. Данные возможности могут быть использованы для обеспечения поддержки специализированных возможностей поддержки.

- Специализированные возможности поддержки, которые предназначены для удовлетворения требований различных комплексных программных систем.

Рис. 1. Эталонная архитектура ИВ

3. Уровень сети, включающий в себя следующие элементы:

- Возможности организации сетей, предоставляющих некоторые функции управления сетевыми соединениями, такими как функции управления доступом, транспортным ресурсом, мобильностью, функциями AAA (аутентификация, авторизация, учет сетевых ресурсов).

- Возможности транспортировки, предоставляющие соединения для передачи информации по сетям в виде пакетов данных, относящихся к услугам и приложениям ИВ, а также передачи управляющих сообщений.

4. Уровень устройства, включающий в себя следующие элементы:

- Возможности устройства, которые включают в себя следующие

функции:

A. Прямое взаимодействие с сетью связи. Устройства ИВ способны отправлять информацию напрямую, без использования возможностей шлюзов ИВ, из сетей связи общего пользования (далее ССОП) и получать информацию из ССОП.

B. Непрямое взаимодействие с сетью связи. Устройства ИВ способны отправлять информацию в ССОП непрямым образом, с помощью возможностей шлюзов ИВ и получать информацию из ССОП.

C. Организацию специальных сетей. Устройства ИВ могут поддерживать возможность строить сети произвольным, динамическим способом.

D. Спящий режим и пробуждение. Устройства ИВ могут поддерживать высокоэффективные энергосберегающие механизмы (такие как «глубокий сон») и возможности их пробуждения.

- Возможности шлюза, которые включают в себя следующие функции:

A. Поддержку множества сетевых интерфейсов. Шлюз ИВ может поддерживать сразу несколько проводных и беспроводных технологий для передачи данных между устройствами ИВ на канальном (например, CAN, ZigBee, Bluetooth, Wi-Fi и др.) и сетевом (например, ТфОП, 2G, 3G, 4G, DSL, спутниковые сети и др.) уровнях.

B. Поддержку преобразования протоколов. Шлюз ИВ должен обеспечивать возможность взаимодействия устройств ИВ путем взаимного преобразования сетевых сообщений на канальном, сетевом, транспортном и прикладном уровнях.

В число нефункциональных входят следующие уровни:

1. Уровень управления (возможности управления). Системы ИВ должны предоставлять методы управления сетями связи ИВ, обеспечивать обработку возникающих ошибок, учет сетевых ресурсов, предоставление отчета о работе

сетевого оборудования. Важнейшими функциями данного уровня являются:

- Управление устройствами ИВ, например диагностика, дистанционное управление активацией и деактивацией устройств, обновление программного обеспечения устройства, управление состоянием устройства и др.
- Управление структурой локальной сети ИВ.
- Управление трафиком и перегрузками, например обнаружение перегрузок и их предпосылок, резервирование ресурсов и другое.

2. Уровень обеспечения безопасности (возможности обеспечения безопасности). Системы ИВ должны включать в себя основные общие возможности обеспечения безопасности передачи пользовательских данных и поддержку опциональных специальных методов обеспечения безопасности сети. Важнейшими функциями данного уровня являются:

- На прикладном уровне: аутентификация, авторизация, защита конфиденциальности и целостности данных приложений, защита неприкосновенности пользовательских данных, контроль безопасности и антивирусная защита.
- На уровне сети: аутентификация, авторизация, защита конфиденциальности и целостности данных о работе сети и сигнализации, а также защита целостности данных сигнализации.
- На уровне устройства: аутентификация, авторизация, защита конфиденциальности и целостности данных об устройстве, управление доступом.

На основе эталонной архитектуры ИВ в МСЭ-Т была разработана функциональная архитектура систем «умного производства», основанная на решениях ПИВ, описанная в стандарте МСЭ-Т Y.4003 «Обзор умных производств в контексте промышленного Интернета вещей» и изображенная на рисунке 2.

Представленная на рисунке 2 архитектура делится на следующие уровни:

1. Уровень управления жизненными циклами. Данный уровень отвечает за

управление различными жизненными циклами работы производственного предприятия и охватывает широкий ряд систем в производственном предприятии, например системы для проектирования, производства, управления и технического обслуживания производимой продукции. В качестве основных жизненных циклов предприятия можно выделить следующие:

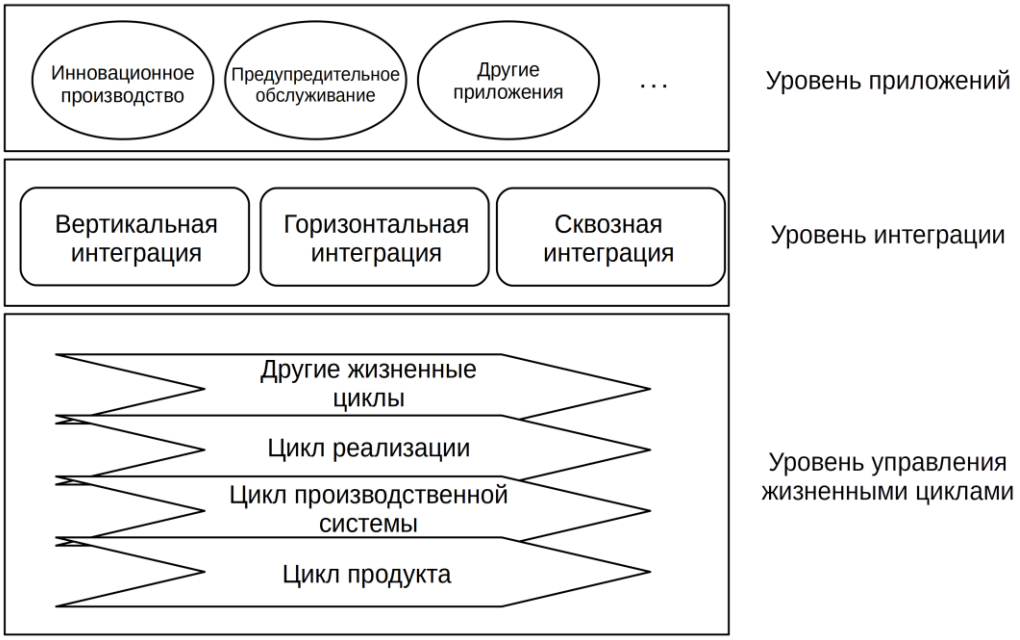


Рис. 2. Функциональная архитектура систем «умного производства»

- Цикл продукта, включающий в себя проектирование и разработку соответствующей производственной системы, проектирование, разработку, производство, тестирование, техническое обслуживание выпускаемой продукции, использование продукта пользователем, переработку или уничтожение отработавшей продукции.
- Цикл производственной системы, включающий в себя проектирование, сбор, эксплуатацию, техническое обслуживание и вывод из эксплуатации всей производственной системы.
- Цикл реализации, включающий в себя функции, связанные с взаимодействием поставщика и клиента.
- Другие жизненные циклы, которые также могут быть включены в рассматриваемую систему, при наличии особенных требований к «умному

предприятию».

2. Уровень интеграции, обеспечивающий интеграцию всех ресурсов, систем и процессов, участвующих в различных жизненных циклах, связанных с созданием продукции, через все уровни производственной системы для создания среды для приложений «умного производства». Данный уровень включает в себя следующие виды интеграции:

- Вертикальная интеграция, отвечающая за то, чтобы новые технологические решения были включены в уже существующую систему через вышестоящие уровни производственной системы.
- Горизонтальная интеграция, отвечающая за то, чтобы новые технологические решения были интегрированы в уже существующую систему на одном системном уровне.
- Сквозная интеграция, позволяющая соединить каждую фазу жизненного цикла производимого продукта через всю цепочку реализации продукта, в том числе через различные предприятия.

3. Уровень приложений, который отвечает за реализацию конечных приложений, применяющихся для решения различных задач, возникающих на «умных производствах». В качестве примера можно привести следующие приложения:

- Инновационное производство является одним из видов «умного производства» и включает в себя такие приложения, как виртуальное производство, гибкое производство и индивидуальное производство. Виртуальное производство позволяет имитировать производственные процессы на предприятии и проводить компьютерное моделирование. Гибкое производство позволяет быстро реагировать в случае прогнозируемых и непрогнозируемых изменений. Индивидуальное производство позволяет реализовать товар таким образом, чтобы удовлетворить потребности каждого отдельного клиента.
- Предупредительное обслуживание отвечает за анализ данных,

поступающих от производственных инструментов, оборудованных различного рода датчиками, собирающими информацию о текущем состоянии оборудования, и за принятие решений на основе результатов анализа, что потенциально может привести к предотвращению сбоев оборудования.

Таким образом, МСЭ-Т не выделяет отдельную эталонную архитектуру для описания систем ПИВ, а использует уже ранее разработанную архитектуру ИВ, добавляя к ней новые требования, связанные со спецификой работы промышленных предприятий.

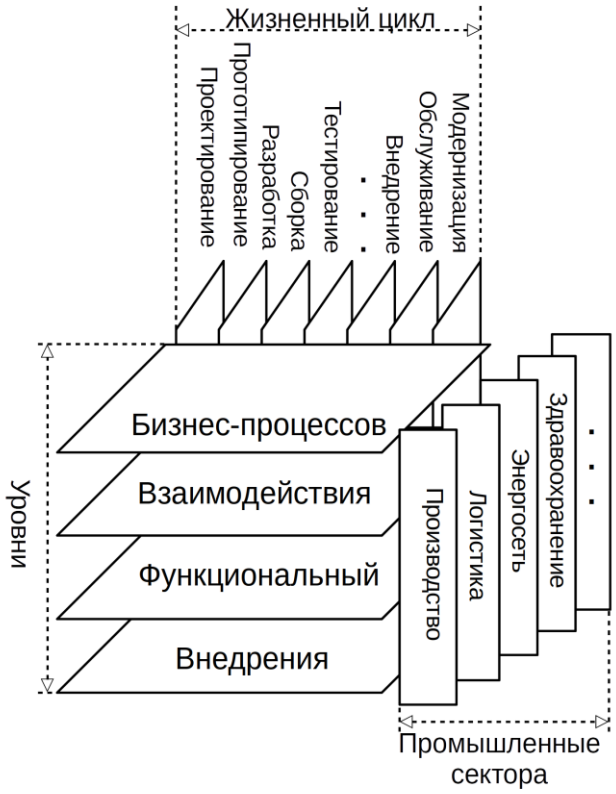


Рис. 3. Общая структура взаимодействия между уровнями рассмотрения ЭА ПИВ, промышленными секторами и жизненными циклами продуктов

В отличие от МСЭ-Т IIC выделяет специальную эталонную архитектуру ПИВ в стандарте «The Industrial Internet of Things Volume G1: Reference Architecture», где определяет эталонную архитектуру как результат применения шаблона архитектуры к существующим системам для управления, идентификации, анализа и решений общих архитектурных проблем. Эталонная архитектура может

использоваться в качестве шаблона для конкретной реализации систем ПИВ при проектировании.

На рисунке 3 указана структура взаимодействия между уровнями рассмотрения ЭА ПИВ, промышленными секторами и жизненными циклами продуктов.

ЭА ПИВ включает в себя несколько уровней рассмотрения каждого отдельного решения ПИВ. Всего можно выделить четыре уровня:

1. Уровень бизнес-процессов. Этот уровень включает в себя проблемы определения заинтересованных сторон, их задач, целей, бизнес-планов при создании системы ПИВ в ее деловом и правовом контексте. Далее на этом уровне определяется, каким образом система ПИВ достигает заявленных целей, посредством сопоставления с основными возможностями системы.

2. Уровень взаимодействия. Этот уровень включает в себя проблемы, возникающие при использовании системы пользователями (людьми или приложениями).

3. Функциональный уровень. Этот уровень включает в себя проблемы, возникающие при работе различных функциональных компонентов в системах ПИВ, в их структуре, интерфейсах и механизмах взаимодействия между ними, а также при взаимодействии системы с внешними внесистемными элементами.

4. Уровень внедрения. Данный уровень рассматривает проблемы, которые связаны с работой технологий, необходимых для реализации функциональных компонентов (функциональный уровень), структуры их взаимодействия и жизненного цикла. Эти компоненты координируются действиями пользователей (уровень взаимодействия) и поддержкой бизнес-процессов (уровень бизнес-процессов).

Данные уровни рассмотрения ЭА ПИВ могут быть реализованы на разных этапах жизненного цикла производимого продукта и могут быть внедрены в различные промышленные сектора, что и отображено на рисунке 3.

С технической точки зрения в данном документе особенный интерес

представляет функциональный уровень. На рисунке 4 изображена диаграмма потоков данных на функциональном уровне ЭА ПИВ, где зеленые стрелки обозначают информационные потоки, красные — управляющие потоки, а серые — потоки принятия решений.

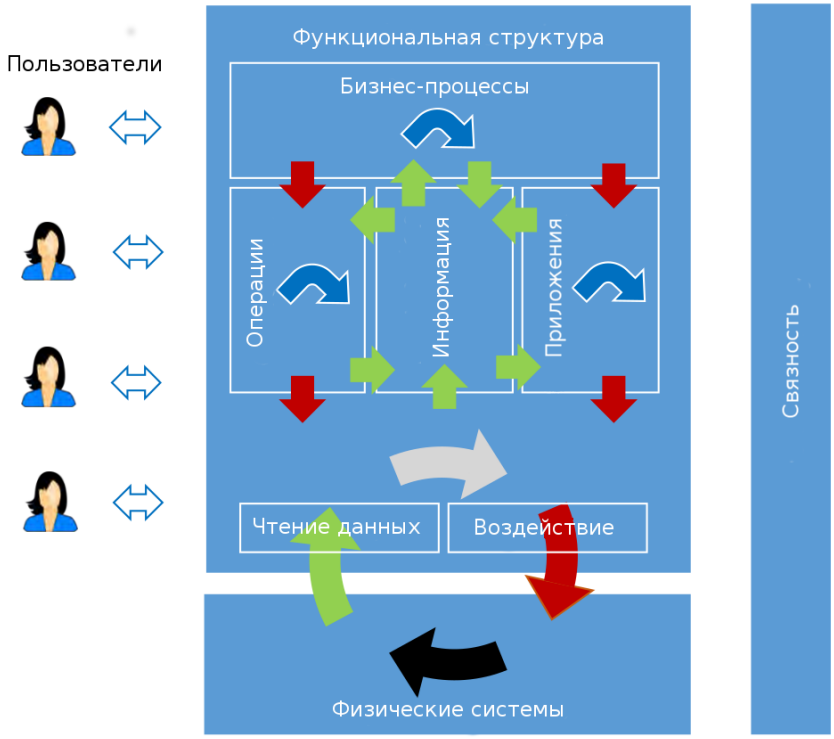


Рис. 4. Диаграмма потоков данных на функциональной структуре эталонной архитектуры ПИВ

Данная диаграмма включает в себя следующие области:

1. Управление (включает в себя чтение данных и воздействие) — это функциональная область, используемая для реализации систем управления устройствами ПИВ. Она представляет собой совокупность функций, выполняемых промышленными системами управления и автоматизации. Ядро этих функций включает считывание данных с датчиков, применение базовых логических правил работы и осуществление воздействия на физическую систему через исполняющие команды.

2. Операции — это функциональная область, используемая для управления работой приложений и устройств, относящихся к области управления. Данная область представляет собой совокупность функций, ответственных за управление,

мониторинг и оптимизацию работы систем, относящихся к области управления.

3. Информация — это функциональная область, отвечающая за обработку данных. Данная область представляет собой набор функций для сбора данных из различных областей, в первую очередь из области управления и преобразования, сохранения и моделирования или анализа этих данных, для получения высокоуровневой информации обо всей системе. Функции сбора и анализа данных в этой области дополняют функции, реализованные в области управления. В области управления эти функции участвуют в непосредственном управлении физическими системами, в то время как в информационной области они предназначены для содействия принятию решений, оптимизации общесистемных операций и совершенствования моделей систем в долгосрочной перспективе.

4. Приложения — это функциональная область, используемая для реализации логики работы приложений. Данная область представляет собой набор функций, реализующих логику работы приложения, реализующего определенные бизнес-процессы.

5. Бизнес-процессы — это функциональная область для реализации логики работы бизнес-процессов. Данная область представляет собой функции, поддерживающие бизнес-процессы, которые система ПИВ должна поддерживать для обеспечения сквозных жизненных циклов внутри решения ПИВ. В качестве примеров таких бизнес-процессов можно привести системы ERP, CRM, PLM, MES, HRM и др.

6. Также данная функциональная структура расширена областью «Связность», описанной в документе IIC «The Industrial Internet of Things Volume G5: Connectivity Framework». Данная область обеспечивает возможность обмена информацией между элементами в пределах одной функциональной области, между функциональными областями и между различными системами. Обмен данными может включать в себя обновления информации с датчиков, события, сигналы тревоги, управляющие команды и обновления конфигурации.

1.4.2. Протоколы передачи данных промышленного Интернета вещей

Системы ПИВ имеют высокие требования к показателям надежности доставки сообщений, вследствие чего очень часто разработчики систем ПИВ используют специальные отраслевые протоколы передачи данных, используемые в сфере промышленной автоматизации. Для исследования протоколов передачи данных ПИВ были выбраны следующие технологии:

- CoAP (Constrained Application Protocol) [13, 64, 69, 107].
- MQTT (Message Queuing Telemetry Transport) [29, 69, 125].
- XMPP (Controller Area Network) [69].
- HTTP (HyperText Transfer Protocol) [125].
- ModBus [68].
- OPC UA (Open Platform Communications Unified Architecture) [74, 80].

CoAP (Constrained Application Protocol) — протокол передачи данных прикладного уровня, основанный на клиент-серверной архитектуре. CoAP разрабатывался как протокол, предназначенный для использования в беспроводных сенсорных сетях с возможностью интеграции в ССОП, обеспечивающейся с помощью прокси-серверов CoAP, преобразующих данные из сети с поддержкой CoAP в формат REST (HTTP). CoAP является протоколом стека TCP/IP, поддерживает протоколы IPv4, IPv6, 6LoWPAN и работает поверх транспортного протокола UDP.

Сеть CoAP имеет следующие типы устройств (рис. 5):

- Оконечный узел (CoAP Node). Может устанавливать соединение с ОУ, сервером и прокси-сервером CoAP.
- Сервер (CoAP Server). Может устанавливать соединение с ОУ, сервером и прокси-сервером CoAP.
- Прокси-сервер CoAP (CoAP Proxy). Может устанавливать соединение с ОУ, сервером и прокси-сервером CoAP и с сервером HTTP.

CoAP имеет два уровня QoS:

- Доставка сообщения без подтверждения.

- Доставка сообщения с подтверждением.

Данный протокол имеет следующие типы сообщений:

- GET — запрос необходимой информации у сервера с помощью формирования запроса в строке URI.
- PUT — отправка информации к серверу на указанный в запросе URI.
- POST — отправка информации к серверу на указанный в запросе URI.
- DELETE — удаление указанного в URI ресурса.

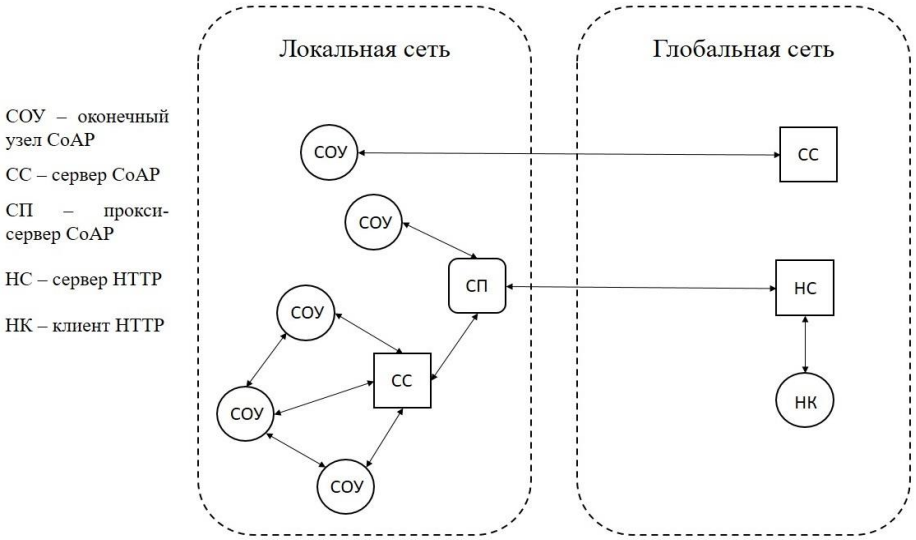


Рис. 5. Архитектура сети CoAP

Для обеспечения безопасности передачи данных протокол CoAP использует алгоритм DTLS.

MQTT (Message Queue Telemetry Transport) — протокол передачи данных прикладного уровня, функционирующий на основе принципа «издатель — подписчик» (publisher-subscriber). MQTT обладает низкой вычислительной сложностью и поэтому может быть использован во встраиваемых устройствах, в том числе устройствах ПИВ.

MQTT является протоколом стека TCP/IP, поддерживает протоколы IPv4, IPv6 и работает поверх транспортного протокола TCP.

Принцип «издатель — подписчик» реализован в MQTT следующим образом (рис. 6):

1. Издатель устанавливает соединение с брокером.

2. Далее брокер ожидает запроса соединения от подписчика и при получении устанавливает его.

3. Затем подписчик подписывается на некую тему (topic), MQTT-брокер прикрепляет данного подписчика к этой теме.

4. Затем если на издателе обновляется какая-либо информация, связанная с этой темой, издатель сообщает это брокеру.

5. Брокер, в свою очередь, передает эту информацию всем подписанным на эту тему подписчикам.

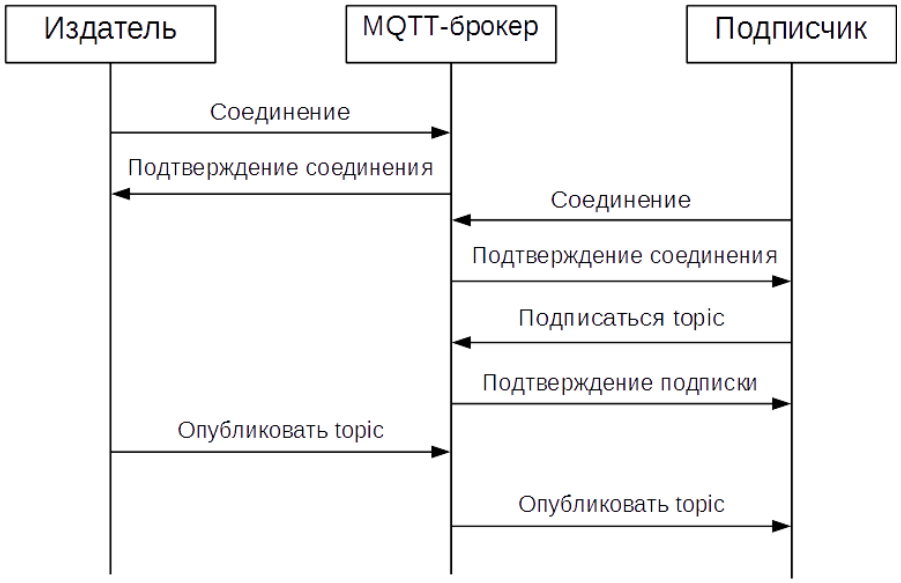


Рис. 6. Сценарий взаимодействия «издатель — подписчик» для MQTT

Данный протокол имеет три уровня качества обслуживания (Quality of Service):

- Уровень 0, означает, что издатель и брокер пытаются выполнить однократную доставку сообщения, но для подтверждения доставки используют только стандартные процедуры подтверждения TCP/IP.
- Уровень 1, означает, что издатель и брокер проверяют доставку сообщения и оно может быть отправлено более одного раза.
- Уровень 2, означает, что издатель и брокер проверяют доставку сообщения и оно может быть отправлено только один раз.

MQTT имеет следующие виды сообщений:

- ADVERTISE — шлюз широковещательно оповещает все узлы в сети о своем существовании.
- SEARCHGW — клиент отправляет широковещательное сообщение для поиска шлюза.
- GWINFO — шлюз отвечает клиенту, отправившему запрос SEARCHGW.
- CONNECT — запрос на установление соединения со шлюзом.
- CONNACK — подтверждение соединения.
- DISCONNECT — запрос на разрыв соединения со шлюзом.
- REGISTER — регистрация темы на шлюзе и присвоение ей идентификатора темы (topic id).
- REGACK — ответ на сообщение регистрации темы на шлюзе.
- PUBLISH — отправка измененного значения темы для клиентов и шлюзов.
- PUBACK — ответ на сообщение о публикации данных на шлюзе, удовлетворяющий значениям QoS 1, 2.
- PUBREC, PUBREL, PUBCOMP — отправляются вместе с сообщением PUBLISH для сообщения о QoS уровня 2.
- SUBSCRIBE — запрос клиента на оповещение об изменении информации по заданной теме.
- SUBACK — ответ на сообщение SUBSCRIBE.
- UNSUBSCRIBE — запрос клиента на отмену оповещения об изменении информации по заданной теме.
- UNSUBACK — ответ на сообщение UNSUBSCRIBE.
- PINGREQ — сообщение, периодически отправляемое клиентом и опрашивающее устройства об их работоспособности.
- PINGRESP — сообщение, отправляемое устройствами в ответ на сообщение PINGREQ и подтверждающее их функционирование в сети.

Для обеспечения безопасности передачи данных протокол использует алгоритм SSL/TLS.

XMPP (Extensible Messaging and Presence Protocol) — открытый децентрализованный протокол передачи данных прикладного уровня, изначально предназначенный для сервисов мгновенного обмена сообщениями и функционирующий на основе принципа «издатель — подписчик» (publisher-subscriber), использующий формат XMP как основную форму передачи данных. В настоящее время протокол нашел применение в сфере ПИВ.

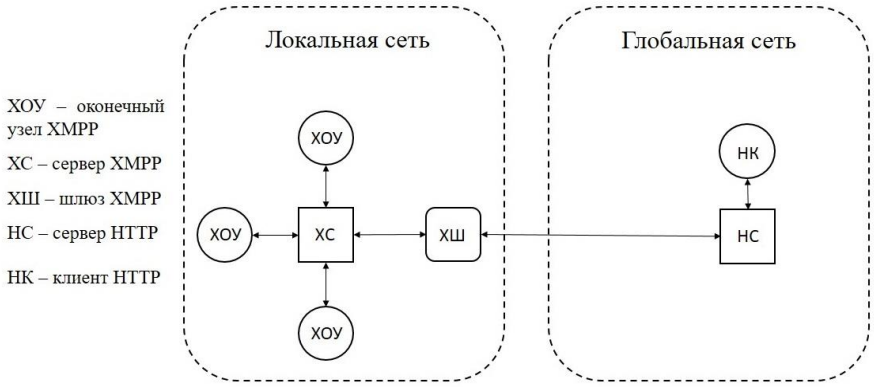


Рис. 7. Архитектура сети XMPP

XMPP является протоколом стека TCP/IP, поддерживает протоколы IPv4, IPv6 и работает поверх транспортного протокола TCP.

Сеть XMPP имеет следующие типы устройств (рис. 7):

- Сервер XMPP. Может устанавливать соединение со шлюзом XMPP и клиентом XMPP.
- Клиент XMPP. Может устанавливать соединение с сервером XMPP.
- Шлюз XMPP. Может устанавливать соединение с сервером XMPP и внешними серверами.

Данный протокол имеет три уровня качества обслуживания (Quality of Service):

- Без подтверждения доставки.
- С подтверждением доставки и возможностью многократной отправки

пакета.

- С подтверждением доставки и однократной передачей пакета.

Для обеспечения безопасности передачи данных протокол XMPP использует алгоритм SSL/TLS.

HTTP (HyperText Transfer Protocol) — протокол передачи гипертекстовых данных прикладного уровня, основанный на клиент-серверной архитектуре. Изначально использовался как протокол передачи гипертекстовой информации, но на настоящий момент используется для передачи производных данных. Основным методом доступа к информации является адрес ресурса URI.

HTTP является протоколом стека TCP/IP, поддерживает протоколы IPv4, IPv6 и работает поверх транспортного протокола TCP.

Сеть HTTP имеет следующие типы устройств (рис. 8):

- Сервер HTTP. Может устанавливать соединение с клиентом HTTP.
- Клиент HTTP. Может устанавливать соединение с сервером HTTP.

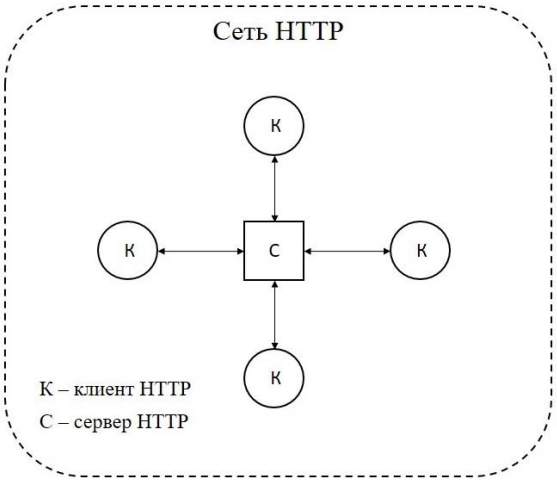


Рис. 8. Архитектура сети HTTP

Данный протокол имеет следующие типы сообщений:

- GET — запрос необходимой информации у сервера с помощью формирования запроса в строке URI.
- PUT — отправка информации к серверу на указанный в запросе URI.
- POST — отправка информации к серверу на указанный в запросе URI.

- DELETE — удаление указанного в URI ресурса.

Для обеспечения безопасности передачи данных протокол HTTP использует алгоритм SSL/TLS.

Modbus — открытый промышленный коммуникационный стандарт, применяемый для передачи данных между электронными вычислительными устройствами, функционирующий по модели взаимодействия «ведущий — ведомый». Широко распространен и является одним из наиболее поддерживаемых протоколов в промышленном оборудовании. Включает в себя три следующих подвида:

- Modbus ASCII (Modbus American standard code for information interchange) — разновидность протокола, в которой сообщения кодируются с помощью ASCII-символов. Сообщения разделяются символами «:» и CR/LF. В качестве канала передачи данных используются технологии для передачи данных по последовательным портам (например, RS-232, RS-485, RS-422).

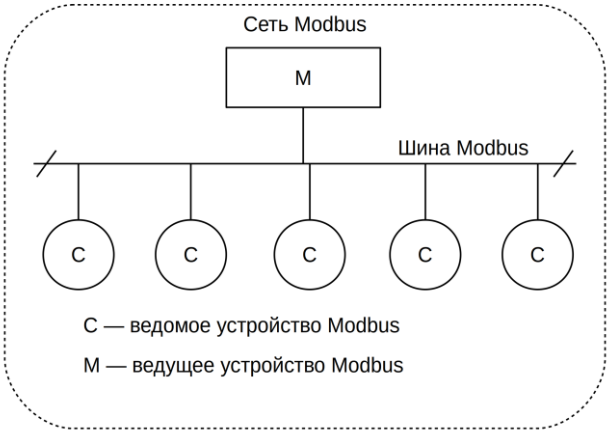


Рис. 9. Архитектура сети Modbus

- Modbus RTU (Modbus Remote Terminal Unit) — разновидность протокола, в которой сообщения кодируются в битовом виде. Между собой сообщения разделяются временной паузой в 3,5 символа при заданной скорости передачи. Является протоколом реального времени. В качестве канала передачи данных используются технологии для передачи данных по последовательным портам (например, RS-232, RS-485, RS-422).

- Modbus TCP (ModBus over Transmition Control Protocol) — разновидность протокола для передачи сообщений Modbus RTU поверх сообщений TCP/IP. В качестве канала передачи данных используются технологии пакетной передачи данных, поддерживающие сетевые протоколы IPv4 и IPv6 (например, Ethernet, WiFi).

Из всего ряда протоколов Modbus в рамках ПИВ наиболее часто используются протоколы Modbus RTU, Modbus TCP.

Сеть Modbus имеет следующие типы устройств (рис. 9):

- Ведущее устройство Modbus (Modbus master). Является активным устройством, устанавливает соединение с ведомыми устройствами и производит управление и сбор данных с них.
- Ведомое устройство Modbus (Modbus slave). Является пассивным устройством, ожидает соединение с ведущим устройством и получает от него команды управления.

Существует несколько видов команд, которые может отправить ведущее устройство ведомым в ходе взаимодействия. Данные команды перечислены ниже:

- Команда Modbus на чтение дискретного вывода (команда 0x01).
- Команда Modbus на чтение дискретного ввода (команда 0×02).
- Команда Modbus на чтение аналогового вывода (команда 0×03).
- Команда Modbus на чтение аналогового ввода (команда 0×04).
- Команда Modbus на запись дискретного вывода (команда 0×05).
- Команда Modbus на запись аналогового вывода (команда 0×06).
- Команда Modbus на запись нескольких дискретных выводов (команда 0x0F).
- Команда Modbus на запись нескольких аналоговых выводов (команда 0×10).

OPC UA (Open Platform Communications Unified Architecture) — промышленная спецификация, описывающая передачу данных в локальных

вычислительных сетях промышленных предприятий и взаимодействие устройств в них между собой. Существует две спецификации форматов передачи данных для сообщений OPC UA: наиболее часто используемый бинарный формат и формат SOAP/XML. Передача данных в OPC UA организована на базе модели сетевого взаимодействия «сервер — клиент». В настоящее время данный стандарт активно развивается в области повсеместного внедрения в решения ПИВ, например, сейчас идет активная разработка новой версии стандарта, поддерживающего технологии синхронизации в сетях связи TSN (Time-Sensitive Networking). Наиболее часто решения OPC UA можно встретить в различных реализациях SCADA-систем.

Сеть OPC UA имеет следующие типы устройств (рис. 10):

- Сервер OPC UA. Является пассивным устройством, ожидает подключение клиентов.
- Клиент OPC UA. Является активным устройством, подключается к серверу и передает управляющие сообщения и данные по мере необходимости.

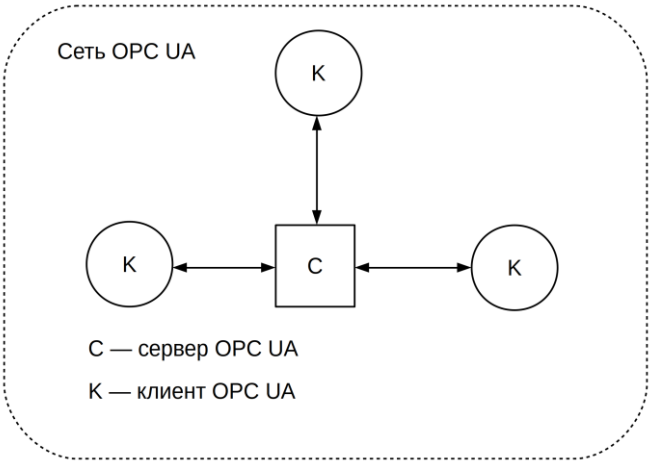


Рис. 10. Сеть OPC UA

Существуют следующие виды сообщений, которые передаются по протоколу OPC UA:

- HELLO (HEL), которое служит маркером начала передачи данных между клиентом и сервером.
- ACKNOWLEDGE (ACK), которое служит ответом на запрос клиента.

- OPEN (OPN), которое содержит уникальный идентификатор канала передачи данных, а также показывает, какой метод шифрования используется сервером.
- MESSAGE (MSG), которое содержит идентификатор канала передачи данных, тип запроса или ответа, временную метку, массивы передаваемых данных и др.
- CLOSE (CLO), которое сигнализирует об окончании сессии передачи данных, после чего соединение обрывается.

1.5. Подходы к реализации концепции промышленного Интернета вещей

1.5.1. Автоматизация работы промышленного оборудования

В настоящее время существует множество решений для автоматизации работы промышленных предприятий, такие как системы Supervisory Control And Data Acquisition (SCADA) [76, 98, 109].

Системы SCADA — это программно-аппаратный комплекс, состоящий из вычислительного устройства, включающего в себя различные физические интерфейсы для сбора данных с промышленного оборудования и из программного обеспечения, отвечающего за взаимодействие с данным оборудованием и обработку данных, получаемых от них. Основная задача систем SCADA — сбор информации с множества удаленных устройств, отображение данной информации в едином центре контроля состояния оборудования и при необходимости управление данным оборудованием. Основными задачами систем SCADA являются:

- взаимодействие с промышленными вычислительными устройствами в реальном времени;
- анализ информации в реальном времени;
- визуализация полученной информации;
- хранение поступающей от оконечного оборудования информации в специальных базах данных;

• сигнализация между устройствами в промышленных сетях, в том числе в аварийных ситуациях;

• генерация отчетов о ходе производственного процесса;

• обеспечение взаимодействия с внешними системами (СУБД, облачные сервера и др.).

Система SCADA состоит из трех основных компонентов (рис. 11):

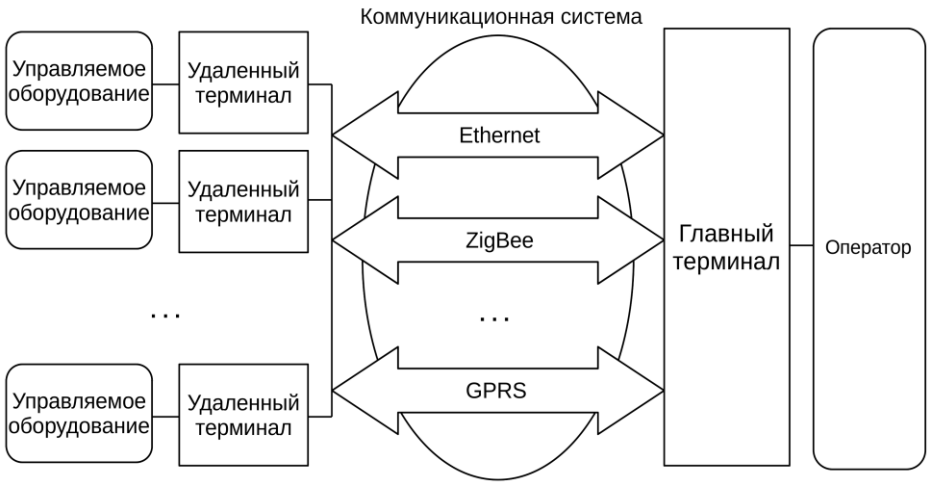


Рис. 11. Структура системы SCADA

• Удаленный терминал (Remote Terminal Unit — RTU). Удаленный терминал подключается к управляемому оборудованию и осуществляет управление и сбор данных о его состоянии в режиме реального времени.

• Главный терминал (Master Terminal Unit — MTU). Главный терминал осуществляет сбор данных с удаленных терминалов и обеспечивает их обработку, обеспечивает человеко-машинное взаимодействие, а также управление всей системой.

• Коммуникационная система (Communication system — CS). Данная система используется для передачи данных между удаленными и главным терминалами. Для передачи данных могут быть использованы мобильные сети, проводные сети, беспроводные сети, аналоговые телефонные линии, ISDN-сети.

Данные системы имеют высокие требования к безопасности передачи и хранения данных, к времени реакции системы во время аварийных ситуаций, к

отказоустойчивости и к точности работы. Ранее данные системы функционировали локально, без подключения к ССОП, но возрастающая конкуренция, возникающая из-за внедрения в отрасль новых технологий, вынуждает промышленные предприятия внедрять свои системы в общую централизованную систему через ССОП. Для обеспечения безопасности передачи данных и реализации дополнительных алгоритмов анализа и хранения данных в рамках ПИВ предлагается использовать такие технологии, как облачные, граничные и туманные вычисления.

1.5.2. Облачные, граничные и туманные вычисления

Под облачными вычислениями (cloud computing — CC) подразумевается удаленная серверная система с возможностью предоставления различных удаленных услуг пользователям, через удаленный сервер из любой точки ССОП [105, 108, 117]. Основной выгодой в использовании облачных сервисов является снижение вычислительной нагрузки на оборудование пользователя, удобный инструментарий для разработки собственного решения, доступ из любого места, с помощью ССОП и др. Обычно, когда говорят о CC, подразумевается три типа удаленных услуг:

- Программное обеспечение как услуга (от англ. software-as-a-service — SaaS). Данный тип услуг подразумевает предоставление удаленного доступа пользователю к некому программному обеспечению, функционирующему на сервере поставщика услуги.
- Платформа как услуга (от англ. platform-as-a-service — PaaS). Пользователю предоставляется доступ к удаленному облачному серверу для размещения собственного программного обеспечения и разработки и предоставление собственной удаленной услуги. Обычно в состав таких систем входит определенный набор инструментов для разработки ПО, в зависимости от направленности платформы.
- Инфраструктура как услуга (от англ. infrastructure-as-a-service — IaaS).

Данный тип услуг включает в себя большой набор различного программного и аппаратного обеспечения и позволяет развернуть в ССОП полностью рабочую сетевую инфраструктуру для создания собственной сетевой инфраструктуры, состоящей из таких элементов, как серверы обработки данных, базы данных, веб-серверы, виртуальные машины и др.

Облачные платформы впервые предоставили сетевую архитектуру, которая отвечала за предоставление удаленного доступа пользователю к какому-либо программному обеспечению, данным, серверам и др.

Несмотря на удобства, которые облачные сервисы предоставляли своим пользователям, возникали и очевидные проблемы, связанные с удаленным расположением обслуживающих серверов. Из самых распространенных проблем следует перечислить следующие:

- Показатель сетевой задержки увеличивается по мере удаленности пользователя от месторасположения облачного сервера (например, показатель сетевой задержки при использовании веб-сервисов Amazon из России может достигать значений 100–150 мс, когда для таких видов информации, как речевой и видеотрафик, рекомендуемая сетевая задержка составляет не более 100 мс).
- Зависимость пользователя от работы облачных серверов. В случае неполадок у поставщика или сетевой недоступности пользовательское решение, созданное на базе облачного сервиса, не будет функционировать.
- Нарушение конфиденциальности информации, особенно в случае с коммерческими предприятиями, у которых одним из важных пунктов является неразглашение информации о сотрудниках или клиентах и др.

Из-за этих проблем поставщики облачных решений создавали компромиссные решения, позволяющие частично или в редких случаях полностью отказаться от использования облачных сервисов.

Одним из таких решений стала концепция граничных вычислений (edge computing — EC) [87, 97]. Данная концепция подразумевает использование, совместно с глобальными удаленными облачными серверами, локальные серверы

для выполнения части функций облачных решений. Например, граничные серверы могут выполнять функции сбора и первичной обработки данных, затем передавать обработанную информацию на облачный сервер. Данное решение сохраняет преимущества использования облачных серверов для удаленных вычислений, удаленного мониторинга и управления из любой точки сети и в то же время позволяет реализовать локальную систему, частично или полностью независимую от облачной платформы, например, в области хранения персональных данных, аварийной локальной работы в случае утраты работоспособности облачного сервиса, выполнения отдельных чувствительных к задержкам задач и т. д.

Другая технология, которая является развитием идей облачных и граничных вычислений применительно к таким технологиям, как 5G/IMT-2020, машинное обучение и Интернет вещей, называется «туманные вычисления» (fog computing — FC) [15]. Данная технология развивается на базе группы стандартов OpenFog, описывающей распределенную сетевую инфраструктуру, которая будет использовать вычислительные возможности каждого устройства, подключенного к сети для выполнения различных задач. Данная технология использует в качестве вычислительных систем как облачные и граничные сервера, так и оконечные устройства пользователей. Данное решение было обосновано появлением и развитием концепции Интернета вещей и активным развитием идей анализа больших массивов данных (от англ. big data — BD) и машинного обучения (от англ. machine learning — ML), которые являются на настоящий момент одними из самых распространенных технологий в области искусственного интеллекта. Одной из причин появления данной концепции является опасение, что в случае увеличения доли межмашинного трафика, характерного для все растущего числа устройств Интернета вещей, в глобальной сети и использования методов искусственного интеллекта для их обработки современные технологии не позволят производить требуемого для этого количества электроэнергии, поэтому эта концепция подразумевает энергоэффективное использование всех вычислительных устройств в ССОП для интеллектуальной распределенной обработки данных. На настоящий

момент FC — самое передовое направление развития облачных вычислений.

Туманные вычисления наследуют преимущества таких технологий, как облачные и граничные вычисления, но также решают множество других проблем, таких как:

- неэффективное энергопотребление;
- решено и стандартизовано взаимодействие с системами интеллектуальной обработки данных (или системами искусственного интеллекта);
- внедрены технологии распределенных вычислений, разработана система управления данной процедурой;
- на базе данной технологии возможна реализация многоуровневой системы доступа к услуге, посредством взаимодействия группы серверов, находящихся на различных уровнях сетевой инфраструктуры (на стороне поставщика услуги, на стороне магистрального провайдера, на стороне провайдера доступа к сети Интернет, на стороне пользователя услуги и др.).

1.5.3. Системы хранения данных

В качестве систем хранения данных на промышленных предприятиях чаще всего применяются системы, называемые базами данных реального времени (БДРВ) [31]. Данные системы отличаются от более традиционных систем управления базами данных (СУБД) тем, что данные системы имеют высокую скорость выполнения операций, связанных с записью, чтением и исправлением хранимых данных, оптимизированы на работы с высокоскоростным аппаратным обеспечением и позволяют работать с огромными объемами данных в рамках одной базы данных (БД).

Базы данных реального времени должны учитывать следующие аспекты:

- Параллельная обработка. БДРВ должна обеспечивать параллельную обработку данных из разных источников.
- Распределенность. БДРВ должна быть динамически расширяемой и поддерживать распределенные хранение и поиск данных, а также обработку

запросов.

- Логическая согласованность данных. БДРВ должна поддерживать функции логического согласования данных по различным типам устройств и их предназначению, форматам данных, местонахождению и др.
- Временная согласованность. БДРВ должна обеспечивать временную согласованность, как времени обработки операций, так и временную согласованность данных.
- Очередность и обработка операций. БДРВ должна обеспечивать строгую очередность обработки операций и данных, поступающих из разных источников.
- Управление потоками ввода/вывода и очередями обработки данных. БДРВ должна динамически подстраиваться под поступающие потоки данных и иметь функции их перераспределения на другие потоки ввода/вывода, а также управлять очередями обработки данных.

Все операции БДРВ относятся к трем следующим типам запросов:

- запись данных в БД;
- чтение данных из БД;
- обновление содержания БД.

Также операции БДРВ имеют разные степени качества обслуживания для различных операций и устройств в рамках промышленных систем. В частности, можно привести следующие показатели качества обслуживания:

- Жесткое реальное время. Операция имеет наивысший приоритет и имеет критическое значение для стабильности работы системы.
- Мягкое реальное время. Данная операция всегда будет выполнена один раз, даже при условии ее позднего поступления.
- Толерантные к потерям. Данная операция после истечения срока, отданного на ее обработку, может быть отброшена из очереди выполнения.

В качестве примеров БДРВ можно привести следующие системы: IndustrialSQL Server, Wonderware Historian Server, RiakKV/RiakTS, OracleDB,

RedisDB и др.

1.5.4. Системы помощи принятия решений на основе систем машинного обучения

Системы помощи принятия решений (СППР, Decision Support System) — автоматизированные компьютерные системы, используемые для помощи людям, ответственным за принятие решений в сложных условиях, когда оператор не может самостоятельно принять рациональное, обоснованное решение за короткий промежуток времени [65, 70].

СППР являются одной из важнейших частей систем ПИВ. Огромное количество данных, генерируемых системами ПИВ, не могут быть обработаны оператором системы в реальном времени. За обработку данных и их представление в удобном для оператора виде отвечают системы СППР. Так как анализ такого объема данных от множества различных типов устройств в ПИВ представляет собой сложную вычислительную задачу, для помощи в принятии решений в рамках промышленных предприятий предлагается использовать более современный вид систем помощи принятия решений — интеллектуальные системы помощи принятия решений (ИСППР). ИСППР отличаются от более традиционных систем СППР тем, что данные системы используют методы анализа больших объемов информации, машинного обучения и моделирования процессов в реальном времени для помощи принятия решения оператором системы, в случае необходимости. Одним из важнейших элементов ИСППР является направление машинного обучения.

Машинное обучение (МО, Machine Learming) — это направление в информационных технологиях, отвечающее за интеллектуальный анализ информации и основанное на применении самообучающихся алгоритмов. Обучение систем МО происходит следующим образом — на вход системы поступает информация, за анализ которой отвечает ядро системы МО (алгоритм обработки данных, например многослойный персептрон, метод опорных векторов, логистическая регрессия и др.).

1.6. Шлюзы Интернета вещей

В настоящее время идет активное развитие и внедрение такого класса устройств в сетях Интернета вещей и промышленного Интернета вещей, как шлюзы. Данные устройства отвечают за обеспечение взаимодействия специфических технологий связи и передачи данных ИВ и ПИВ, как между собой, так и с ССОП.

Рекомендация МСЭ-Т Y.4101/Y.2067 «Основные требования и возможности шлюзов для приложений промышленного Интернета вещей» [20] дает следующее определение шлюза Интернета вещей — это устройство ИВ, соединяющее другие устройства с сетями связи. Оно выполняет необходимые преобразования между протоколами, используемыми в сетях связи, и протоколами, используемыми устройствами.

В настоящее время существует целый ряд решений, предназначенных для подключения устройств ПИВ в сетевую инфраструктуру промышленных предприятий. Например, в число шлюзов ПИВ входят следующие устройства: Dell Edge Gateway 3001, ADLINK MXE-101i, NEXCOM NIO-100, ICP DAS UA-5231.

Выводы по главе 1

1. Проведено исследование концепции промышленного Интернета вещей и перспектив ее развития.
2. Разработана классификация сфер автоматизации для промышленных предприятий, в рамках внедрения систем промышленного Интернета вещей.
3. Проведен обзор существующих на данный момент международных стандартов в области ПИВ по архитектуре систем ПИВ, рассмотрены подходы к их реализации.
4. Исследованы существующие решения, реализующие функции гетерогенного шлюза в рамках сетевой инфраструктуры промышленных предприятий.

Глава 2. РАЗРАБОТКА МОДЕЛЕЙ ФРАГМЕНТА СЕТИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

2.1. Классификация трафика промышленного Интернета вещей

2.1.1. Классификация источников трафика промышленного Интернета вещей

Для разработки модельной сети, которую предлагается использовать для исследования свойств трафика ПИВ, необходимо определить возможные типы источников трафика ПИВ. В качестве основных источников трафика для решений промышленного Интернета вещей следует выделить [41, 99]:

- Датчики и актуаторы. Используются для автоматизации работы промышленного оборудования. Могут подключаться как напрямую к промышленному оборудованию и управляться через специальные приложения (например, с помощью ЧПУ), так и через специальные системы контроля и управления работы промышленного оборудования (например, SCADA, SAP Hana, OPC UA и др.).
- Бизнес-приложения (CRM, ERM и др.). Одним из наиболее важных аспектов работы предприятия является автоматизация работы бизнес-процессов предприятия.
- Открытые веб-данные. Информация из открытых источников или веб-страниц в Сети может использоваться как для обеспечения функционирования различных бизнес-процессов, так и для целей оптимизации работы предприятия, с помощью различных аналитических алгоритмов.
- Мультимедийные системы. В качестве источников могут выступать видеокамеры и микрофоны, которые используются для систем обеспечения безопасности предприятия.
- Системы позиционирования. Данные системы могут использоваться для позиционирования промышленного оборудования, людей и транспорта, как

в рамках предприятия, так и глобально, в масштабах региона или планеты.

Предположительно, каждый из вышеперечисленных видов трафика будет иметь уникальные сетевые параметры, такие как характер поступления, характер распределения размера сетевых пакетов, коэффициент самоподобия, тип протоколов сетевого, транспортного и прикладного уровней, наличие или отсутствие криптографических протоколов для обеспечения безопасности при передаче данных и др.

2.1.2. Классификация сценариев функционирования устройств, систем и сетей промышленного Интернета вещей

Каждый из источников трафика может работать по собственному уникальному сценарию сетевого взаимодействия, поэтому в рамках данного исследования необходимо выделить следующие сценарии работы различных типов устройств в промышленном Интернете вещей [66]:

- Регулярный. Оконечное устройство ПИВ отправляет пакеты данных на удаленное устройство хранения данных предприятия (например, сервер систем управления базами данных, системы промышленного управления и контроля работы предприятия и др.), с заранее заданной периодичностью.
- Событийно-ориентированный. Оконечное устройство ПИВ отправляет пакеты данных на удаленное устройство хранения данных предприятия по какому-либо событию (запрос данных пользователем или другим устройством, отправка информации об изменении состояния датчика и др.).
- По расписанию. Оконечное устройство ПИВ отправляет пакеты данных на удаленное устройство хранения данных предприятия согласно заранее заданному расписанию.

2.1.3. Классификация трафика промышленного Интернета вещей по качеству обслуживания

Также приложения и услуги ПИВ имеют собственные требования ко времени обслуживания. В частности, имеет смысл выделить следующие типы обслуживания:

- Реального времени. Данные приложения и услуги имеют жесткие ограничения по времени доставки сообщений, и поэтому данный тип сообщений доставляется за минимально возможное время.
- Толерантные к задержкам. Данные приложения и услуги не имеют жестких ограничений по времени доставки сообщений.

2.2. Структура рассматриваемого фрагмента сети промышленного Интернета вещей

Согласно предложенной классификации источников трафика ПИВ были исследованы следующие существующие реальные системы, применяемые в решениях промышленной автоматизации:

1. Сеть, состоящая из промышленных устройств для аддитивного производства, соответствующих пункту «Датчики и актуаторы» приведенной выше классификации источников трафика для систем ПИВ, и состоящая из следующих устройств:
   - Trumpf TruPrint 1000 — промышленная система аддитивной печати металлических изделий.
   - 3D Systems ProJet 4500 — промышленная система аддитивной печати пластиковых изделий.
2. Система контроля ресурсов предприятия на основе системы «1С-Битрикс», соответствующая пункту «Бизнес-приложения» [46].
3. Системы передачи мультимедийной информации для решения задач видеонаблюдения, соответствующие пункту «Мультимедийные системы»:
   - Система для организации видеомониторинга в режиме реального времени на основе программного обеспечения с открытым исходным кодом Open Broadcast Server (OBS).
   - Система видеомониторинга для хранения и предоставления видеоданных по запросу, основанная на облачном решении Ivideon, поставляемом вместе с IP-камерой OCo OP-2220F-MSD [47].

4. Открытые веб-приложения, соответствующие пункту «Открытые веб-данные»:

- Open Weather Maps (OWM) — открытое веб-приложение, используемое для определения текущего состояния окружающей среды (температура, атмосферное давление, уровень влажности и т. д.) на заданной территории.
- Open Street Maps (OSM) — открытое веб-приложение, используемое для определения местоположения различных объектов (техника, сотрудники, животные и т. д.) в глобальной системе координат.

5. Система локального позиционирования объектов на производстве Nanotron NanoPAN 5375, соответствующая пункту «Системы позиционирования».

В рамках проведения данного исследования, на основе рассматриваемых систем промышленной автоматизации, была разработана модельная сеть, на основе которой проводился анализ сетевого трафика от различных систем ПИВ.

На рисунке 12 представлена структура разработанной на базе лаборатории Интернета вещей СПбГУТ [36, 96] модельной сети [22].

Представленная модельная сеть состоит из следующих элементов:

- Промышленный сервер — программно-аппаратный комплекс, реализующий функции серверного устройства для исследуемых систем [48].
- Промышленная система (ПС Trumpf TruPrint 1000, ПС 3D Systems ProJet 4500) — программно-аппаратный комплекс, реализующий функции клиентского устройства для источников трафика типа «Датчики и акутаторы».
- Система контроля работы предприятия (СКРП «1С-Битрикс») — программно-аппаратный комплекс, реализующий функции клиентского устройства для источников трафика типа «Бизнес-приложения».
- Система видеомониторинга — программно-аппаратный комплекс, реализующий функции клиентского устройства для источников трафика типа «Мультимедийные системы».
- Система позиционирования (СП Nanotron NanoPAN 5375) — программно-аппаратный комплекс, реализующий функции клиентского устройства

для источников трафика типа «Системы позиционирования».

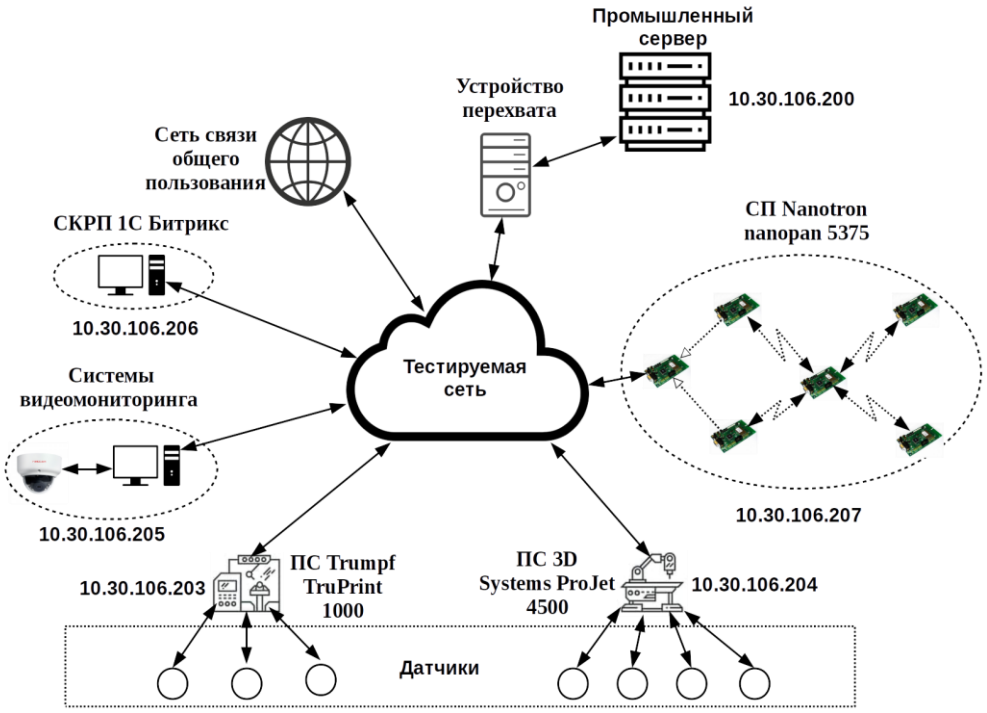


Рис. 12. Структура модельной сети для тестирования систем ПИВ

- Подключение к сети связи общего пользования (ССОП) необходимо для проведения исследования систем, соответствующих источнику трафика типа «Открытые веб-данные».
- Устройство перехвата — программно-аппаратный комплекс, реализующий функции устройства перехвата и анализа сетевого трафика [100].
- Тестируемая сеть — локальная вычислительная сеть, имитирующая архитектуру локальной сети промышленного предприятия.

Созданная модельная сеть может быть использована как для исследования трафика, поступающего от систем ПИВ, так и для исследования влияния данных систем на тестируемую сеть.

На базе разработанной модельной сети возможно провести исследование свойств трафика от приложений, устройств и систем, применяемых в рамках промышленного Интернета вещей.

2.3. Исследование трафика промышленного Интернета вещей

2.3.1. Постановка целей и задач исследования трафика промышленного Интернета вещей

Для разработки структуры имитационной модели для проведения анализа работы систем ПИВ необходимо исследовать свойства генерации и обслуживания трафика ПИВ на основе определенной в пункте 2.1.1 классификации источников трафика ПИВ. Основными свойствами, которые необходимы для разработки имитационной модели работы фрагмента сети ПИВ, являются распределения времени между поступлениями пакетов, распределения размеров пакетов, распределения времени обслуживания поступающих пакетов, коэффициент самоподобия трафика. Чтобы получить данные свойства трафика ПИВ, необходимо решить следующие задачи:

- Провести эксперимент на базе разработанной модельной сети, описывающей работу фрагмента сети ПИВ, перехватить трафик, поступающий от оконечных устройств ПИВ, и трафик, поступающий на обслуживающее устройство.
- На основе перехваченного трафика провести исследование времени поступления трафика ПИВ.
- На основе перехваченного трафика провести исследование распределения размеров пакетов для поступающего трафика ПИВ.
- На основе перехваченного трафика провести исследование времени обслуживания каждого пакета, поступающего на обслуживающее устройство.
- На основе перехваченного трафика провести исследование свойств самоподобия поступающего трафика ПИВ.

2.3.2. Основные исследуемые характеристики трафика промышленного Интернета вещей

В качестве основных свойств для анализа трафика, полученного от систем, функционирующих в рамках разработанного фрагмента сети, были выбраны:

- распределение интенсивности поступления сообщений от каждого из

источников трафика;

- распределение объема пакетов от источника трафика и средний размер пакета от каждого из источников трафика;
- распределение времени обслуживания одного пакета от источника трафика и среднее время обслуживания для каждого из источников трафика;
- коэффициент Хёрста (самоподобия) для трафика от каждого из источников.

2.3.3. Структура экспериментальной сети для исследования характеристик трафика промышленного Интернета вещей

Для анализа трафика ПИВ на основе разработанной архитектуры ПАК предлагается использовать модельную сеть, изображенную на рисунке 13.

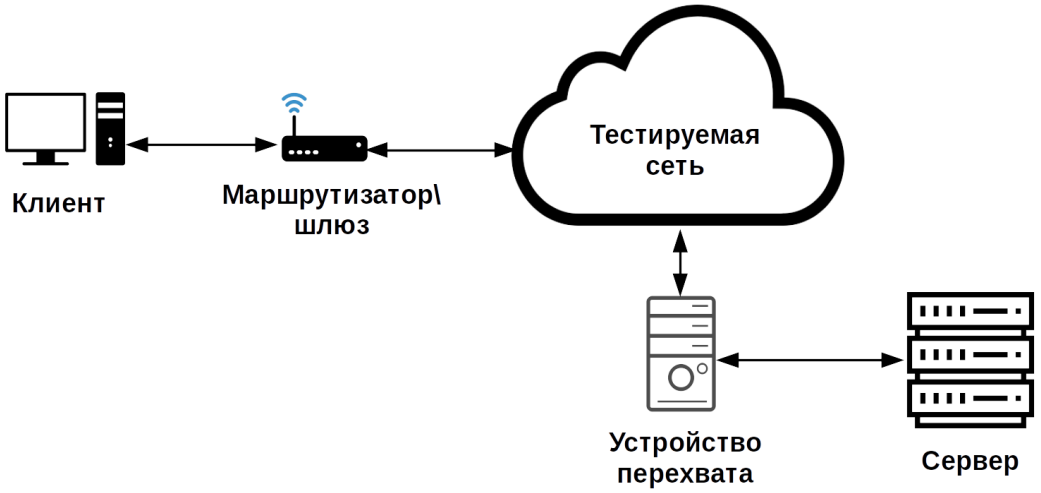


Рис. 13. Модельная сеть для тестирования генерации трафика ПИВ

На представленной модельной сети имеются следующие элементы:

- Сервер — программно-аппаратный комплекс, реализующий функции серверного устройства.
- Клиент — программно-аппаратный комплекс, реализующий функции клиентского устройства.
- Устройство перехвата — программно-аппаратный комплекс, реализующий функции устройства перехвата и анализа сетевого трафика.

- Маршрутизатор/шлюз — вычислительное устройство, выступающее локальным маршрутизатором или шлюзом для подключения клиента к тестируемой сети.
- Тестируемая сеть — локальная вычислительная сеть, имитирующая архитектуру локальной сети промышленного предприятия.

2.3.4. Алгоритм исследования характеристик трафика

На основе экспериментальной сети, описанной в 2.3.3, и систем, представленных в 2.2, была произведена генерация трафика в режиме активной работы представленного оборудования и был произведен перехват трафика в количестве не менее 2000 пакетов.

Для анализа интенсивности поступления пакетов от источника были использованы временные значения, представляющие собой интервалы времени между поступлениями пакетов на сетевой интерфейс. Получившаяся выборка была разбита на 100 равноразмерных временных отрезков (между максимальным и минимальным значением выборки), и с их помощью была построена вероятностно-временная характеристика для исследуемого трафика. Для каждого из получившегося распределения с помощью критерия согласия Колмогорова-Смирнова подбиралось наиболее подходящее вероятностное распределение. Затем с помощью метода наименьших квадратов и алгоритма обобщенного приведенного градиента была проведена аппроксимация исходных данных [37, 44].

Далее был произведен идентичный процесс для анализа распределения объемов сетевых пакетов для перехваченного трафика и распределения времени обслуживания поступающих пакетов.

Далее был рассчитан коэффициент Хёрста для выборок, ранее полученных и исследованных при анализе интенсивности поступления сообщений [101].

2.3.5. Аналитическая модель работы сети промышленного Интернета вещей

Для проведения математического моделирования случайных распределений для различных параметров перехваченного трафика и времени его обслуживания

были выбраны следующие вероятностные распределения [27]:

- экспоненциальное;
- двухпараметрическое гамма;
- Эрланга m-го порядка;
- двухпараметрическое бета первого рода;
- Вейбулла-Гнеденко.

Экспоненциальное распределение случайных величин представлено далее и описывается функцией распределения:

$$F(x) = 1 - e^{-\lambda x}, \quad (1)$$

где λ — параметр масштаба ($\lambda > 0$).

Классическое двухпараметрическое гамма-распределение случайных величин представлено далее и описывается функцией распределения:

$$F(x) = \frac{1}{\Gamma(\alpha)} * \int_0^{\lambda x} t^{\alpha - 1} e^{-t} dt, \quad (2)$$

где α — параметр формы, λ — параметр масштаба ($\alpha > 0$, $\lambda > 0$),

$$\Gamma(\alpha) = \int_0^{\infty} t^{\alpha - 1} e^{-t} dt \text{ — гамма-функция.} \quad (3)$$

Распределение Эрланга случайных величин m-го порядка представлено далее и описывается функцией распределения:

$$F(x) = 1 - e^{-\lambda x} \sum_{i=0}^{m-1} \frac{(\lambda x)^i}{i!}, \quad (4)$$

где λ — параметр масштаба, а m — параметр формы, целое положительное число ($\lambda > 0$, $m \geq 1$).

Классическое бета-распределение случайных величин первого рода представлено далее и описывается функцией распределения:

$$F(x) = \frac{B_x(\alpha,\beta)}{B(\alpha,\beta)}, \quad (5)$$

где α, β — параметры формы ($\alpha > 0, \beta > 0$),

$$B_x(\alpha,\beta) = \int_0^x t^{\alpha - 1} (1-t)^{\beta - 1} dt \text{ — неполная бета-функция,} \quad (6)$$

$$B(\alpha,\beta) = \int_0^{\infty} \frac{t^{\alpha - 1}}{(1+t)^{\alpha+\beta}} dt \text{ — бета-функция.} \quad (7)$$

Классическое распределение случайных величин Вейбулла-Гнеденко первого рода представлено далее и описывается функцией распределения:

$$\mathrm{F}(x) = 1 - exp\left[-\left(\frac{x}{\alpha}\right)^{c}\right], \quad (8)$$

где α — параметр масштаба, а c — параметр формы ($\alpha > 0$, $c > 0$).

Поиск оптимальных значений для построения вероятностных распределений был произведен с помощью метода обобщенного приведенного градиента на основе коэффициента, полученного при помощи метода наименьших квадратов [38]:

$$\mathrm{К_{МНК}}(t) = \sum_{1}^{100}[\mathrm{P}(t_i) - \mathrm{P}(t_i, t_{i+1})]^2, \quad (9)$$

где $\mathrm{P}(t)$ — вероятность попадания случайного значения интервала времени между поступлениями сообщений в промежутке от t_i до $t_{(i+1)}$, согласно экспериментальным данным, а

$$\mathrm{P}(t_i, t_{i+1}) = |\mathrm{F}(t_{i+1}) - \mathrm{F}(t_i)| \quad (10)$$

— вероятность попадания случайного значения интервала времени между поступлениями сообщений, согласно выбранному закону распределения F(t).

Сходимость теоретических и практических распределений сверялась с помощью критерия согласия Колмогорова-Смирнова при доверительной вероятности 95 % [39, 71]:

$$D_n = \max[F_n(x) - F(x)], \quad (11)$$

где D_n — статистика критерия для эмпирической функции распределения $F_n(x)$. Если D_n не входит в табличное значение квантилей распределения Колмогорова K_α, то используется исправленное значение статистики критерия D_n^*, рассчитываемое по формуле:

$$D_n^* = \sqrt{\frac{n*m}{n+m}}D_n, \quad (12)$$

где n — размер выборки для практического распределения, а m — размер выборки для теоретического распределения. Если D_n^* не превышает значение квантиля распределения Колмогорова, то гипотеза об идентичности практического

и теоретического распределений принимается:

$$D_n^* \leq K_\alpha, \quad (13)$$

где K_α — квантиль распределения Колмогорова, который в случае достаточно высокой приближенности значения уровня значимости α к единице может быть рассчитан как:

$$K_\alpha = \sqrt{-\frac{1}{2}\ln\frac{1-\alpha}{2}}. \quad (14)$$

Коэффициент Хёрста (H) — это параметр, характеризующий самоподобие системы и используемый в анализе временных рядов [88]. H может принимать следующие значения:

- при $0 < H < 0{,}5$ — временной ряд не самоподобный, антиперсистентный, для него более вероятна смена направления отклонения, высокие значения отклонения следуют за низкими и наоборот;
- при $H = 0{,}5$ — временной ряд является абсолютно случайным, следующее значение не зависит от предыдущих значений;
- при $0{,}5 < H < 1$ — временной ряд самоподобный, персистентный.

В данной работе коэффициент Хёрста рассчитывается на основе ряда различных методов, таких как нормированный размах (*RS*), мультифрактальный анализ дисперсии детрендированных остатков (*MFDFA*), метод периодограмм Даниэля (*Daniell*), на основе наклона спектральной плотности и метода Виттла (*Whittle*), являющегося модификацией метода Даниэля [59]. Расчет показателей Хёрста проводится на базе интервалов времени между поступлением пакетов.

RS-анализ

RS-анализ основан на оценке отношения величины размаха — разности между максимальным и минимальным значением отклонения — и значения стандартного отклонения по одной и той же выборке [26, 88]. Расчет производится по следующему алгоритму:

1. Ряд N, который является выборкой интервалов времени между поступлениями сетевых пакетов, делится на A смежных промежутков E длиной n,

где a — номер промежутка a ∈ (1, 2, 3... A). Среднее значение E_a для каждого из промежутков I_a определяется следующим образом:

$$E_a = \frac{1}{n}\sum_{k=1}^{n} N_{k,a}, \text{ где } k \in (1, 2, 3... n). \quad (15)$$

2. Временной ряд накопленных отклонений $X_{k,a}$ от среднего значения E_a для каждого из промежутков I_a, при $k \in (1, 2, 3... n)$рассчитывается как:

$$X_{k,a} = \sum_{i=1}^{k}(N_{i,a} - E_a), \text{ где } i \in (1, 2, 3... k). \quad (16)$$

3. Размах диапазона накопленных отклонений R_a рассчитывается как разница максимального и минимального значения отклонения $X_{k,a}$ в пределах каждого промежутка I_a:

$$R_a = \max(X_{k,a}) - \min(X_{k,a}), \text{ где } 1 \le k \le n. \quad (17)$$

4. Стандартное отклонение S_a рассчитывается для каждого промежутка I_a как:

$$S_a = \frac{1}{n}\sum_{k=1}^{n}(N_{k,a} - E_a)^2, \text{ где } k \in (1, 2, 3... n). \quad (18)$$

5. Нормированный размах диапазона отклонений для каждого промежутка можно получить путем деления размаха диапазона накопленных отклонений R_a на стандартное отклонение S_a. Таким образом, нормированный размах диапазона отклонений $(R/S)_n$ для периода с n элементов в промежутке определяется как:

$$(R/S)_n = \frac{\sum_{a=1}^{A}(R_a/S_a)}{A}, \quad (19)$$

где A — количество промежутков, а $a \in (1, 2, 3... A)$.

6. Пункты от 1 до 6 повторяются при увеличенном значении n — количества элементов в промежутке вплоть до значения $N/2$.

7. Далее выполняется регрессия с помощью метода наименьших квадратов на $\log n$, где n — количество элементов в промежутке, и $\log(R/S_n)$, где R/S_n — нормированный размах диапазона отклонений. В результате получится уравнение $\log(R/S_n) = H\log(n) + c$, где наклон уравнения H — коэффициент Хёрста. Таким образом, расчет показателя Хёрста можно описать следующим уравнением:

$$H=\frac{n\sum_{i=1}^{n}\ln i\ln(R_i/S_i)-\sum_{i=1}^{n}\ln i\sum_{i=1}^{n}\ln(R_i/S_i)}{n\sum_{i=1}^{n}(\ln i)^2-\left(\sum_{i=1}^{n}\ln i\right)^2}$$, где $i \in (2, 3... n)$. (20)

Анализ MFDFA

MFDFA (Multifractal DFA) является методом, основанным на разбиении исходной выборки на выборку, состоящую из значений детрендированной функции отклонения для каждого из сегментов выборки [26, 93, 126]. Расчет производится по следующему алгоритму:

1. На основе выборки интервалов времени между поступлениями сетевых пакетов x размером N рассчитывается среднее значение выборки $\bar{x}$ и затем согласно кумулятивной функции отклонения рассчитывается массив остатков по формуле:

$Y_i = \sum_{k=1}^{i}(x_k - \bar{x})$, где (21)

Y_i — значение выборки Y, содержащей кумулятивное отклонение для элемента i, а $i = 1, 2, \dots, N$.

2. Далее необходимо разбить выборку Y на $N_s = integer(N/s)$ участков равного размера s. Во избежание случаев, когда выборка целочисленно не делится на N_s сегментов, к исходной выборке добавляется данная выборка в обратном порядке. В результате получается выборка размером $2N_s$.

3. Далее необходимо получить выборку Y_v, состоящую из значений тренда по линейной функции, с помощью ряда Y и метода наименьших квадратов. Таким образом, значения отклонения a и угла наклона b тренда можно вычислить следующим образом:

$$b=\frac{2N_S\sum_{i=1}^{2N_S}iY_i-\sum_{i=1}^{2N_S}i\sum_{i=1}^{2N_S}Y_i}{2N_S\sum_{i=1}^{2N_S}(i)^2-\left(\sum_{i=1}^{2N_S}i\right)^2}$$, где $i \in (1, 2, 3... 2N_S)$, (22)

$$a=\frac{\sum_{i=1}^{2N_S}Y_i-b\sum_{i=1}^{2N_S}i}{2N_s}$$, где $i \in (1, 2, 3... 2N_S)$. (23)

На основе данных коэффициентов можно рассчитать выборку $\mathrm{F}^2(v,s)$, состоящую из значений функции детрендированного массива, по следующему правилу:

$$\mathrm{F}^2(v,s) =$$

$$\begin{cases} \frac{1}{s}\sum_{i=1}^{s}(Y[(v-1)s+i]-aY[(v-1)s+i]-b)^2, \\ \text{для } v=1,\ 2,\ \dots\ N_s \\ \frac{1}{s}\sum_{i=1}^{s}(Y[N-(v-N_s)s+i]-aY[N-(v-N_s)s+i]-b)^2, \\ \text{для } v=N_s+1, N_s+2,\ \dots\ 2N_s. \end{cases} \quad (24)$$

4. Для получения флуктуационной функции, которая будет сопоставлена со значением коэффициента Хёрста, необходимо сложить все сегменты предыдущей выборки согласно следующему правилу:

$$\mathrm{F}_q(s)=\sqrt{\frac{1}{2}N_s\sum_{v=1}^{2N_s}F^2(v,s)} \quad (25)$$

5. На основе соотношения

$$\mathrm{F}_q(s)\sim s^{H+1} \quad (26)$$

и с помощью метода наименьших квадратов вычисляем значение показателя b по логарифмическому соотношению ln $F_q(s)$ к ln s, где N_{F_q} — размер выборки $F_q(s)$:

$$b=\frac{N_{F_q}\sum_{i=1}^{N_{F_q}}lns_i lnF_q(s_i)-\sum_{i=1}^{N_{F_q}}lns_i\sum_{i=1}^{N_{F_q}}F_q(s_i)}{N_{F_q}\sum_{i=1}^{N_{F_q}}(lns_i)^2-\left(\sum_{i=1}^{N_{F_q}}lns_i\right)^2}, \text{ где } i\in\left(1,\ 2,\ 3\dots N_{F_q}\right), \quad (27)$$

затем с помощью b вычисляем значение коэффициента Хёрста по следующему правилу:

$H=b-1$, где H — коэффициент Хёрста. (28)

Метод периодограмм

Метод периодограмм, или метод Даниэля, является методом, основанным на оценке наклона спектральной плотности, и заключается в оценке угла наклона функции спектральной плоскости, полученной путем преобразования исходной выборки [26, 72-73]. Алгоритм расчета коэффициента самоподобия методом периодограмм представлен ниже:

1. На основе выборки интервалов времени между поступлениями сетевых пакетов X рассчитываются значения выборки периодограмм I_N от частоты $\omega=\frac{2\pi m}{N}$, где N — длина выборки X,$m\in(2,\ 3,\ \dots,\ N/2)$ — размер подвыборки:

$$I_N(\omega)=\frac{1}{2\pi N}\left|\sum_{j=1}^{N}X(j)\mathrm{e}^{\mathrm{i}j\omega}\right|^2, \quad (29)$$

где i — мнимая часть комплексного числа, т. к. согласно формуле Эйлера $e^{i\pi} = -1$, то выражение (30) можно представить в следующем виде, удобном для компьютерных вычислений:

$$I_N(\omega) = \frac{1}{2\pi N}\left|\sum_{j=1}^{N} X(j)(-1)^{\frac{2mj}{N}}\right|^2. \quad (30)$$

2. Так как величина $I_N(\omega)$ пропорциональна значению $|\omega|^{1-2H}$:

$$I_N(\omega) \sim |\omega|^{1-2H}, \quad (31)$$

то значение коэффициента Хёрста H можно рассчитать с помощью метода наименьших квадратов и значения тангенса угла наклона b по соотношению $\ln I_N(\omega)$ от $\ln \omega$, где N_ω — длина ряда I_N:

$$b = \frac{N_\omega \sum_{i=1}^{N_\omega} ln\omega_i ln I_N(\omega_i) - \sum_{i=1}^{N_\omega} ln\omega_i \sum_{i=1}^{N_\omega} I_N(\omega_i)}{N_\omega \sum_{i=1}^{N_\omega} (ln\omega_i)^2 - \left(\sum_{i=1}^{N_\omega} ln\omega_i\right)^2}, \text{ где } i \in (1, 2, 3 \ldots N_\omega), \quad (32)$$

тогда значение коэффициента Хёрста можно вычислить с помощью следующего уравнения:

$$H = \frac{1-b}{2}. \quad (33)$$

Локальный метод Виттла

Локальный метод Виттла является методом, основанным на оптимизационном методе оценки параметра Хёрста с помощью периодограмм [28, 72-73, 83]. Алгоритм расчета коэффициента самоподобия методом Виттла представлен ниже:

1. Рассчитывается выборка периодограмм по исходной выборке интервалов времени между поступлениями пакетов X для значений размеров подвыборки $m \in (2,\ 3,\ \ldots,\ N/2)$, согласно пункту 1 метода периодограмм и формулам (30–31).

2. Далее необходимо получить минимум функции $R(H)$, по значению коэффициента H, с шагом $dH \leq 0{,}01$:

$$R(H) = ln\frac{1}{n}\frac{\sum_{i=1}^{n} I(\omega_i)}{\omega_i^{1-2H}} + \frac{1-2H}{n}\sum_{i=1}^{n}\omega_i \to \min, \quad (34)$$

где $n = \frac{N}{2}$, а N — размер изначальной выборки X, а $\omega = \frac{2\pi m}{N}$ — частота. Значение H, которое необходимо подставить, чтобы получить $\operatorname{argmin} R(H)$, и является коэффициентом самоподобия по методу Виттла.

2.3.6. Результаты исследования характеристик трафика промышленного Интернета вещей

В результате проведения экспериментального исследования характеристик трафика для каждого из различных источников были получены:

- вероятностные распределения, описывающие распределение временных интервалов между поступлениями сетевых пакетов (интенсивность поступления сетевых пакетов);
- вероятностные распределения, описывающие распределение размеров сетевых пакетов;
- вероятностные распределения, описывающие распределение времени обслуживания сетевых пакетов (интенсивность обслуживания сетевых пакетов);
- вероятностные распределения, описывающие распределение времени сетевой задержки между клиентским и серверным устройством в модельной сети;
- значения коэффициента самоподобия (Хёрста), которые были получены с помощью четырех методов: RS-анализа, MFDFA-анализа, метода периодограмм, локального метода Виттла.

Результаты анализа времени между поступлениями сетевых пакетов от различных источников трафика отображены в таблице 1. В таблице показаны выбранные вероятностные распределения и их коэффициенты для каждого из исследуемых типов трафика.

Таблица 1. Вероятностные распределения, описывающие интенсивность поступления сетевых пакетов

Источник трафика	Исследуемые временные интервалы, мкс	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Trumpf TruPrint 1000	0–60 000	43,70	Бета первого рода	$\alpha = 36\,681{,}97$; $\beta = 670\,238{,}20$
	0–350 000	44,32	Бета первого рода	$\alpha = 7081{,}16$; $\beta = 19\,719{,}89$
	350 000–1 015 000	4,25	Равномерное непрерывное	–
	3 950 000–5 000 000	6,32	Равномерное непрерывное	–
3D Systems ProJet 4500	0–100 000	49,93	Бета первого рода	$\alpha = 15\,012{,}99$; $\beta = 276\,073{,}23$
	0–300 000	49,89	Бета первого рода	$\alpha = 13\,629{,}12$; $\beta = 38\,227{,}91$
Система OBS	0–200 000	99,92	Экспоненциальное	$\lambda = 189{,}21$
Система Ivideon	0–800 000	99,99	Экспоненциальное	$\lambda = 311{,}76$
«1С-Битрикс»	0–50 000	72,07	Экспоненциальное	$\lambda = 47{,}33$
	0–5 000 000	25,98	Гамма	$\alpha = 0{,}88$; $\lambda = 9{,}25$
Веб-приложение OWM	0–100 000	99,02	Экспоненциальное	$\lambda = 2059{,}22$
Веб-приложение OSM	0–100 000	99,09	Экспоненциальное	$\lambda = 2188{,}52$
Nanotron NanoPAN 5375	0–240 000	99,30	Эрланга	$m = 3$; $\lambda = 40{,}00$

Результаты анализа размеров сетевых пакетов от различных источников трафика отображены в таблице 2. В таблице показаны выбранные вероятностные распределения и их коэффициенты для каждого из исследуемых типов трафика, а также средние значения размера сетевых пакетов при доверительной вероятности 95 %. Для корректного отображения размеров пакетов для веб-приложения *OWM* необходимо умножить значения, генерируемые экспоненциальным распределением, на 1000.

Таблица 2. Вероятностные распределения, описывающие характер распределения объема сетевых пакетов

Источник трафика	Среднее значение размера пакета, байт	Исследуемые интервалы, байт	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Trumpf TruPrint 1000	966 ± 10	184	12,73	Эмпирическое дискретное	–
		184	12,73	Эмпирическое дискретное	–
3D Systems ProJet 4500	573 ± 7	67	49,99	Равномерное дискретное	–
		1080	49,90		
Система OBS	1285 ± 4	74–437	3,17	Равномерное непрерывное	–
		437–703	10,05	Гамма	$\alpha = 5{,}80$; $\lambda = 16{,}67$
		703–1433	5,86	Равномерное непрерывное	–
		1434	80,92	Детерминированное	–
Система Ivideon	1451 ± 2	1458	78,99	Эмпирическое дискретное	–
		1514	19,51		
«1С-Битрикс»	1019 ± 26	66	15,65	Эмпирическое дискретное	–
		74	5,19		
		203	3,45		
		276	3,54		
		574	4,22		
		1079	2,70		
		1466	61,80		
Веб-приложение OWM	945 ± 22	66	20,98	Детерминированное	–
		67–302	8,32	Экспоненциальное	$\lambda = 66{,}67$
		302–990	8,11	Равномерное непрерывное	–
		990–1420	14,61	Вейбулла-Гнеденко	$c = 10{,}58$; $\alpha = 276{,}27$
		1434	47,78	Детерминированное	–
Веб-приложение OSM	1326 ± 6	66–1433	11,35	Равномерное непрерывное	–
		1434	88,65	Детерминированное	–

Продолжение таблицы 2

Источник трафика	Среднее значение размера пакета, байт	Исследуемые интервалы, байт	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Nanotron NanoPAN 5375	366 ± 3	74	11,87	Детерминированное	–
		75–437	19,55	Гамма	α = 18,86; λ = 11,11
		438	68,53	Детерминированное	–

Результаты анализа времени обработки сетевых пакетов на сервере ПИВ для каждого из различных видов источников трафика отображены в таблице 3. В таблице показаны выбранные вероятностные распределения и их коэффициенты для каждого из исследуемых типов трафика.

Таблица 3. Вероятностные распределения, описывающие интенсивность обработки сетевых пакетов

Источник трафика	Исследуемые временные интервалы, мкс	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Trumpf TruPrint 1000	48 800–52 223	66,54	Гамма	α = 201,68; λ = 144 183,00
	48 800–59 075	6,19	Гамма	α = 17 670,00; λ = 1 752 979,00
	48 800–60 445	23,88	Гамма	α = 29 038,00; λ = 2 628 594,00
3D Systems ProJet 4500	48 800–52 223	66,70	Гамма	α = 133,73; λ = 98 155,00
	48 800–59 623	3,43	Гамма	α = 17 481,00; λ = 1 735 705,00
	48 800–60 308	26,58	Гамма	α = 44 198,00; λ = 4 007 327,00
Система OBS	0–100 000	97,86	Экспоненциальное	λ = 100,47
Система Ivideon	0–1600	5,39	Экспоненциальное	λ = 2039,70
	0–40 000	90,72	Эрланга	m = 5; λ = 824,39

Продолжение таблицы 3

Источник трафика	Исследуемые временные интервалы, мкс	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
«1С-Битрикс»	0–1500	7,41	Экспоненциальное	$\lambda = 3176{,}18$
	0–22 000	87,51	Эрланга	$m = 5$; $\lambda = 816{,}02$
Веб-приложение OWM	0–20 000	94,64	Экспоненциальное	$\lambda = 2357{,}74$
	0–100 000	5,36	Экспоненциальное	$\lambda = 32{,}38$
Веб-приложение OSM	0–100 000	95,21	Экспоненциальное	$\lambda = 6931{,}66$
Nanotron NanoPAN 5375	0–240 000	98,41	Экспоненциальное	$\lambda = 53{,}32$

В таблице 4 отображены средние показатели круговой сетевой задержки для каждого из выбранных источников трафика при доверительной вероятности 95 %.

Таблица 4. Доверительный интервал для среднего значения круговой сетевой задержки

Источник трафика	Круговая сетевая задержка, мкс	Джиттер, мкс
Trumpf TruPrint 1000	1948 ± 420	1761
3D Systems ProJet 4500	1887 ± 279	652
Система OBS	61 882 ± 290	5334
Система Ivideon	3243 ± 134	2131
«1С-Битрикс»	53 544 ± 628	11 957
Веб-приложение OWM	66 720 ± 778	14 757
Веб-приложение OSM	24 696 ± 1045	19 719
Nanotron NanoPAN 5375	2023 ± 234	976

Вероятностные распределения показателей сетевой задержки для каждого из представленных типов трафика отображены в таблице 5.

Таблица 5. Вероятностные распределения, описывающие характер сетевых задержек

Источник трафика	Исследуемые временные интервалы, мкс	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Trumpf TruPrint 1000	1812–3535	96,89	Экспоненциальное	$\lambda = 8417{,}60$
3D Systems ProJet 4500	1732–3347	98,33	Экспоненциальное	$\lambda = 7198{,}91$
Система OBS	53 424–60 711	25,05	Гамма	$\alpha = 1{,}47$; $\lambda = 867{,}08$
	53 424–91 775	72,44	Гамма	$\alpha = 59{,}23$; $\lambda = 6923{,}51$
Система Ivideon	1422–1600	25,18	Гамма	$\alpha = 14{,}38$; $\lambda = 111\,310{,}04$
	1422–9939	74,81	Экспоненциальное	$\lambda = 513{,}53$
«1С-Битрикс»	48 500–185 805	99,69	Экспоненциальное	$\lambda = 302{,}50$
Веб-приложение OWM	49 541–77 358	81,19	Вейбулла-Гнеденко	$c = 35{,}63$; $\alpha = 0{,}014$
	49 541–195 945	18,81	Гамма	$\alpha = 40{,}00$; $\lambda = 2380{,}95$
Веб-приложение OSM	13 033–27 561	87,24	Вейбулла-Гнеденко	$c = 5{,}22$; $\alpha = 0{,}006$
	13 033–194 637	12,76	Гамма	$\alpha = 4{,}54$; $\lambda = 231{,}28$
Nanotron NanoPAN 5375	1462–2876	99,98	Гамма	$\alpha = 22{,}73$; $\lambda = 25\,242{,}96$

Полученные значения коэффициента Хёрста для каждого из исследуемых источников трафика и агрегированного потока трафика отображены в таблице 6.

Таблица 6. Коэффициенты самоподобия для исследуемого трафика

Источник трафика	Коэффициент Хёрста					
	RS-анализ	Анализ MFDFA	Метод периодограмм	Метод Виттла	Среднее значение	Ср. квад. откл.
Trumpf TruPrint 1000	0,93	0,36	0,67	0,62	0,65	0,23
3D Systems ProJet 4500	0,46	0,57	0,78	0,49	0,58	0,14
Система OBS	0,60	0,52	0,63	0,62	0,59	0,05
Система Ivideon	0,67	0,60	0,51	0,48	0,60	0,09

Продолжение таблицы 6

Источник трафика	Коэффициент Хёрста					
	RS-анализ	Анализ MFDFA	Метод периодограмм	Метод Виттла	Среднее значение	Ср. квад. откл.
«1С-Битрикс»	0,67	0,60	0,58	0,52	0,60	0,06
Веб-приложение OWM	0,67	0,69	0,52	0,53	0,57	0,09
Веб-приложение OSM	0,50	0,78	0,49	0,50	0,56	0,14
Nanotron NanoPAN 5375	0,37	0,51	0,52	0,44	0,49	0,04
Агрегированный поток	0,78	0,72	0,57	0,57	0,66	0,11

На рисунке 14 отображено вероятностное распределение, которое отображает интенсивность поступления пакетов для агрегированного потока. Эмпирическое распределение агрегированного потока сходится с аналитическим экспоненциальным распределением с параметром $\lambda = 7603$ по критерию Колмогорова-Смирнова ($0{,}75 < 1{,}36$).

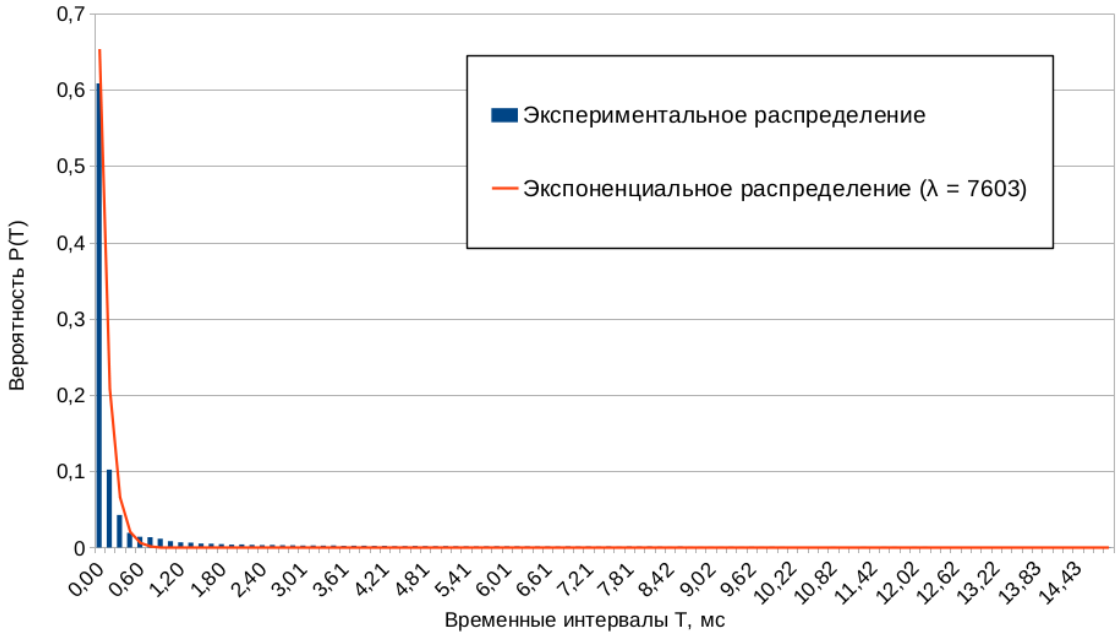


Рис. 14. Интенсивность поступления пакетов для агрегированного потока

На рисунке 15 отображены графики, отражающие способы нахождения коэффициента Хёрста для агрегированного потока [119].

На основе результатов анализа трафика от систем, применяемых в ПИВ, могут быть сделаны следующие выводы:

1. Все исследуемые типы трафика, за исключением трафика от системы позиционирования Nanotron NanoPAN 5375, имеют самоподобный характер по среднему значению коэффициента Хёрста по четырем приведенным методам расчета. Трафик от системы позиционирования Nanotron NanoPAN 5375 показывает антиперсистентный характер с высокой степенью приближенности к случайному пуассоновскому потоку. Общий, агрегированный трафик от всех типов источников трафика ПИВ также показывает самоподобный характер.

2. Полученные вероятностные распределения для интенсивности поступления и объема сетевых пакетов для каждого из источников трафика могут быть использованы для моделирования идентичного сетевого потока при тестировании сетевой инфраструктуры предприятий перед внедрением исследуемых решений, а также других подобных им систем.

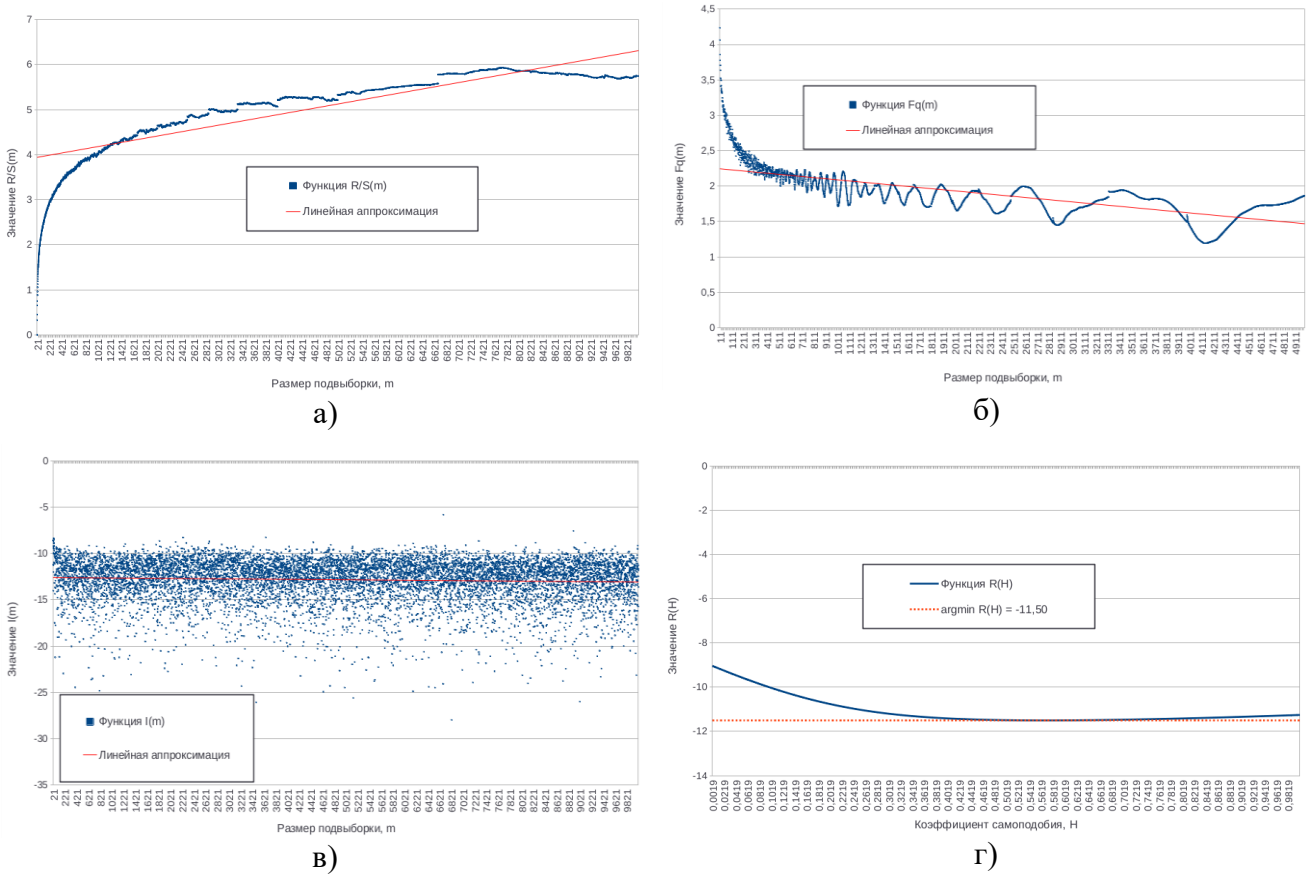


Рис. 15. Графики нахождения коэффициента Хёрста для агрегированного потока для методов: а) RS-анализа; б) MFDFA-анализа; в) метода периодограмм; г) локального метода Виттла

3. Для получения более точных данных о вероятностно-временных характеристиках работы систем ПИВ необходимо составить классификацию конкретных сценариев работы систем для каждого из исследуемых типов.

4. Общий агрегированный поток показывает свойства самоподобного потока и может быть описан с помощью экспоненциального распределения.

2.4. Разработка моделей для описания работы фрагмента сети промышленного Интернета вещей

2.4.1. Общее представление фрагмента сети промышленного Интернета вещей как системы массового обслуживания

На рисунке 16 изображена модель от одного источника трафика ПИВ, основанная на аналитических моделях, полученных в пункте 2.3.

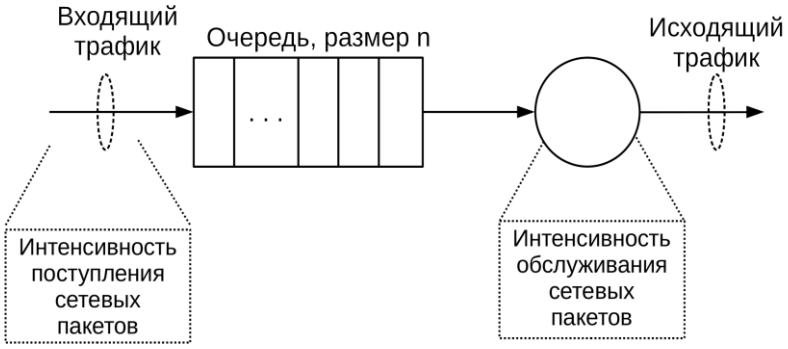


Рис. 16. Модель источника трафика ПИВ G/G/1/n

На данной схеме изображена модель G/G/1/n, согласно модели Кендалла-Башарина [33, 35, 38], включающая в себя интенсивность поступления (G — произвольный характер поступления пакетов) и обработки сетевых пакетов (G — произвольный характер обслуживания пакетов), которые описаны в пункте 2.3.6, одно обслуживающее устройство и буфер размером n, который рассчитывается как время задержки, умноженное на пропускную способность канала связи.

Модель, готовая к проведению имитационного моделирования, должна включать в себя несколько источников заявок, обработчиков заявок, оператора выбора обработчика заявок, буфер для хранения заявок, точку поступления заявок,

точку отклонения заявок при переполнении буфера и модель, имитирующую работу канала связи в локальной сети. Данная структура изображена на рисунке 17.

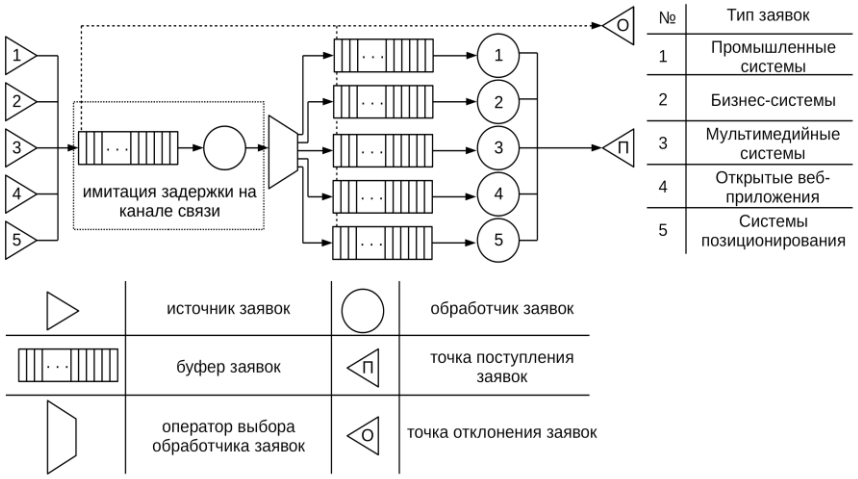


Рис. 17. Структура модели фрагмента сети ПИВ

Данная модель (рис. 17) включает в себя систему имитации задержки на канале связи, которая соответствует модели G/G/1/N, где N — размер очереди заявок, а время обслуживания заявки равно [24, 67]:

$$\tau_i = \frac{L_{\text{пак}}(i)}{Q}, \tag{35}$$

где $i \in (1,\ 2,\ \ldots, N_{\text{пак}})$ — индекс обслуживаемой заявки, $N_{\text{пак}}$ — общее количество обслуживаемых заявок, $L_{\text{пак}}(i)$ — размер обслуживаемого пакета (байт), Q — пропускная способность канала связи (байт/с).

2.4.2. Имитационная модель работы сети промышленного Интернета вещей

На рисунке 18 изображена имитационная модель фрагмента сети ПИВ, разработанная в системе агентного моделирования AnyLogic [79]. Данная модель включает в себя восемь видов источников трафика и обслуживающих устройств ПИВ, согласно вероятностным распределениям, полученным в пункте диссертации 2.3.6.

Функция распределения поступления заявок $\mathrm{F}_q^i(x)$ для каждого из видов источников заявок (src_ind_1, src_ind_2, src_mul_1, src_mul_2, src_business,

src_web1, src_web2, src_pos) задается согласно параметрам вероятностных распределений, указанным в таблице 1, пункте диссертации 2.3.6.

Функция распределения размеров пакетов $F_l^i(x)$ для каждого из видов трафика задается согласно параметрам вероятностных распределений, указанным в таблице 2, пункте диссертации 2.3.6.

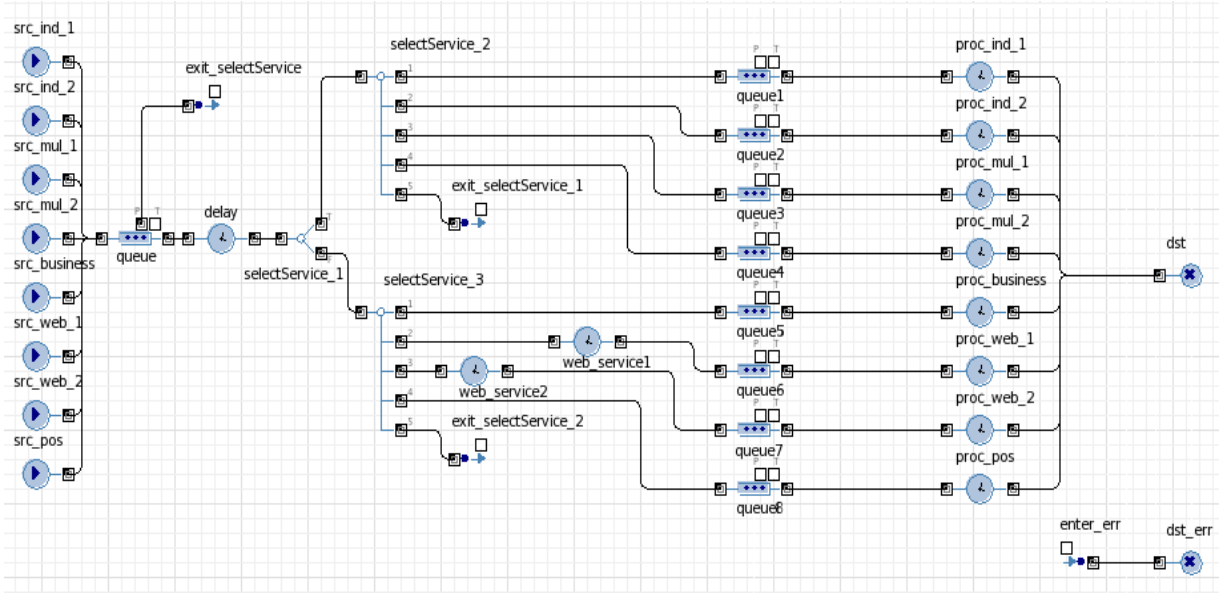


Рис. 18. Структура имитационной модели фрагмента сети ПИВ

Функция распределения обслуживания заявок $F_s^i(x)$ для каждого из видов обслуживающих устройств (proc_ind_1, proc_ind_2, proc_mul_1, proc_mul_2, proc_business, proc_web1, proc_web2, proc_pos) вычисляется согласно следующему правилу:

$$F_s^i(x) = F_{об}^i(x) - F_з^i(x), \quad (36)$$

где $i \in (1,\ 2,\ \ldots,\ N_{ит})$ — индекс обслуживающего устройства, x — текущая обслуживаемая заявка, $N_{ит}$ — общее количество источников трафика, $F_{об}^i(x)$ — функция распределения обслуживания заявок, согласно данным, указанным в таблице 3, пункте диссертации 2.3.6, $F_з^i(x)$ — функция распределения сетевых задержек, согласно данным, указанным в таблице 5, пункте диссертации 2.3.6.

Оператор выбора обслуживающего устройства задается согласно следующей системе уравнений:

$$F_s(x) = \begin{cases} F_s^1(x), \text{при } i = 1 \\ F_s^2(x), \text{при } i = 2 \\ F_s^3(x), \text{при } i = 3 \\ F_s^4(x), \text{при } i = 4 \\ F_s^5(x), \text{при } i = 5 \\ F_s^6(x), \text{при } i = 6 \\ F_s^7(x), \text{при } i = 7 \\ F_s^8(x), \text{при } i = 8 \end{cases}. \quad (37)$$

Элементы web_service1 и web_service2 отвечают за внесение задержек при передаче заявок от оператора выбора к обслуживающим устройствам. Время задержки для элемента web_service1 зависит от вероятностных распределений $F_з^6(x)$, параметры которых указаны в таблице 5, пункте диссертации 2.3.6 для источника трафика «Веб-приложение OWM», а задержка для элемента web_service2 зависит от вероятностных распределений $F_з^7(x)$, параметры которых указаны там же для источника трафика «Веб-приложение OSM».

Моделирование проводится в течение 600 единиц модельного времени (600 с, или 10 мин). В ходе моделирования собираются данные по интенсивности поступления заявок от всех источников трафика на элемент очереди канала связи queue, времени обслуживания заявок на устройстве обслуживания канала связи delay, количеству потерянных и успешно обслуженных заявок.

2.4.3. Анализ результатов моделирования

Во время работы имитационной модели была получена выборка интервалов времени между поступлениями пакетов для агрегированного потока, которая может быть описана с помощью экспоненциального распределения с коэффициентом $\lambda = 4770$. Данное аналитическое распределение сходится с полученным в ходе моделирования эмпирическим распределением по критерию согласия Колмогорова-Смирнова (0,01 < 1,36). На рисунке 19 отображено

отношение эмпирического распределения с аналитическим экспоненциальным.

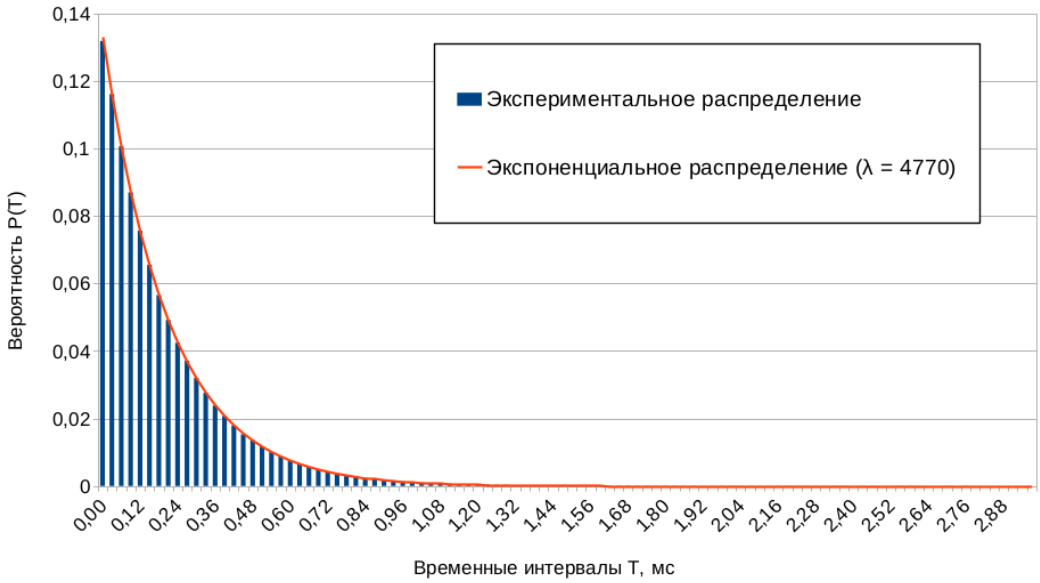


Рис. 19. Интенсивность поступления пакетов для агрегированного потока в имитационной модели

На рисунке 20 отображены графики, отражающие коэффициенты Хёрста для агрегированного потока в имитационной модели. Получившиеся значения коэффициента Хёрста отображены в таблице 7.

Таблица 7. Коэффициенты самоподобия для исследуемого трафика

Метод расчета коэффициента Хёрста	Значение коэффициента Хёрста	Среднее значение	Среднеквадратичное отклонение
RS-анализ	0,60	0,52	0,06
Анализ MFDFA	0,52		
Метод периодограмм	0,49		
Метод Виттла	0,48		

Таким образом, имитационная модель подтверждает гипотезу об экспоненциальном характере трафика фрагмента сети промышленного Интернета вещей и его самоподобии. Тем не менее, поток заявок в данной модели имеет значения коэффициента Хёрста, близкие к значению 0,5, т. е. данный поток стремится к пуассоновскому потоку, что может быть связано как с более высоким

объемом полученной в ходе имитационного моделирования выборки, так и с отличиями формата сценария поступления сетевых пакетов, которые имеются при сравнении любого источника из имитационной модели с тем же источником трафика на модельной сети.

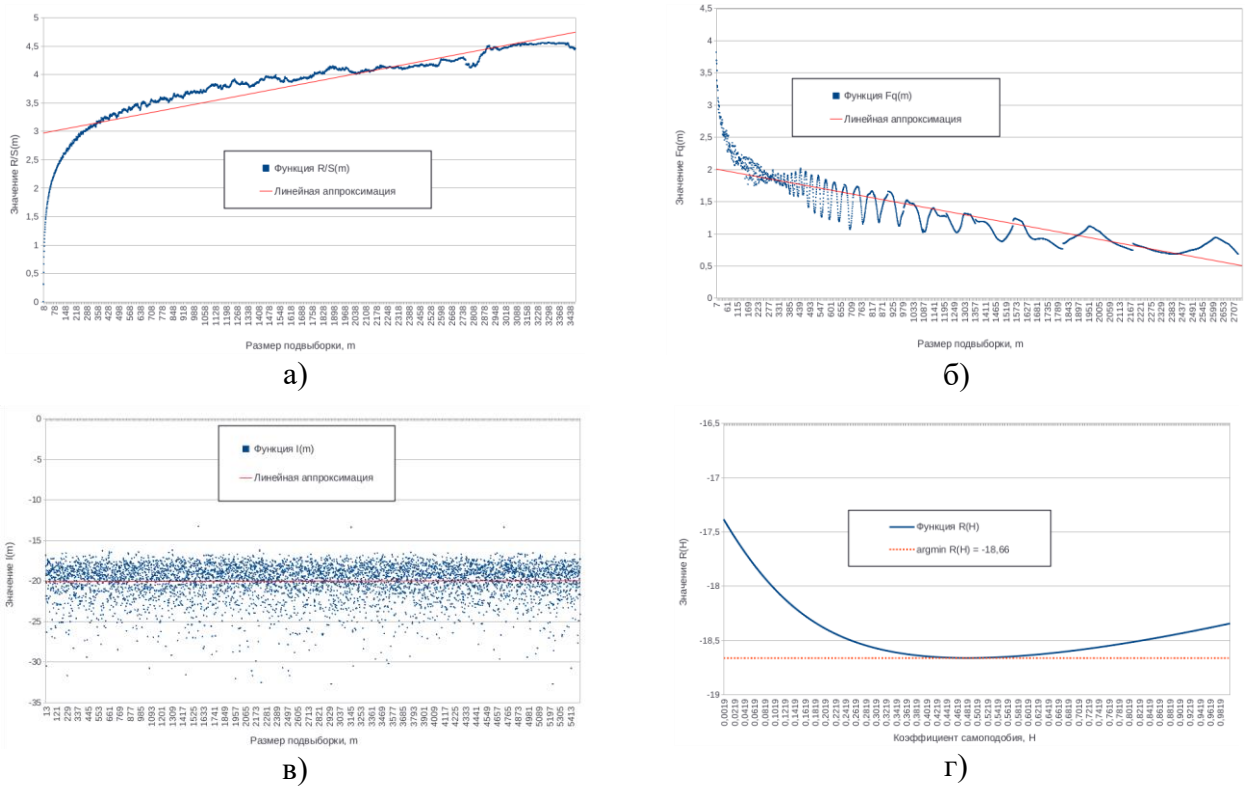


Рис. 20. Графики нахождения коэффициента Хёрста для агрегированного потока в имитационной модели для методов: а) RS-анализа; б) MFDFA-анализа; в) метода периодограмм; г) локального метода Виттла

Далее на основе полученных показателей интенсивности поступления и обслуживания заявок, а также соотношения потерянных заявок на основе оценки, предложенной В. В. Липаевым и С. Ф. Яшковым для модели G/G/1/n, согласно классификации Кендалла-Башарина (38), было проведено сопоставление процента потерянных заявок в ходе работы имитационной модели и значения процента потерянных пакетов, полученного с помощью оценки Липаева-Яшкова, при различных значениях пропускной способности локального канала связи — 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 Мбит/с (рис. 21). Оценку Липаева-Яшкова можно

описать с помощью следующего уравнения [32]:

$$P_n = \frac{1 - \rho}{1 - \rho^{\frac{2n}{C_a^2 + C_s^2} + 1}} \rho^{\frac{2n}{C_a^2 + C_s^2}}, \quad (38)$$

где C_a^2 — квадратический коэффициент вариации распределения входящего потока, C_s^2 — квадратический коэффициент вариации распределения времени обслуживания, $\rho = \frac{\lambda_a}{\lambda_s}$ — коэффициент загрузки модели, где λ_a — среднее значение интенсивности поступления заявок, λ_s — среднее значение интенсивности обслуживания заявок. Результаты исследования предельного значения пропускной способности локального канала связи для фрагмента сети промышленного Интернета вещей отображены на рисунке 20. Гипотеза о сходимости ряда, полученного при работе имитационной модели, и ряда, полученного с помощью оценки Липаева-Яшкова, подтверждаются согласно критерию согласия Колмогорова-Смирнова (0,01 < 1,36), при доверительной вероятности 95 %.

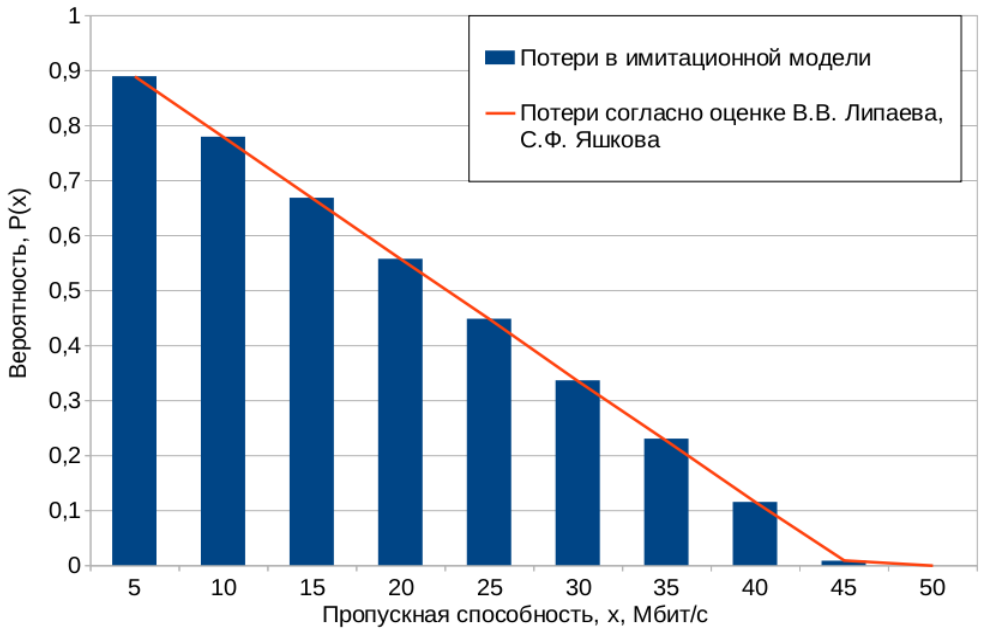


Рис. 21. Соотношение процента потерь заявок в имитационной модели и согласно оценке Липаева-Яшкова

Таким образом, потери в представленной модели начинаются после

ограничения пропускной способности канала связи в локальной сети до 45 Мбит/с. Таким образом, для представленной конфигурации сети 50 Мбит/с является наиболее приемлемой оценкой. При масштабировании количества источников трафика в модели для оценки числа потерянных заявок может использоваться оценка Липаева-Яшкова (38).

Выводы по главе 2

1. Разработана классификация трафика ПИВ по источникам трафика, сценарию взаимодействия и качеству обслуживания.

2. На основе полученной классификации трафика ПИВ разработана модельная сеть, имитирующая работу фрагмента сети ПИВ и включающая в себя реальные системы, используемые в сфере промышленной автоматизации.

3. На базе разработанной модельной сети и классификации трафика ПИВ проведен анализ различных типов трафика ПИВ. В ходе анализа были получены аналитические модели интенсивности поступления и обслуживания трафика, модель распределения размера сетевых пакетов, а также значения коэффициента самоподобия (Хёрста) для каждого из ранее определенных видов источников трафика ПИВ.

4. Произведена оценка интенсивности поступления сетевых пакетов и значения коэффициента Хёрста для агрегированного трафика и была доказана гипотеза о его самоподобном характере.

5. На базе полученных аналитических данных была разработана имитационная модель, описывающая работу фрагмента сети ПИВ, с помощью которой была произведена оценка минимально приемлемой пропускной способности для выбранного фрагмента сети промышленного Интернета вещей и была подтверждена гипотеза о возможности применения оценки потери пакетов В. В. Липаева и С. Ф. Яшкова в модели G/G/1/n для сетей промышленного Интернета вещей.

Глава 3. РАЗРАБОТКА МЕТОДА СЕМАНТИЧЕСКОГО ПРЕОБРАЗОВАНИЯ СООБЩЕНИЙ ДЛЯ ГЕТЕРОГЕННОГО ШЛЮЗА ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

3.1. Структура гетерогенного шлюза промышленного Интернета вещей

Гетерогенный шлюз Интернета вещей — устройство, обеспечивающее взаимодействие различных технологий Интернета вещей как между собой, так и с сетью связи общего пользования (ССОП) на всех уровнях модели OSI [17, 78, 95, 102, 116]. На рисунке 22 изображена архитектура гетерогенного шлюза Интернета вещей. Данная система обеспечивает взаимодействие различных технологий физического, канального и сетевого уровня и с помощью специального программного обеспечения, функционирующего в виртуальном окружении, позволяет преобразование данных между используемыми технологиями на прикладном уровне. Таким образом, данная система состоит из следующих компонентов:

Рис. 22. Архитектура гетерогенного шлюза Интернета вещей

- Физические интерфейсы, поддерживающие различные технологии Интернета вещей.
- Операционная система, системные драйвера, ПО, позволяющие поддерживать функционирование протоколов физического, канального, сетевого

и транспортного уровней на гетерогенном шлюзе ИВ.

- Виртуальное окружение (эмуляторы, контейнеры, виртуальные машины и др.), позволяющее добавлять новые возможности и услуги для гетерогенного шлюза.

- ПО, функционирующее в виртуальном окружении и позволяющее гетерогенным шлюзам расширять существующую функциональность. Например, данное ПО позволяет расширить возможности гетерогенного шлюза за счет поддержки новых протоколов, услуг и технологий.

Гетерогенный шлюз состоит из основной части, позволяющей поддерживать различные технологии Интернета вещей, системы виртуализации, и из прикладной части, функционирующей в виртуальном окружении и позволяющей внедрять без изменения основного рабочего окружения гетерогенного шлюза новые технологии и услуги. Одной из таких технологий является семантический шлюз ИВ.

3.2. Задачи семантического преобразования сообщений для гетерогенного шлюза промышленного Интернета вещей

Семантический шлюз Интернета вещей — программное обеспечение, позволяющее производить преобразование прикладных протоколов ИВ между собой и обеспечивающее общее адресное пространство для всех устройств, взаимодействующих с данным ПО [84, 49, 110]. Таким образом, семантический шлюз решает проблемы взаимодействия различных прикладных технологий ИВ на уровне метаданных.

Проблема преобразования данных между различными протоколами на семантическом уровне является актуальной и для промышленного Интернета вещей. При использовании различных промышленных решений возникает проблема стыковки технологий как на физическом, канальном, сетевом, транспортном уровнях, так и на прикладном уровне. Для решения данной проблемы предлагается использовать гетерогенный шлюз ИВ [51-52].

Проблема взаимодействия протоколов на уровне метаданных решается

использованием специального ПО, которое и будет являться промышленным семантическим шлюзом. Данное ПО выделяет ключевую информацию от каждого из пакетов данных, прикладной уровень которых основан на одном из промышленных протоколов, и преобразует в общий промежуточный формат Industrial Internet of Things Conversion Format (IICF). В случае необходимости используются функции ПО для преобразования полученных данных в поддерживаемые протоколы и дальнейшей их отправки в пункт назначения.

На рисунке 23 изображена структура ПО для преобразования протоколов ПИВ. Данное ПО состоит из следующих основных функций:

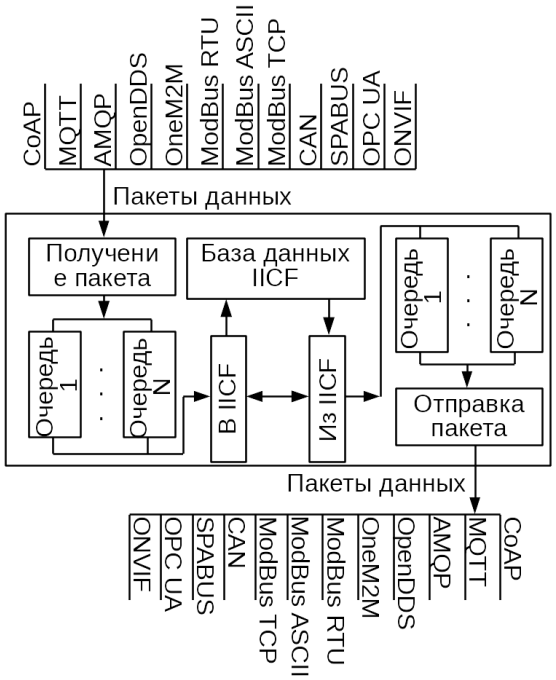


Рис. 23. Структура семантического шлюза промышленного Интернета вещей

- «Получение пакета» — отвечает за прием и фильтрацию пакетов, основанных на одном из поддерживаемых протоколов ИВ. Данное ПО анализирует все приходящие на активный сетевой интерфейс пакеты и принимает те пакеты, формат которых основан на одном из поддерживаемых протоколов.
- «Очередь 1..N» — очередь пакетов, поступающих в ПО, как для обработки, так и для отправки.
- «В IICF» — преобразование поступающих пакетов в общий формат IICF.

- «База данных IICF» — отвечает за хранение пакетов. Может представлять собой встраиваемую в ПО систему хранения данных, ограниченный буфер, программный интерфейс для взаимодействия с внешними системами хранения данных и др. Может хранить информацию о протоколе, который поддерживает пункт назначения, прописанный в конкретном пакете.
- «Из IICF» — отвечает за преобразование данных из формата IICF в необходимый формат, согласно протоколу.
- «Отправить пакет» — отвечает за отправку сформированного пакета в нужный пункт назначения.

В качестве прикладного решения для семантического шлюза ПИВ предлагается использовать гетерогенный шлюз ПИВ, Heterogeneous Industrial Internet of Things Gateway (HIIG) — шлюз, устанавливаемый в рамках одного решения ИВ и отвечающий за преобразования протоколов промышленного Интернета вещей между собой.

На рисунке 24 изображен пример программно-аппаратного комплекса (ПАК), объединяющего различные подсети, функционирующие на базе различных протоколов промышленного Интернета вещей, с помощью HIIG.

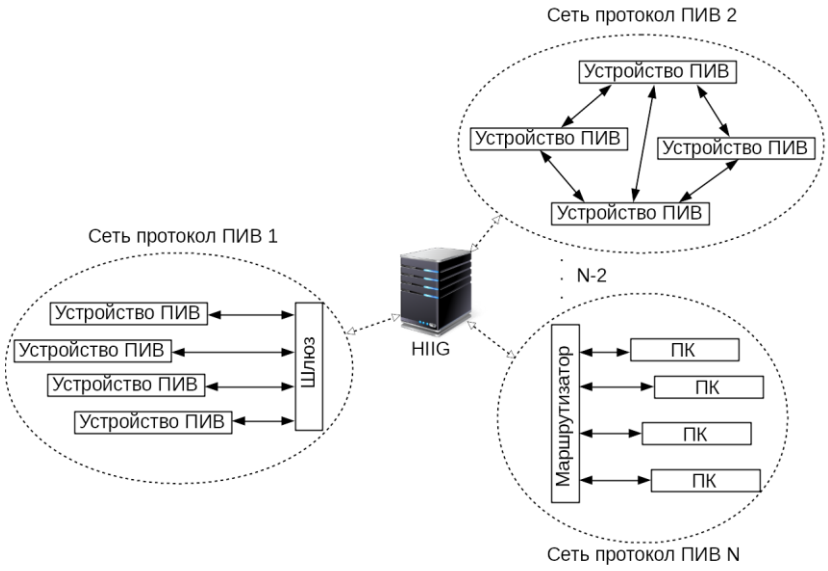


Рис. 24. Структура программно-аппаратного комплекса, включающего в себя гетерогенный шлюз ПИВ

3.3. Анализ протоколов передачи данных, используемых в сетях промышленного Интернета вещей

Для разработки структуры системы, отвечающей за преобразование и формирование пакетов на базе известных форматов данных различных протоколов ИВ в формат IICF, необходимо исследовать форматы данных различных промышленных протоколов и выделить общие поля данных. Для данного исследования были выбраны следующие наиболее распространенные протоколы:

- CoAP;
- MQTT;
- XMPP;
- ModBus RTU;
- ModBus TCP;
- OPC UA;
- HTTP.

Формат метаданных для протокола CoAP отображен на рисунке 25. Основные поля в данном протоколе:

- версия CoAP (2 бит);
- тип сообщения (2 бит);
- число дополнительных опций (4 бит);
- код — метод запроса данных или код запроса (8 бит), например GET (1), POST (2), PUT (3), DELETE (4);
- идентификатор сообщения (16 бит);
- опции сообщения (необязательно);
- полезные данные сообщения (необязательно).

В формате опций также встречается поле, содержащее URI сервера CoAP.

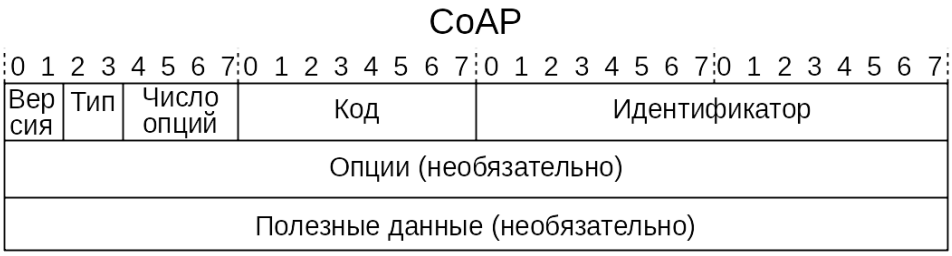


Рис. 25. Структура метаданных протокола CoAP

Формат метаданных для протокола MQTT отображен на рисунке 26. Основные поля в данном протоколе:

- тип сообщения (4 бит);
- флаг перезапроса сообщения — DUP (1 бит);
- уровень QoS (2 бита);
- флаг сохранения сообщения (1 бит);
- длина опциональной информации (8 бит);
- опционально: переменная длина заголовка сообщений (от 8 бит);
- опционально: переменная длина полезных данных сообщения (от 8 бит).

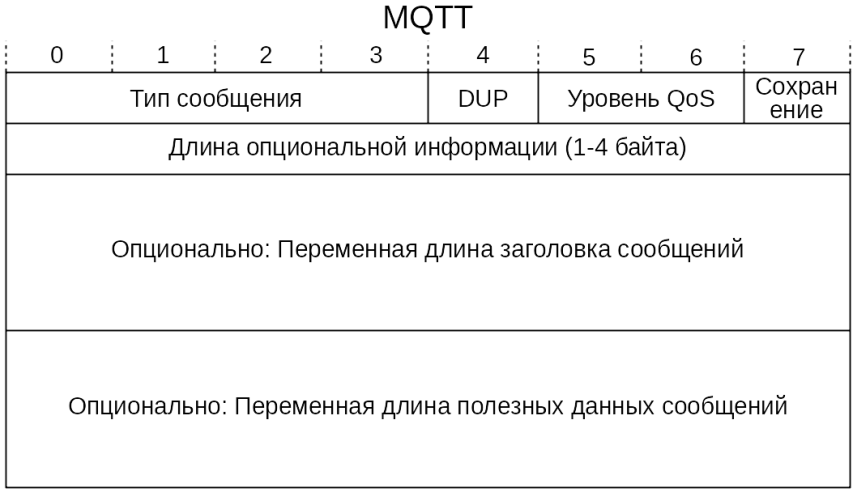


Рис. 26. Структура метаданных протокола MQTT

Формат метаданных для протокола XMPP отображен на рисунке 27. Основные поля в данном протоколе:

Рис. 27. Структура метаданных протокола XMPP

- версии заголовка XML;
- тип сообщения;
- идентификатор сессии;
- версия XML;
- идентификатор сообщения;
- идентификатор отправителя;
- идентификатор получателя;
- язык сообщения;
- адрес потока;
- текст сообщения.

Формат метаданных для протокола ModBus RTU отображен на рисунке 28. Основные поля в данном протоколе:

- стартовый флаг (≥ 3,5 символа — 28 бит);
- адрес ModBus (8 бит);
- функции ModBus (8 бит);
- поле данных (8 — N × 8 бит);
- закрывающий флаг (≥ 3,5 символа — 28 бит).

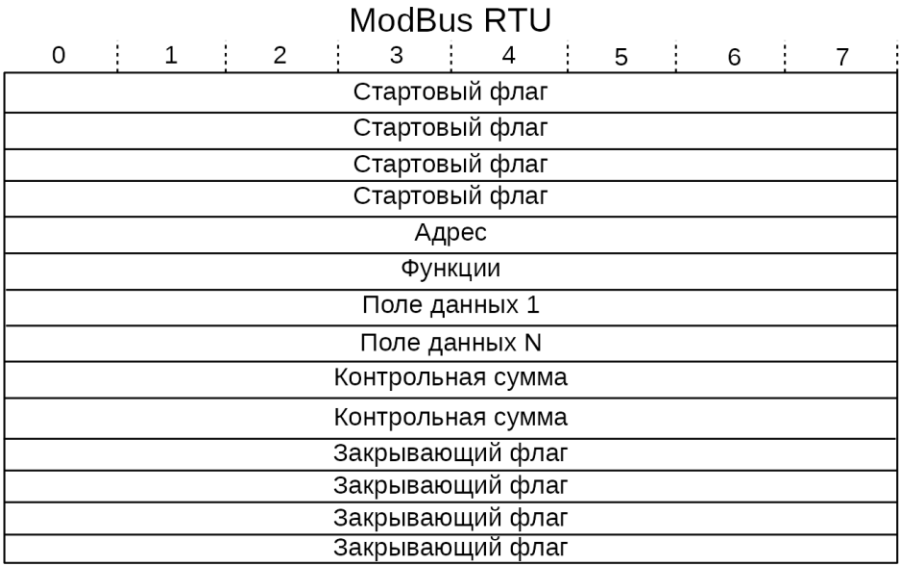


Рис. 28. Структура метаданных протокола ModBus RTU

Формат метаданных для протокола ModBus TCP отображен на рисунке 29. Основные поля в данном протоколе:

- идентификатор сообщения (2 байта);
- идентификатор протокола (2 байта);
- длина сообщения (2 байта);
- идентификатор устройства (8 бит);
- код функции ModBus (8 бит);
- поле данных (8–8 × N бит).

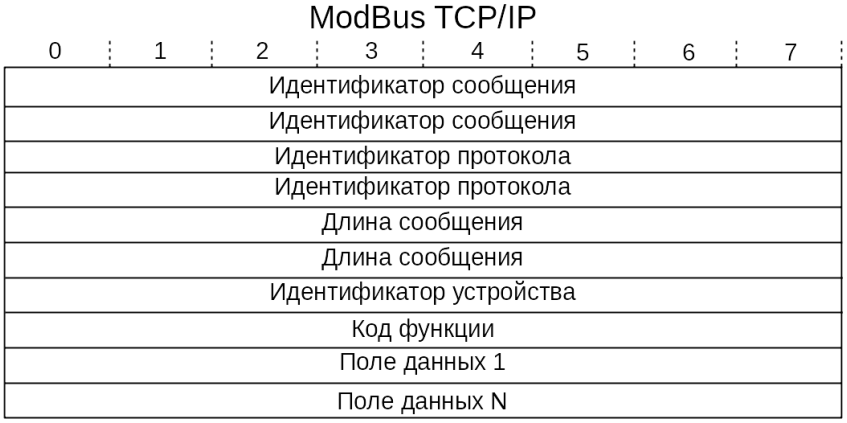


Рис. 29. Структура метаданных протокола ModBus TCP

Формат метаданных для протокола OPC UA отображен на рисунке 30.

Основные поля в данном протоколе:

- тип сообщения (3 байта);
- тип фрагментации (1 байт);

Рис. 30. Структура метаданных протокола OPC UA

- размер сообщения (4 байта);
- идентификатор защищенного канала (4 байта);
- идентификатор токена (ключа безопасности, 4 байта);
- номер защищенной последовательности (4 байта);
- идентификатор защищенного запроса (4 байта);
- идентификатор типа OPC UA сообщения (4 байта);
- время (8 байт);
- обработчик сообщения (4 байта);
- результат обработки сообщения (4 байта);
- маска кодирования обработчика (1 байт);
- размер данных заголовка (4 байта);
- данные заголовка;
- добавочный заголовок;
- размер массива данных (1 байт);
- маска кодирования данных (1 байт);
- тип данных (1 байт);
- данные массива;

- время на сервере (8 байт);
- размер массива диагностики (4 байта);
- данные диагностики.

Формат метаданных для протокола HTTP отображен на рисунке 31. Основные поля в данном протоколе:

- тип запроса;
- запрашиваемый URI-домен;
- версия HTTP-запроса;
- URI-адрес назначения;
- опции соединения;
- опции контроля кэша;
- данные о пользовательском клиенте;
- данные запроса;
- кодирование данных;
- язык данных;
- данные о сервере;
- время.

HTTP

Тип запроса
Запрашиваемый URI
Версия HTTP для запроса
Адрес URI назначения
Опции соединения
Опции контроля кэша
Данные о пользовательском клиенте
Данные запроса
Кодирование данных
Язык данных
Данные о сервере
Время

Рис. 31. Структура метаданных протокола HTTP

3.4. Промежуточный формат преобразования сообщений промышленного Интернета вещей

На базе рассмотренных форматов промышленных протоколов ИВ можно сделать вывод о полях данных, необходимых в промежуточном формате преобразования. В частности, предполагается, что формат IICF будет содержать следующие поля (рис. 32):

- Используемый протокол канального уровня (2 байта). Позволяет определить, какой протокол канального уровня использовался для отправки исходного сообщения от источника.
- Канальный идентификатор источника (10 байт). Идентификатор канального уровня для устройства-источника.
- Канальный идентификатор приемника (10 байт). Идентификатор канального уровня для устройства-приемника.

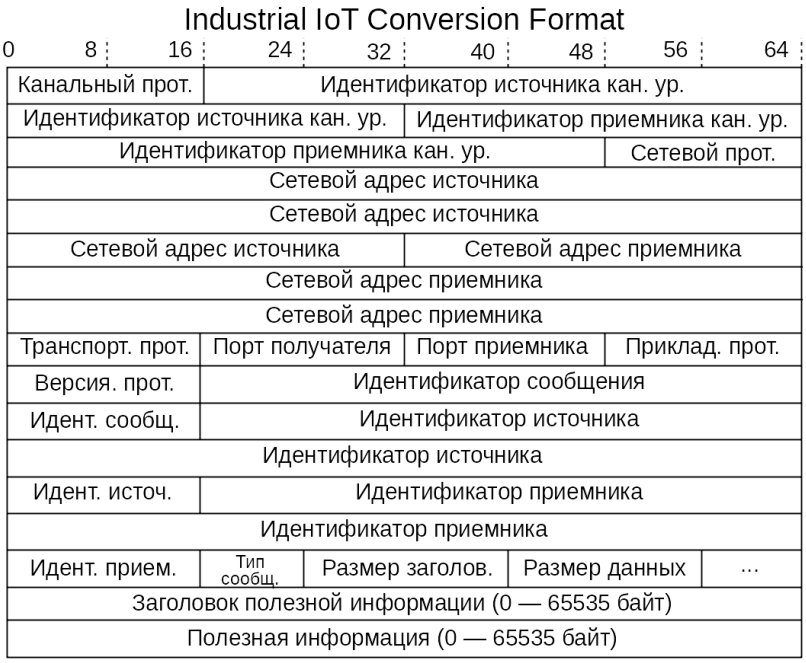


Рис. 32. Структура промежуточного формата IICF

- Используемый протокол сетевого уровня (2 байта). Позволяет определить, какой сетевой протокол использовался для отправки исходного сообщения от источника.

- Сетевой адрес источника (20 байт). Идентификатор сетевого уровня для устройства-источника.
- Сетевой адрес приемника (20 байт). Идентификатор сетевого уровня для устройства-приемника.
- Используемый протокол транспортного уровня (2 байта). Позволяет определить, какой транспортный протокол использовался для отправки исходного сообщения от источника.
- Порт источника (2 байта). Порт, используемый протоколом транспортного уровня для устройства-источника.
- Порт приемника (2 байта). Порт, используемый протоколом транспортного уровня для устройства-приемника.
- Используемый прикладной протокол (2 байта). Позволяет определить, какой прикладной протокол использовался для отправки исходного сообщения от источника.
- Версия протокола (2 байт). Позволяет определить, какая версия исходного протокола была использована.
- Идентификатор сообщения (8 байт). Уникальный идентификатор сообщения, обеспечивающий возможность его хранения и доступа к нему в рамках системы преобразования промышленных протоколов.
- Идентификатор источника (16 байт). Уникальный идентификатор устройства-источника в рамках системы преобразования промышленных протоколов.
- Идентификатор приемника (16 байт). Уникальный идентификатор устройства-приемника в рамках системы преобразования промышленных протоколов.
- Тип сообщения (1 байт), например: запрос, ответ, обновление данных, удаление данных и др.
- Размер заголовка полезной информации (2 байт). Размер заголовка,

в котором могут храниться различные дополнительные параметры, специфичные для какого-либо определенного протокола, в символьном виде. Например, дополнительные опции протокола, уровень QoS, различные параметры процедур обмена данными и др.

- Размер полезной информации (2 байт). Размер поля, содержащего полезную нагрузку в символьном виде.
- Заголовок полезной информации (0–65 535 байт). Заголовок, в котором могут храниться различные дополнительные параметры, специфичные для какого-либо определенного протокола, в символьном виде. Например, дополнительные опции протокола, уровень QoS, различные параметры процедур обмена данными и др.
- Полезная информация (0–65 535 байт). Поле, содержащее полезную нагрузку в символьном виде.

3.5. Исследование процедур семантического преобразования сообщений

3.5.1. Постановка цели и задач процедур семантического преобразования сообщений

Для оценки работы предложенного метода построения семантических гетерогенных шлюзов промышленного Интернета вещей необходимо оценить время взаимного преобразования протоколов ПИВ между собой. Для этого необходимо оценить время преобразования заданных протоколов через промежуточный формат преобразования IICF. Для этого предлагается решить следующие задачи:

- Разработать структуру модельной сети для оценки времени преобразования протоколов ПИВ, а также разработать программное обеспечение для оценки времени преобразования протоколов.
- Получить аналитические модели, позволяющие оценить время преобразования из формата прикладного протокола в формат IICF — прямое преобразование (ПП), а также из формата IICF в формат прикладного протокола —

обратное преобразование (ОП).

- Получить аналитические модели, позволяющие оценить время преобразования из одного формата полезных данных в другой.

3.5.2. Структура модельной сети для исследования работы семантического гетерогенного шлюза промышленного Интернета вещей

Время обслуживания одного сообщения на семантическом шлюзе можно оценить с помощью аналитических моделей, описывающих вероятностное распределение значения времени обслуживания для двух основных задач: приема и преобразования сообщения в промежуточный формат семантического шлюза, а также обратного преобразования и отправки сообщений в требуемом формате. Данные модели могут быть разработаны с помощью данных, полученных в ходе анализа времени обработки одного сообщения во время процедуры преобразования сообщений для реальной экспериментальной системы (рис. 33) [42]. Для проведения данного испытания было разработано специальное программное обеспечение. Данное программное обеспечение обеспечивает преобразования сообщений из одного формата в другой на основе следующих часто применяемых прикладных протоколов ПИВ: CoAP, MQTT, Modbus, STOMP, OPC UA, HTTP.

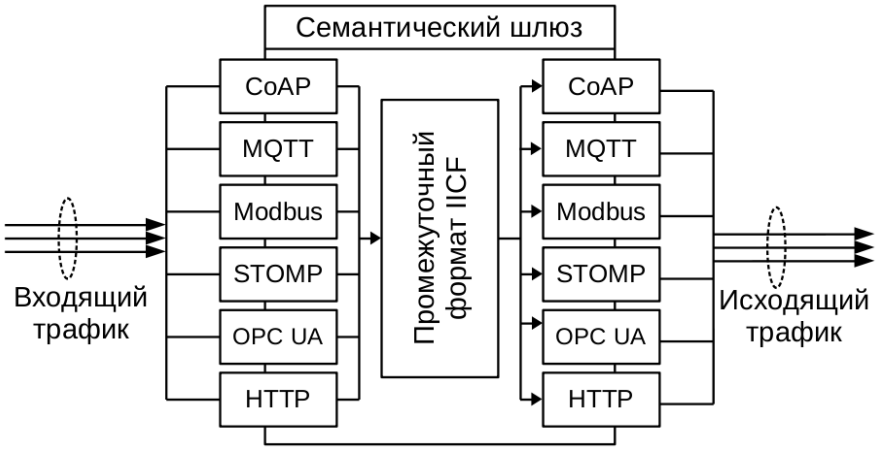


Рис. 33. Структура семантического шлюза ПИВ

Для оценки времени обслуживания одного сообщения было разработано специальное приложение для генерации, приема и преобразования сообщений [45, 50, 104]. Для проведения эксперимента были разработаны следующие приложения

для каждого из исследуемых протоколов (табл. 8):

- Приложения для генерации сообщений (генератор трафика).
- Приложения для преобразования формата сообщения в промежуточный формат Industrial Internet of Things Conversion Format (IICF) и обратного преобразования в исходный формат сообщения (семантический шлюз).
- Приложения для приема сообщений (сервер).

Таблица 8. Выбранные программные инструменты

Протокол	Язык программирования	Название программного инструмента
CoAP	C	cantcoap
MQTT	C++	Eclipse Paho MQTT
Modbus	C	libmodbus
STOMP	C++	BoostStomp
OPC UA	C++	freeopcua
HTTP	C	libcurl

3.5.3. Аналитические модели работы семантического гетерогенного шлюза промышленного Интернета вещей

На основе семантических шлюзов была произведена оценка времени преобразования формата сообщения в формат IICF (ПП) и оценка времени обратного преобразования из IICF в исходный формат сообщения (ОП), на основе которых были построены аналитические модели, использованные для разработки имитационной модели. В таблицах 9 и 10 [92, 94, 113] указаны параметры полученных с помощью методов наименьших квадратов и обобщенного приведенного градиента аналитических моделей распределения времени преобразования, t_0 — начальное значение распределения, а $\bar{t}$ — среднее значение времени обслуживания, при значении доверительной вероятности 95 %.

Таблица 9. Аналитические модели времени преобразования прикладных протоколов

Протокол	Процедура	$\bar{t}$, мкс	Вероятностное распределение	t_0, мкс	Критерий согласия Колмогорова-Смирнова
CoAP	ПП	99,71 ± 4,41	Гамма (α = 32,42; λ = 312 838,05)	0	0,43 < 1,36
	ОП	111,33 ± 15,08	Гамма (α = 193,68; λ = 1 686 833,17)	0	0,24 < 1,36
MQTT	ПП	399,54 ± 13,83	Экспоненциальное (λ = 2273,56)	0	0,28 < 1,36
	ОП	405,71 ± 13,78	Экспоненциальное (λ = 2414,62)	26	0,16 < 1,36
Modbus	ПП	45,57 ± 2,76	Гамма (α = 43,06; λ = 1 024 851,60)	0	0,18 < 1,36
	ОП	26,51 ± 1,56	Гамма (α = 36,72; λ = 1 420 156,40)	0	0,72 < 1,36
STOMP	ПП	201,00 ± 7,46	Экспоненциальное (λ = 9096,67)	35	0,42 < 1,36
	ОП	12,54 ± 0,37	Экспоненциальное (λ = 110 220,83)	5	0,26 < 1,36
OPC UA	ПП	1257,11 ± 53,81	Гамма (α = 144,36; λ = 123 317,84)	0	0,26 < 1,36
	ОП	121,82 ± 3,41	В 27 % случаев: экспоненциальное (λ = 94 305,55)	76	0,18 < 1,36
			В 73 % случаев: гамма (α = 11,70; λ = 181 520,03)		
HTTP	ПП	414,46 ± 11,66	Экспоненциальное (λ = 6503,96)	280	0,24 < 1,36
	ОП	117,68 ± 3,37	Экспоненциальное (λ = 33 806,45)	84	0,30 < 1,36

Таким образом, модель преобразования сетевых пакетов на семантическом шлюзе ПИВ можно описать с помощью следующей формулы плотности вероятности:

$$f(x) = p_1 \frac{{\lambda_1}^{\alpha_1}}{\Gamma(\alpha_1)}(x - c_1)e^{-\lambda_1(x - c_1)} +$$
$$+ \left(p_2 \frac{{\lambda_2}^{\alpha_2}}{\Gamma(\alpha_2)}(x - c_2)e^{-\lambda_2(x - c_2)} + p_3 \frac{{\lambda_3}^{\alpha_3}}{\Gamma(\alpha_3)}(x - c_3)e^{-\lambda_3(x - c_3)}\right) +, \quad (39)$$
$$+ \left(p_4 \frac{{\lambda_4}^{\alpha_4}}{\Gamma(\alpha_4)}(x - c_4)e^{-\lambda_4(x - c_4)} + p_5 \frac{{\lambda_5}^{\alpha_5}}{\Gamma(\alpha_5)}(x - c_5)e^{-\lambda_5(x - c_5)}\right)$$

где $f(x)$ — плотность вероятности общего времени преобразования пакета из формата протокола 1 в формат протокола 2, $\Gamma(\alpha_i)$ — гамма-функция, p_1, p_2, p_3, p_4, p_5 — вероятности попадания в заданное вероятностное распределение, где $p_2 + p_3 = \begin{cases} 1, \text{если происходит преобразование форматов полезных данных,} \\ 0, \text{если оно не происходит} \end{cases}$ — относится к вероятности попадания в заданные распределения преобразования форматов полезных данных и $p_3 + p_4 = 1$ — относится к вероятности попадания в заданные распределения ОП, α_1, λ_1, c_1 — коэффициенты смещенного гамма-распределения для описания процедуры ПП, $(\alpha_2; \alpha_3), (\lambda_2; \lambda_3), (c_2; c_3)$ — коэффициенты смещенных гамма-распределений для описания процедуры преобразования форматов полезных данных пакетов, $(\alpha_4; \alpha_5), (\lambda_4; \lambda_5), (c_4; c_5)$ — коэффициенты смещенных гамма-распределений для описания процедуры преобразования форматов полезных данных пакетов.

Таблица 10. Аналитические модели времени преобразования форматов полезных данных

Формат данных	Среднее время преобразования, мкс	Вероятностное распределение	Вероятность попадания в выборку, %	Критерий Колмогорова
CSV/JSON	53,18 ± 0,33	Гамма (α = 1303,25; λ = 25 946 283,00)	81,30	0,09 < 1,36
		Гамма (α = 1303,25; λ = 25 946 283,00)	18,70	
CSV/XML	47,00 ± 0,30	Гамма (α = 955,68; λ = 21 871 927,61)	80,50	0,64 < 1,36
		Гамма (α = 4,57; λ = 10 218 335,97)	19,50	

Продолжение таблицы 10

Формат данных	Среднее время преобразования, мкс	Вероятностное распределение	Вероятность попадания в выборку, %	Критерий Колмогорова
JSON/CSV	92,17 ± 0,52	Гамма (α = 3422,74; λ = 38 971 993,00)	84,65	0,34 < 1,36
		Гамма (α = 2,56; λ = 3 921 215,00)	15,35	
JSON/XML	96,28 ± 0,32	Гамма (α = 1922,76; λ = 20 252 983,00)	100,00	0,46 < 1,36
XML/CSV	426,19 ± 2,58	Гамма (α = 1347,98; λ = 3 417 864,00)	79,00	0,75 < 1,36
		Гамма (α = 2,92; λ = 386 040,00)	21,00	
XML/JSON	404,54 ± 1,31	Гамма (α = 1864,7; λ = 4 695 517,00)	100,00	0,76 < 1,36

3.6. Разработка методов исследования работы семантического гетерогенного шлюза промышленного Интернета вещей на базе имитационной модели

3.6.1. Общее представление работы семантического гетерогенного шлюза промышленного Интернета вещей в виде СМО

Для оценки работы семантического гетерогенного шлюза ПИВ предлагается разработать модель его функционирования на базе систем дискретно-событийного моделирования. Для разработки данной модели необходимо определить, как может быть представлен семантический шлюз в рамках систем массового обслуживания. Для этого был проведен анализ структуры семантического шлюза, отображенной на рисунке 33, и были определены три основных этапа преобразования, представленных далее:

- Преобразование сетевого пакета из формата протокола 1 в промежуточный формат IICF. Данная процедура может быть описана с помощью следующего уравнения плотности вероятности:

$$f_{\text{пп}}(x) = p_1 \frac{{\lambda_1}^{\alpha_1}}{\Gamma(\alpha_1)} (x - c_1) e^{-\lambda_1 (x - c_1)}, \quad (40)$$

где $f_{\text{пп}}(x)$ — плотность вероятности для преобразования из формата прикладного протокола 1 в формат IICF.

- Преобразование формата полезных данных в необходимый формат. Данная процедура может быть описана с помощью следующего уравнения плотности вероятности:

$$f_{\text{фпд}}(x) = p_2 \frac{{\lambda_2}^{\alpha_2}}{\Gamma(\alpha_2)}(x - c_2)e^{-\lambda_2(x - c_2)} + p_3 \frac{{\lambda_3}^{\alpha_3}}{\Gamma(\alpha_3)}(x - c_3)e^{-\lambda_3(x - c_3)}, \quad (41)$$

где $f_{\text{фпд}}(x)$ — плотность вероятности для преобразования из исходного формата полезных данных в необходимый.

- Преобразование промежуточного формата IICF в формат прикладного протокола 2. Данная процедура может быть описана с помощью следующего уравнения плотности вероятности:

$$f_{\text{оп}}(x) = p_4 \frac{{\lambda_4}^{\alpha_4}}{\Gamma(\alpha_4)}(x - c_4)e^{-\lambda_4(x - c_4)} + p_5 \frac{{\lambda_5}^{\alpha_5}}{\Gamma(\alpha_5)}(x - c_5)e^{-\lambda_5(x - c_5)}, \quad (42)$$

где $f_{\text{оп}}(x)$ — плотность вероятности для преобразования из промежуточного формата IICF в формат прикладного протокола 2.

Таким образом, общее уравнение плотности вероятности преобразования сетевого пакета из формата прикладного протокола 1 в формат протокола 2 согласуется с ранее определенным уравнением плотности вероятности (39) и равно:

$$f(x) = f_{\text{пп}}(x) + f_{\text{фпд}}(x) + f_{\text{оп}}(x). \quad (43)$$

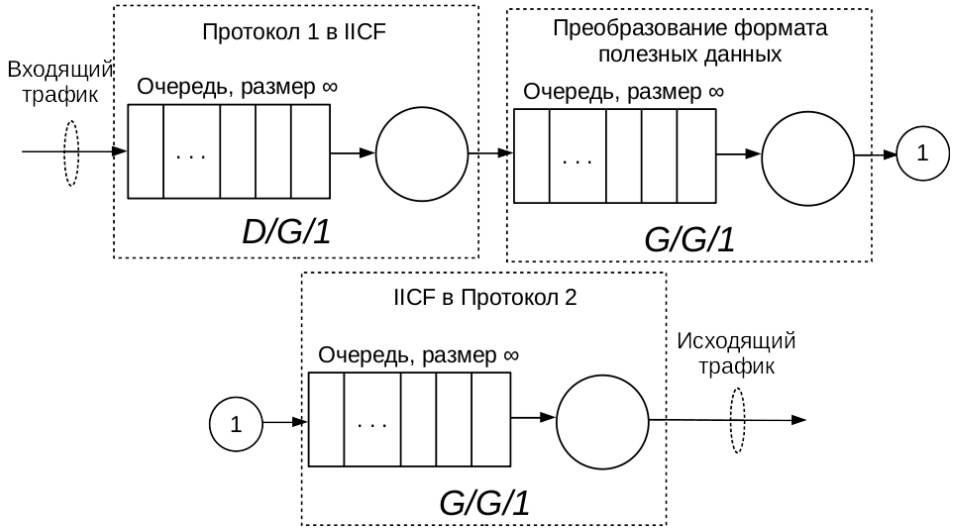


Рис. 34. Имитационная модель семантического преобразования сообщений

На рисунке 34 отображена структура описанной модели в виде системы массового обслуживания, содержащей модели D/G/1, G/G/1, G/G/1. Для простоты входящий поток описывается детерминированным законом поступления заявок.

3.6.2. Имитационная модель работы семантического шлюза промышленного Интернета вещей

На основе структуры, отображенной на рисунке 33, и полученных аналитических моделей, описанных в таблицах 9 и 10, предлагается разработать имитационную модель работы семантического шлюза ПИВ. Модель была разработана с помощью программных инструментов языка программирования Python для имитационного моделирования Ciw [60, 112], общее время моделирования составляет 10 с.

Также для оценки эффективности работы семантического гетерогенного шлюза ПИВ было проведено сравнение с другим методом, используемым для преобразования прикладных протоколов и форматов прикладных данных между собой, — методом инкапсуляции полезных данных (МИПД). Этот метод применяется для передачи данных по сети, не поддерживающей протокол передачи данных поступающего пакета, и выполняет инкапсуляцию заголовка протокола и всех содержащихся в нем данных в формат протокола, поддерживаемого сетью [6-7]. МИПД также может использоваться для передачи полезных данных, относящихся к прикладным протоколам, если точка назначения — оконечный узел (ОУ) — не имеет встроенной поддержки прикладного протокола (программного обеспечения) [63].

Для сравнения эффективности работы модели семантического шлюза ПИВ и данного метода была разработана модель отправки запросов на оконечные узлы сети ПИВ. Модель включает в себя шлюз для преобразования прикладных протоколов и форматов полезных данных прикладных протоколов между собой, оконечный узел, выполняющий обработку поступающих пакетов. Модель сети для СШ ПИВ и для шлюза, функционирующего по МИПД, представлена на рисунке 35.

Оконечный узел представляет собой модель G/G/1/n, согласно классификации Кендалла-Башарина с буфером размера n. Шлюз, выполняющий инкапсуляцию полезных данных, реализован как модель D/G/1. Ниже приведены параметры, используемые для оценки эффективности работы модели:

1. Общее время обслуживания поступающей заявки:

$$T_{\text{об}} = \bar{t_1} + \bar{t_2} + \bar{t_3} + \bar{t_4}, \quad (44)$$

где $T_{\text{об}}$ — общее время обслуживания заявки (с); $\bar{t_1}$ — среднее время пребывания заявки в буфере шлюза (с); $\bar{t_2}$ — среднее время обслуживания заявки на шлюзе (с); $\bar{t_3}$ — среднее время пребывания заявки в буфере оконечного узла (с), $\bar{t_4}$ — среднее время обслуживания заявки на оконечном узле (с).

2. Мощность оконечного узла за время моделирования *T:*

$$P_{\text{оу}} = \rho U I_a + (1 - \rho) U I_s, \quad (45)$$

где $P_{\text{оу}}$ — мощность оконечного узла (Вт); U — рабочее напряжение оконечного узла (В); I_a — сила тока оконечного узла в активном состоянии (А); I_s — сила тока оконечного узла в неактивном режиме (А);

$$\rho = \frac{Q}{\mu} = \frac{\bar{t_\mu}}{\bar{t_q}}, \quad (46)$$

где ρ — показатель загруженности обслуживающего устройства оконечного узла, Q — интенсивность поступления заявок (заявок/с), μ — интенсивность обслуживания заявок (заявок/с), $\bar{t_\mu}$ — среднее время обслуживания заявки (с); $\bar{t_q}$ — среднее время между поступлениями заявок (с).

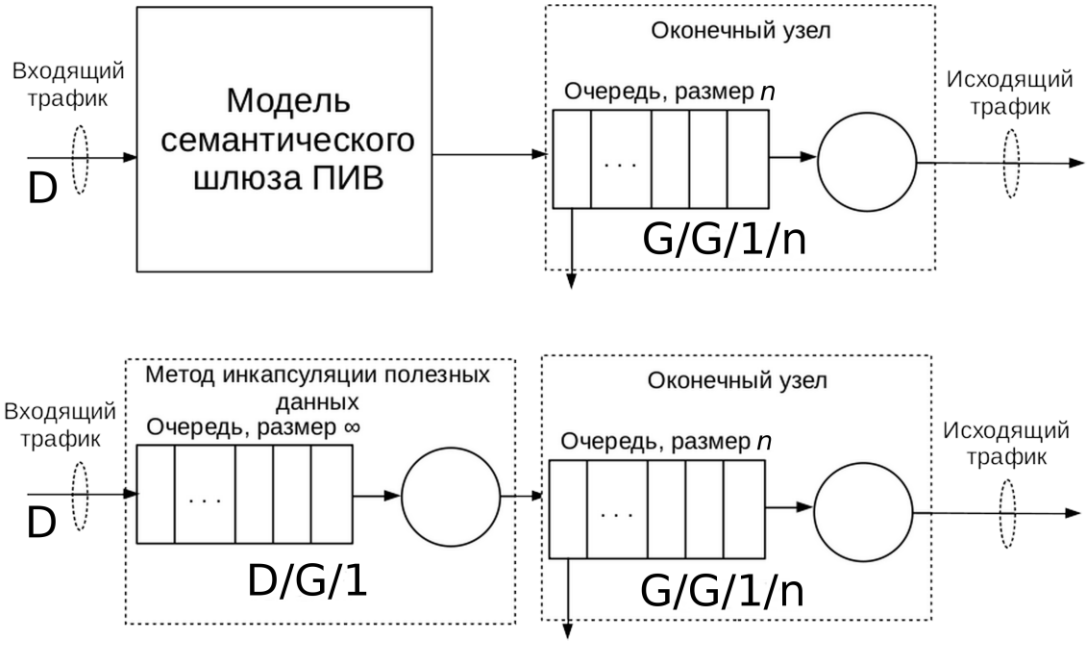


Рис. 35. Модель отправки запросов на оконечные узлы сети ПИВ

Перед проведением моделирования был разработан программно-аппаратный комплекс, отвечающий за преобразование пакетов из формата Modbus TCP в формат CoAP, при использовании методов преобразования полезных данных на семантическом гетерогенном шлюзе ПИВ, на основе которого проанализировано время обслуживания поступающих пакетов для семантического шлюза ПИВ, шлюза МИПД и оконечного устройства для двух конфигураций разработанной модели:

- Конфигурации, состоящей из семантического шлюза ПИВ и оконечного устройства. Оконечное устройство выполняет прием и обработку заголовка CoAP, а также разбор полезных данных пакета.

- Конфигурации, включающей шлюз МИПД и оконечное устройство. Оконечное устройство выполняет прием и обработку заголовка CoAP, инкапсулированного заголовка Modbus TCP, а затем преобразовывает полезные данные пакета в необходимый вид. В качестве оконечного устройства использован комплект разработчика VoCore1.

В результате исследования трафика, полученного с помощью данного программно-аппаратного комплекса, были получены аналитические модели, описывающие время обслуживания сетевых пакетов для всех видов устройств, используемых в данной модели. Результаты исследования приведены в таблице 11.

Таким образом, согласно результатам, отображенным в таблице 11, работа устройств в данной модели может быть описана с помощью следующих уравнений плотности вероятности:

$$f_{\text{сш}}(x) = p_1 \frac{{\lambda_1}^{\alpha_1}}{\Gamma(\alpha_1)}(x - c_1)\mathrm{e}^{-\lambda_1(x - c_1)} + p_2 \frac{{\lambda_2}^{\alpha_2}}{\Gamma(\alpha_2)}(x - c_2)\mathrm{e}^{-\lambda_2(x - c_2)}, \quad (47)$$

где $f_{\text{сш}}(x)$ — плотность вероятности времени обслуживания сетевого пакета на семантическом шлюзе, $p_1, \lambda_1, \alpha_1, c_1$ — коэффициенты вероятностного распределения, описывающего прием сетевого пакета протокола 1 и его преобразование в формат *IICF*, а также преобразования формата полезных данных, $p_2, \lambda_2, \alpha_2, c_2$ — коэффициенты вероятностного распределения, описывающего формирование и отправку сетевого пакета из формата IICF в формат прикладного протокола 2.

$$f_{\text{мипд}}(x) = p_3 \frac{{\lambda_3}^{\alpha_3}}{\Gamma(\alpha_3)}(x - c_3)e^{-\lambda_3(x - c_3)}, \quad (48)$$

где $f_{\text{мипд}}(x)$ — плотность вероятности времени обслуживания сетевого пакета на шлюзе МИПД, $p_3, \lambda_3, \alpha_3, c_3$ — коэффициенты вероятностного распределения, описывающего прием сетевого пакета протокола 1 и его преобразование в формат прикладного протокола 2 и дальнейшую его отправку.

$$f_{\text{оу}}(x) = p_4 \frac{{\lambda_4}^{\alpha_4}}{\Gamma(\alpha_4)}(x - c_4)\mathrm{e}^{-\lambda_4(x - c_4)} + p_5 \frac{{\lambda_5}^{\alpha_5}}{\Gamma(\alpha_5)}(x - c_5)\mathrm{e}^{-\lambda_5(x - c_5)}, \quad (49)$$

где $f_{\text{оу}}(x)$ — плотность вероятности времени обслуживания сетевого пакета на оконечном устройстве, $p_1 + p_2 = 1$, $(\lambda_4, \lambda_5), (\alpha_4, \alpha_5), (c_4, c_5)$ — коэффициенты вероятностных распределений, описывающих прием и обработку пакетов на оконечном устройстве.

Таблица 11. Аналитические модели, применяемые для описания устройств, используемых в модели

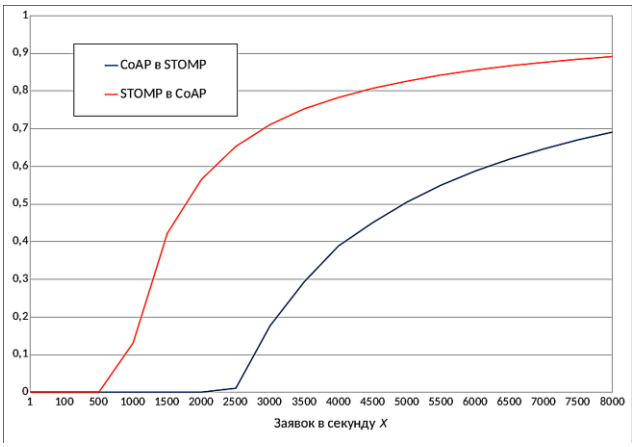
Вид устройства	Действие	Среднее время обработки пакета, мкс	Вероятностное распределение	Критерий согласия Колмогорова
Семантический шлюз	Прием пакета Modbus TCP и его преобразование в IICF	127,28 ± 2,06	В 100 % случаев: гамма (α = 147,30; λ = 1 219 512,20)	0,16 < 1,36
	Преобразование IICF в CoAP и отправка пакета	210,21 ± 1,77	В 100 % случаев: гамма (α = 97,02; λ = 471 698,12)	0,20 < 1,36
Шлюз МИПД	Прием и инкапсуляция пакета Modbus TCP и отправка пакета	261,19 ± 1,78	В 100 % случаев: гамма (α = 114,86; λ = 450 232,35)	0,23 < 1,36
Оконечное устройство	При работе с семантическим шлюзом	2310,99 ± 65,75	В 79 % случаев: гамма (α = 207,01; λ = 106 382,98)	0,36 < 1,36
			В 21 % случаев: гамма (α = 567,00; λ = 142 857,14)	
	При работе со шлюзом МИПД	2713,69 ± 40,44	В 76 % случаев: гамма (α = 72,99; λ = 32 258,06)	0,46 < 1,36
			В 24 % случаев: гамма (α = 764,27; λ = 178 571,42)	

3.6.3. Анализ результатов моделирования

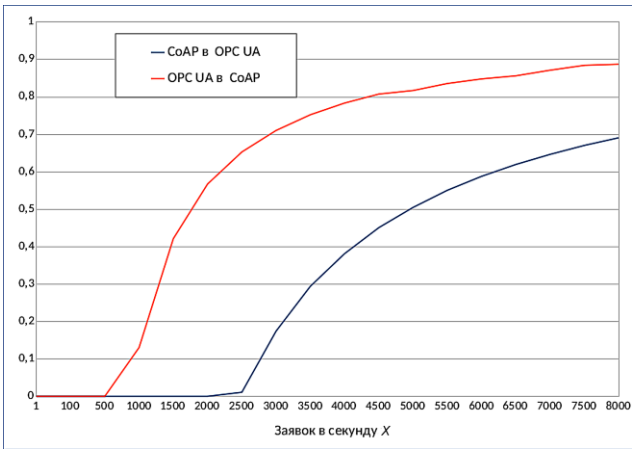
Для тестирования разработанной имитационной модели было проведено исследование времени семантического преобразования между протоколами CoAP и MQTT по сценариям CoAP-MQTT, MQTT-CoAP. Результаты тестирования отображены в таблице 12. На рисунке 36 приведены графики, показывающие соотношение количества сгенерированных пакетов к необслуженным.

Согласно результатам тестирования имитационной модели, представленным в таблице 12 и на рисунке 36, для сценария преобразования CoAP-MQTT теоретический предел количества обрабатываемых пакетов за 10 с близок к 50 000 пакетам, а для сценария MQTT-CoAP — к 40 000. Разработанная имитационная модель может быть использована как для дальнейшего теоретического исследования времени преобразования форматов сообщений ПИВ, так и для построения программно-аппаратного комплекса по сопровождению интеграции

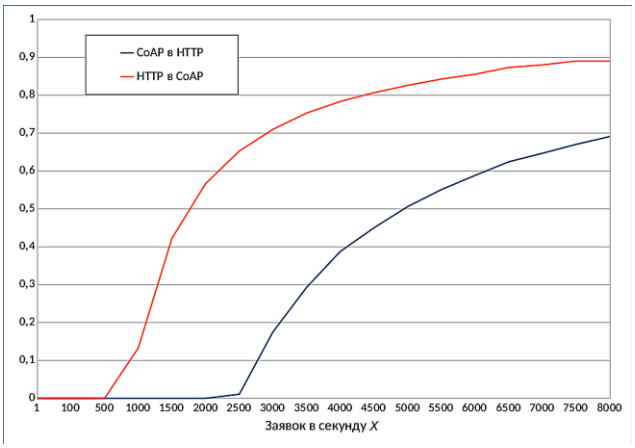
семантических шлюзов ПИВ в уже существующую сетевую инфраструктуру промышленных предприятий.



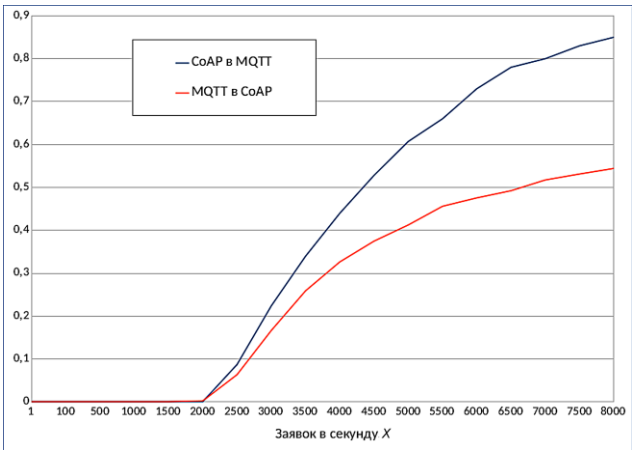
а)



б)



в)



г)

Рис. 36. Отношение необслуженных заявок к общему числу сгенерированных заявок для: а) CoAP-STOMP; б) CoAP-OPC UA; в) CoAP-HTTP; г) CoAP-MQTT

Таблица 12. Результаты тестирования имитационной модели семантического гетерогенного шлюза ПИВ

Интенсивность поступления пакетов	Сценарий	Среднее значение времени	
		обслуживания, с	ожидания, с
1	CoAP-MQTT	99,41E-06 ± 7,25E-06	0
	MQTT-CoAP	359,39E-06 ± 261,17E-06	0
500	CoAP-MQTT	108,03E-06 ± 8,33E-06	0
	MQTT-CoAP	516,02E-06 ± 153,79E-06	0

Продолжение таблицы 12

Интенсивность поступления пакетов	Сценарий	Среднее значение времени	
		обслуживания, с	ожидания, с
1000	CoAP-MQTT	103,70E-06 ± 4,03E-06	0
	MQTT-CoAP	385,94E-06 ± 74,85E-06	0
2000	CoAP-MQTT	104,61E-06 ± 2,75E-06	0
	MQTT-CoAP	390,76E-06 ± 54,29E-06	0
3000	CoAP-MQTT	103,66E-06 ± 0,69E-06	0
	MQTT-CoAP	448,37E-06 ± 17,30E-06	0
4000	CoAP-MQTT	103,80E-06 ± 0,36E-06	0
	MQTT-CoAP	437,74E-06 ± 8,44E-06	76,71E-06 ± 5,08E-06
5000	CoAP-MQTT	103,79E-06 ± 0,25E-06	0
	MQTT-CoAP	438,21E-06 ± 6,03E-06	1602,98E-06 ± 26,10E-06
6000	CoAP-MQTT	143,80E-06 ± 1,83E-06	54,47E-03 ± 1,69E-03
	MQTT-CoAP	444,41E-06 ± 5,81E-06	2,27 ± 0,02
7000	CoAP-MQTT	199,22E-06 ± 2,45E-06	65,27E-02 ± 1,08E-02
	MQTT-CoAP	445,81E-06 ± 5,79E-06	3,62 ± 0,03
8000	CoAP-MQTT	204,88E-06 ± 2,44E-06	1,86 ± 0,02
	MQTT-CoAP	439,78E-06 ± 5,71E-06	4,30 ± 0,03

Далее было произведено моделирование работы модели, отображенной на рисунке 35. На основе данной модели и полученных вероятностных распределений (табл. 11) было проведено имитационное моделирование на базе языка программирования Python и библиотеки дискретно-событийного моделирования Ciw. Поток поступающих заявок задан с помощью детерминированного распределения, общее время одного эксперимента составляло 60 с.

На рисунке 37 отображены результаты имитационного моделирования – отношение различных величин к количеству генерируемых сетевых пакетов в секунду. Наибольший прирост производительности СШ наблюдается при приближении интенсивности поступления заявок к пороговым значениям (700 —

СШ, 600 — шлюз МИПД) для каждой из конфигураций моделирования (рис. 5в). На диаграмме рисунка 5г можно видеть, что наибольший прирост показателя общего времени обработки пакетов приходится на момент, когда ОУ для конфигурации со шлюзом МИПД начинает отклонять поступающие заявки. При достаточно высоком показателе интенсивности поступления заявок (от 500) разрыв между общим временем обслуживания для СШ и временем для шлюза МИПД увеличивается. Семантический шлюз ПИВ показывает общее время обслуживания на 14 % ниже, чем шлюз МИПД (без учета показателей для значений интенсивности поступления заявок 650 и 700). Также СШ демонстрирует на 8 % более высокий уровень энергоэффективности работы оконечного узла при $\rho \leq 1$.

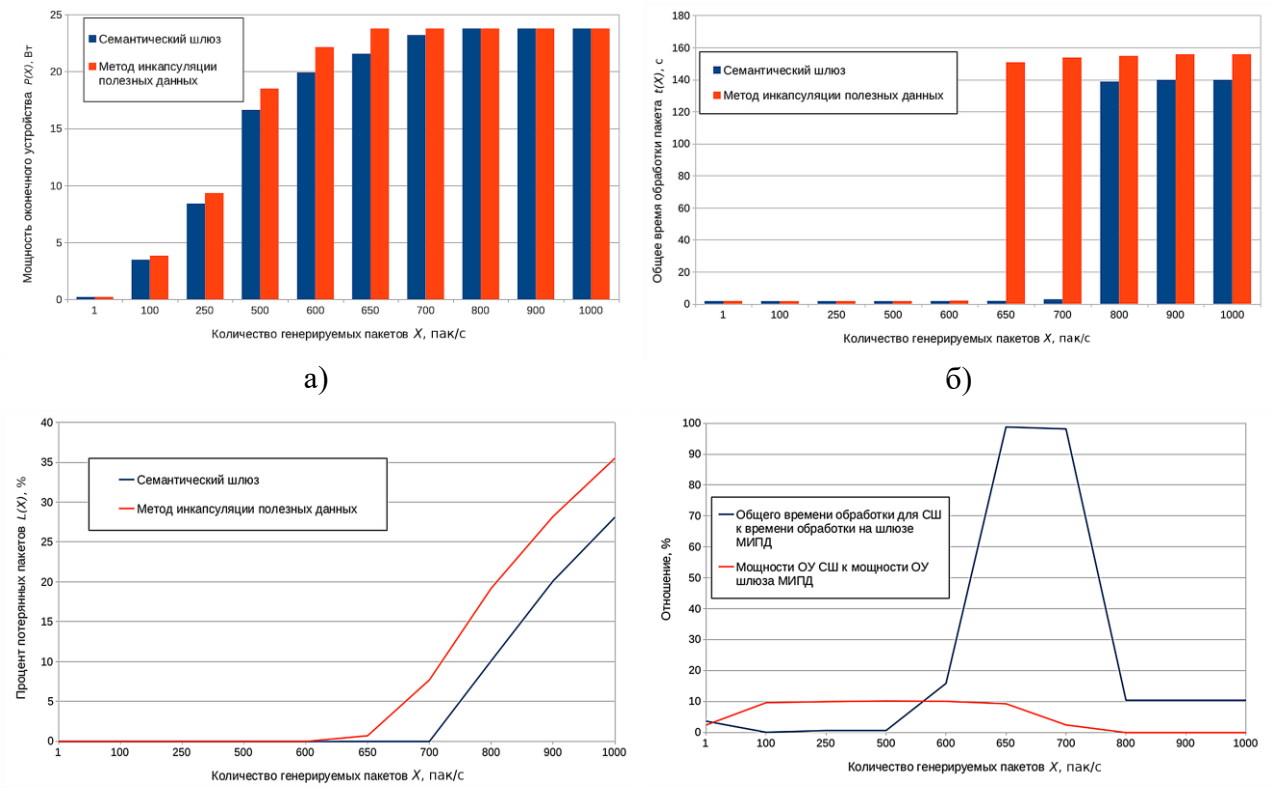


Рис. 37. Результаты имитационного моделирования: а) мощность оконечного устройства (Вт); б) общее время обработки пакета (мс); в) процент потерянных пакетов (%); г) прирост показателей общего времени обработки пакетов и мощности ОУ при сравнении СШ и шлюза МИПД (%)

Выводы по главе 3

1. Разработаны структуры гетерогенного и семантического шлюза ПИВ, позволяющие обеспечить совместимость различных сетевых технологий ПИВ между собой.

2. Разработан промежуточный формат для взаимного преобразования протоколов ПИВ между собой на основе форматов полезных данных существующих сетевых протоколов.

3. Получены аналитические модели по времени преобразования форматов полезных данных XML, JSON, CSV и прикладных протоколов CoAP, MQTT, Modbus TCP, STOMP, OPC UA, HTTP между собой.

4. На базе полученных аналитических моделей разработана имитационная модель семантического шлюза ПИВ, и на ее основе были испытаны свойства семантического гетерогенного шлюза ПИВ во время его работы при разной интенсивности поступления пакетов.

5. Для оценки производительности разработанной модели семантического шлюза проведено сопоставление моделей семантического гетерогенного шлюза ПИВ и шлюза, основанного на методе инкапсуляции полезных данных, где семантический шлюз ПИВ показал более высокий уровень производительности для системы, состоящей из шлюза и оконечного устройства.

Глава 4. РАЗРАБОТКА МЕТОДИКИ КОМПЛЕКСНОГО ТЕСТИРОВАНИЯ СИСТЕМ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

4.1. Обзор методов и методик тестирования телекоммуникационного оборудования и сетей и систем связи

В настоящее время существует множество методов и методик тестирования сетей и систем связи. Множество из данных методик может быть применено для проведения испытаний в рамках систем ПИВ. Таким образом, перед разработкой методики тестирования систем ПИВ необходимо провести исследование существующих на настоящее время стандартов тестирования сетей и систем связи. В данной работе будут проанализированы следующие стандарты тестирования:

- ГОСТ Р 56920-2016 «Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения» [23], основанный на ISO/IEC/IEEE 29119-1:2013 [1] и имеющий ряд терминов, описывающих основные виды тестирования в рамках программной и системной инженерии.
- МСЭ-Т Q.3900 «Методы тестирования и архитектура модельных сетей для тестирования технических средств СПП, используемых в сетях электросвязи общего пользования» [22], описывающий основные виды тестирования на модельных сетях.
- МСЭ-Т Y.1564 «Методология тестирования подключения услуг Ethernet» [18] и IETF RFC 2544 «Методология нагрузочного тестирования для устройств межсетевого взаимодействия» [8], описывающие методологию тестирования устройств связи в рамках сетей связи, основанных на технологии Ethernet.

ГОСТ Р 56920-2016 «Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения» описывает основные термины и понятия тестирования программного обеспечения, в рамках которого даны определения основных видов тестирования ПО, которое может быть

применено в рамках тестирования сетей и систем связи. Следующие виды тестирования, определенные в данном стандарте, могут быть использованы для тестирования сетей и систем связи:

- тестирование производительности (performance testing) — вид тестирования, проводимый для оценки степени, с которой тестируемый элемент выполняет свои функции при заданных ограничениях времени, и других различных ресурсов;
- тестирование устойчивости (endurance testing) — вид тестирования производительности системы, определяющий, может ли тестируемый элемент постоянно выдерживать установленную загрузку в течение определенного периода времени;
- нагрузочное тестирование (load testing) — вид тестирования производительности системы, проводимый для оценки поведения тестируемого элемента при определенных условиях загрузки системы, обычно для случаев ожидаемых уровней низкого, обычного и пикового использования;
- стрессовое тестирование (stress testing) — вид тестирования производительности системы, проводимый для оценки поведения тестируемого элемента при условиях нагрузки выше ожидаемого уровня или уровня, указанного в требованиях к производительности, или при доступности ресурсов ниже минимального уровня, указанного в требованиях;
- тестирование вместимости (capacity testing) — вид тестирования производительности системы для оценки уровня, при котором с увеличением нагрузки (числа пользователей, транзакций, элементов данных и т. д.) тестируемый элемент не обеспечивает требуемую производительность;
- тестирование совместимости (compatibility testing) — вид тестирования, который измеряет степень того, насколько удовлетворительно тестируемый элемент функционирует параллельно с другими независимыми элементами в общей среде (co-existent) и, по мере необходимости, взаимодействует с другими системами или элементами систем (compatibility);

- тестирование надежности (reliability testing) — вид тестирования, проводимый для оценки возможности тестируемого элемента выполнять свои функции, включая оценку частоты отказов системы, при использовании в заданных условиях и в течение определенного периода времени.

Большинство видов тестирования, определенных как допустимые для использования в сетях и системах связи, относятся к тестированию производительности, например тестирование устойчивости, нагрузочное тестирование, стрессовое тестирование, тестирование вместимости. Также были выбраны следующие методы тестирования, не относящиеся к тестированию производительности: тестирование совместимости и тестирование надежности.

В Рекомендации МСЭ-Т Q.3900 «Методы тестирования и архитектура модельных сетей для тестирования технических средств СПП, используемых в сетях электросвязи общего пользования», в которой определяются основные тестируемые элементы и функции, описываются основные процедуры тестирования в сетях связи и дается определение модельных сетей — прототипов действующих сетей электросвязи общего пользования, базирующихся на оборудовании сетей последующих поколений (СПП), с помощью которых возможно выполнение видов тестирования, проводимых для выявления особенностей функционирования и совместимости проверяемого оборудования под нагрузкой, что обеспечивает более высокое качество и объективность тестирования.

В рамках данной Рекомендации определяются основные элементы систем, которые подлежат тестированию и которые перечислены далее:

1. Система управления сеансами вызовов:
    - контроллер медиашлюза (MGC);
    - прокси-сервер SIP (PS);
    - мультимедийная IP-подсистема (IMS).
2. Система передачи голоса и сигнализации:
    - медиашлюз (GW);

- шлюз сигнализации (SG);
- оборудование транспортной сети (TNE).

3. Серверы приложений:
   - сервер приложений (AS);
   - медиасервер (MDS);
   - сервер обмена сообщениями (MeS).
4. Система управления и выставления счетов:
   - система управления СПП (NMS);
   - система выставления счетов (BS).

В рамках ПИВ наиболее важными тестируемыми элементами, упомянутыми в данном стандарте, являются сервера приложений (AS, MDS и MeS) и шлюзы (GW, SG).

Также стоит упомянуть об основных функциях, требующих обязательного тестирования:

1. Функции аспекта транспортирования:
   - функции транспортирования;
   - функции управления транспортированием;
   - функции профиля пользователя транспортирования.
2. Функции аспекта обслуживания:
   - функции управления услугами;
   - функции поддержки приложений/услуг;
   - функции профиля пользователя услуг.
3. Функции конечного пользователя.
4. Функции управления.

Также не менее важным пунктом в контексте тестирования систем ПИВ являются основные процедуры тестирования, которые делятся на два уровня:

1. Локальное тестирование технических средств СПП, которое включает в себя:

- Тестирование функциональных возможностей. Методика тестирования технических средств СПП на данном уровне предполагает проверку реализуемых оборудованием функциональных возможностей в соответствии с классификацией тестируемых функций, приведенной выше. Данная процедура включает в себя следующие тесты:
  - ✓ Проверка перечня и состава обязательных и дополнительных функциональных возможностей системы.
  - ✓ Проверка корректности и полноты реализации функциональных возможностей системы.
- Нагрузочное тестирование. Методика тестирования на данном уровне предполагает проверку функционирования системы в условиях произвольной нагрузки. Тестирование должно включать в себя проверку корректности и полноты реализации функциональных возможностей системы при пиковых нагрузках.
- Тестирование на соответствие. Методика тестирования системы на соответствие предполагает проверку используемых в данной системе протоколов и интерфейсов и полноты их реализации в соответствии с международными стандартами. Данная процедура включает в себя следующие тесты:
  - ✓ Проверка протоколов и интерфейсов систем на их соответствие одному из видов оборудования СПП и заложенных в нем функциональных возможностей.
  - ✓ Проверка корректности и полноты реализации протоколов данной системы согласно международным рекомендациям и стандартам.

2. Тестирование комплексных решений СПП, или тестирование сетей СПП (NUT — тестируемая сеть), которое включает в себя:

- Тестирование функциональных возможностей. Классификация оборудования СПП и реализуемые в решениях услуги позволяют определить возможность использования и область применения данного оборудования.

Взаимодействие оборудования СПП различных типов друг с другом определяется по готовым решениям, которые выполняют определенные задачи.

- Тестирование межсетевого взаимодействия. Данный уровень включает ряд тестов для проверки взаимодействия оборудования различных производителей на технических средствах NUT. Тестирование включает в себя проверки работы оборудования в режиме «точка — точка» и тесты на функциональную совместимость, исключая применение внешних средств, проверка которых должна осуществляться на уровне сквозного тестирования. Данная процедура включает в себя следующие тесты:
  - ✓ Проверка выполнения заданных функциональных возможностей систем при их взаимодействии в рамках NUT.
  - ✓ Проверка соответствия достаточности и полноты реализации протоколов в тестируемых системах, необходимых для оценки заданных функциональных возможностей.
  - ✓ Проверка соответствия возможностей систем, тестируемых во время взаимодействия, в части объема и качества реализации заложенных в них услуг.
- Тестирование услуг. Данный уровень включает тесты по проверке реализуемых в NUT услуг связи. Основные услуги СПП, тестируемые в рамках NUT, включают в себя:
  - ✓ Услуги электросвязи для абонентов.
  - ✓ Услуги транзита трафика.
  - ✓ Дополнительные услуги.
- Сквозное тестирование. Тестирование функциональной совместимости предполагает проверку работоспособности технических средств NUT в рамках полного цикла организации связи. Данная процедура включает в себя следующие тесты:
  - ✓ Сквозной — предназначен для проверки корректности процедуры

организации связи на всех уровнях при его прохождении по NUT на уровне пользователя.

- ✓ «Узел — узел» — предназначен для испытания отдельных узлов в NUT.

- Тестирование качества обслуживания. Методика локального тестирования технических средств СПП предполагает проведение измерения показателей качества обслуживания и проверки наличия реализации системы управления качеством связи в технических средствах NUT.

- Тестирование мобильности и роуминга. Методика тестирования NUT на данном уровне предполагает проведение оценки возможностей мобильности абонентов и их роуминга. Данная процедура включает в себя следующие тесты:

  - ✓ Проверка реализации мобильности на тестируемой NUT и заложенных в ней функциональных возможностей.
  - ✓ Проверка корректности и полноты реализации протоколов в NUT для поддержания функций мобильности и роуминга.

Наиболее важными испытаниями, упомянутыми в данной Рекомендации, для систем ПИВ можно считать следующие тесты: тестирование функциональных возможностей, нагрузочное тестирование, тестирование межсетевого взаимодействия, сквозное тестирование, тестирование качества обслуживания.

Рекомендации МСЭ-Т Y.1564 «Методология тестирования подключения услуг Ethernet» и IETF RFC 2544 «Методология нагрузочного тестирования для устройств межсетевого взаимодействия» описывают процедуру тестирования каналов связи Ethernet, включая структуру и сценарии тестирования.

Рекомендация IETF RFC 2544 описывает следующие виды структур тестирования локальных каналов связи:

- Структура тестирования «тестируемое устройство (DUT, или ТУ) — устройство тестирования (УТ)». В данной структуре ТУ подключается проводным соединением к УТ. Данная структура отражена на рисунке 38а.

- Структура тестирования «отправитель — тестируемое устройство — получатель». В данной структуре отправитель подключается проводным соединением к ТУ, которое затем подключается к получателю. Данная структура отражена на рисунке 38б.
- Структура тестирования «тестируемое устройство 1 (DUT 1, или ТУ 1) — тестируемое устройство 2 (DUT 2, или ТУ 2)». Данная структура повторяет структуру ТУ-УТ, но с условием тестирования сразу нескольких единиц оборудования. Данная структура отражена на рисунке 39.

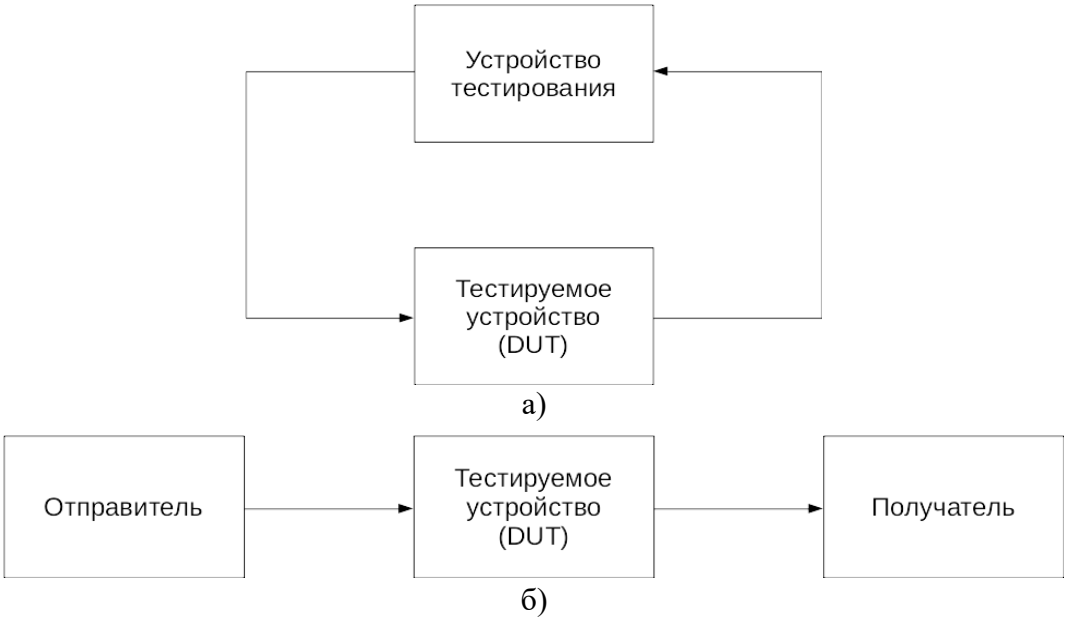


Рис. 38. Структура тестирования: а) ТУ-УТ; б) отправитель — ТУ — получатель

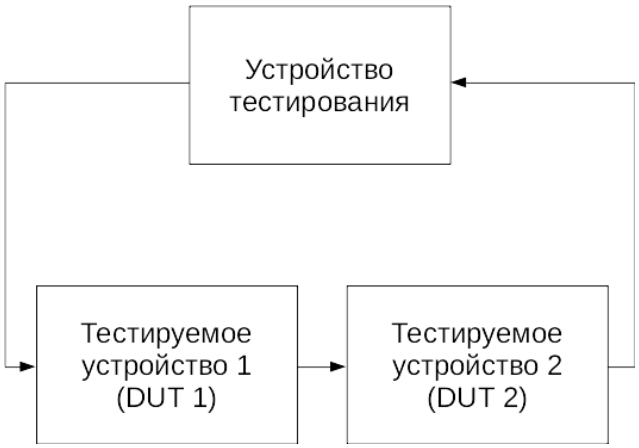


Рис. 39. Структура тестирования для нескольких ТУ

Также в данных рекомендациях указаны следующие параметры оценки

качества работы канала связи:

1. Пропускная способность канала связи (ПС, Throughput). Пропускная способность оценивается как по Рекомендации IETF RFC 1242 [9], так и по величине ПС, при которой нет потерь кадров.

2. Сетевая задержка (Latency). Сетевая задержка определяется как по Рекомендации IETF RFC 1242, так и для каждого кадра выборочно.

3. Потеря кадров (Frame Loss). Потеря кадров оценивается как по Рекомендации IETF RFC 1242 на всем диапазоне скоростей передачи данных и объема кадров, так и на основе оценки потерь в зависимости от интенсивности поступления кадров.

4. Оценка работы оборудования при высокой интенсивности поступления кадров (Back-to-back). Работа оборудования оценивается как по методике, представленной в IETF RFC 1242, для кадров, поступающих с минимально возможным интервалом, так и по времени работы при заданной интенсивности.

5. Восстановление системы. Система оценивается по времени восстановления полноценной работы после возникновения ошибки при перегрузке сетевым трафиком.

6. Перезагрузка. Время восстановления полноценной работы системы после программного или аппаратного сбоя.

7. Сетевое дрожание, или джиттер (Jitter). Оценка отклонения сетевых задержек относительно среднего значения между поступлениями кадров.

8. Комплексный траффик (Complex traffic). Сетевое оборудование подвергается воздействию нескольких потоков тестового трафика. В ходе данного теста измеряются значения пропускной способности канала связи, величина потерь кадров.

4.2. Структура программы и методики комплексного тестирования систем промышленного Интернета вещей

Для проведения комплексного тестирования систем промышленного Интернета вещей на основе существующих стандартов и рекомендаций по тестированию сетей связи необходимо дополнить существующую методику тестирования для элементов систем ПИВ, которые ранее не использовались в решениях промышленной автоматизации. Такими элементами являются семантические гетерогенные шлюзы ПИВ (СШ), граничные (ГС) и облачные сервера (ОС) ПИВ. Данная методика была разработана и внедрена в проект стандарта ИСО/МЭК 30162 «Интернет вещей (IoT) — Требования к совместимости и структуре модельных сетей для устройств, относящихся к системам промышленного Интернета вещей» [2], а также в Рекомендациях МСЭ-Т Q.4060 «Структура проведения тестирования гетерогенных шлюзов Интернета вещей в лабораторных условиях» [17] и Q.3056 «Процедуры сигнализации между зондами, которые используются для дистанционного тестирования параметров сетей связи» [19, 43, 54, 103].

В рамках Стандарта ИСО/МЭК 30162 «Интернет вещей (IoT) — Требования к совместимости и структуре модельных сетей для устройств, относящихся к системам промышленного Интернета вещей» были определены требования к совместимости систем промышленного Интернета вещей, требования к структуре систем ПИВ, элементы систем ПИВ, такие как семантический гетерогенный шлюз ПИВ (описанный в главе 3 данной работы) и граничные шлюзы ПИВ. Также были сформированы существующие методы взаимодействия систем ПИВ между собой и была определена последовательность проведения испытаний СШ и сервера ПИВ (граничного или облачного).

В Рекомендации МСЭ-Т Q.4060 «Структура проведения тестирования гетерогенных шлюзов Интернета вещей в лабораторных условиях» была описана структура семантического гетерогенного шлюза Интернета вещей, структура сетей, в которых данное устройство может быть использовано, и основные параметры его

производительности.

В Рекомендации МСЭ-Т Q.3056 «Процедуры сигнализации между зондами, которые используются для дистанционного тестирования параметров сетей связи» описана структура системы удаленного тестирования сетей связи через закрытые для тестирования сегменты ССОП, которая разрабатывалась для тестирования систем ПИВ. Данная система включает в себя описание структуры ПАК удаленного тестирования, методы прохождения трафика через системы трансляции сетевых адресов (NAT) [10], описание сценария тестирования через системы NAT.

В приложении А данной работы приведена разработанная методика комплексного тестирования систем ПИВ, которая описывает процедуру комплексного тестирования семантических гетерогенных шлюзов ПИВ, граничных и облачных серверов ПИВ и включает в себя следующие этапы испытаний данных систем:

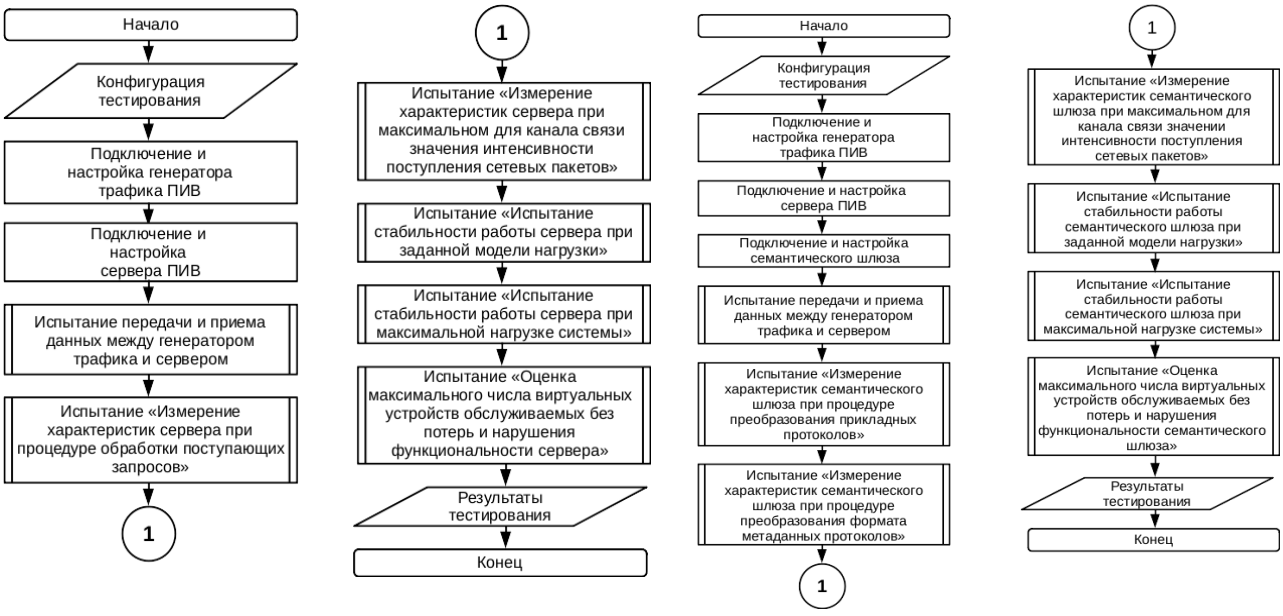
- измерение характеристик работы элементов систем ПИВ в режиме нагрузочного и стрессового тестирования систем ПИВ (тестирование производительности);
- испытание стабильности работы элементов систем ПИВ в режиме нагрузочного и стрессового тестирования систем ПИВ (тестирование надежности);
- оценка максимального числа устройств ПИВ, поддерживаемых элементом системы ПИВ (тестирование вместимости).

Также данная методика включает в себя описания порядка проведения испытаний и последовательность действий для тестирования как серверов ПИВ, так и СШ (рис. 40).

4.3. Генерация трафика для тестирования систем ПИВ

Для проведения тестирования производительности систем ПИВ и их отдельных элементов необходимо определить, каким образом проходит тестирование сетевой инфраструктуры промышленного предприятия. Для этого необходимо:

- определить тестируемые элементы сетевой инфраструктуры и разработать модельную сеть для оценки устойчивости существующей сетевой инфраструктуры к трафику ПИВ;



а) б)

Рис. 40. Последовательность действий для проведения тестирования: а) граничных и облачных серверов ПИВ; б) семантического шлюза ПИВ

- определить виды источников трафика и характер формирования сетевых пакетов;
- разработать структуру программно-аппаратного комплекса для проведения нагрузочного и стрессового тестирования [55-56];
- провести тестирование производительности существующей сетевой инфраструктуры при воздействии трафиком ПИВ согласно разработанным или ранее выбранным методикам и методам тестирования [57].

Генератор трафика ПИВ (далее ГТ) необходим для проведения большинства видов тестов производительности систем ПИВ, включая следующие: нагрузочное, стрессовое, вместимости и надежности. Структура системы тестирования существующей сетевой инфраструктуры промышленных предприятий на основе генератора трафика ПИВ изображена на рисунке 41. На данной структуре отображена система тестирования, состоящая из генератора трафика и ГС, ОС,

выступающими устройствами контроля тестирования, а также СШ, выполняющим сетевое преобразование.

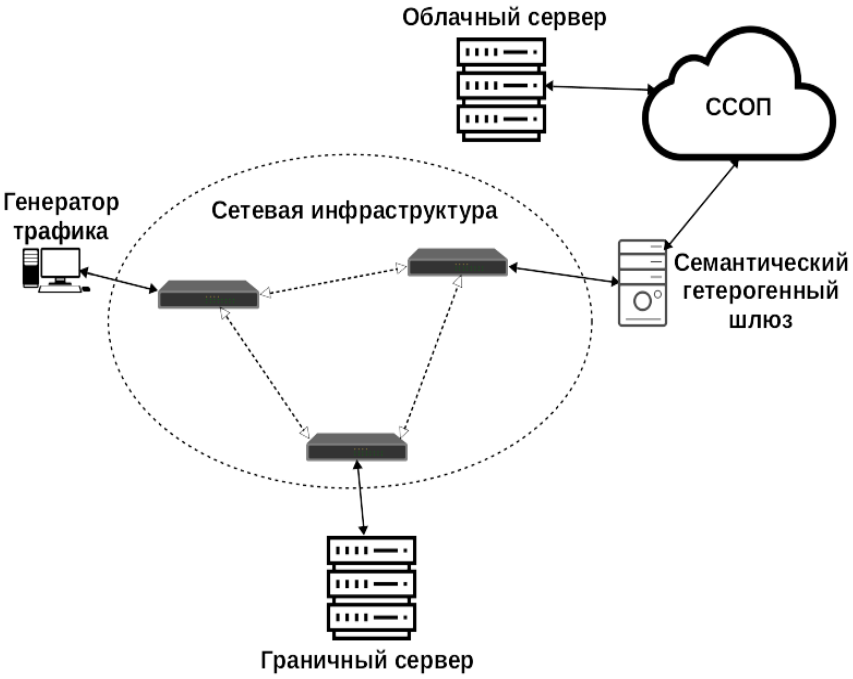


Рис. 41. Структура системы тестирования производительности существующей сетевой инфраструктуры при воздействии трафиком ПИВ

ГТ может включать в себя множество виртуальных устройств ПИВ, которые генерируют трафик согласно своей роли и характеристикам интенсивности поступления сетевых пакетов, которые были получены в главе 2, в ходе исследований модели фрагмента сетей ПИВ. Семантический гетерогенный шлюз функционирует согласно модели, разработанной в главе 3, в ходе исследования метода построения семантических гетерогенных шлюзов ПИВ.

4.4. Метод удаленного тестирования систем ПИВ

Для проведения удаленного тестирования систем ПИВ, например между различными филиалами одного промышленного предприятия, предлагается использовать систему, разработанную в ходе подготовки Рекомендации МСЭ-Т Q.3056 «Процедуры сигнализации между зондами, которые используются для дистанционного тестирования параметров сетей связи» и отображенную на

рисунке 41.

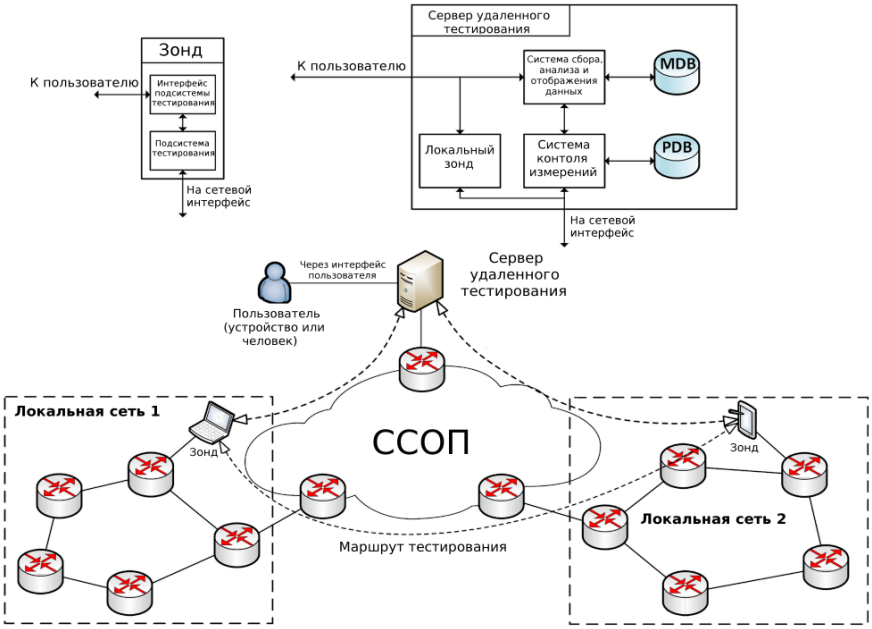


Рис. 42. Структура программно-аппаратного комплекса для удаленного тестирования МСЭ-Т Q.3056

В данный программно-аппаратный комплекс входят следующие элементы:

1. Зонд — клиент системы мониторинга качества услуг связи. Включает в себя следующие подсистемы:

- подсистема тестирования;
- интерфейс взаимодействия подсистемы тестирования.

2. Сервер удаленного тестирования параметров сети и услуг связи. Включает в себя следующие подсистемы:

- система контроля тестирования (измерений);
- система сбора, анализа и отображения данных;
- база данных тестов (MDB);
- база данных зондов (PDB).

Данный ПАК позволяет проводить измерение следующих параметров сетей связи:

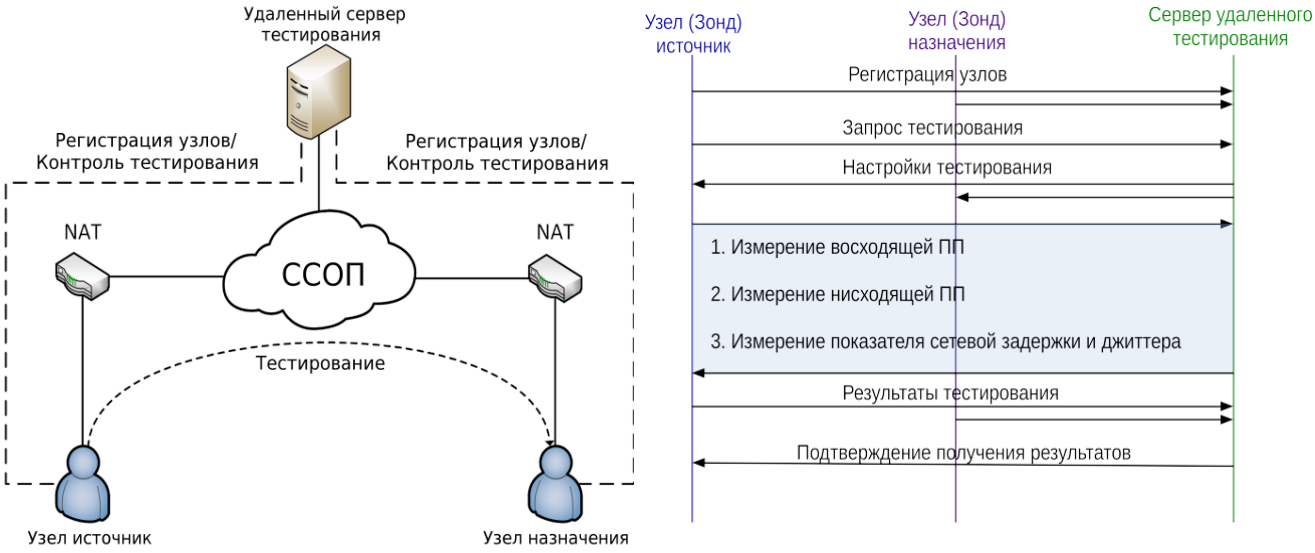
- круговая сетевая задержка RTT (latency);
- сетевой джиттер (jitter);
- восходящая пропускная способность (uplink);

- нисходящая пропускная способность (downlink);
- потери сетевых пакетов (package loss).

Данный ПАК позволяет проводить тестирование приведенных параметров между двумя удаленными сегментами сетевой инфраструктуры, даже при условии отсутствия выделенного адреса в ССОП, через системы трансляции сетевых адресов (NAT). Для этого данная система использует механизмы обхода устройств NAT — STUN (Session Traversal Utilities for NAT) [11] и TURN (Traversal Using Relay NAT) [12].

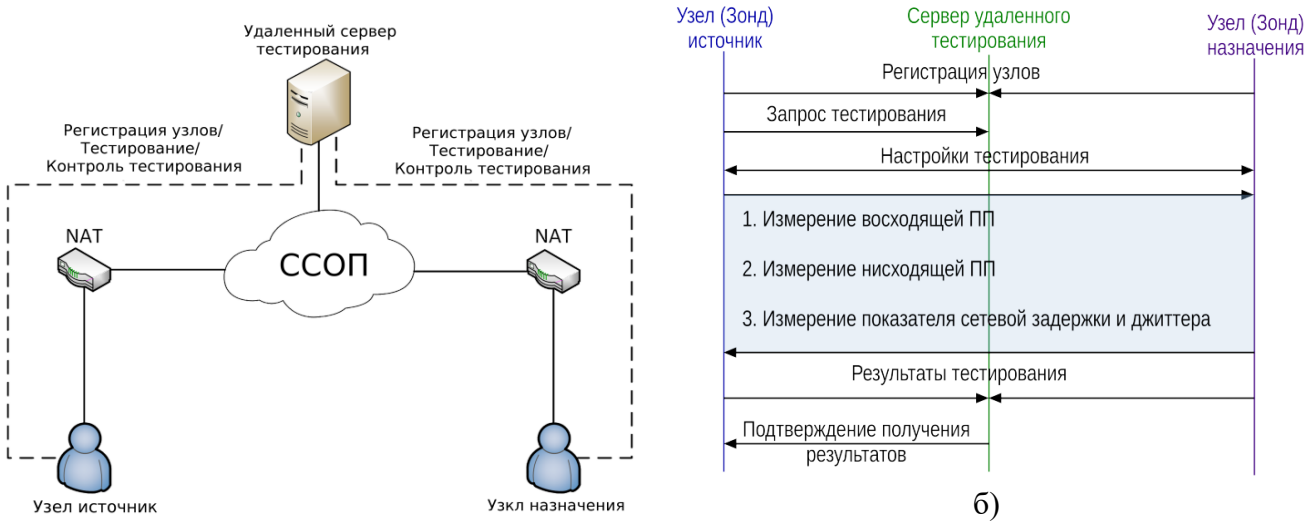
На рисунке 43 отображена структура системы обхода устройств NAT и сценарий измерения параметров сетей связи для механизма STUN. Механизм STUN использует в качестве транспортного протокола протокол UDP и заключается в определении внешнего сетевого адреса и порта, выдаваемого NAT для каждого из устройств в подсетях с помощью специального сервера тестирования, имеющего выделенный адрес в ССОП. Затем одно из устройств, получившее внешний адрес и порт другого сопряженного устройства, начинает процедуру тестирования параметров сети между данными устройствами.

На рисунке 44 отображена структура системы обхода устройств NAT и сценарий измерения параметров сетей связи для механизма TURN. Механизм TURN использует в качестве основного транспортного протокола протокол TCP, но имеет возможность использования UDP и заключается в отправке всего трафика сопряженному устройству, не имеющему внешнего сетевого адреса, с помощью специального сервера тестирования, имеющего выделенный сетевой адрес в ССОП. Затем одно из устройств начинает процедуру тестирования параметров сети между данными устройствами через промежуточный сервер тестирования.



а) б)

Рис. 43. Система удаленного тестирования, функционирующая на основе механизма STUN, где а) структура данной системы; б) сценарий тестирования



а) б)

Рис. 44. Система удаленного тестирования, функционирующая на основе механизма TURN, где а) структура данной системы; б) сценарий тестирования

4.5. Тестирование генератора трафика для систем промышленного Интернета вещей

4.5.1. Цель и задачи тестирования генератора трафика ПИВ

Для проведения испытания существующей сетевой инфраструктуры на базе разработанной методики комплексного тестирования систем ПИВ необходимо

разработать и протестировать систему генерации трафика, которая будет использоваться как элемент системы комплексного тестирования систем ПИВ. Для решения данной задачи необходимо:

- разработать структуру фрагмента модельной сети для тестирования работы генератора трафика ПИВ;
- разработать алгоритм работы генератора трафика;
- определить алгоритмы генерации последовательностей псевдослучайных значений;
- провести испытание работы генератора трафика на основе определенных в главе 2 вероятностных распределений, описывающих характер различных видов трафика ПИВ.

4.5.2. Структура модельной сети для тестирования генератора трафика ПИВ

Для проведения тестирования работы генератора трафика предлагается структура модельной сети, представленная на рисунке 45 [41, 99]. Данный программно-аппаратный комплекс, отвечающий за анализ трафика, создаваемого ГТ, включает в себя следующие элементы:

1. Клиентское устройство (клиент) — вычислительное устройство, имитирующее работу оконечных устройств ПИВ и выступающее генератором трафика. Включает в себя следующие программные компоненты:

- клиентское ПО, отвечающее за формирование и отправку сообщений серверу с помощью специальных прикладных, транспортных и сетевых протоколов;
- генератор временных интервалов — подпрограмма клиентского ПО, отвечающая за генерацию значений выборок интервалов времени между отправляемыми сообщениями;
- генератор данных — подпрограмма клиентского ПО, отвечающая за генерацию полезной нагрузки сообщений.

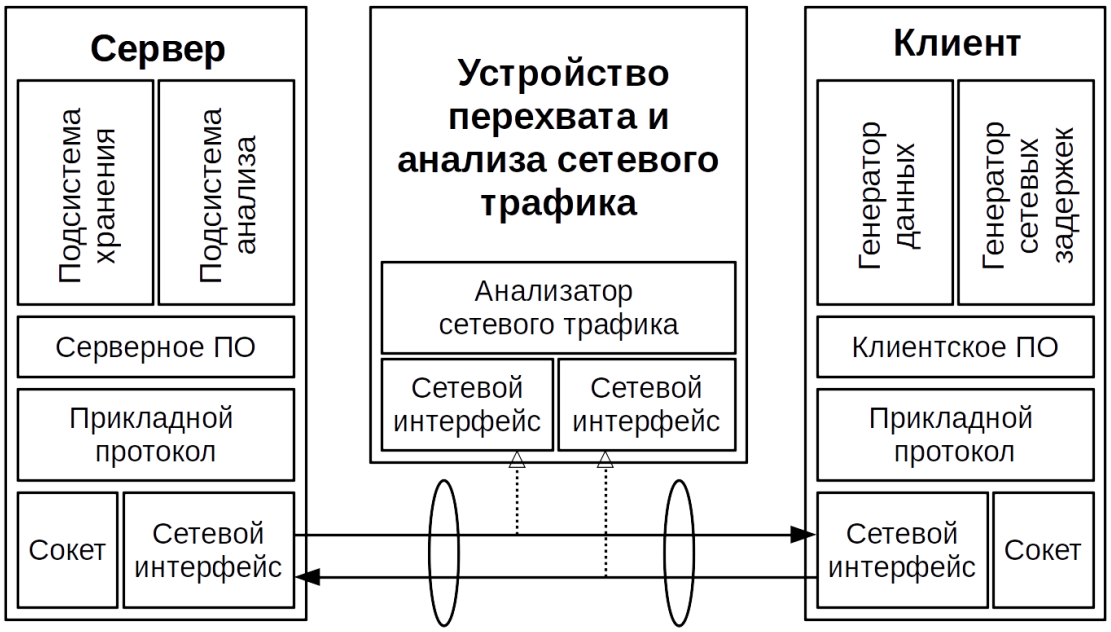


Рис. 45. Структура модельной сети для тестирования работы генератора трафика ПИВ

2. Серверное устройство (сервер) — вычислительное устройство, выступающее в роли сервера ПИВ, агрегирующего, хранящего и анализирующего информацию. Включает в себя следующие программные компоненты:

- серверное ПО, отвечающее за сбор, хранение и анализ сообщений, поступающих от клиентов, с помощью специальных прикладных, транспортных и сетевых протоколов;
- подсистема хранения — подпрограмма серверного ПО, отвечающая за сбор полезной нагрузки сообщений и за взаимодействие с системой хранения данных (например, с системой управления базами данных — СУБД);
- подсистема анализа — подпрограмма серверного ПО, отвечающая за анализ поступающей от клиента информации; например, данная подсистема отвечает за анализ как полезной нагрузки сообщений, так и характеристик самого сетевого трафика.

3. Устройство перехвата и анализа сетевого трафика — вычислительное устройство, отвечающее за перехват сетевого трафика во время взаимодействия сервера и клиента, а также за анализ данной информации с помощью специального

ПО, называемого анализатором сетевого трафика.

Также на данной архитектуре присутствуют следующие элементы:

1. Сетевой интерфейс — сетевой интерфейс вычислительного устройства.
2. Сокет — программный интерфейс, встроенный в операционную систему вычислительного устройства и отвечающий за мультиплексирование/демультиплексирование сетевого трафика на основе адреса устройства в сети и номера порта, а также выступающий в качестве программного инструмента для взаимодействия с сетевым интерфейсом для приема или передачи сообщений из сети.

4.5.3. Алгоритм работы генератора трафика

Для разработки алгоритма генерации трафика промышленного Интернета вещей на основе проведенного исследования в первую очередь необходимо определить методы генерации случайных чисел для следующих распределений:

- непрерывное равномерное распределение;
- двухпараметрическое гамма-распределение;
- двухпараметрическое бета-распределение первого рода;
- двухпараметрическое распределение Вейбулла-Гнеденко;
- экспоненциальное распределение;
- распределение Эрланга m-го порядка.

На основе выбранных вероятностных распределений был разработан общий алгоритм генерации псевдослучайных последовательностей согласно заданному закону распределения. Алгоритмы работы генератора трафика промышленного Интернета вещей изображены на рисунках 46 и 47 [40].

Приведенные в данных блок-схемах переменные обозначают:

- C — количество источников трафика;
- N — количество сетевых пакетов, отправляемых каждым из источников.

D (*Dt, Dm*) — параметры вероятностных распределений для интервалов времени между отправкой сообщений (*Dt*) и для объема сетевых пакетов (*Dm*). В *D*

входят следующие параметры:

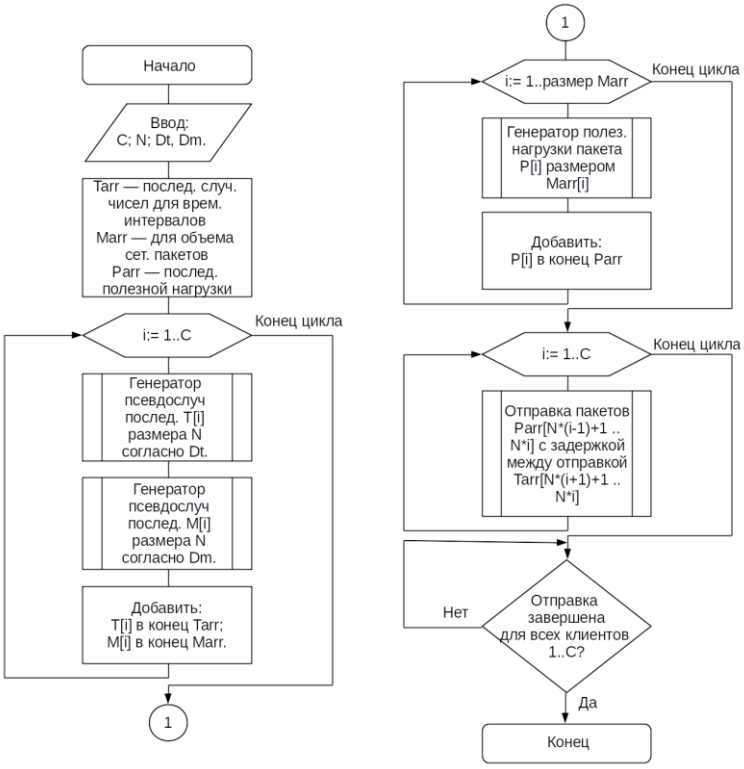


Рис. 46. Алгоритм работы генератора трафика ПИВ

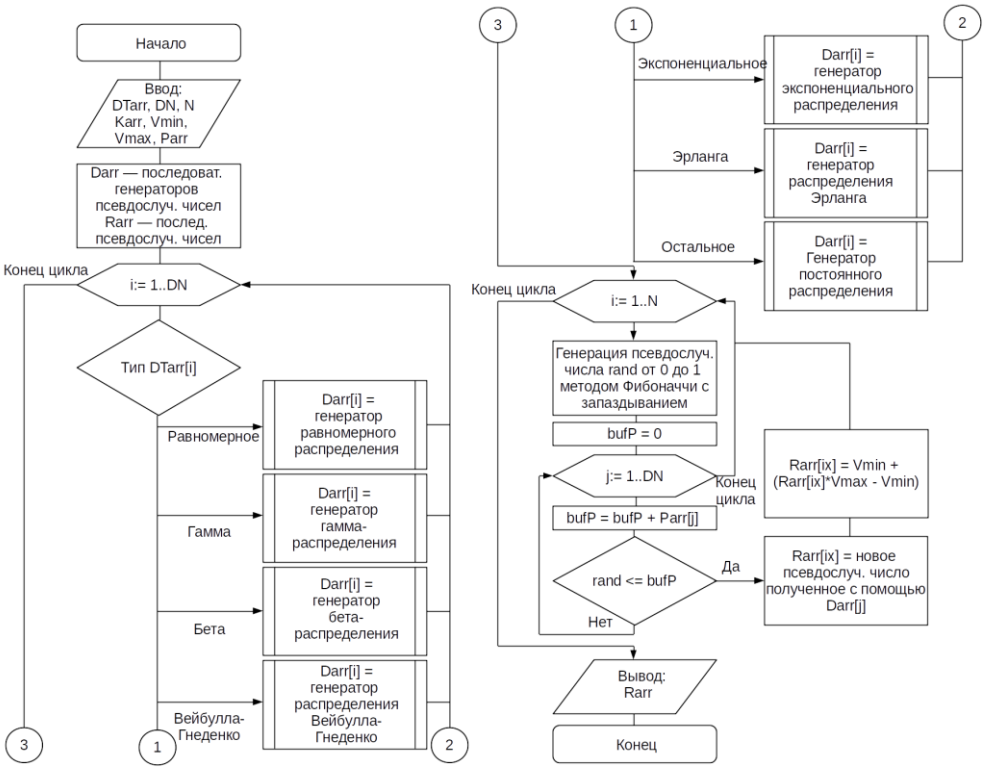


Рис. 47. Алгоритм работы метода генерации псевдослучайных чисел согласно заданным вероятностным распределениям

- *DTarr* — последовательность, содержащая типы вероятностных

распределений, применяемых для генерации трафика;

- *DN* — количество типов вероятностных распределений;
- *Karr* — последовательность коэффициентов для используемых типов вероятностных распределений;
- *Parr* — вероятность попадания псевдослучайного значения в тот или иной тип вероятностного распределения;
- *V*min, *V*max — минимальное и максимальное значение для псевдослучайного числа.

4.5.4. Алгоритмы генерации выборок псевдослучайных чисел

Для генерации выборок псевдослучайных чисел, согласно выбранным законам распределения, был реализован метод генерации псевдослучайных чисел Фибоначчи с запаздыванием [34], с параметрами $\alpha = 55$ и $\beta = 24$:

$$x_i = \begin{cases} x_{i-\alpha} - x_{i-\beta}, \text{при } x_{i-\alpha} \geq x_{i-\beta} \\ x_{i-\alpha} - x_{i-\beta} + 1, \text{при } x_{i-\alpha} < x_{i-\beta} \end{cases}, \quad (50)$$

где x_i — новое псевдослучайное число последовательности псевдослучайных вещественных чисел *x*.

Для генерации псевдослучайных чисел методом Фибоначчи с запаздыванием, при параметрах $\alpha = 55$ и $\beta = 24$, необходимо генерировать начальную последовательность, состоящую из 55 чисел. Данная последовательность создается при помощи встроенного в операционные системы на базе ядра Linux псевдоустройства «/dev/random», генератора случайных последовательностей на основе тепловых шумов, получаемых от драйверов аппаратного обеспечения [25]. С помощью «/dev/random» создается строка, состоящая из 55 символов. Далее каждый из символов переводится в целочисленное положительное значение (от 0 до 255), затем данное значение делится на 255 и получившиеся число (от 0 до 1) записывается в массив положительных вещественных чисел, который и является начальной последовательностью для метода генерации псевдослучайных чисел Фибоначчи

с запаздыванием (рис. 48).

Далее перед началом генерации трафика происходит определение массива, содержащего интервалы между отправкой сообщений. Данные интервалы генерируются с помощью различных методов для генерации псевдослучайных чисел согласно выбранным законам распределения.

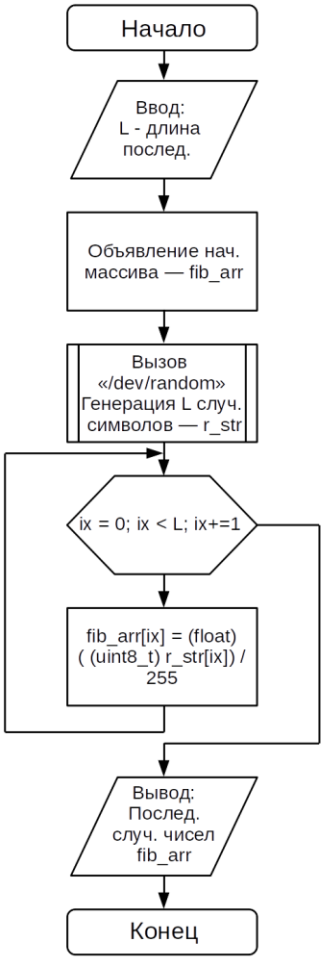


Рис. 48. Алгоритм генерации случайной начальной последовательности чисел

Метод генерации псевдослучайных чисел для гамма-распределения отображен на рисунке 49 [30]. Вначале происходит генерация трех псевдослучайных чисел с помощью метода Фибоначчи с запаздыванием ($rand_1, rand_2, rand_3$), затем происходит вычисление выражений $S_1 = rand_1^{1/a}$, $S_2 = rand_2^{1/(1-a)}$, если выражение $S_1 + S_2 \leq 1$ правдиво, то происходит генерация

случайного интервала времени между отправкой пакетов, согласно выражению $x = \frac{S_1 ln(rand_3)}{\beta(S_1+S_2)}$, где x — новый случайный вещественный интервал. В обратном случае генерация псевдослучайных чисел $(rand_1, rand_2, rand_3)$ и вычисление выражений S_1, S_2повторяется.

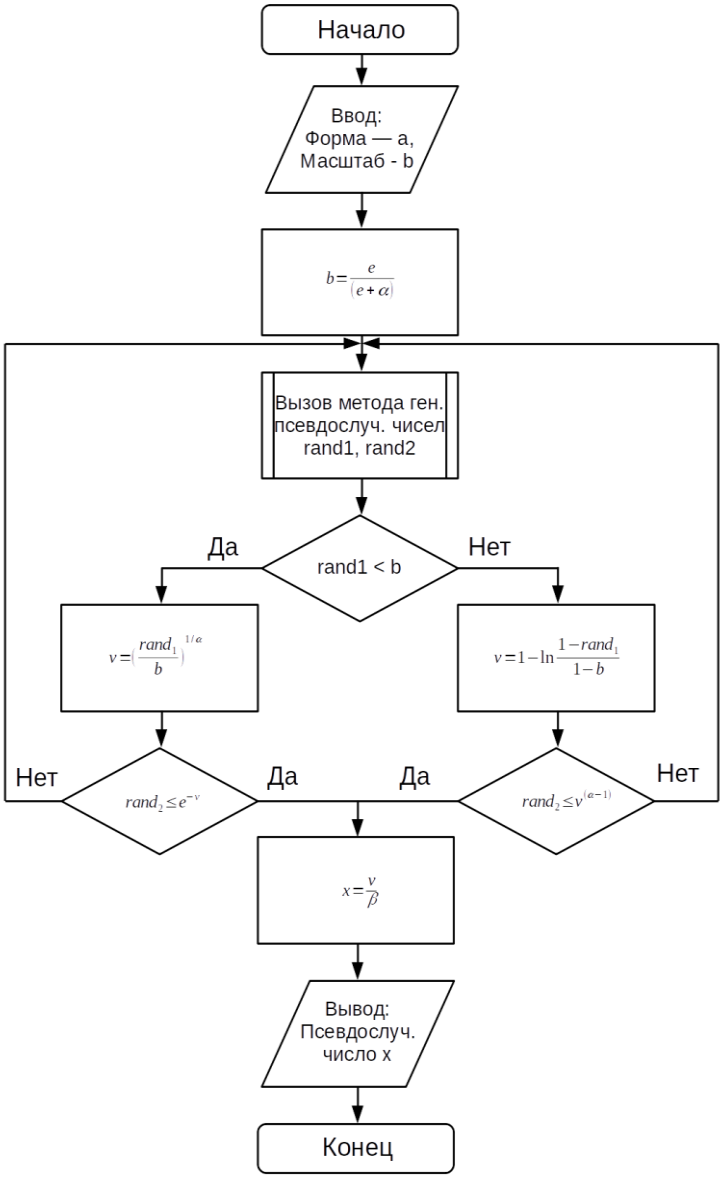


Рис. 49. Алгоритм генерации псевдослучайной величины для гамма-распределения, при условии что $\alpha > 1$

В случаях, когда $\alpha > 1$, происходит расчет выражения $b = \frac{e}{(e+\alpha)}$, затем происходит генерация двух псевдослучайных чисел с помощью метода Фибоначчи с запаздыванием $(rand_1, rand_2)$, затем проверка выражения *rand1* < *b*, если

выражение правдиво, то происходит вычисление выражения

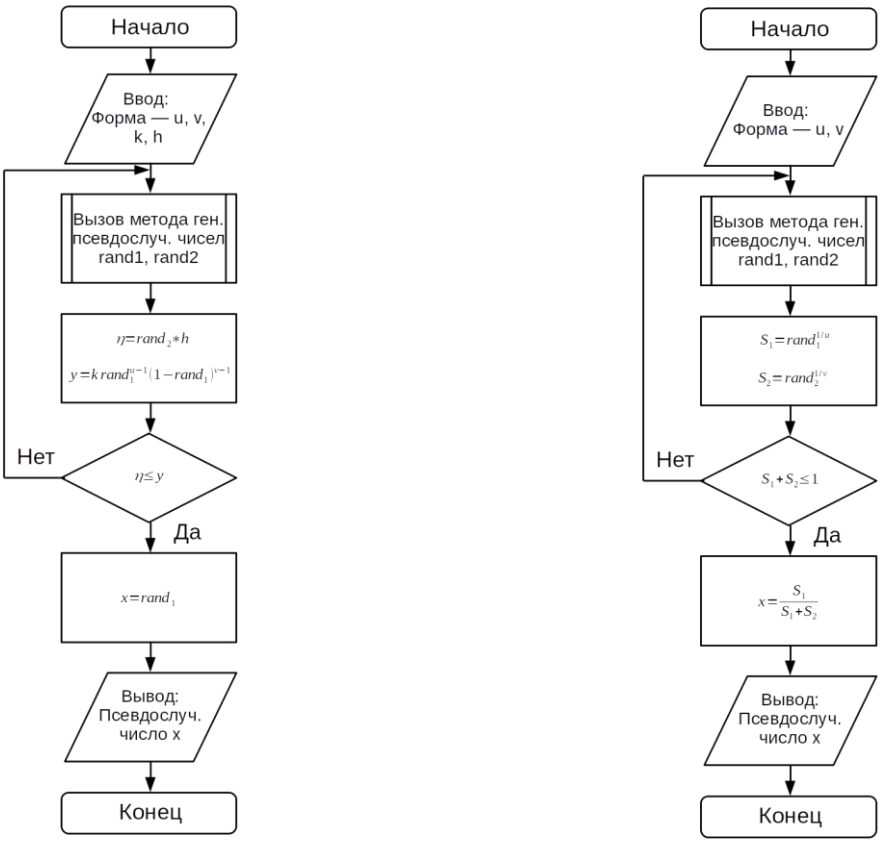
$$v = \left(\frac{rand_1}{b}\right)^{1/\alpha}, \quad (51)$$

если ложно, то

$$v = 1 - ln\frac{1 - rand_1}{1 - b}. \quad (52)$$

После выполнения выражения (51) проводится проверка условия $rand_2 \leq e^{-\beta}$, а после выполнения выражения (52) условия $rand_2 \leq \beta^{(\alpha-1)}$, если любое из условий правдивое, то происходит вычисление псевдослучайного значения $x = \frac{v}{\beta}$, если ложное, то алгоритм повторяется.

Методы генерации псевдослучайных чисел для бета-распределения отображены на рисунке 50 [27].



а) б)

Рис. 50. Алгоритм генерации псевдослучайной величины для бета-распределения: а) при условии $u > 1$ и $v > 1$; б) для остальных случаев

В случае если $u > 1$ и $v > 1$, происходит генерация двух псевдослучайных

чисел с помощью метода Фибоначчи с запаздыванием $(rand_1, rand_2)$, затем происходит вычисление выражений $\eta = rand_2 h,\ y = k rand_1^{u-1}(1 - rand_1)^{v-1}$, если выражение $\eta \le y$ правдиво, то происходит генерация случайного интервала, согласно $x = rand_1$, где x — новый случайный вещественный интервал. В обратном случае генерация псевдослучайных чисел $(rand_1, rand_2)$ и вычисление выражений η, y повторяется. Данный алгоритм отображен на рисунке 49а.

Значения h и k предварительно вычисляются по следующим формулам:

$$k = \frac{\Gamma(u+v)}{\Gamma(u)\Gamma(v)} \text{ и} \tag{53}$$

$$h = \frac{k(u-1)^{u-1}(v-1)^{v-1}}{(u+v-2)^{u+v-2}}. \tag{54}$$

Вначале происходит генерация двух псевдослучайных чисел с помощью метода Фибоначчи с запаздыванием $(rand_1, rand_2)$, затем происходит вычисление выражений $S_1 = rand_1^{1/u}$, $S_2 = rand_2^{1/v}$, если выражение $S_1 + S_2 \le 1$ правдиво, то происходит генерация случайного интервала, согласно $x = \frac{S_1}{S_1+S_2}$, где x — новый случайный вещественный интервал. В обратном случае генерация псевдослучайных чисел $(rand_1, rand_2)$ и вычисление выражений S_1, S_2 повторяется.

Для генерации псевдослучайных чисел для классического двухпараметрического распределения Вейбулла-Гнеденко был выбран следующий метод [27]:

$$x = \beta(-lnrand)^{1/\alpha}, \tag{55}$$

где x — новый случайный вещественный интервал, α — параметр формы, β — параметр масштаба ($\alpha > 0$, $\beta > 0$), а $rand$ — новое псевдослучайное число, полученное с помощью метода Фибоначчи с запаздыванием.

Для генерации псевдослучайных чисел для экспоненциального распределения был выбран следующий метод [27]:

$$x = \frac{-1}{\beta} \ln rand, \tag{56}$$

где x — новый случайный вещественный интервал, β — параметр масштаба

($\beta > 0$), а *rand* — новое псевдослучайное число, полученное с помощью метода Фибоначчи с запаздыванием.

Для генерации псевдослучайных чисел для распределения Парето был выбран следующий метод [27]:

$$x = x_0 rand^{-1/\beta}, \quad (57)$$

где x — новый случайный вещественный интервал, β — параметр масштаба, x_0 — параметр положения, левая граница области возможных значений ($\beta > 0$, $x_0 > 0$), а *rand* — новое псевдослучайное число, полученное с помощью метода Фибоначчи с запаздыванием.

Для генерации псевдослучайных чисел для классического двухпараметрического распределения Эрланга m-го порядка был выбран следующий метод [27]:

$$x = \frac{-1}{\beta} ln(rand_1 * rand_2 *\ldots* rand_m), \quad (58)$$

где x — новый случайный вещественный интервал, m — параметр формы или порядок распределения, целое положительное число, β — параметр масштаба ($m \geq 1$, $\beta > 0$), а ($rand_1, rand_2, rand_m$) — новые псевдослучайные числа, полученные с помощью метода Фибоначчи с запаздыванием.

После генерации псевдослучайных выборок интервалов времени между отправкой пакетов, согласно выбранному методу генерации, производится считывание значений температуры с датчиков, установленных на центральном процессоре (ЦП), в градусах Цельсия и значений загрузки ядер ЦП в МГц. Считывание проводится с помощью псевдоустройств UNIX-подобных операционных систем «/sys/class/thermal/thermal_zone{Номер датчика}/temp» и «/sys/bus/cpu/devices/cpu{Номер ядра}/cpufreq/scaling_cur_freq» [25]. В результате формируется следующее сообщение в формате строки:

```
query?temp [0]={Значение}&… &temp [n]={Значение}&cpufr
[0]={Значение}&...&cpufr [m]={Значение},
```

где n — количество датчиков температуры, а m — количество ядер

центрального процессора.

Далее сообщение с помощью прикладного протокола CoAP [13], используемого в промышленном Интернете вещей, отправляется на удаленный сервер CoAP. Для реализации клиентской и серверной составляющей программного обеспечения используется библиотека libcoap.

На рисунке 51 изображена диаграмма классов UML [14] для разработанного программного обеспечения для генерации трафика промышленного Интернета вещей.

Данное ПО включает в себя четыре класса:

- main — основной класс программы, который отвечает за управление работой приложения;
- distr_calc — класс, отвечающий за генерацию псевдослучайных чисел, согласно исследуемым законам распределения;
- standalone_func — класс, объединяющий различные функции, не включенные ни в один из остальных классов;
- coap_sender — класс, отвечающий за отправку сообщений.

На базе разработанного программного обеспечения был разработан программно-аппаратный комплекс [58], состоящий из клиентского и серверного вычислительных устройств, представляющих собой персональные компьютеры, с предустановленной операционной системой Debian 9 на базе ядра Linux 4.9.0-8-amd64 (клиент и сервер). Клиент имеет предустановленное, описанное ранее программное обеспечение — генератор трафика ПИВ, написанный на языке C/C++. На сервере функционирует сервер CoAP, приложение для перехвата трафика tcpdump.

Разработанное ПО было включено в ранее разработанную модельную сеть в качестве источника трафика. Далее было проведено тестирование модельной сети, с применением разработанного ПО. Данное программное обеспечение генерирует поток сетевых пакетов, имитируя работу одного или более ранее исследованных источников трафика. В качестве исходных моделей для

имитации трафика ПИВ были выбраны аналитические модели интенсивности поступления трафика на сетевой интерфейс, которые были ранее определены в главе 2, таблицах 1–6.

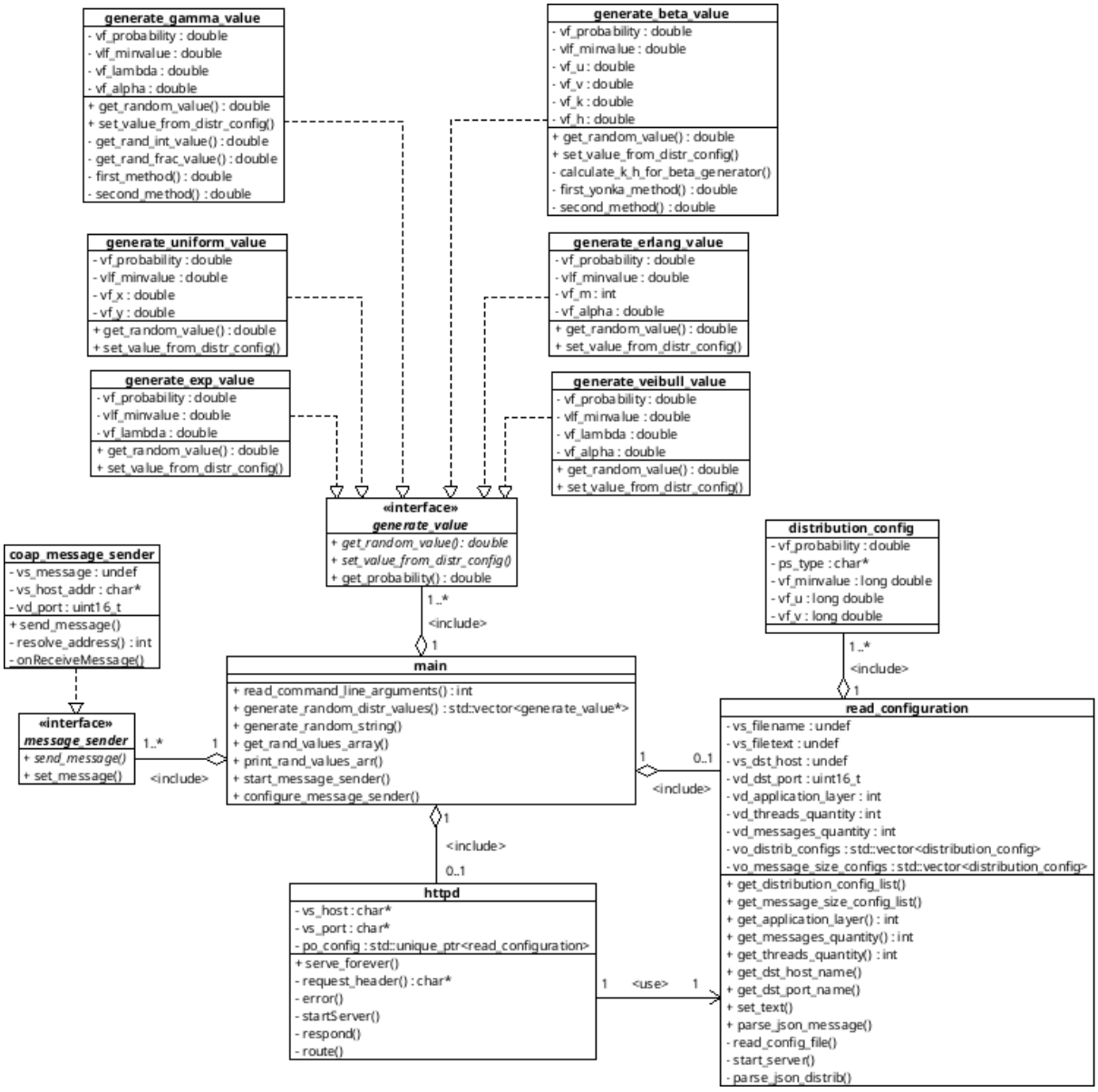


Рис. 51. Диаграмма классов UML, описывающая структуру генератора трафика ПИВ

4.5.5. Анализ результатов тестирования генератора трафика

Далее на базе разработанной модельной сети для тестирования работы генератора трафика ПИВ было проведено испытание корректности его работы. Для

тестирования генератору задавалось время между поступлениями сетевых пакетов с помощью вероятностных распределений для различных видов трафика ПИВ, которые были указаны в главе 2, таблице 1. Далее генерируемый трафик перехватывался и было проведено исследование интенсивности поступления сетевых пакетов. Результаты данного исследования были аппроксимированы, с помощью метода наименьших квадратов и оптимизационного алгоритма обобщенного приведенного градиента, а затем были сопоставлены с исходными вероятностными распределениями, с помощью критерия согласия Колмогорова-Смирнова. Также в ходе исследования интервалов времени между поступлением сетевых пакетов было получено среднее значение интенсивности поступления пакетов для экспериментальных данных и данных, полученных на основе аналитической модели.

Результаты проведенного сравнения при выбранном уровне доверительной вероятности 95 % указаны в таблице 13.

Таблица 13. Результаты сравнения исходной и экспериментальной интенсивности поступления сетевых пакетов

Промышленная система	Исходное распределение	Вероятность попадания в распределение	Ср. значение интенсивности поступления пакетов, мс		Критерий согласия Колмогорова
			Экспериментальное (эксп.)	Мат. модель (мат.)	
Trumpf TruPrint 4500	Бета (α = 36 681,97; β = 670 238,20)	43,70	139,29 ± 5,43	138,98 ± 5,45	0,21 < 1,36
	Бета (α = 7081,16; β = 19 719,89)	44,32			
3D Systems ProJet	Бета (α = 15 012,99; β = 276 073,23)	49,93	156,84 ± 8,26	156,48 ± 8,13	0,40 < 1,36
	Бета (α = 13 629,12; β = 38 227,91)	49,89			
Система OBS	Экспоненциальное (λ = 189,21)	99,92	5,55 ± 0,10	5,34 ± 0,10	0,07 < 1,36
Система Ivideon	Экспоненциальное (λ = 311,76)	99,99	3,42 ± 0,05	3,23 ± 0,05	0,09 < 1,36

Продолжение таблицы 13

Промышленная система	Исходное распределение	Вероятность попадания в распределение	Ср. значение интенсивности поступления пакетов, мс		Критерий согласия Колмогорова
			Экспериментальное (эксп.)	Мат. модель (мат.)	
«1С-Битрикс»	Экспоненциальное ($\lambda = 47{,}33$)	72,07	46,00 ± 3,27	47,18 ± 3,19	0,12 < 1,36
	Гамма ($\alpha = 0{,}88$; $\lambda = 9{,}25$)	25,98			
Веб-приложение OWM	Экспоненциальное ($\lambda = 2059{,}22$)	99,02	0,51 ± 0,01	0,48 ± 0,01	0,06 < 1,36
Веб-приложение OSM	Экспоненциальное ($\lambda = 2188{,}52$)	99,09	0,47 ± 0,01	0,45 ± 0,01	0,03 <1,36
Nanotron nanopan 5375	Эрланга ($m = 3$; $\lambda = 40$)	99,30	69,44 ± 0,23	73,45 ± 0,22	0,02 <1,36

На рисунках 52–53 представлены сравнения аппроксимированных экспериментальных распределений и исходных распределений, выбранных для описания характера трафика различных систем ПИВ.

На основании результатов тестирования разработанного алгоритма можно сделать вывод, что интервалы времени между поступлением сообщений для генерируемого трафика имеют высокую степень приближения к интервалам времени, соответствующим исходным аналитическим моделям.

Тем не менее, при значениях интенсивности поступления сетевых пакетов менее 1000 мкс возникают проблемы, связанные с программными задержками отправки сетевых пакетов. Данная проблема связана с особенностями разработанного ПО и может быть решена путем оптимизации работы модуля программы, отвечающего за отправку сетевых пакетов.

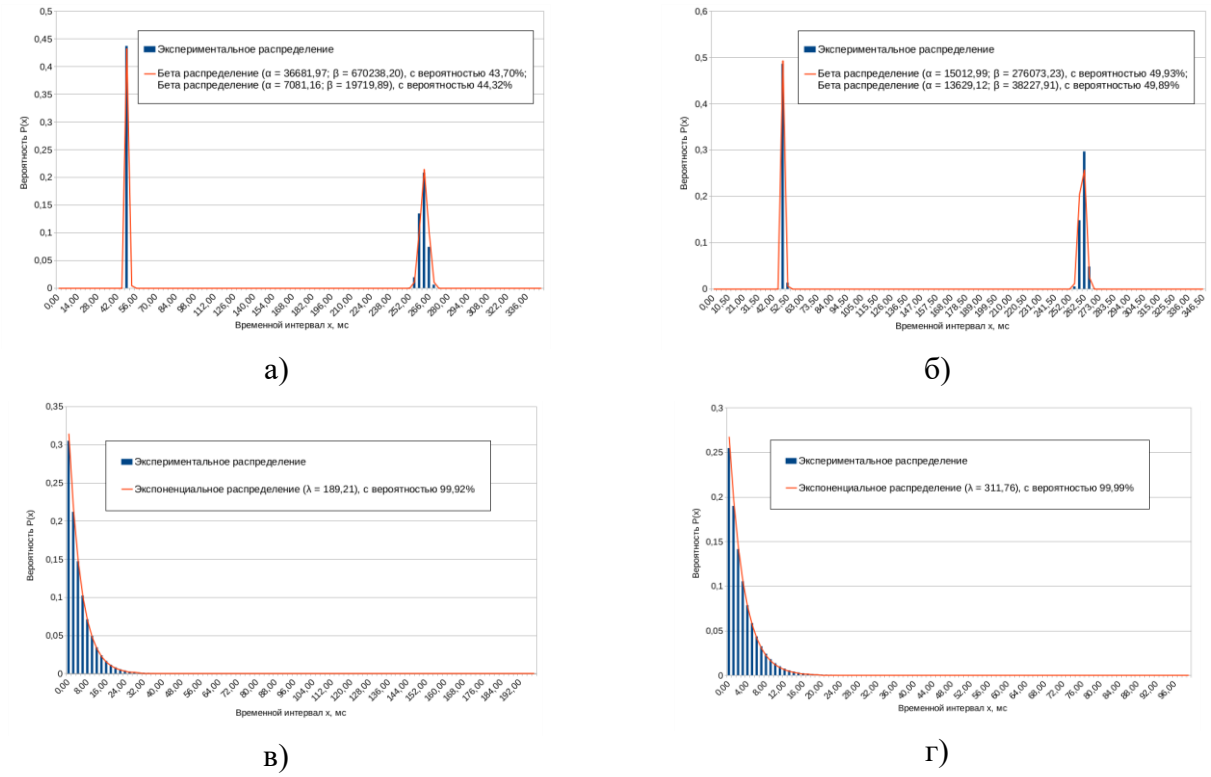


Рис. 52. Сравнение исходных аналитических моделей и экспериментальных данных для: а) Trumpf TruPrint 4500; б) 3D Systems ProJet; в) Система OBS; г) Система Ivideon

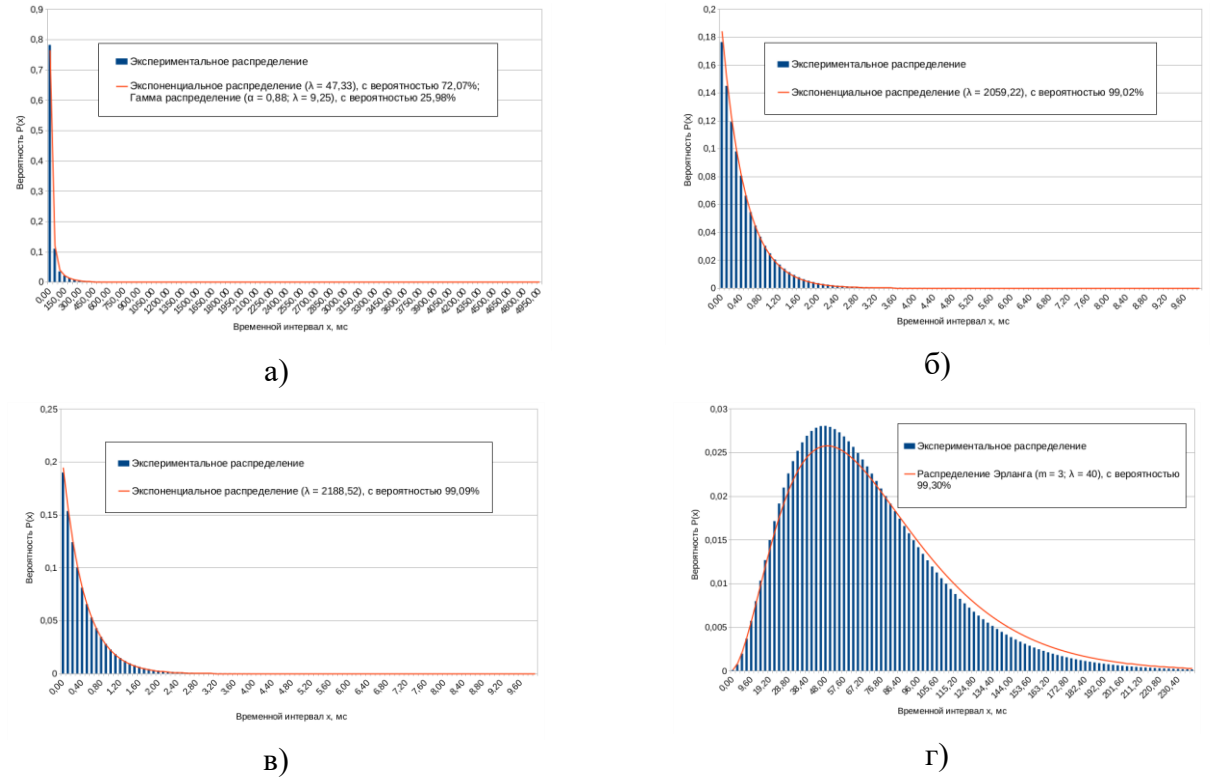


Рис. 53. Сравнение исходных аналитических моделей и экспериментальных данных для: а) «1С-Битрикс»; б) веб-приложения OWM; в) веб-приложения OSM; г) Nanotron nanopan 5375

Разработанный алгоритм может быть использован для имитации потока сетевых пакетов от исследованных на базе разработанной модельной сети типов источников трафика ПИВ.

Выводы по главе 4

1. На базе существующих методов тестирования сетевого оборудования разработана комплексная методика тестирования систем ПИВ, включающая в себя различные виды тестирования производительности и надежности работы следующих трех элементов систем ПИВ: семантического гетерогенного шлюза, граничного и облачного серверов.

2. Разработан метод удаленного тестирования, который может использоваться для тестирования удаленных сегментов систем ПИВ.

3. Разработан генератор трафика и модельная сеть для его тестирования, которые могут использоваться для испытания устойчивости существующей сетевой инфраструктуры к трафику ПИВ по разработанной методике тестирования.

4. На базе разработанной модельной сети проведено тестирование работы генератора трафика ПИВ на основе вероятностных распределений, полученных ранее в главе 2. Аппроксимированные аналитические функции, полученные при анализе сетевых пакетов, создаваемых генератором трафика, показали высокую степень сходимости с исходными аналитическими моделями, согласно критерию согласия Колмогорова-Смирнова.

ЗАКЛЮЧЕНИЕ

В ходе данной диссертационной работы решены следующие задачи:

1. Проведено исследование концепции промышленного Интернета вещей и перспектив ее развития.

2. Разработана классификация сфер автоматизации для промышленных предприятий, в рамках внедрения систем промышленного Интернета вещей.

3. Проведен обзор существующих на данный момент международных стандартов в области ПИВ по архитектуре систем ПИВ, рассмотрены подходы к их реализации.

4. Исследованы существующие решения, реализующие функции гетерогенного шлюза в рамках сетевой инфраструктуры промышленных предприятий.

5. Разработана классификация трафика ПИВ по источникам трафика, сценарию взаимодействия и качеству обслуживания.

6. На основе полученной классификации трафика ПИВ разработана модельная сеть, имитирующая работу фрагмента сети ПИВ и включающая в себя реальные системы, используемые в сфере промышленной автоматизации.

7. На базе разработанной модельной сети и классификации трафика ПИВ проведен анализ различных типов трафика ПИВ. В ходе анализа были получены аналитические модели интенсивности поступления и обслуживания трафика, модель распределения размера сетевых пакетов, а также значения коэффициента самоподобия (Хёрста) для каждого из ранее определенных видов источников трафика ПИВ.

8. Произведена оценка интенсивности поступления сетевых пакетов и значения коэффициента Хёрста для агрегированного трафика и была доказана гипотеза о его самоподобном характере.

9. На базе полученных аналитических данных была разработана

имитационная модель, описывающая работу фрагмента сети ПИВ, с помощью которой была произведена оценка минимально приемлемой пропускной способности для выбранного фрагмента сети промышленного Интернета вещей и была подтверждена гипотеза о возможности применения оценки потери пакетов В. В. Липаева и С. Ф. Яшкова в модели G/G/1/n для сетей промышленного Интернета вещей.

10. Разработаны структуры гетерогенного и семантического шлюза ПИВ, позволяющие обеспечить совместимость различных сетевых технологий ПИВ между собой.

11. Разработан промежуточный формат для взаимного преобразования протоколов ПИВ между собой на основе форматов полезных данных существующих сетевых протоколов.

12. Получены аналитические модели по времени преобразования форматов полезных данных XML, JSON, CSV и прикладных протоколов CoAP, MQTT, Modbus TCP, STOMP, OPC UA, HTTP между собой.

13. На базе полученных аналитических моделей разработана имитационная модель семантического шлюза ПИВ и на ее основе были испытаны свойства семантического гетерогенного шлюза ПИВ во время его работы при разной интенсивности поступления пакетов.

15. Для оценки производительности разработанной модели семантического шлюза проведено сопоставление моделей семантического гетерогенного шлюза ПИВ и шлюза, основанного на методе инкапсуляции полезных данных, где семантический шлюз ПИВ показал более высокий уровень производительности для системы, состоящей из шлюза и оконечного устройства.

16. На базе существующих методов тестирования сетевого оборудования разработана комплексная методика тестирования систем ПИВ, включающая в себя различные виды тестирования производительности и надежности работы следующих трех элементов систем ПИВ: семантического гетерогенного шлюза, граничного и облачного серверов.

17. Разработан метод удаленного тестирования, который может использоваться для тестирования удаленных сегментов систем ПИВ.

18. Разработан генератор трафика и модельная сеть для его тестирования, которые могут использоваться для испытания устойчивости существующей сетевой инфраструктуры к трафику ПИВ по разработанной методике тестирования.

19. На базе разработанной модельной сети проведено тестирование работы генератора трафика ПИВ на основе вероятностных распределений, полученных ранее в главе 2. Аппроксимированные аналитические функции, полученные при анализе сетевых пакетов, создаваемых генератором трафика, показали высокую степень сходимости с исходными аналитическими моделями, согласно критерию согласия Колмогорова-Смирнова.

В диссертационной работе получены следующие научные результаты, которые могут быть использованы для внедрения в сетевую инфраструктуру промышленных предприятий:

1. Разработана классификация источников трафика промышленного Интернета вещей, которая может быть использована для исследования свойств трафика ПИВ.

2. Получены аналитические модели характеристик интенсивностей поступления и обслуживания сетевых пакетов, распределения размеров сетевых пакетов, распределения времени сетевых задержек для каждого из полученных источников трафика ПИВ. Данные модели могут быть использованы для имитации потока сетевых пакетов от заданных источников трафика при тестировании производительности сетевой инфраструктуры при воздействии трафиком ПИВ.

3. Разработана имитационная модели фрагмента сети промышленного Интернета вещей, которая включает в себя все определенные в классификации источники трафика и позволяет оценить минимально допустимый уровень пропускной способности каналов связи в локальной сети. Данная модель может быть использована для проектирования сетевой инфраструктуры при внедрении систем ПИВ.

4. В ходе исследования агрегированного потока сетевых пакетов от различных видов источников трафика ПИВ определено, что трафик ПИВ имеет самоподобный характер и может быть описан с помощью модели G/G/1/*n*, по классификации Кендалла-Башарина.

5. Разработан метод построения семантического гетерогенного шлюза промышленного Интернета вещей, который может использоваться для преобразования прикладных протоколов и форматов полезных данных между собой. Семантический гетерогенный шлюз может быть использован для решения задач совместимости на прикладном и семантическом (формата полезных данных) уровне.

6. Разработана методика комплексного тестирования систем промышленного Интернета вещей, позволяющая провести комплексное тестирование следующих элементов систем ПИВ: семантического гетерогенного шлюза, облачного и граничного серверов ПИВ. Данная методика может быть использована для проведения тестирования производительности существующей сетевой инфраструктуры при воздействии трафиком ПИВ.

Перспективное направление дальнейших исследований может быть связано с разработкой программно-аппаратного комплекса для проведения комплексного тестирования, согласно полученной методике тестирования.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ИВ	Интернет вещей.
ПИВ	промышленный Интернет вещей.
МСЭ-Т	Международный союз электросвязи — сектор стандартизации электросвязи.
ГОСТ	межгосударственный стандарт.
ССОП	сети связи общего пользования.
БДРВ	базы данных реального времени.
СУБД	системы управления базами данных.
БД	база данных.
ПС	промышленная система.
СКРП	система контроля работы предприятия.
СП	система позиционирования.
ПАК	программно-аппаратный комплекс.
ПО	программное обеспечение.
МИПД	метод инкапсуляции полезных данных.
ОУ	оконечный узел.
СШ	семантический шлюз.
ПС	пропускная способность.
ГС	граничный сервер.
ОС	облачный сервер.
ГТ	генератор трафика.
ЦП	центральный процессор.
ITU-T	International Telecommunication Union — Telecommunication

	sector.
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission.
IIC	Industrial Internet Consortium.
IP	Internet protocol.
QoS	Quality of service.
SCADA	Supervisory control and data acquisition.
ISDN	Integrated Services Digital Network.
CC	Cloud computing.
EC	Edge computing.
OSI	Open Systems Interconnection.
IICF	Industrial Internet of Things Conversion Format.
HIIG	Heterogeneous Industrial Internet of Things Gateway.
URI	Uniform Resource Identifier.
DUT	Device under testing.
NAT	Network address translation.
STUN	Session traversal utilities for NAT.
TURN	Traversal using relay NAT.

СПИСОК ЛИТЕРАТУРЫ

[1] ISO/IEC/IEEE 29119-1:2013. Software and systems engineering — Software testing — Part 1: Concepts and definitions. — Введ. 2013-09-01. — M.: ISO/IEC JTC 1/SC 7. — 2013. — 90 c.

[2] ISO/IEC 30162. Internet of Things (IoT) — Compatibility requirements and model for devices within industrial IoT systems. — M.: ISO/IEC JTC 1/SC 41. — 2018.

[3] Lin, S.-W. Industrial Internet of Things. Volume G1: Reference Architecture / S.-W. Lin, B. Miller, J. Durand, G. Bleakley, A. Chigani, R. Martin et al. — Industrial Internet Consortium. — 2017.

[4] Joshi, R. The Industrial Internet of Things. Volume G5: Connectivity Framework / R. Joshi, P. Didier, J. Jimenez, T. Carey et al. — Industrial Internet Consortium. — 2017.

[5] Anderson, N. The Industrial Internet of Things. Volume T3: Analytics Framework / N. Anderson, W. W. Diab, T. French, K. E. Harper, S.-W. Lin, D. Nair, W. Sobel et al. — Industrial Internet Consortium. — 2017.

[6] IETF Draft Recommendation. Encapsulation of TCP and other Transport Protocols over UDP. — M.: IETF Network Working Group, — 2013.

[7] IETF RFC 3031. Multiprotocol Label Switching Architecture. — M.: IETF Network Working Group, — Введ. 2001-01. — 2001.

[8] IETF RFC 2544. Benchmarking Methodology for Network Interconnect Devices. — M.: IETF Network Working Group. — Введ. 1999-03. — 1999.

[9] IETF RFC 1242. Benchmarking Terminology for Network Interconnection Devices. — M.: IETF Network Working Group. — Введ. 1991-07. — 1991.

[10] IETF RFC 2663. IP Network Address Translator (NAT) Terminology and Considerations. — Введ. 1999-08. — M.: IETF Network Working Group, — 1999.

[11] IETF RFC 5389 Session Traversal Utilities for NAT (STUN). — Введ. 2008-10. — M.: IETF Network Working Group. — 2008.

[12] IETF RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). — Введ. 2010-04. — М.: IETF Network Working Group. — 2010.

[13] IETF RFC 7252. The Constrained Application Protocol (CoAP). — Введ. 2014-06. — М.: IETF Network Working Group, — 2014.

[14] OMG Unified Modeling Language (UML). Version 2.5.1. — Введ. 2017-12. — М.:OMG, — 2017.

[15] OpenFog Reference Architecture for Fog Computing. OpenFog Consortium. — 2017. — P. 162.

[16] МСЭ-Т Y.4003. Overview of smart manufacturing in the context of the industrial Internet of things. — Введ. 2018-06-29. — М.: МСЭ-Т, — 2018. — 26 с.

[17] МСЭ-Т Q.4060 The structure of the testing of heterogeneous Internet of things gateways in a laboratory environment. — Введ. 2018-10-14. — М.: МСЭ-Т, — 2018. — 16 с.

[18] МСЭ-Т Y.1564 Ethernet service activation test methodology. — Введ. 2016-02-29. — М.: МСЭ-Т. — 2016. — 38 с.

[19] МСЭ-Т Q.3056 Signalling procedures of the probes to be used for remote testing of network parameters. — Введ. 2019-12-14. — М.: МСЭ-Т. — 2019.

[20] МСЭ-Т Y.4101/Y.2067. Общие требования и возможности шлюза для приложений интернета вещей. — Введ. 2017-10-29. — М.: МСЭ-Т, — 2017. — 26 с.

[21] МСЭ-Т Y.4000/Y.2060. Обзор Интернета вещей. — Введ. 2012-06-15. — М.: МСЭ-Т, 2012. — 22 с.

[22] МСЭ-Т Q.3900. Методы тестирования и архитектура модельных сетей для тестирования технических средств СПП, используемых в сетях электросвязи общего пользования. — Введ. 2006-09-29. — М.: МСЭ-Т, — 2006. — 29 с.

[23] ГОСТ Р 56920-2016. Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения. — Введ. 2017-06-01. — М.: ТК 22, — 2017. — 93 с.

[24] Афонцев, Э. В. О выборе размера буфера маршрутизатора компьютерной сети, нагруженного интенсивным трафиком реального времени /Э. В. Афонцев, М. К. Гребенкин, С. В. Поршнев // Известия Томского политехнического университета. — 2008. — Т. 313. — № 5. — 183 с. — С. 106–109.

[25] Баррет, Д. Дж. Карманный путеводитель по Linux / Д. Дж. Баррет // Пер. с англ. — М.: Кудиц-Образ, — 2007. — 288 с.

[26] Боровиков, И. М. Показатель Хёрста: способы, расчеты и возможности использования в задачах портфельного инвестирования / И. М. Боровиков, Т. В. Куликова, В. И. Тинякова // Современная экономика: проблемы и решения. — № 10 (22). — 2011. — 181 с. — С. 125–143.

[27] Вадзинский, Р. Н. Справочник по вероятностным распределениям / Р. Н. Вадзинский. — СПб.: Наука, — 2001. — 295 с.

[28] Выборнова, А. И. Методы определения степени самоподобия и долговременной зависимости трафика /А. И. Выборнова, А. Е. Кучерявый / Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сборник научных статей (АПИНО 2014). — 2014. — 1291 с. — С. 230–235.

[29] Гойхман, В. Ю. Протоколы Интернета вещей / В. Ю. Гойхман, А. А Савельева // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей V Международной научно-технической и научно-методической конференции. — Т. 1. — 2016. — 601 с. — С. 329–334.

[30] Емельянов, А. А. Лаг-генераторы для моделирования рисковых ситуаций в системе Actor Pilgrim / А. А. Емельянов // Прикладная информатика. — 2011. — № 5 (35). — С. 98–117.

[31] Зайкин, И. С. Основы разработки баз данных реального времени / И. С. Зайкин, В. Г. Корхов // Молодой ученый. — № 23 (103). — 2015. — 1137 с. — С. 143–146.

[32] Зелигер, Н. Б. Проектирование сетей и систем передачи дискретных сообщений: учебное пособие электротехн. ин-тов связи спец. /Н. Б. Зелигер, О. С. Чугреев, Г. Г. Яновский. — М.: Радио и связь, — 1984. — 175 с.: ил.; 21 см.

[33] Ионин, Г. Л. Статистическое моделирование систем телетрафика / Г. Л. Ионин, Я. Я. Седол. — М.: Радио и связь, — 1982. — 184 с.

[34] Кормен, Т. Алгоритмы: построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест // Пер. с англ. под ред. А. Шеня. — М.: МЦНМО. — 2002. — 960 с. — 263 ил.

[35] Карташевский, В. Г. Основы теории массового обслуживания: учебник для вузов /В. Г. Карташевский. — М.: Горячая линия — Телеком, — 2013. — 130 с. — ISBN 978-5-9912-0346-3.

[36] Киричек, Р. В. Модельные сети для Интернета вещей и программируемых сетей / Р. В. Киричек, А. Г. Владыко, М. В. Захаров, А. Е. Кучерявый // Информационные технологии и телекоммуникации. — 2015. — № 3 (11). — С. 17–26.

[37] Климов, Г. П. Теория вероятностей и математическая статистика / Г П. Климов. — М.: МГУ, — 2011. — 368 с.

[38] Климов, Г. П. Теория массового обслуживания /Г. П. Климов — М.:МГУ, — 2011. — 312 с. — ISBN 978-5-211-05827-9.

[39] Колмогоров, А. Н. К вопросу о пригодности найденных статистическим путем формул прогноза / А. Н. Колмогоров // Журнал геофизики. — 1933. — Т. 3. — № 1. — СС. 78–82.

[40] Кулик, В. А. Исследование и генерация трафика Промышленного Интернета Вещей / В. А. Кулик, Р. В. Киричёк // Труды учебных заведений связи. — Т. 5. — № 3. — 2019. 109 с. — С. 27-36. — DOI: 10.31854/1813-324X-2019-5-3-27-36.

[41] Кулик, В. А. Классификация и исследование трафика Промышленного Интернета Вещей на модельной сети / В. А. Кулик, Р. В. Киричёк, А. И. Парамонов // Электросвязь. — № 8. — 2019. — 76 с. С. 22-28.

[42] Кулик, В.А. Модель семантического преобразования пакетов для гетерогенного шлюза промышленного Интернета вещей / В. А. Кулик, С. А. Вахитов, Р. В. Киричёк // Электросвязь. — № 3. — 2020. — 68 с. — С. 49-54.

[43] Кулик, В. А. Программно-аппаратный комплекс для тестирования качества услуг связи на базе Рекомендации МСЭ-Т Q.3960 / О. А. Губская, Е. А. Алисевич, В. А. Кулик, Р. В. Киричек, А. С. Бородин // Электросвязь. — № 8. — 2017. — 68 с. — С. 25-32.

[44] Кулик, В. А. Программа имитационного моделирования самоконфигурируемой сети связи, навигации и передачи данных / Е. Г. Борисов, Р. В. Киричек, А. И. Парамонов, А. Г. Владыко, В. А. Кулик // свидетельство о регистрации программы для ЭВМ RUS 2016617039. Рег. — 2016-04-26.

[45] Кулик, В. А. Анализ производительности шлюза умного дома на базе облачной платформы AllJoyn / А. А. Хакимов, А. С. Мутханна, В. А. Кулик, Р. В. Киричек // Информационные технологии и телекоммуникации. — 2016. — Т. 4. — № 2. — С. 77-85.

[46] Кулик, В. А. Исследование взаимодействия приложений дополненной реальности с облачными сервисами 1С / М. А. Маколкина, Д. В. Окунева, В. А. Кулик, В. А. Тельтевская, А. С. Щербак, Р. В. Киричек // Электросвязь. — № 12. — 2017. — 108 с. — С. 49-53.

[47] Кулик, В. А. Разработка и исследование моделей семантической совместимости различных платформ и услуг Интернета вещей / Н. П. Слепцова, В. А. Кулик // В сборнике: актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) сборник научных статей VIII международной научно-технической и научно-

методической конференции. В 4-х томах. Под. редакцией С.В. Бачевского. — Т. 1. — 2019. — 834 с. — С. 641-645.

[48] Кулик, В. А. Основные типы платформ промышленного Интернета вещей / Л. А. Власенко, В. А. Кулик, Р. В. Киричек // В сборнике: интернет вещей и 5G (INTHITEN 2017) 3-я международная научно-техническая конференция студентов, аспирантов и молодых ученых. Под редакцией А. Е. Кучерявого. — 2017. — 150 с. — С. 171-175.

[49] Кулик, В. А. Обзор гетерогенных и семантических шлюзов Интернета вещей / Л. А. Власенко, В. А. Кулик, Р. В. Киричек // информационные технологии и телекоммуникации. — Т. 5. — 2017. — № 3. — С. 30-37.

[50] Кулик, В. А. Шлюз для подключения и управления IoT-устройствами на базе WiFi-модуля NodeMCU / В. Д. Фам, В. А. Кулик, Р. В. Киричек // В сборнике: Интернет вещей и 5G (INTHITEN 2016) 2-я международная научно-техническая конференция студентов, аспирантов и молодых ученых "Интернет вещей и 5G". — 2016. — 79 с. — С. 26-30.

[51] Кулик, В. А. Разработка требований к тестированию гетерогенных шлюзов интернета вещей / В. А. Кулик, Р. В. Киричек // В сборнике: молодежная научная школа по прикладной теории вероятностей и телекоммуникационным технологиям (АРТСТ-2017) материалы молодежной научной школы. Российский университет дружбы народов; под общей редакцией К. Е. Самуйлова, Е. А. Кучерявого, А. Н. Дудина. — 2017. — 331 с. — С. 146-149.

[52] Кулик, В. А. Исследование производительности программных инструментов межсетевого взаимодействия для семантических шлюзов Интернета вещей / Л. А. Власенко, В. Д. Фам, В. А. Кулик, Р. В. Киричек // Информационные технологии и телекоммуникации. — Т. 5. — 2017. — № 1. — С. 44-53.

[53] Кулик, В. А. Требования к производительности семантических шлюзов для различных услуг в гетерогенных сетях / Л. А. Власенко, В. А. Кулик, Р. В.

Киричек // В сборнике: 72-я всероссийская научно-техническая конференция, посвященная дню радио труды конференции. — 2017. — 560 с. — С. 215-217.

[54] Кулик, В. А. Протокол тестирования качества услуг связи на базе Рекомендации МСЭ-Т Q.3960 / В. А. Кулик, Р. В. Киричек // в сборнике: интернет вещей и 5G (INTHITEN 2017) 3-я международная научно-техническая конференция студентов, аспирантов и молодых ученых. Под редакцией А. Е. Кучерявого. — 2017. — 150 с. — С. 151-158.

[55] Кулик, В. А. Методы комплексного тестирования устройств Интернета вещей / В. А. Кулик, А. И. Выборнова // В сборнике: распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2016). — Т. 3. — 2016. — 499 с. — С. 305-312.

[56] Кулик, В. А. Программно-аппаратный комплекс для тестирования устройств Интернета вещей / В. А. Кулик, Р. В. Киричек, А. Е. Кучерявый // Информационные технологии и телекоммуникации. — 2015. — № 4(12). — С. 67-76.

[57] Кулик, В.А. Влияние трафика Интернета вещей на работу сетевого оборудования / А. А. Серебрякова, В. Д. Фам, В. А. Кулик, Р. В. Киричек // В сборнике: Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2016). — Т. 1. — 2016. — 499 с. — С. 388-393.

[58] Кулик, В. А. Генератор трафика промышленного Интернета вещей // Облачная система контроля версий Bitbucket. — URL: https://bitbucket.org/vslavk/generate_iiot_traffic/src/master (дата обращения 20.12.2019).

[59] Кулик, В. А. Программа для расчета коэффициента Хёрста // Облачная система контроля версий Bitbucket. — URL: https://bitbucket.org/vslavk/lua-hurst/src/master/ (дата обращения 23.12.2019).

[60] Кулик, В. А. Имитационная модель работы семантического шлюза промышленного Интернета вещей // Облачная система контроля версий

Bitbucket. — URL: https://bitbucket.org/vslavk/ciw_iiot_sem_gateway_model/src/master/ (дата обращения 23.12.2019).

[61] Кучерявый, А. Е. Интернет вещей / А. Е. Кучерявый //Электросвязь. — 2013. — № 1. — С. 21–24.

[62] Кучерявый, А. Е. Перспективы научных исследований в области сетей связи на 2017–2020 годы / А. Е. Кучерявый, А. Г. Владыко, Р. В. Киричек и др. // Информационные технологии и телекоммуникации. — Т. 4. — № 3. — 2016. — 106 с. — С. 1–14.

[63] Кучерявый, А. Е. Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый. — М.: СПб.: Любавич, — 2011. — 312 с.

[64] Мутханна, А. С. Сравнение протоколов Web-вещей / А. С. Мутханна, А. А. Хакимов // Информационные технологии и телекоммуникации. — Т. 3. — № 4. — 2015. — 119 с. — С. 97–107.

[65] Нургалина, Р. Г. Разработка системы принятия решений / Р. Г. Нургалина, Е. А. Ильина // Актуальные проблемы современной науки, техники и образования. — Т. 2. — № 71. — 2013. — 354 с. — С. 82–86.

[66] Парамонов, А. И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования: автореф. дис.... док. техн. наук: 05.12.13 / А. И. Парамонов. — М., — 2014. — 22 с.

[67] Попов, А. С. Определение оптимального размера буфера маршрутизатора мультисервисной телекоммуникационной сети /А. С. Попов, С. С. Попов, А. С. Корсунский, Т. Н. Масленникова // Автоматизация процессов управления. — 2015. — Т. 313. — № 2 (40). — 128 с. — С. 50–54.

[68] Рушкин, Е. И. Анализ применения протокола Modbus для управления электроприводом на горных предприятиях / Е. И. Рушкин, А. С. Семенов, П. В. Саввинов // Фундаментальные исследования. — № 11–12. — 2014. — 2772 с. — С. 2615–2619.

[69] Селезнев, С. П. Архитектура промышленных приложений IoT и протоколы AMQT, MQTT, JMS, REST, CoAP, XMPP, DDS / С. П. Селезнев, В. В. Яковлев // International journal of open information technologies. — Т. 7. — № 5. — 2019. — 115 с. — С. 17–28.

[70] Скрыль, И. Д. Система поддержки принятия решений в управлении экономической устойчивостью промышленного предприятия / И. Д. Скрыль // Вестник Кузбасского государственного технического университета. — № 5 (111). — 2015. — 248 с. — С. 222–228.

[71] Смирнов, Н. В. О критерии симметрии закона распределения случайной величины / Н. В. Смирнов // Доклады АН СССР. — 1947. — Т. 56. — № 1. — СС. 13–16.

[72] Шелухин, О. И. Самоподобие и фракталы. Телекоммуникационные приложения /О. И. Шелухин, А. В. Осин, С. М. Смольский. Под ред. О. И. Шелухина. — М.: ФИЗМАТЛИТ, — 2008. — 368 с. — ISBN 978-5-9221-0949-9.

[73] Шелухин, О. И. Мультифракталы. Инфокоммуникационные приложения /О. И. Шелухин — М.: Горячая линия — Телеком, — 2014. — 579 с. — ISBN 978-5-9912-0142-1.

[74] Фортин, Т. OPC UA и роль стандартов связи в развитии промышленного Интернета вещей / Т. Фортин, Б. Хокинсон // Автоматизация в промышленности. — № 8. — 2016. — 64 с. — С. 40–46.

[75] Abbas, S. S. A. Self Configurations, Optimization and Protection Scenarios with wireless sensor networks in IIoT / S. S. A. Abbas, K. L. Priya // 2019 International Conference on Communication and Signal Processing (ICCSP). — 2019. — PP. 679–684. — DOI: 10.1109/ICII.2018.00030.

[76] Almas, M. S. Open source SCADA implementation and PMU integration for power system monitoring and control applications / M. S. Almas, L. Vanfretti, S. Løvlund, J. O. Gjerde // 2014 IEEE PES General Meeting | Conference & Exposition. — 2014. — DOI: 10.1109/PESGM.2014.6938840.

[77] Al-Masri, E. QoS-Aware IIoT Microservices Architecture / E. Al-Masri // 2018 IEEE International Conference on Industrial Internet (ICII). — 2018. — PP. 171–172. — DOI: 10.1109/ICII.2018.00030.

[78] Bergmann, O. A coap-gateway for smart homes / O. Bergmann, K. T. Hillmann, S. Gerdes // in Computing, Networking and Communications (ICNC). International Conference on IEEE. — 2012. — PP. 446–450. — DOI: 10.1109/ICCNC.2012.6167461.

[79] Borshchev, A. Multi-method modelling: AnyLogic / A. Borshchev // Discrete-Event Simulation and System Dynamics for Management Decision Making. — 2014. — P. 279. — PP. 248–279.

[80] Cavalieri, S. A web-based platform for OPC UA integration in IIoT environment / S. Cavalieri, D. D. Stefano, M. G. Salafia, M. S. Scroppo // 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). — 2017. — DOI: 10.1109/ETFA.2017.8247713.

[81] Chamekh, M. Secured Distributed IoT Based Supply Chain Architecture / M. Chamekh, M. Hamdi, S. E. Asmi, T. H. Kim // Proceedings of the 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). — 2018. — PP. 199–202. — DOI: 10.1109/WETICE.2018.00045.

[82] Cho, H. Implementation and Performance Analysis of Power and Cost-Reduced OPC UA Gateway for Industrial IoT Platforms / H. Cho, J. Jeong // Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC). — 2018. — DOI: 10.1109/ATNAC.2018.8615377.

[83] Contreras-Cristán, A. A Note on Whittle's Likelihood / A. Contreras-Cristán, E. Gutiérrez-Peña, S. G. Walker // Communications in Statistics — Simulation and Computation. — 2006. — Vol. 35. — № 4. — PP. 857–875. — DOI: 10.1080/03610910600880203.

[84] Desai, P. Semantic Gateway as a Service Architecture for IoT Interoperability / P. Desai, A. Sheth, P. Anantharam // IEEE International Conference on Mobile Services. — 2015. — PP. 313–319. — DOI: 10.1109/MobServ.2015.51.

[85] Escudero, J. I. Multimedia in the operation of large industrial networks / J. I. Escudero, F. Gonzalo, M. Mejias, M. Parada, J. Luque // Proceeding of the IEEE International Symposium on Industrial Electronics (ISIE). — 1997. — Vol. 3. — PP. 1281–1285. — DOI: 10.1109/ISIE.1997.648929.

[86] Gerardi, C. The AMPERE project: development of innovative European heterojunction bifacial cell and module technology in an industrial automated manufacturing plant / C. Gerardi, C. Colletti, F. Bizzarri, B. Strahm, A. Richter, D. Munoz, M. Izzi, J. Levrat et al. // 2019 IEEE 46th Photovoltaic Specialists Conference (PVSC). — 2019. — DOI: 10.1109/PVSC40753.2019.8980685.

[87] Gusev, M. Going Back to the Roots — The Evolution of Edge Computing, An IoT Perspective / M. Gusev, S. Dustdar // IEEE Internet Computing. — Vol. 22. — № 2. — 2018. — PP. 5–15. — DOI: 10.1109/MIC.2018.022021657.

[88] Hurst, H. E. Long-term storage capacity of reservoirs. / H. E. Hurst // Trans. Am. Soc. Civ. Eng. — 1951. — P. 116. — PP. 770–799.

[89] Iqbal, A. Positioning and Navigation Toolkit (PoiNT) — A tool for industry and academia / A. Iqbal, F. A. Khan, S. Z. Jamal, I. Khan. — 2015. — PP. 152–157. — DOI: 10.1109/IconSpace.2015.7283825.

[90] Iradier, E. NOMA-based 802.11n for Broadcasting Multimedia Content in Factory Automation Environments / E. Iradier, J. Montalban, L. Fanari, P., Seijo O. Angueira, I. Val // 2019 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). — 2019. — DOI: 10.1109/BMSB47279.2019.8971844.

[91] Jayaram, A. An IIoT quality global enterprise inventory management model for automation and demand forecasting based on cloud / A. Jayaram // 2017 International Conference on Computing, Communication and Automation (ICCCA). — 2017. — PP. 1258–1263. — DOI: 10.1109/CCAA.2017.8230011.

[92] Jian-Xin, Y. The Research and Development of Coal IoT Reasoning Engine Based on XML Model / Y. Jian-Xin // 2015 Seventh International Conference on

Measuring Technology and Mechatronics Automation. — 2015. — PP. 1266–1269. — DOI: 10.1109/LCOMM.2017.2730859.

[93] Kantelhardt, J. W. Multifractal detrended fluctuation analysis of nonstationary time series / J. W. Kantelhardt, S. A. Zschiegner, K. Koscielny-Bunde, S. Havlin, A. Hunde, H. E. Stanley // Elsevier Science: Physica A. — № 316. — 2002. — PP. 87–114. — DOI: 10.1016/S0378-4371(02)01383-3.

[94] Kibria, M. G. A framework to support data interoperability in web objects based IoT environments / M. G. Kibria, S. Ali, M. A. Jarwar, I. Chong // 2017 International Conference on Information and Communication Technology Convergence (ICTC). — 2017. — PP. 29–31. — DOI: 10.1109/ICTC.2017.8190935.

[95] Kim, S.-M. IoT home gateway for auto-configuration and management of MQTT devices / S.-M. Kim, H.-S. Choi, W.-S. Rhee // in Proceedings of the IEEE Conference on Wireless Sensors (ICWiSe 15). — 2015. — PP. 12–17. — DOI: 10.1109/ICWISE.2015.7380346.

[96] Kirichek, R. Model networks for Internet of Things and SDN / A. Vladyko, M. Zakharov, A. Koucheryavy, R. Kirichek // 18th International conference on advanced communication technology (ICACT). — 2016. — PP. 76–79. — DOI: 10.1109/ICACT.2016.7423280.

[97] Kitagami, S. Proposal of a Multi-agent Based Flexible IoT Edge Computing Architecture Harmonizing Its Control with Cloud Computing / S. Kitagami, T. Ogino, T. Suganuma, N. Shiratori // 2017 Fifth International Symposium on Computing and Networking (CANDAR). — 2017. — DOI: 10.1109/CANDAR.2017.28.

[98] Klein, S. A. An open source SCADA toolkit / S. A. Klein // 2006 IEEE Power Engineering Society General Meeting. — 2006. — DOI: 10.1109/PES.2006.1709143.

[99] Kulik, V. Industrial Internet of Things classification and analysis performed on a model network / V. Kulik, R. Kirichek R., A. Sotnikov // Lecture Notes in

Computer Science. 19th International Conference NEW2AN 2019 and 12th Conference, ruSMART 2019. — V. 11660. — 2019. — P. 548-561. — DOI: 10.1007/978-3-030-30859-9_48.

[100] Kulik, V. False clouds for Internet of Things and methods of protection / V. Kulik, R. Kirichek, A. Koucheryavy // The 18th International conference on advanced communications technology. — 2016. — P. 201-205. — DOI: 10.1109/ICACT.2016.7423328.

[101] Kulik, V. The home network traffic models investigation / M. Golubeva, V. Kulik, R. Kirichek, A. Koucheryavy // The 18th International conference on advanced communications technology. — 2016. — P. 97-100. — DOI: 10.1109/ICACT.2016.7423288.

[102] Kulik, V. The heterogeneous gateways in the Industrial Internet of Things / V, Kulik, R. Kirichek // 2018 10th International congress on ultra modern telecommunications and control systems and workshops (ICUMT) — 2018. — P. 1-6. — DOI: 10.1109/ICUMT.2018.8631232.

[103] Kulik, V. Measurement system architecture for measuring network parameters of e2e services / V. Kulik, R. Kirichek, A. Borodin, A. Koucheryavy // Communications in Computer and Information Science. 20th International Conference Distributed Computer and Communication Networks (DCCN 2017). — V. 700. — 2017. — P. 291-306. — DOI: 10.1007/978-3-319-66836-9_25.

[104] Kulik, V. The study of semantic gateway performance / V. Kulik, A. Muthanna, V. Pham, A. Hakimov, R. V. Kirichek, R. Ya. Pirmagomedov // Электросвязь. — № 6. — 2017. — 76 с. — С. 69-73.

[105] Liu, H. GridBatch: Cloud Computing for Large-Scale Data-Intensive Batch Applications / H. Liu, D. Orban // 8th IEEE International Symposium on Cluster Computing and the Grid (CCGRID '08). — 2008. — DOI: 10.1109/CCGRID.2008.30.

[106] Macagnano, D. Indoor positioning: A key enabling technology for IoT applications / D. Macagnano, G. Destino, G. Abreu // Proceeding of the IEEE World Forum on Internet of Things (WF-IoT). — 2014. — DOI: 10.1109/WF-IoT.2014.6803131.

[107] Manveer, J., Bikram, P. K. CoAP protocol for constrained networks / J. Manveer, P. K. Bikram // International journal of wireless and microwave technologies. — Т. 5. — № 6. — 2015. — 62 с. — С. 1–10.

[108] McKinley, P. K. Service Clouds: A Distributed Infrastructure for Constructing Autonomic Communication Services / P. K. McKinley, F. A. Samimi, J. K. Shapiro, C. Tang // 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. — 2006. — DOI: 10.1109/DASC.2006.44.

[109] Medrano, K. Development of SCADA using a RTU based on IoT controller / K. Medrano, D. Altuve, K. Belloso, C. Bran // 2018 IEEE International Conference on Automation / XXIII Congress of the Chilean Association of Automatic Control (ICA-ACCA). — 2018. — DOI: 10.1109/ICA-ACCA.2018.8609700.

[110] Narayanan, R. A probabilistic framework for protocol conversions in IIoT networks with heterogeneous gateways / R. Narayanan, C. S. R. Murthy // IEEE Communications Letters. — 2017. — Vol. 21. — Iss. 11. — PP. 2456–2459. — DOI: 10.1109/LCOMM.2017.2730859.

[111] Nichols, M. E. Applications for satellite positioning technology in the construction industry / M. E. Nichols // Proceedings of Position, Location and Navigation Symposium — PLANS '96. — 1996. — PP. 15–18. — DOI: 10.1109/PLANS.1996.509050.

[112] Palmer, G. I. Ciw: An open-source discrete event simulation library / G. I. Palmer, V. A. Knight, P. R. Harper, A. L. Hawa // Journal of Simulation. — 2018. — PP. 68–82. — DOI: 10.1080/17477778.2018.1473909.

[113] Pöhls, H. C. JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application / H. C. Pöhls // 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. — 2015. — PP. 306–312. — DOI: 10.1109/IMIS.2015.48.

[114] Popescu, C. Verification of the Consistency of Timing Constraints of the Orchestration of Factory Automation Web Services / C. Popescu, J. L. M. Lastra // 2007 5th IEEE International Conference on Industrial Informatics. — 2007. — PP. 785–790. — DOI: 10.1109/INDIN.2007.4384873.

[115] Puttonen, J. Semantics-Based Composition of Factory Automation Processes Encapsulated by Web Services / J. Puttonen, A. Lobov, J. L. M. Lastra // IEEE Transactions on Industrial Informatics. — 2013. — Vol. 9. — Iss. 4. — PP. 2349–2359. — DOI: 10.1109/TII.2012.2220554.

[116] Rahman, A. A gateway architecture for interconnecting smart objects to the internet / A. Rahman, D. Gellert, D. Seed // Proceedings of the Workshop Interconnecting Smart Objects with the Internet. — 2011. — Vol. 25. — PP. 1–3.

[117] Samimi, F. A. Service Clouds: Distributed Infrastructure for Adaptive Communication Services / F. A. Samimi, P. K. McKinley, S. M. Sadjadi, C. Tang, J. K. Shapiro, Z. Zhou // IEEE Transactions on Network and Service Management. — Vol. 4. — № 2. — 2007. — PP. 84–95. — DOI: 10.1109/TNSM.2007.070901.

[118] Shahzad, A. Secure IoT Platform for Industrial Control Systems / A. Shahzad, Y. G. Kim, A. Elgamoudi // Proceedings of the International Conference on Platform Technology and Service (PlatCon). — 2017. — DOI: 10.1109/PlatCon.2017.7883726.

[119] Shi, J. Merging and Splitting Self-similar Traffic / J. Shi, H. Zhu // Fifth Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference on Communications. — 1999. — PP. 110–114. — DOI: 10.1109/APCC.1999.824481.

[120] Smit, H. Service-oriented Architectures in Industrial Automation / H. Smit, I. M. Delamer // Proceedings of the 4th IEEE International Conference on Industrial Informatics (INDIN). — 2006. — DOI: 10.1109/INDIN.2006.275707.

[121] Tom, R. J. IoT based SCADA integrated with Fog for power distribution automation / R. J. Tom, S. Sankaranarayanan // Proceedings of the 12th Iberian

Conference on Information Systems and Technologies (CISTI). — 2017. — DOI: 10.23919/CISTI.2017.7975732.

[122] Wei, J. Design and analysis of centralized wireless positioning system based on ZigBee / J. Wei, H. Dai, X. Gu, L. He // Proceedings of 2011 International Conference on Electronics and Optoelectronics. — 2011. — Vol. 2. — PP. 370–373. — DOI: 10.1109/ICEOE.2011.6013259.

[123] Wollschlaeger, M. Framework for Web integration of factory communication systems / M. Wollschlaeger // ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings. — 2001. — DOI: 10.1109/ETFA.2001.996377.

[124] Wu, C.-H. Enabling multimedia applications for factory automation. / C.-H. Wu, J. D. Irwin, F. F. Dai // IEEE Transactions on Industrial Electronics. — Vol. 48. — Iss. 5. — 2010. — PP. 913–919. — DOI: 10.1109/41.954555.

[125] Yokotani, T. Comparison with HTTP and MQTT on required network resources for IoT / T. Yokotani, Y. Sasaki // 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC). — 2017. — DOI: 10.1109/ICCEREC.2016.7814989.

[126] Zhang, X. A Modified Multifractal Detrended Fluctuation Analysis (MFDFA) Approach for Multifractal Analysis of Precipitation in Dongting Lake Basin, China / X. Zhang, G. Zhang, L. Qiu, B. Zhang, Y. Sun, Z. Gui, Q. Zhang // MDPI: Water Open Access Journal. — 2019. — DOI: 10.3390/w11050891.

Приложение А. МЕТОДИКА КОМПЛЕКСНОГО ТЕСТИРОВАНИЯ СИСТЕМ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Программная методика испытаний (ПМИ) систем промышленного Интернета вещей (ПИВ) разработана на основе ГОСТ 19.301-2000 «Программа и методика испытаний, требования к содержанию и оформлению» и предназначена для проведения испытаний, измерения характеристик и метрик элементов систем ПИВ.

При разработке методики также использовались спецификации МСЭ-Т — Y.4003 «Overview of smart manufacturing in the context of the industrial Internet of things», Y.4101 «Common requirements and capabilities of a gateway for Internet of things applications», МСЭ-Т Y.1564 «Ethernet service activation test methodology» и спецификация IETF RFC 2544 «Benchmarking Methodology for Network Interconnect Devices».

Целью программы испытаний является разработка способов оценки программно-аппаратных характеристик для семантических гетерогенных шлюзов (СШ), граничных (ГС) и облачных серверов (ОС) ПИВ, с целью использования их на реальных сетях связи.

Представленная программа может быть использована специалистами по тестированию и разработчиками систем промышленного Интернета вещей.

1. **Объект испытаний**

Наименование объекта:

Объектом предварительных испытаний являются элементы систем промышленного Интернета вещей.

Обозначение:

Элементы ПИВ, IIoT entities.

Область применения:

Семантические гетерогенные шлюзы ПИВ предназначены для взаимного

преобразования прикладных протоколов и метаданных от различных источников между собой.

Граничные сервера ПИВ предназначены для сбора, хранения и обработки информации, поступающей от оконечных узлов ПИВ.

Облачные сервера ПИВ предназначены для обработки информации, поступающей на сервер от ГС и оконечных узлов ПИВ, и составления различных рекомендаций по эксплуатации и обслуживанию данного оборудования на основе данной информации.

2. **Цель испытаний**

- Проведение нагрузочного тестирования семантического шлюза и серверов ПИВ, с целью измерения их характеристик.
- Проверка разработанной методологии испытаний, при проведении натурных экспериментов на базе модельной сети, с целью выявления недостатков и доработки методики.
- Анализ измеренных характеристик, и определение граничных значений.

3. **Требования к методике**

- Методика должна обеспечивать соответствие взаимодействия программных и аппаратных характеристик семантического шлюза и сервера ПИВ и обеспечивать оценку их граничных значений.
- Методика должна быть универсальной вне зависимости от реализаций данных систем.

4. **Средства и порядок испытаний**

4.1. **Требования к архитектуре системы**

Сетевая инфраструктура тестируемой системы должна включать в себя следующие устройства:

1. Генератор трафика ПИВ.
2. Семантический гетерогенный шлюз ПИВ.
3. Граничный сервер ПИВ.

4. Облачный сервер ПИВ.
5. Коммутатор.
6. Маршрутизатор.

Представленные устройства должны быть подключены к одной общей локальной вычислительной IP-сети, иметь собственный адрес канального и сетевого уровня и иметь возможность обоюдосторонней передачи данных между собой. Сервера и генератор трафика ПИВ должны иметь подключение друг к другу через СШ.

4.2. **Требования к программному обеспечению**

Генератор трафика ПИВ должен включать в себя предварительно инсталлированное специальное программное обеспечение, отвечающее за генерацию трафика промышленного Интернета вещей согласно заранее заданным различным типам трафика ПИВ.

СШ должен включать в себя предварительно инсталлированное специальное программное обеспечение, отвечающее за преобразование сообщений, получаемых от систем промышленного Интернета вещей согласно заранее заданным моделям преобразования прикладных протоколов и форматов метаданных.

ГС должен включать в себя предварительно инсталлированное специальное программное обеспечение, отвечающее за прием, обработку и хранение информации от систем промышленного Интернета вещей.

ОС должен включать в себя предварительно инсталлированное специальное программное обеспечение, отвечающее за прием, обработку информации и составление рекомендаций по эксплуатации, хранению и обслуживанию систем ПИВ.

4.3. **Перечень руководящих документов**

Настоящая методика разработана в соответствии со следующими документами:

- МСЭ-Т Y.4003 — «Overview of smart manufacturing in the context of the industrial Internet of things».

- МСЭ-Т Y.4101 — «Common requirements and capabilities of a gateway for Internet of things applications».
- МСЭ-Т Y.1564 — «Ethernet service activation test methodology».
- IETF RFC 2544 — «Benchmarking Methodology for Network Interconnect Devices».
- ГОСТ 19.301-79 — «Программа и методика испытаний. Требования к содержанию и оформлению».

4.4. **Место и продолжительность испытаний**

1. Испытательный стенд находится на территории Университета телекоммуникаций имени проф. Бонч-Бруевича, на базе лаборатории Интернета вещей кафедры сетей связи и передачи данных.

2. Тестирования проводились в течение 14 дней.

4.5. **Перечень ранее проведенных испытаний**

Испытания по тестированию семантических шлюзов ранее проводились в рамках работ по разработке рекомендаций МСЭ-Т Q.3056 «Процедуры сигнализации между зондами, которые используются для дистанционного тестирования параметров сетей связи», Q.4060 «The structure of the testing of heterogeneous Internet of things gateways in a laboratory environment» и стандарта ИСО/МЭК 30162 «Internet of Things (IoT) — Compatibility requirements and model for devices within industrial IoT systems».

4.6. **Перечень предъявляемых на испытания документов**

Документация, используемая в тестировании:

- Описание программного и аппаратного обеспечения для тестирования.
- Сценарии тестирования.
- Методика тестирования.

5. **Объем испытаний**

5.1. **Перечень этапов испытаний**

Этапы испытаний семантического шлюза ПИВ представлены в таблице А.1.

ТАБЛИЦА А.1. Этапы испытаний семантического шлюза ПИВ

№	Объект испытаний	Требование	Наименование испытания	Вид испытания	Оцениваемые характеристики (мера измерения)
1	СШ	Время каждого испытания составляет не менее 60 секунд	Измерение характеристик семантического шлюза при процедуре преобразования прикладных проколов	Нагрузочное тестирование	• Время преобразования пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%].
2	СШ	Время каждого испытания составляет не менее 60 секунд	Измерение характеристик семантического шлюза при процедуре преобразования формата метаданных проколов	Нагрузочное тестирование	• Время преобразования пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%].
3	СШ	Время каждого испытания составляет не менее 60 секунд	Измерение характеристик семантического шлюза при максимальном для канала связи значении интенсивности поступления сетевых пакетов	Стрессовое тестирование	• Время преобразования пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%].
4	СШ	Время каждого испытания составляет не менее 24 часов	Испытание стабильности работы семантического шлюза при заданной модели нагрузки	Тестирование надежности	• Время преобразования пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%]. • Количество отказов.
5	СШ	Время каждого испытания составляет не менее 24 часов	Испытание стабильности работы семантического шлюза при максимальной нагрузке системы	Тестирование надежности	• Время преобразования пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%]. • Количество отказов.
Примечание: %* — мера измерения, показатель количества от общего числа.					

ТАБЛИЦА А.1 (продолжение). Этапы испытаний семантического шлюза ПИВ

№	Объект испытаний	Требование	Наименование испытания	Вид испытания	Оцениваемые характеристики (мера измерения)
6	СШ	Время каждого испытания составляет не менее 60 секунд, количество виртуальных устройств на ГТ последовательно возрастает для каждого измерения	Оценка максимального числа виртуальных устройств, обслуживаемых без потерь и нарушения функциональности семантического шлюза	Тестирование потенциальных возможностей	• Время преобразования пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%] • Количество подключенных виртуальных устройств.
Примечание: %* — мера измерения, показатель количества от общего числа.					

Этапы испытаний серверов ПИВ (как ГС, так и ОС) представлены в таблице А.2.

ТАБЛИЦА А.2. Этапы испытаний сервера ПИВ

№	Объект испытаний	Требование	Наименование испытания	Вид испытания	Оцениваемые характеристики (мера измерения)
1	Сервер ПИВ	Время каждого испытания составляет не менее 60 секунд	Измерение характеристик сервера при обработке поступающих пакетов	Нагрузочное тестирование	• Время обслуживания пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%].
2	Сервер ПИВ	Время каждого испытания составляет не менее 60 секунд	Измерение характеристик сервера при максимальном для канала связи значении интенсивности поступления сетевых пакетов	Стрессовое тестирование	• Время обслуживания пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%].
3	Сервер ПИВ	Время каждого испытания составляет не менее 24 часов	Испытание стабильности работы сервера при заданной модели нагрузки	Тестирование надежности	• Время обслуживания пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%]. • Количество отказов.
Примечание: %* — мера измерения, показатель количества от общего числа.					

ТАБЛИЦА А.2 (продолжение). Этапы испытаний сервера ПИВ

№	Объект испытаний	Требование	Наименование испытания	Вид испытания	Оцениваемые характеристики (мера измерения)
4	Сервер ПИВ	Время каждого испытания составляет не менее 24 часов	Испытание стабильности работы сервера при максимальной нагрузке системы	Тестирование надежности	• Время обслуживания пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%]. • Количество отказов.
5	Сервер ПИВ	Время каждого испытания составляет не менее 60 секунд, количество виртуальных устройств на ГТ последовательно возрастает для каждого измерения	Оценка максимального числа виртуальных устройств, обслуживаемых без потерь и нарушения функциональности сервера	Тестирование потенциальных возможностей	• Время обслуживания пакетов [с]. • Загрузка ЦП [%]. • Загрузка ОП [%]. • Потерянные пакеты [%]. • Количество подключенных виртуальных устройств.
Примечание: %* — мера измерения, показатель количества от общего числа.					

5.2. **Порядок проведения испытаний**

Последовательность проведения испытаний представляет собой алгоритм, состоящий из четырех этапов. Испытания, присутствующие на следующем этапе, не начинаются, пока не завершатся все процессы предыдущего этапа.

Этап 1. Разработка методик испытаний элементов системы ПИВ.

Для проведения испытаний шлюза были разработаны следующие методики тестирования:

1. Для определения характеристик семантического шлюза при преобразовании поступающих пакетов из одного прикладного протокола в другой предлагается провести измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени преобразования (ВП) и процента потерянных сетевых пакетов в режиме нагрузочного тестирования, в зависимости от количества виртуальных устройств, функционирующих на генераторе трафика

ПИВ (1, 10, 50, 100, 250, 500, 1000, 2500, 5000, 10 000 и более при условии корректной работы), при фиксированном времени работы генератора графика 60 секунд.

2. Для определения характеристик семантического шлюза при преобразовании поступающих пакетов из одного формата метаданных поля полезной нагрузки в другой предлагается провести измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени преобразования (ВП) и процента потерянных сетевых пакетов в режиме нагрузочного тестирования, в зависимости от количества виртуальных устройств, функционирующих на генераторе трафика ПИВ (1, 10, 50, 100, 250, 500, 1000, 2500, 5000, 10 000 и более при условии корректной работы), при фиксированном времени работы генератора графика 60 секунд.

3. Для определения характеристик семантического шлюза в режиме штатной работы предлагается провести стрессовое тестирование при максимальном значении интенсивности поступления сетевых пакетов для пропускной способности канала связи. В ходе испытания проводится измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени преобразования (ВП) и процента потерянных пакетов, при фиксированном времени работы генератора графика 60 секунд.

4. Испытание надежности работы семантического шлюза при заданной модели нагрузки. Измерение производительности семантического шлюза в режиме нагрузочного тестирования, которое проводится с помощью заранее известных аналитических моделей трафика ПИВ, при фиксированном количестве виртуальных устройств на генераторе и времени работы t = 24 часа (86 400 секунд). По результатам испытания проводится подсчет количества отказов во время работы СШ.

5. Испытание надежности работы семантического шлюза при максимальной нагрузке системы. Измерение производительности семантического шлюза в режиме стрессового тестирования, которое проводится с помощью

предварительно полученного в ходе нагрузочного тестирования граничного значения интервалов времени между сетевыми пакетами для каждого типа трафика, при фиксированном количестве виртуальных устройств на генераторе трафика ПИВ (10 000) и времени работы t = 24 часа (86 400 секунд). По результатам испытания проводится подсчет количества отказов во время работы СШ.

6. Для оценки максимального числа виртуальных устройств, обслуживаемых без потерь и нарушения функциональности семантического шлюза, предлагается провести измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени преобразования (ВП) и процента потерянных сетевых пакетов при различном количестве виртуальных устройств, функционирующих на генераторе трафика ПИВ (1, 10, 50, 100, 250, 500, 1000, 2500, 5000, 10 000 и более при условии корректной работы), а также при фиксированном времени работы генератора графика 60 секунд.

Для проведения испытаний шлюза были разработаны следующие методики тестирования:

1. Для определения характеристик сервера при процедуре обработки поступающих запросов предлагается провести измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени обслуживания (ВО) пакета и процента потерянных сообщений в режиме нагрузочного тестирования, в зависимости от количества виртуальных устройств, функционирующих на генераторе трафика ПИВ (1, 10, 50, 100, 250, 500, 1000, 2500, 5000, 10 000 и более при условии корректной работы), при фиксированном времени работы генератора графика 60 секунд.

2. Для определения характеристик работы сервера ПИВ в режиме штатной работы предлагается провести стрессовое тестирование при максимальном значении интенсивности поступления сетевых пакетов для пропускной способности канала связи. В ходе испытания проводится измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени обслуживания (ВО) и процента потерянных пакетов при фиксированном времени

работы генератора графика 60 секунд.

3. Испытание стабильности работы сервера при заданной модели нагрузки. Измерение производительности сервера в режиме нагрузочного тестирования, которое проводится с помощью заранее известных аналитических моделей трафика ПИВ, при фиксированном количестве виртуальных устройств на генераторе (1000, 5000, 10 000) и времени работы t = 24 часа (86 400 секунд). По результатам испытания проводится подсчет количества отказов во время работы сервера.

4. Испытание стабильности работы сервера при стрессовом тестировании. Измерение производительности сервера в режиме стрессового тестирования, которое проводится с помощью предварительно полученного в ходе нагрузочного тестирования граничного значения интервалов времени между сообщениями для каждого типа запросов, при фиксированном количестве виртуальных устройств на генераторе трафика ПИВ (1000, 5000, 10 000) и времени работы t = 24 часа (86 400 секунд). По результатам испытания проводится подсчет количества отказов во время работы сервера.

5. Для оценки максимального числа виртуальных устройств, обслуживаемых без потерь и нарушения функциональности сервера, предлагается провести измерение значений загрузки центрального процессора (ЦП), оперативной памяти (ОП), времени обслуживания (ВО) и процента потерянных сетевых пакетов при различном количестве виртуальных устройств, функционирующих на генераторе трафика ПИВ (1, 10, 50, 100, 250, 500, 1000, 2500, 5000, 10 000 и более при условии корректной работы), а также при фиксированном времени работы генератора графика 60 секунд.

Измерение производительности семантического шлюза и сервера ПИВ проводится с помощью фонового приложения, проводящего измерение значений ВП, загрузки ЦП и ОП, с предварительно заданной периодичностью измерений (1 раз в 10,00; 1,00; 0,10; 0,01 секунды). Оценка процента потерянных пакетов происходит по следующему закону $F_{\text{пот}} = 1 - \frac{v}{v_{\text{отп}}}$, где $F_{\text{пот}}$ — процент потерянных

сообщений, $v_{\text{отп}}$ — количество отправленных генератором сообщений, а v — количество корректно полученных сообщений для протоколов без контроля доставки сообщений или количество перезапросов сообщений для протоколов, включающих контроль доставки сообщений.

Все измеряемые значения измеряются по среднему значению выборки, полученной в ходе испытания, и доверительного интервала, при различных значениях доверительной вероятностей (90, 95, 99 %).

Этап 2. Проведение первичных испытаний элементов системы ПИВ.

Этап 3. Выявления ошибок ПМИ и их корректировка.

Этап 4. Проведение главных испытаний и анализ результатов.

5.3. Последовательность действий при проведении испытаний

Последовательность действий при проведении испытаний семантического шлюза ПИВ описана в таблице А.3.

ТАБЛИЦА А.3. Последовательность действий при проведении испытаний семантического шлюза ПИВ

№	Действие	Описание	Результат
I. Предварительная настройка программного и аппаратного обеспечения			
1	Подключение и настройка генератора трафика ПИВ (ГТ)	А. ГТ подключается к тестируемой сети через сетевой интерфейс.	Генератор трафика готов к испытанию
		Б. Проводится настройка ГТ на базе протоколов канального и сетевого уровней.	
		В. Проверяется доступность ГТ для устройств в сети.	
		Г. Проводится настройка ГТ.	
		Д. Проводится тестовая генерация трафика ПИВ. Для подтверждения работы ГТ используется локальный анализатор сетевых пакетов.	
2	Подключение и настройка сервера ПИВ	А. Сервер подключается к тестируемой сети через сетевой интерфейс.	Сервер ПИВ готов к приему сетевых пакетов
		Б. Проводится сетевая настройка сервера.	
		В. Проверяется доступность сервера для устройств в сети.	
		Г. Проводится проверка работы следующих базовых функций сервера: регистрация	

№	Действие	Описание	Результат
		устройства ПИВ, прием и сохранение данных, чтение данных.	
		Д. На базе приложения для тестирования уровня загрузки ЦП и объема используемой ОП проводится тестирование СШ с локально функционирующим сервером.	
3	Подключение и настройка семантического шлюза (СШ)	А. СШ подключается к тестируемой сети через сетевой интерфейс.	Семантический шлюз готов к испытанию
		Б. Проводится сетевая настройка СШ и проверяется его доступность для других устройств в сети.	
		В. В фоновом режиме запускается приложение для тестирования загрузки центрального процессора (ЗЦП) и объема используемой оперативной памяти (ИОП) и измеряется без поступающего трафика ПИВ.	
4	Испытание передачи и приема данных между генератором трафика и сервером	Проводится испытание приема и передачи сетевых пакетов для системы, состоящей из ГТ и ГС (с помощью поддерживаемых ГС прикладных протоколов). Поток сетевых пакетов генерируется одним виртуальным устройством для каждого из поддерживаемых ГТ видов трафика поочередно.	Система, состоящая из генератора трафика и сервера, готова к приему и передаче данных
II. Испытание «Измерение характеристик семантического шлюза при процедуре преобразования прикладных проколов»			
1	Испытание работы семантического шлюза совместно с сервером	На СШ проводится испытание преобразования всех поддерживаемых ГТ прикладных протоколов поочередно с постоянно возрастающим количеством виртуальных устройств.	Семантический шлюз готов к работе
2	Испытание преобразования протоколов на семантическом шлюзе	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при нагрузочном тестировании с помощью ГТ, для каждого из поддерживаемых ГТ прикладных протоколов с постоянно возрастающим количеством виртуальных устройств.	Семантический шлюз готов к преобразованию прикладных протоколов ПИВ
		Б. Проводится ряд измерений, подобных описанным в предыдущем пункте, при условии формирования сразу множества сетевых пактов, каждый из которых соответствует какому-либо одному прикладному протоколу, с постоянно возрастающим количеством виртуальных устройств на ГТ.	
		В. Результаты проведенных испытаний используются для разработки рекомендаций по	

№	Действие	Описание	Результат
		работе СШ.	
III. Испытание «Измерение характеристик семантического шлюза при процедуре преобразования формата метаданных проколов»			
1	Испытание работы семантического шлюза совместно с сервером	А. Проводится сравнение формата метаданных, формируемых СШ и форматом сервера ПИВ. Если результат сравнения неудачен, то формат метаданных СШ изменяется под формат, принятый у сервера.	Семантический шлюз готов к работе
		Б. На СШ проводится испытание преобразования при нагрузочном тестировании с помощью ГТ, всех поддерживаемых ГТ (при условии наличия на СШ алгоритма их преобразования в формат сервера) метаданных поочередно с постоянно возрастающим количеством виртуальных устройств.	
2	Испытание преобразования метаданных на семантическом шлюзе	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при нагрузочном тестировании с помощью ГТ, для каждого из поддерживаемых ГТ форматов метаданных с постоянно возрастающим количеством виртуальных устройств.	Семантический шлюз готов к преобразованию форматов метаданных
		Б. Проводится ряд измерений, подобных описанным в предыдущем пункте, при условии формирования сразу множества сетевых пактов, каждый из которых соответствует какому-либо одному формату метаданных с постоянно возрастающим количеством виртуальных устройств на ГТ.	
		В. Результаты проведенных испытаний используются для разработки рекомендаций по работе СШ.	
IV. Испытание «Измерение характеристик семантического шлюза при максимальном для канала связи значении интенсивности поступления сетевых пакетов»			
1	Измерение характеристик семантического шлюза при максимальном для канала связи значении интенсивности поступления сетевых пакетов	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при стрессовом тестировании с помощью ГТ, где частота поступления сетевых пакетов определяется максимальной пропускной способностью канала связи и сетевого интерфейса ГТ.	Определены характеристики СШ при максимальном значении интенсивности поступления пакетов
		Б. Результаты проведенных испытаний используются для разработки рекомендаций по работе СШ.	
V. Испытание «Испытание стабильности работы семантического шлюза при заданной модели			

№	Действие	Описание	Результат
нагрузки»			
1	Испытание стабильности работы семантического шлюза	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при нагрузочном тестировании с помощью ГТ, согласно заранее заданным характеристикам для всех поддерживаемых ГТ типов трафика ПИВ.	Семантический шлюз готов к работе
		Б. После истечения заданного времени проведения испытания проводится подсчет количества отказов во время работы СШ.	
		В. Результаты проведенных испытаний используются для разработки рекомендаций по работе СШ.	
VI. Испытание «Испытание стабильности работы семантического шлюза при максимальной нагрузке системы»			
1	Испытание стабильности работы семантического шлюза	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при стрессовом тестировании с помощью ГТ, согласно заранее измеренным верхним граничным значениям.	Семантический шлюз готов к работе
		Б. После истечения заданного времени проведения испытания проводится подсчет количества отказов во время работы СШ.	
		В. Результаты проведенных испытаний используются для разработки рекомендаций по работе СШ.	
VII. Испытание «Оценка максимального числа виртуальных устройств, обслуживаемых без потерь и нарушения функциональности семантического шлюза»			
1	Оценка максимального числа обслуживаемых виртуальных устройств	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при стрессовом тестировании с помощью ГТ с постоянно возрастающим количеством виртуальных устройств. Удовлетворительным значением является максимальное число обслуживаемых семантическим шлюзом виртуальных устройств, после которого начинаются потери сетевых пакетов.	Определено максимальное значение обслуживаемых СШ устройств без потерь и нарушения функциональности работы СШ
		Б. Результаты проведенных испытаний используются для разработки рекомендаций по работе СШ.	

Последовательность действий при проведении испытаний серверов ПИВ описана в таблице А.4.

ТАБЛИЦА А.4. Последовательность действий при проведении испытаний сервера ПИВ

№	Действие	Описание	Результат
I. Предварительная настройка программного и аппаратного обеспечения			
1	Подключение и настройка генератора трафика ПИВ (ГТ)	А. ГТ подключается к тестируемой сети через сетевой интерфейс.	Генератор трафика готов к испытанию
		Б. Проводится настройка ГТ на базе протоколов канального и сетевого уровней.	
		В. Проверяется доступность ГТ для устройств в сети.	
		Г. Проводится настройка ГТ.	
2	Подключение и настройка сервера ПИВ	А. Сервер подключается к тестируемой сети через сетевой интерфейс.	Сервер ПИВ готов к приему сетевых пакетов
		Б. Проводится сетевая настройка сервера.	
		В. Проверяется доступность сервера для устройств в сети.	
		Г. Проводится проверка работы всех тестируемых функций сервера.	
		Д. На базе приложения для тестирования уровня загрузки ЦП и объема используемой ОП проводится тестирование СШ с локально функционирующим сервером.	
3	Испытание передачи и приема данных между генератором трафика и сервером	А. Проводится сравнение формата метаданных, формируемых ГТ и форматом сервера. Если результат сравнения неудачен, то формат метаданных ГТ изменяется под формат, принятый у сервера.	Система, состоящая из генератора трафика и сервера, готова к приему и передаче данных
		Б. Проводится испытание приема и передачи сетевых пакетов для системы, состоящей из ГТ и ГС (с помощью поддерживаемых ГС прикладных протоколов). Поток сетевых пакетов генерируется одним виртуальным устройством для каждого из поддерживаемых ГТ видов трафика поочередно.	
II. Испытание «Измерение характеристик сервера при процедуре обработки поступающих запросов»			
1	Испытание преобразования протоколов на семантическом шлюзе	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП сервера для всех тестируемых функций с постоянно возрастающим количеством виртуальных устройств от ГТ.	Сервер готов к обработке запросов
		Б. Результаты проведенных тестов используются для разработки рекомендаций по работе сервера.	
III. Испытание «Измерение характеристик сервера при максимальном для канала связи			

№	Действие	Описание	Результат
значении интенсивности поступления сетевых пакетов»			
1	Измерение характеристик сервера при максимальном для канала связи значении интенсивности поступления сетевых пакетов	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП сервера при стрессовом тестировании с помощью ГТ, где частота поступления сетевых пакетов определяется максимальной пропускной способностью канала связи и сетевого интерфейса ГТ.	Определены характеристики сервера при максимальном значении интенсивности поступления пакетов
		Б. Результаты проведенных испытаний используются для разработки рекомендаций по работе сервера.	
IV. Испытание «Испытание стабильности работы сервера при заданной модели нагрузки»			
1	Испытание стабильности работы сервера	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП сервера при нагрузочном тестировании с помощью ГТ, согласно заранее заданным характеристикам для всех поддерживаемых ГТ типов запросов.	Сервер готов к работе
		Б. После истечения заданного времени проведения испытания проводится подсчет количества отказов во время работы сервера.	
		В. Результаты проведенных испытаний используются для разработки рекомендаций по работе сервера.	
V. Испытание «Испытание стабильности работы сервера при максимальной нагрузке системы»			
1	Испытание стабильности работы сервера	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП сервера при стрессовом тестировании с помощью ГТ, согласно заранее измеренным верхним граничным значениям.	Сервер готов к работе
		Б. После истечения заданного времени проведения испытания проводится подсчет количества отказов во время работы сервера.	
		В. Результаты проведенных испытаний используются для разработки рекомендаций по работе сервера.	
VI. Испытание «Оценка максимального числа виртуальных устройств, обслуживаемых без потерь и нарушения функциональности сервера»			
1	Оценка максимального числа обслуживаемых виртуальных устройств	А. Поочередно проводится ряд измерений ВО, ЗЦП и ИОП СШ при стрессовом тестировании с помощью ГТ с постоянно возрастающим количеством виртуальных устройств. Удовлетворительным значением является максимальное число обслуживаемых сервером виртуальных устройств, после которого начинаются потери сетевых пакетов.	Определено максимальное значение обслуживаемых сервером устройств без потерь и нарушения

№	Действие	Описание	Результат
		Б. Результаты проведенных испытаний используются для разработки рекомендаций по работе сервера.	функциональности работы сервера

5.4. Требования по испытаниям элементов систем ПИВ

- Испытания должны быть проведены в той последовательности, которая указана в пункте 5.2.
- Должны быть проведены испытания определенных программно-аппаратных характеристик семантического шлюза и сервера ПИВ.
- Испытания должны показать, что определенные характеристики семантического шлюза, граничного и облачного сервера ПИВ удовлетворяют заданным критериям оценок и метрикам тестирования.

5.5. Перечень работ, проводимых после завершения испытаний

По завершении испытаний полученные результаты заносят в книгу испытаний, которая находится в лаборатории. Также оформляется протокол испытаний, который содержит соответствующие общие и специальные данные.

Общие данные:

- описание материальной стороны испытуемого объекта — наименование, цвет, применение, предприятие-изготовитель и др.;
- даты проведения испытаний и состав лиц, принимавших участие в испытаниях;
- условия нахождения испытуемого объекта до проведения испытаний;
- условия испытаний — относительная влажность воздуха в помещении, температура окружающей среды, атмосферное давление и др.;
- измерительные приборы с указанием их класса точности и описанием лабораторного стенда для испытаний.

Специальные данные обуславливаются назначением и методом испытаний, особенностями испытуемого объекта.

Протокол подписывает руководитель и исполнители, проводившие

испытания.

6. Условия и порядок проведения испытаний

6.1. Условия проведения испытаний

Испытания должны проводиться в нормальных климатических условиях по ГОСТ 22261-94. Условия проведения испытаний приведены ниже:

- температура окружающего воздуха, °С — 20 ± 5;
- относительная влажность, % — от 30 до 80;
- атмосферное давление, кПа — от 84 до 106;
- частота питающей электросети, Гц — 50 ± 0,5;
- напряжение питающей сети переменного тока, В — 220 ± 4,4.

6.2. Условия начала и завершения отдельных этапов испытаний

Необходимым и достаточным условием завершения этапа испытаний и начала последующего этапа является успешное завершение проверок, проводимых на этом этапе. Перечень проверок должен включать в себя:

1) проверку комплектности программной документации (ПД);

2) проверку комплектности состава технических и программных средств.

6.3. Меры, обеспечивающие безопасность и безаварийность проведения испытаний

При проведении испытаний необходимо обеспечить соблюдение требований безопасности, установленных ГОСТ 12.2.007.0-75 «Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности», «Правилами техники безопасности при эксплуатации электроустановок потребителей» и «Правилами технической эксплуатации электроустановок потребителей».

6.4. **Материально-техническое обеспечение испытаний**

Для проведения испытаний необходимо обеспечить достаточную материально-техническую базу и выполнить все первичные действия, с помощью которых проводятся испытания.

Под материально-техническим обеспечением в данной работе понимается:

- ✓ лабораторный стенд, состоящий из разных аппаратно-программных комплексов (АПК), таких как:

- сервер, как головной управляющий элемент сети, на котором установлено программное обеспечение граничного сервера ПИВ;
- сервер, как устройство обработки информации с оконечных устройств и граничного сервера ПИВ, на котором установлено программное обеспечение облачного сервера ПИВ;
- семантический шлюз ПИВ, основной обязанностью которого является преобразование сообщений между различными поддерживаемыми прикладными протоколами и форматами метаданных;
- коммутатор, основной обязанностью которого является коммутация элементов ПИВ;
- генератор трафика ПИВ, отвечающий за генерацию сетевых пакетов и заявок;
- маршрутизатор, обеспечивающий маршрутизацию сетевых пакетов.

Под первичными действиями для проведения испытаний понимается:

- сборка лабораторного стенда для проведения испытаний;
- установка необходимого программного обеспечения на клиентское и серверное оборудование лабораторного стенда;
- обеспечение стабильного взаимодействия элементов стенда;
- общая организация процесса испытаний.

Приложение Б. Документы, подтверждающие внедрение основных результатов диссертационной работы

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Юридический адрес: набережная реки Мойки,
д. 61, Санкт-Петербург, 191186

Почтовый адрес: пр. Большевиков, д. 22, корп. 1,
Санкт-Петербург, 193232
Тел.(812) 3263156, Факс: (812) 3263159
E-mail: rector@sut.ru
ИНН 7808004760 КПП 784001001
ОГРН 1027809197635 ОКТМО 40909000

16.01.2020 №_____
на №_____ от_____

Утверждаю

Проректор по научной работе
Шестаков А.В.

Акт
о внедрении научных результатов,
полученных Куликом Вячеславом Андреевичем в диссертационной работе
"Модели и методы тестирования устройств, сетей и систем Промышленного Интернета Вещей"

Комиссия в составе декана факультета Инфокоммуникационных сетей и систем Л.Б. Бузюкова, доцента кафедры сетей связи и передачи данных М.А. Маколкиной и заведующей лабораторией кафедры сетей связи и передачи данных О.И. Ворожейкиной составила настоящий акт в том, что научные результаты, полученные Куликом Вячеславом Андреевичем в диссертации " Модели и методы тестирования устройств, сетей и систем Промышленного Интернета Вещей", использованы:

1. При чтении лекций и проведении практических занятий по курсу Интернет Вещей (Рабочая Программа № 18.05/1198-Д, утверждена Первым проректором-проректором по учебной работе Г.М. Машковым 05.07.2018), раздел Программы:

- Ad Hoc или самоорганизующиеся сети. Приложения самоорганизующихся сетей. Всепроникающие сенсорные сети как технологическая основа внедрения концепции Интернета Вещей. Кластеризация сенсорных сетей и основные методы кластеризации, включая биоподобные алгоритмы.

2. При чтении лекций и проведении практических занятий по курсу Современные проблемы науки в области инфокоммуникаций (Рабочая Программа № 18.05/496-Д, утверждена Первым проректором-проректором по учебной работе Г.М. Машковым 05.07.2018), раздел Программы:

- Концепции развития сетей связи. Текущее состояние развития сетей. Прогнозы развития сетей связи. На основе анализа текущего состояния развития сетей связи, в том числе количественных оценок клиентской базы Всемирной сети связи, а также прогнозов ведущих специалистов и ученых отрасли формируется концепция развития сети, получившая название Интернета вещей. Рассматриваются и иные составляющие сети Интернета будущего: Интернет людей. Интернет энергии и т.д.

В указанных дисциплинах используются следующие новые научные результаты, полученные Куликом Вячеславом Андреевичем в диссертационной работе:

- Модели фрагментов сети Промышленного Интернета Вещей, позволяющие оценить эффективность работы систем и сетей ПИВ в условиях высокой нагрузки и рационально планировать размещение элементов сети на этапе развертывания и масштабирования;

- Методика комплексного тестирования сетей Промышленного Интернета Вещей, предназначенная для тестирования уже существующих систем и сетей ПИВ на устойчивость к высокой нагрузке.

Декан факультета ИКСС Л.Б. Бузюков

Доцент кафедры ССиПД М.А. Маколкина

Зав. лабораторией кафедры ССиПД О.И. Ворожейкина

Публичное акционерное общество «Ростелеком»

ул. Гончарная, д. 30
г. Москва, Россия, 115172
тел.: +7 (499) 999-80-22, +7 (499) 999-82-83
факс: +7 (499) 999-82-22
e-mail: rostelecom@rt.ru, web: www.rt.ru

16.01.2020 № _____

На № от

АКТ
о внедрении результатов диссертационной работы
Кулика Вячеслава Андреевича на тему
«Разработка моделей и методов комплексного тестирования систем Промышленного Интернета Вещей» в ПАО «Ростелеком»

Настоящим актом подтверждаем, что научные результаты диссертационной работы Кулика Вячеслава Андреевича «Разработка моделей и методов комплексного тестирования систем Промышленного Интернета Вещей», представленной на соискание ученой степени кандидата технических наук, обладают актуальностью, представляют практический интерес и были внедрены в научно-исследовательской работе «Исследование прикладных платформ управления и организации Индустриального Интернета Вещей», выполненной СПбГУТ им. проф. М.А. Бонч-Бруевича по заказу ПАО «Ростелеком».

Научные результаты диссертационной работы В.А. Кулика, а именно:

- модели фрагментов сети Промышленного Интернета Вещей (ПИВ);
- метод построения семантического гетерогенного шлюза Промышленного Интернета Вещей;
- методика комплексного тестирования сетей Промышленного Интернета Вещей,

использованы при подготовке Рекомендации Сектора стандартизации Международного союза электросвязи (МСЭ-Т) Q.4060 «Структура тестирования гетерогенных шлюзов интернета вещей в лабораторных условиях», Рекомендации МСЭ-Т Q.3056 «Процедуры сигнализации между зондами, которые используются для дистанционного тестирования параметров сетей

связи», а также при разработке проекта Международного стандарта «Интернет вещей. Требования и модели совместимости для устройств в промышленных системах интернета вещей» подкомитета 41 «Интернет вещей и смежные технологии» Совместного технического комитета 1 Международной организации по стандартизации и Международной электротехнической комиссии (ИСО/МЭК СТК 1 ПК41).

Применение перечисленных научных результатов диссертационной работы Кулика В.А. позволило разработать алгоритмы генерации трафика и требования к тестированию, прототипа программно-аппаратного комплекса для тестирования систем Промышленного Интернета Вещей, а также могут быть использованы для разработки систем комплексного тестирования сетевой инфраструктуры в условиях имитации повышенной функциональной нагрузки на базе международных стандартов.

Председатель комиссии:

Руководитель
Представительства ПАО «Ростелеком»
в Международном союзе электросвязи,

А.С. Бородин

Члены комиссии:

Начальник отдела
Департамента международного сотрудничества -
Заместитель Председателя 20-й Исследовательской комиссии
«Интернет вещей, умные города и поселения»
Сектора стандартизации электросвязи Международного союза электросвязи

О.В. Мирошников

Начальник отдела
продуктов и маркетинга операторского сегмента
Блока межоператорского взаимодействия

С.В. Макаров