На правах рукописи

Жук Роман Владимирович

МЕТОДИКА И АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.3.6. Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2021

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Кубанский государственный технологический университет» на компьютерных технологий и информационной безопасности.

Научный руководитель: кандидат технических наук, доцент
Власенко Александра Владимировна

Официальные оппоненты: **Ажмухамедов Искандар Маратович**,
доктор технических наук, профессор,
Астраханский государственный университет,
факультет цифровых технологий и кибербезопасности,
декан факультета

Аникин Игорь Вячеславович,
доктор технических наук, профессор,
Казанский национальный исследовательский
технический университет им. А.Н.Туполева-КАИ,
кафедра систем информационной безопасности,
заведующий кафедрой

Ведущая организация: Федеральное государственное казенное
образовательное учреждение высшего образования
«Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя», г. Москва

Защита состоится 01 декабря 2021 года в 14.00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 01 октября 2021 года.

Ученый секретарь
диссертационного совета 99.2.038.03,
канд. техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В целях унификации перечня угроз безопасности информации (далее – УБИ), в 2015 г. Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) был создан банк данных УБИ (далее – банк угроз), функции которого заключаются в сборе, накопление и корреляции уязвимостей программного обеспечения (далее – уязвимости ПО) и УБИ для информационных систем (далее – ИС).

Однако, создание банка угроз не решило проблемы, связанные с определением УБИ в информационных системах обработки персональных данных (далее – ИСПДн):

– отсутствие понятия актива в ИСПДн, вследствие чего определение масштаба и границ ИСПДн зависят от субъективного мнения эксперта в области ИБ;

– существование фундаментальных различий между методиками определения нарушителей ИБ для ИС и ИСПДн;

– отсутствие методики присвоения потенциала нарушителю ИБ, несмотря на наличие данной характеристики в банке угроз;

– отсутствие связи между уязвимостями ПО, нарушителями ИБ и УБИ.

Значительная часть программных средств, применяемых для автоматизации процесса определения УБИ, не устанавливает связь между уязвимостью ПО и УБИ, что может привести к необоснованному выбору защитных мер и средств защиты информации (далее – СЗИ), включая их некорректную настройку.

Актуальность диссертационной работы заключается в разработке методики определения актуальных УБИ в ИСПДн путем построения взаимосвязи между уязвимостями ПО активов ИСПДн и потенциалом нарушителя ИБ.

Разработанная методика включает в себя следующие этапы:

– выбора активов ИСПДн;

– определения возможных уязвимостей ПО в ИСПДн;

– выбора нарушителя ИБ;

– выбора уязвимостей ПО, которые могут быть реализованы выбранным нарушителем ИБ в ИСПДн;

– определения возможных УБИ в ИСПДн;

– выбора актуальных УБИ в ИСПДн.

Для автоматизации предлагаемой методики планируется разработка программного средства на основе веб-технологий.

Степень разработанности темы исследования. Рассмотрены вопросы, связанные с установлением активов в ИСПДн, определением значимости выбранных активов для бизнес-процессов, обрабатывающих ПДн. Также рассмотрены методы выбора уязвимостей ПО построения взаимосвязи между выбранными уязвимостями с нарушителями ИБ. Наряду с рассматриваемыми методиками проанализированы существующие способы и алгоритмы построения моделей УБИ для различных ИС. По результатам анализа проработанности выбранной темы установлено, что в области разработки моделей УБИ теоретическая и практическая базы формируются усилиями таких ученых как Ю.В. Вайнштейн, С.Л. Демин, И.Н. Кирко, М.М. Кучеров, М.В. Сомова, В.А. Герасименко, А.А. Малюк , А.А. Корниенко , П. Д. Зегжда, Е.А. Рудина, А.А. Шелупанова, В.Г. Мироновой, С.С. Ерохина, А.А. Мицель , В.И. Васильева, Н.В. Белкова, В.В. Сагитова, В.И. Васильева, Е.Н. Тищенко, Е.Ю. Шкаранда, В.В. Меньших И.В. Бондарь и другими.

Объектом исследования является процесс определения УБИ в ИСПДн.

Предметом исследования являются методики и алгоритмы выбора активов, установления границ ИС, выбора уязвимостей ПО, определения нарушителей ИБ и УБИ.

Целью исследования является сокращение временных затрат на подготовку перечня актуальных УБИ в ИСПДн.

Для достижения поставленной цели решались следующие **задачи исследования**:

1. Выбор подхода к определению активов ИСПДн и построению связи с уязвимостями ПО;
2. Разработка способа количественной оценки потенциала нарушителей ИБ и установить связь между нарушителем ИБ и уязвимостями ПО;
3. Разработка способа выбора уязвимостей ПО, которые могут быть реализованы нарушителем ИБ;
4. Разработка способа выбора типа актуальных УБИ для установления уровня защищенности ИСПДн.
5. Разработка способа определения актуальности УБИ в ИСПДн.

Научная задача заключается в разработке методики определения актуальности УБИ в ИСПДн, позволяющей уменьшить нагрузку на персонал и сократить временные затраты на разработку перечня актуальных УБИ в ИСПДн.

Научная новизна результатов исследования заключается;

– в использовании параметров вектора уязвимости ПО из методики оценки уязвимостей ПО для количественной оценки потенциала нарушителя ИБ и его возможностей. А также для определения типа актуальных УБИ в ИСПДн;

– в применении математического аппарата искусственных нейронных сетей для определения актуальности УБИ в ИСПДн.

Теоретическую значимость исследования составляют алгоритмы определения потенциала нарушителя ИБ, взаимосвязь между потенциалом нарушителя ИБ и уязвимостями ПО, а также алгоритм определения типа актуальных УБИ в ИСПДн.

Практическая значимость. Результаты диссертационной работы могут быть применены при разработке моделей УБИ в ИСПДн в организациях и предприятиях независимо от их организационно-правовой формы.

Методы и методология исследования. Для решения поставленных задач были использованы: метод анализа иерархий, метод экспертных оценок, математический аппарат искусственных нейронных сетей. Научная работа разработана с использованием: литературных источников в предметной области, алгоритмов, продукционной модели, диаграмм потоков данных, языка программирования «PHP», реляционных баз данных (далее – БД) и ПО «Matlab».

Положения, выносимые на защиту:

1. Способ количественной оценки потенциала нарушителя ИБ в ИСПДн.
2. Алгоритм выбора уязвимостей ПО, которые могут быть реализованы нарушителем ИБ с заданным потенциалом.
3. Способ определения типа актуальных УБИ в ИСПДн.
4. Алгоритм определения актуальных УБИ в ИСПДн.

Достоверность и обоснованность научных положений подтверждается использованием метода анализа иерархий, метода экспертных оценок и применением математического аппарата ИНС. Научная работа разработана с использованием: литературных источников в предметной области, алгоритмов, продукционной модели, диаграмм потоков данных, языка программирования «PHP», реляционных баз данных (далее – БД) и ПО «Matlab».

Апробация результатов диссертации. Результаты работы были представлены на обсуждение в рамках выступления в Губернаторском конкурсе молодежных инновационных проектов «Премия IQ года» в 2017 г. (3 место в номинации «Лучший инновационный проект в сфере компьютерных технологий и телекоммуникаций»), в рамках менторской сессии «Road Show» Start-Up tour 2016 г., проект БД и модель ЭС был представлен на выступлении «УМНИК» в 2015 г. (1 место по направлению – «Н1. Цифровые технологии»), тезисы работы также были представлены на IV Международной конференции «Автоматизированные информационные и электроэнергетические системы», проходящей на базе ФГБОУ ВО «КубГТУ» в 2016 г.

Публикация результатов работы. По теме научной работы опубликовано 12 печатных работ, в том числе 9 публикаций в ведущих

рецензируемых научных изданиях, рекомендованных ВАК при Минобрнауки России, 1 публикация в научном издании, входящем в международную базу цитирования «SCOPUS», 1 публикация в трудах научных конференций, а также 1 свидетельство о государственной регистрации программы для ЭВМ.

Работа выполнена в соответствии с пунктами паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность по техническим наукам:

– п. 3 «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса»;

– п. 7 «Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения».

Структура и объем диссертации. Диссертация включают в себя введение, четыре главы, выводы по каждой главе, заключение, список используемой литературы и приложений. Диссертационная работа изложена на 156 страницах основного текста, содержит 35 рисунка, 74 таблицы, 9 приложений. В список используемой литературы включено 70 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность исследуемой темы, оценена степень ее научной разработанности, определены объект и предмет исследования, изложены его цели и задачи, дана характеристика теоретических и методологических основ, охарактеризована эмпирическая база исследования, сформулированы основные положения, выносимые на защиту, выявлена теоретическая и практическая значимость работы, изложены основные результаты исследования, их научная новизна и апробация ключевых положений исследования.

В первой главе диссертационной работы была рассмотрена методическая база и основные нормативные документы, регламентирующие процесс моделирования УБИ и обеспечение ИБ в ИСПДн.

Определена зависимость характеристик ИСПДн и их влияние на уровень защищенности ИСПДн

Перечислены основные виды нарушителей ИБ в ИСПДн и их возможности.

Проанализирована международная практика управления рисками ИБ на основе общепринятых стандартов.

Проведено сравнение и установлена взаимосвязь существующих международных методик с отечественной нормативной базой в области ИБ.

Во второй главе разработана авторская методика определения актуальных УБИ в ИСПДн. Предложен подход к определению активов в ИСПДн и выбраны параметры, применяемые для подготовки перечня уязвимостей ПО:

- наименование ПО;
- тип ПО;
- версия ПО.

На основании метода анализа иерархий проведена оптимизация перечня нарушителей ИБ с организацией взаимосвязи их возможностей с потенциалом, пример иерархической модели для отдельных категорий внутренних нарушителей ИБ представлен ниже (рисунок 1).

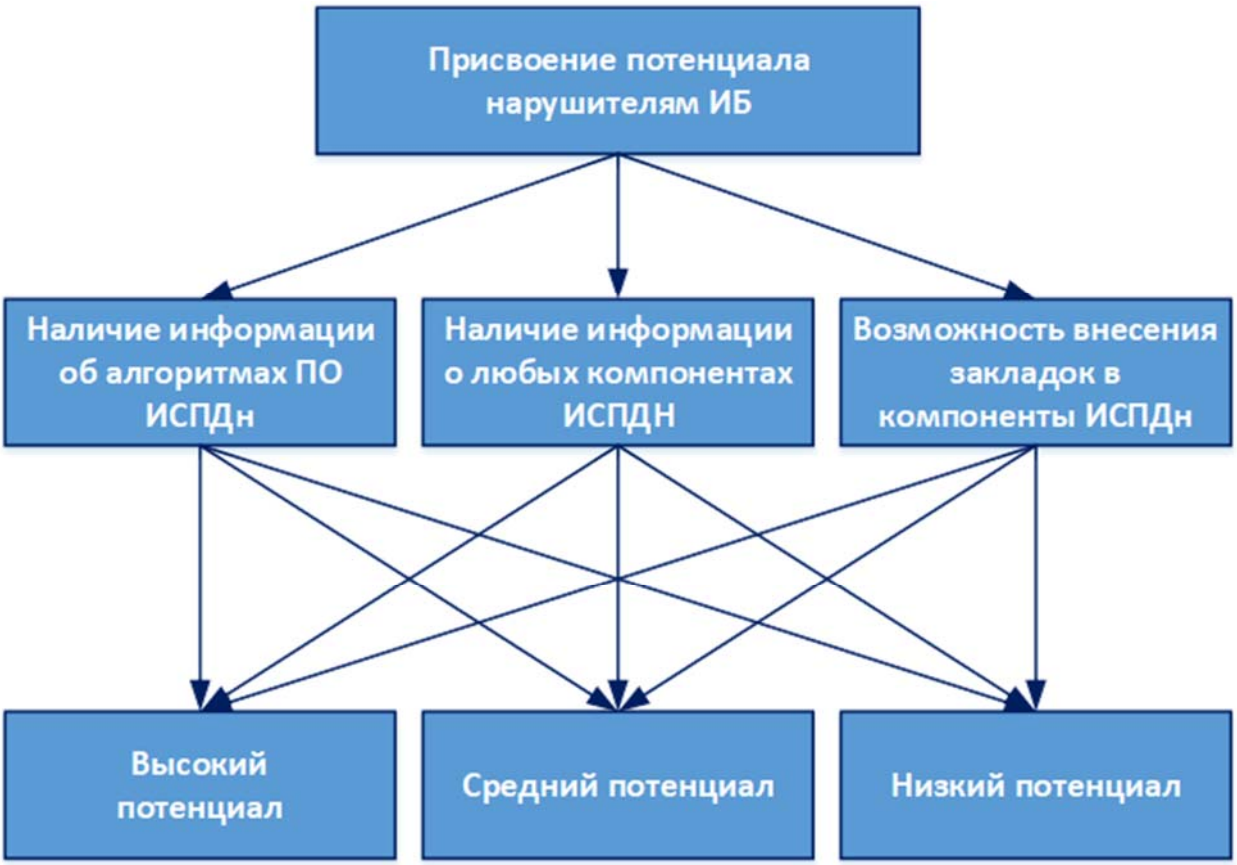


Рисунок 1 – Иерархическая модель отдельных категорий внутренних нарушителей ИБ

На основании построенных матриц весов альтернатив по формуле ниже:

$$A = (z_{ij}) * (y_j), \quad (1)$$

где z_{ij} – весовой коэффициент альтернативы i по j критерию, y_j – весовой коэффициент критерия, было произведено сравнение нарушителей ИБ и подготовлен их унифицированный перечень (рисунок 2).

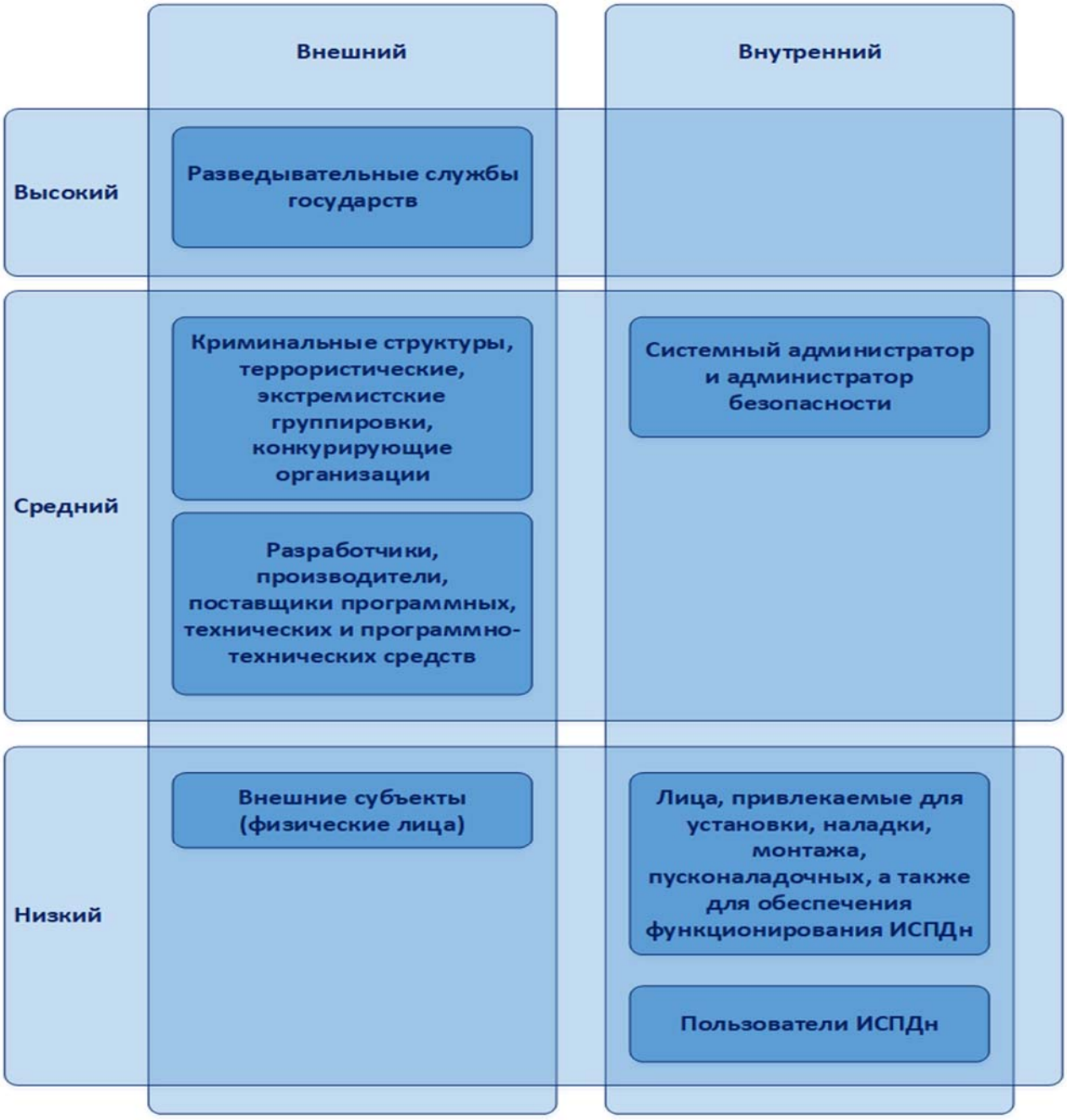


Рисунок 2 – Перечень унифицированных нарушителей ИБ

Аналогичным способом, с использованием метода анализа иерархий были спроецированы параметры метрик уязвимостей ПО на возможности нарушителей ИБ (таблица 1).

Поверка присвоенного потенциала нарушителя ИБ проведена путем вычисления среднеарифметического значения от суммы параметров метрик нарушителя по формуле:

$$P = (AV + UI + RC + AC)/4. \quad (1)$$

Таблица 1 – Метрики, присвоенные потенциалу нарушителя ИБ

Наименование метрики	**Параметры потенциала**	**Метрика**	**Числовое значение**
Возможности физического доступа к активу:	Возможность доступа к ИС	Attack Vector (AV)	
Через сети общего доступа		Network (N)	7
С помощью локально-вычислительной сети		Adjacent Network (A)	4
Физический доступ		Physical (P)	1
Необходимость взаимодействия с пользователем	Знание проекта и информационной системы	User Interaction (UI)	
Необходимо		Required ®	1
Нет необходимости		None (N)	7
Наличие информации об уязвимости в общем доступе	Техническая компетентность нарушителя	Report Confidence (RC)	
Отсутствует описание		Unknown (U)	7
Частично описана		Reasonable ®	4
Полностью описана		Confirmed (C)	1
Возможность применения специальных средств для эксплуатации уязвимости	Оснащенность нарушителя	Attack Complexity (AC)	
Применение специальных средств		High (H)	7
Специальных средства не применяются		Low (L)	1

Результаты проверки представлен в таблице 2 и полностью совпадает с числовой шкалой, принятой при расчете вектора уязвимости ПО CVSS.

Таблица 2 – Вектор потенциала нарушителя ИБ

Нарушитель ИБ	**Потенциал**	**Вектор метрик**	**Оценка**
Разведывательные службы государств	Высокий	AV:N/UI:N/RC:U/AC:H	7
Криминальные структуры, террористические, экстремистские группировки, конкурирующие организации	Средний	AV:N/UI:R/RC:R/AC:H	4,7
Системны администратор и администратор безопасности	Средний	AV:A/UI:N/RC:R/AC:L	4,7
Разработчики, поставщики СВТ, лица, сопровождающие и обеспечивающие ремонт СВТ ИСПДн	Средний	AV:P/UI:N/RC:U/AC:L	4
Лица, привлекаемые для установки, наладки, монтажа СВТ ИСПДн	Низкий	AV:P/UI:R/RC:C/AC:L	1
Пользователи ИСПДн	Низкий	AV:P/UI:R/RC:C/AC:L	1
Внешние субъекты (физические лица)	Низкий	AV:N/UI:R/RC:C/AC:L	2,5

Подготовлены параметры для построения взаимосвязи между активом ИСПДн, уязвимостью ПО и нарушителем ИБ:

– наименование ПО;

– тип ПО;

– версия ПО;

– вектор уязвимости (Attack Vector; User Interaction; Report Confidence; Attack Complexity).

Разработаны продукционные правила для определения актуальных уязвимостей ПО, которые могут быть реализованы выбранным нарушителем ИБ с заданным потенциалом, на основе конструкции «ЕСЛИ-ТО»:

$$R = < A_1, A_2, \dots\dots, A_n : B >. \quad (2)$$

Формализация правила выглядит следующим образом:

– Actual_Vulnerability: если «AV_уязвимости_актива» <= «AV_нарушителя_ИБ» и «UI_уязвимости_актива» <= «UI_нарушителя_ИБ» и «RC_уязвимости_актива» <= «RC_нарушителя_ИБ» и «AC_уязвимости_актива» <= «AC_нарушителя_ИБ», то «Уязвимость_№» = «Актуальная_уязвимость».

– No_Actual_Vulnerability: если «AV_уязвимости_актива» > «AV_нарушителя_ИБ» или «UI_уязвимости_актива» > «UI_нарушителя_ИБ» или «RC_уязвимости_актива» > «RC_нарушителя_ИБ» или «AC_уязвимости_актива» > «AC_нарушителя_ИБ», то «Уязвимость_№» = «Не_Актуальная_уязвимость».

Установлен параметр наличия не декларируемой возможности (далее – НДВ) в активе ИСПДн путем проецирования параметра временной метрикой

вектора уязвимости ПО «RC» (Наличие информации об уязвимости в общем доступе).

Для вычисления типа актуальных УБИ установлена необходимость следующих параметров для актива ИСПДн:

– тип ПО (СПО, ППО);

– временная метрика RC, с параметрами «C» (уязвимость подтверждена производителем ПО), либо «R» (имеется детализированный отчет).

Организации взаимосвязи данной метрики с типом актуальных УБИ позволяет более детализированного и точно определять уровень защищенности ИСПДн, вследствие чего увеличивается обоснованность выбора защитных мер.

Формализованные продукционные правила представлены ниже:

– Actual_Threat_type_1: если «Тип_ПО» = «СПО» и «RC» = «C» или «RC» = «R», то «Тип_актуальных_угроз» = «1»;

– Actual_Threat_type_2: если «Тип_ПО» = «ППО» и «RC» = «C» или «RC» = «R», то «Тип_актуальных_угроз» = «2»;

– Actual_Threat_type_3: если «Тип_ПО» = «ППО» или «СПО» и «RC» НЕ «C» или «R», то «Тип_актуальных_угроз» = «3».

Построена взаимосвязь уязвимостей ПО, имеющих идентификатор «CVE ID», в ИСПДн с группами уязвимостей «CWE», включающими в себя данные идентификаторы.

Подготовлен перечень функциональных характеристики ИСПДн и установлено влияние данных показателей на определение уровня исходной защищенности ИСПДн.

Выбран алгоритм оценки влияния угрозы ИБ на свойства защищенности информации. При выборе угрозы ИБ на основе уязвимости ПО, угрозе ИБ присваиваются показатели нарушения свойств безопасности уязвимостью ПО, посредством которой реализуется данная угроза ИБ. В соответствии с градацией CWE для нарушения свойств защищенности информации в векторе уязвимости ПО используются следующие значения метрик:

– none (0);

– medium (1);

– high (2).

Формализованные продукционные правила определения степени возможного ущерба ИБ представлены ниже:

– High_possible_damage: Если «CI» = 2 или «II» = 2 или «AI» = 2, то «Степень_возможного_ущерба» = «Высокая».

– Medium_possible_damage: Если 2 > «CI» > 1 или 2 > «II»> 1 или 2 > «AI» > 1, то «Степень_возможного_ущерба» = «Средняя».

– Low_possible_damage: Если «CI» < 1 или «II» < 1 или «AI» < 1, то «Степень_возможного_ущерба» = «Низкая»,

Где, CI – нарушение конфиденциальности, II – нарушение целостности, AI – нарушение доступности.

На основании предложенных алгоритмов разработана методика определения актуальных УБИ (рисунок 3).

Рисунок 3 – Методика определения актуальных УБИ.

В третьей главе приведено описание математического аппарата искусственной нейронной сети (далее – ИНС) для определения актуальных угроз безопасности информации. Проведен анализ и выбор типа и архитектуры ИНС (таблица 3).

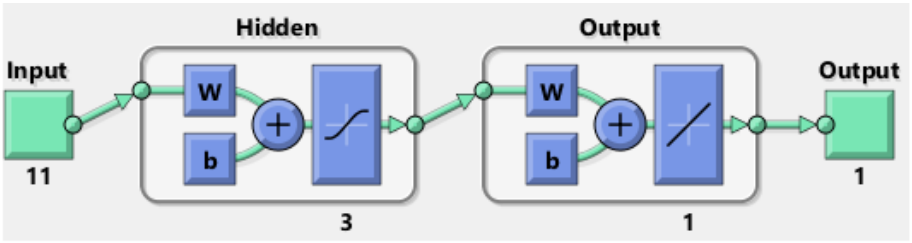
Таблица 3 – Сравнительный анализ сети радиального базиса и многослойного персептрона

Критерий сравнения	**Многослойный персептрон**	**Сеть радиального базиса**
Участие в аппроксимации	Все нейроны	Только ближайшие
Чувствительность к размерности входных данных	Выражается в росте сложности обучения	Выражается в росте размеров сети
Число скрытых слоев	Несколько	Один
Вид функции активации	Различные: сигмоида, гиперболический тангенс, биполярная сигмоида	Гауссова функция
Обучение слоев	Одновременное	Раздельное

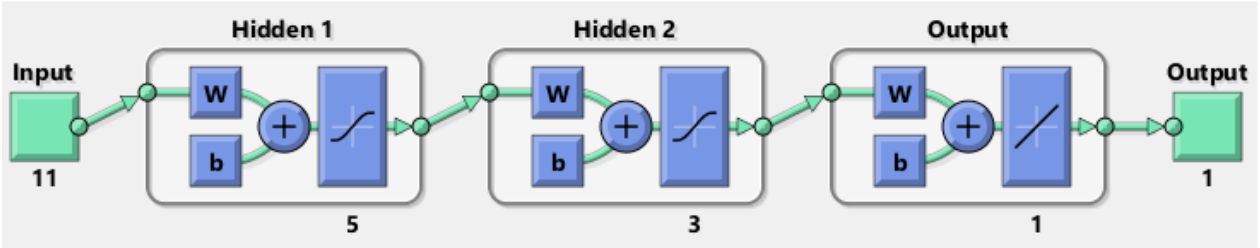
По результатам анализа, в связи с простотой построения, а также неизменностью количества ИН для решения задачи по определению актуальности УБИ принято решение использовать многослойный персептрон.

Для сравнения и выбора топологии ИНС применен принцип упрощения нейронной сети. Разработаны две ИНС, первая с учетом общепринятого для решения задач оценки УБИ количества скрытых слоев ИНС, имеющая 2 скрытых слоя, вторая – с одним скрытым слоем. Количество ИН на каждом слое определяется по эвристическому правилу геометрической пирамиды. Показатели актуальности УБИ, используемые в качестве входных сигналов для ИН входного слоя, включают в себя:

– Архитектуру ИСПДн (А);
– Возможность взаимодействия со сторонними ИСПДн (I_N);
– Возможность взаимодействия с сетями общего пользования (N_W);
– Территориальное размещение ИСПДн (S_{Sq});
– Режим обработки информации в ИСПДн (R_p);
– Разграничение прав доступа (R_{ac});
– Наличие сегментирования ИС (S_{IS})
– Потенциал нарушителя (P_i);
– Показатель нарушения конфиденциальности (CI);
– Показатель нарушения целостности (II);
– Показатель нарушения доступности (AI).



а)



б)

Рисунок 3 – Архитектура ИНС а) с одним скрытым слоем, б) с двумя скрытыми слоями

Сравнение топологий, разработанных ИНС осуществляется средствами приложения nftool модуля «Neural Network Toolbox» ПО Matlab в рамках обучения ИНС с использованием следующих алгоритмов:

– Масштабированный сопряженный градиент (trainscg).

– Обратного распространения Левенберга-Марквардта (trainlm);

– Байесовской регуляризации (trainbr).

Для обучения подготовленная выборка случайным образом разбивается на 3 набора данных:

– Тренировочный сет (70 %) – для обучения, ИНС настраивается на основании полученной на данном этапе ошибкой.

– Подтверждающий сет (15 %) – для остановки обучения, когда обобщение перестает улучшаться.

– Тестовый сет (15 %) – независимый набор данных, используемый для проверки, обученной ИНС.

Сравнение архитектур и обучающих алгоритмов представлено в таблице ниже (Таблица 4).

Таблица 4 – Сравнение обучающих алгоритмов и архитектуры

Кол-во скрытых слоев	**Кол-во ИН на скрытом слое**	**Алгоритм обучения**	**Время, затраченное на обучение, сек.**	**Величина наименьшей ошибки**
2	5, 3	trainscg	0,649	0,0030297
1	3		0,629	0,0016252
2	5, 3	trainlm	0,728	$1{,}1978*10^{-7}$
1	3		0,631	$1{,}0313*10^{-9}$
2	5, 3	trainbr	1,018	0,24129
1	3		0,839	0,24592

Основным критерием выбора архитектуры и алгоритма обучения ИНС является величина ошибки на этапе обучения (рисунок 5).

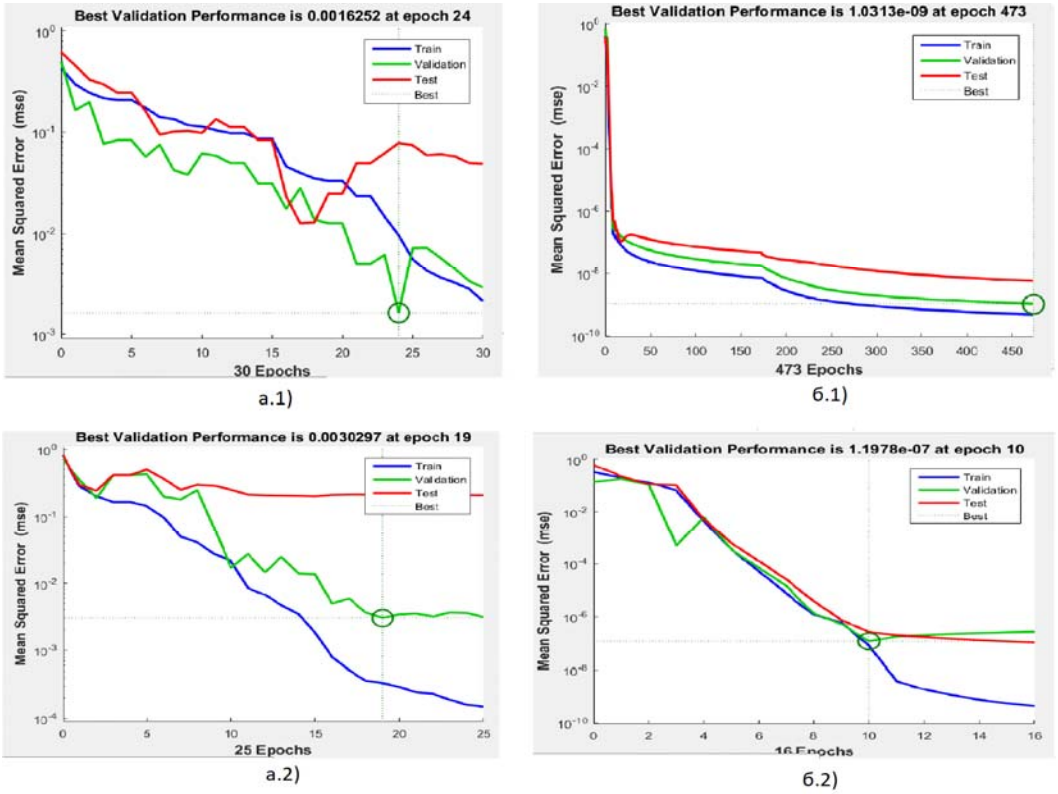


Рисунок 4 – Визуализация вычисления ошибки ИНС: Алгоритм обратного распространения Левенберга-Марквардта: а.1) с одним скрытым слоем; а.2) с двумя скрытыми слоями; Масштабируемый алгоритм сопряженного градиента ИНС: б.1) с одним скрытым слоем; б.2) с двумя скрытыми слоями

На основании принципа упрощения и времени, затраченного на обучение ИНС, для решения задачи определения актуальности УБИ в ИСПДн принято решение применять многослойную ИНС с 1 скрытым слоем, использующую алгоритм обратного распространения Левенберга-Марквардта.

В четвертой главе осуществлялась оценка сокращения временных затрат осуществляется путем сравнения времени затраченного на подготовку перечня актуальных УБИ с применением разработанной методики и существующих методик. Эксперимент с применением методик осуществляется для смоделированной ИСПДн посредством метода экспертных оценок. Опрос экспертов осуществляется в виде анкетирования. Подбор экспертов производится на основании компетентности и заключался в выборе экспертов. По результатам сравнения была подготовлена таблица с основным временем, затрачиваемым на различные этапы определения УБИ согласно рассматриваемым и разработанный методикой (таблица 5).

Полученные в рамках сравнения результаты свидетельствуют о том, что применение разработанной методики, а также перечисленных способа ее автоматизации, позволит существенно сократить временные затраты персонала, задействованного в процессе подготовки перечня УБИ в ИСПДн.

Таблица 5 – Сравнение временных затрат методик определения УБИ

Используемая методика	**Методики определения УБИ**	**Разработанная методика определения УБИ**	**Автоматизированная разработанная методика определения УБИ**
Время, затраченное на выбор показателей ИСПДн (T_x), сек	1380		
Время, затраченное на выбор нарушителей ИБ, составило 15 минут (T_I), сек	900		
Время, затраченное на выбор критичности нарушаемых свойств безопасности информации (T_d), сек	1500		
Время, затраченное на поиск угроз ИБ по заданным критериям фильтрации, (T_s), сек.	5		
Время, затраченное на выделение актуальных угроз ИБ (T_a), сек	1200		
Время, затраченное на выбор вспомогательных активов (T_a), сек		300	120
Время, затраченное на выбор нарушителей ИБ (T_I), сек		420	
Время, затраченное на поиск уязвимостей ПО (T_v), сек		7	
Время, затраченное на выбор актуальных уязвимостей ПО (T_{AV}), сек		60	
Время затраченное на подготовку перечня актуальных угроз ИБ (T_S), сек		2280	
Время затраченное на присвоение количественных значений показателей коэффициента исходной защищенности и потенциалу нарушителя ИБ (T_s) сек			300
Время затраченное на определение актуальности угроз ИБ в ИСПДн (Tnn), сек			1
Общее затраченное время (Т), сек	4995	3427	422

В заключении подводятся основные итоги диссертационного исследования, формулируются основные выводы.

В приложениях представлены листинги скриптов реализации разработанной методики. Так же, приведено 1 свидетельство о государственной регистрации баз данных и 1 свидетельство о государственной регистрации программы для ЭВМ и 3 акта о внедрении результатов научного исследования.

ЗАКЛЮЧЕНИЕ

В диссертационной работе проведены исследования, обеспечивающие сокращение времени определения УБИ в ИСПДн, а также снижения роли эксперта в процессе определения УБИ в ИСПДн. В рамках диссертационной работы получены следующие научные и практические результаты:

– произведен анализ предметной области и сформулированы проблемные вопросы, изучены способы и подходы к выбору уязвимостей ПО, активов ИС, нарушителей ИБ, а также методики определения УБИ в ИС. Выявлены преимущества и недостатки актуальных методик определения УБИ в ИСПДн; выявлены основные проблемы при определении УБИ в ИС: отсутствие связи между активом, нарушителем ИБ и уязвимостью ПО, а также между уязвимостью ПО и УБИ;

– разработана и реализована методика определения актуальности УБИ в ИСПДн, включающая в себя: подход по выбору активов ИСПДн для определения перечня уязвимостей ПО; способ количественной оценки потенциала нарушителя ИБ с использованием параметров оценки уязвимостей ПО; алгоритм выбора уязвимостей ПО, которые могут быть реализованы нарушителем ИБ в ИСПДн; алгоритм выбора типа актуальных УБИ, а также алгоритм определения актуальности УБИ;

– осуществлена автоматизация разработанной методики определения актуальности УБИ с использованием программного средства и математического аппарата ИНС;

– произведены оценка и сравнение временных затрат при использовании разработанной и действующих методики. По результатам сравнения временные затраты на определение актуальности УБИ в ИСПДн при использовании разрабатываемой методики могут быть сокращены более чем в 1,5 раза;

– для получения информации о возможном эффекте от внедрения разработанной методики осуществлена разработка перечней актуальных УБИ в ИС ООО «РН-Учет» в г. Краснодаре, ООО «РН-Краснодарнефтегаз» и ООО «Базовый Авиатопливный Оператор» в г. Краснодаре. Достигнут эффект

сокращения временных затрат специалистов предприятий от использования разработанной методики более чем в 1,4 раза.

Проведенное исследование в области определения актуальных УБИ может значительно сократить временные затраты на определение актуальных УБИ, а также стандартизировать процесс их определения.

СПИСОК РАБОТ ОПУБЛИКОВАНЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях,
рекомендованных ВАК при Минобрнауки России:

1. Жук Р.В., Власенко А.В., Чебанов А.С., Сазонов С.Ю. Методический подход к выбору и разработке моделей оценки эффективности комплексной системы объектов защиты // Известия Юго-Западного государственного университета. – 2012. – № 6 (45). – С. 038-040,
2. Жук Р.В., Власенко А.В., Титенко Е.А. Системы противодействия Инсайдерам // Известия Юго-Западного государственного университета. – 2012. – №6 (45). – С. 30-33;
3. Жук Р.В., Власенко А.В., Титенко Е.А. Классификация информационных систем персональных данных: вчера, сегодня, завтра // Известия Юго-Западного государственного университета. – 2013. – № 1. – С. 87-90,
4. Жук Р.В., Власенко А.В. Модель нарушителя комплексной системы обеспечения информационной безопасности объектов защиты // Известия Юго-Западного государственного университета. – 2013. – № 1. – С. 171-173;
5. Жук Р.В., Власенко А.В., Дзьобан П.И. Защита персональных данных при авторизации пользователя в распределенных информационных системах, построенных на основе Web-технологий // Вестник Адыгейского государственного университета. – 2017. – С. 120-128.
6. А. В. Власенко, П. И. Дзьобан, Р. В. Жук Обзор инструментов машинного обучения и их применения в области кибербезопасности // Прикаспийский журнал: управление и высокие технологии. – 2020. – С.144-155,
7. Жук Р.В., Дзьобан П.И., Власенко А.В. Построение взаимосвязи между нарушителем информационной безопасности и уязвимостями информационных активов в информационных системах обработки персональных данных // Прикаспийский журнал: управление и высокие технологии. – 2020. – С.162-169.
8. Жук Р.В., Дзьобан П.И., Власенко А.В. Определение актуальности угроз информационной безопасности в информационных системах обработки персональных данных с использованием математического аппарата нейронных

сетей // Прикаспийский журнал: управление и высокие технологии. – 2020. – С.169-178.

9. Жук Р.В. Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. – 2021. Т. 7. № 2. – С. 95-101.

Публикации в других изданиях:

10. Жук Р.В., Власенко А.В. Анализ характеристик определения нарушителя при моделировании угроз информационной безопасности в информационных системах персональных данных: науч. тр. КубГТУ. – № 16. – 9-11 сентября 2016 г. – С. 99-104.

11. Roman Zhuk and Alexandra Vlasenko, 2017. Definition of the Method of Determination of the Violator of Information Security in Process of Modeling the Threats of Information Security in the Information Systems of Processing Personal Data. Journal of Engineering and Applied Sciences, 12: 7776-7778.

Свидетельства о государственной регистрации программы для ЭВМ:

12. Жук Р.В., Власенко А.В. Программа определения степени возможности реализации угрозы информационной безопасности в информационных системах персональных данных // Свидетельство о государственной программы для ЭВМ 2018613024. Зарегистрировано в реестре баз данных 11.01.2018 г.

Подписано в печать 29.09.2021. Формат 60×84 1/16.
Печ. л. 1,0. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1