Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский университет науки и технологий»

На правах рукописи

Кучкарова Наиля Вакилевна

ОЦЕНКА АКТУАЛЬНЫХ УГРОЗ И УЯЗВИМОСТЕЙ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ТЕКСТОВ

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, профессор
Васильев Владимир Иванович

Уфа – 2023

ОГЛАВЛЕНИЕ

Введение 4

Глава 1. Анализ современного состояния в области автоматизации процесса оценки и анализа угроз БИ и уязвимостей ПО 11

1.1 Анализ существующих стандартов и нормативной базы в области обеспечения ИБ объектов КИИ 11

1.2 Существующие источники информации об угрозах БИ и уязвимостях ПО объектов КИИ 14

1.3 Методики оценки и анализа угроз БИ и уязвимостей ПО объектов КИИ 20

1.4 Технологии интеллектуального анализа текстов (Text Mining) 26

Анализ методов кластеризации и понижения размерности текстовых данных 35

1.5 Существующие подходы к автоматизации анализа текстовых описаний угроз БИ и уязвимостей ПО 38

1.6 Выводы по первой главе 41

Глава 2. Разработка и исследование алгоритмов автоматической классификации и суммаризации текстов из открытых источников в области ИБ 43

2.1 Общие подходы к решению задачи автоматической классификации и суммаризации 43

2.2 Построение корпуса текстов из открытых источников в области ИБ и векторное представление слов 46

2.3 Шаблон решения задачи классификации и суммаризации текстов с использованием технологии трансформеров 51

2.4 Выводы по второй главе 67

Глава 3. Разработка и исследование алгоритмов оценки угроз и уязвимостей информационной безопасности на основе технологий семантического анализа текстов в соответствии с требованиями Методики ФСТЭК России 69

3.1 Функциональная модель процесса оценки и анализа актуальных угроз безопасности информации в соответствии с Методикой ФСТЭК России..... 69

3.2 Разработка алгоритмов векторизации текстовых описаний угроз, уязвимостей, тактик (техник) и кластеризации угроз БИ и уязвимостей ПО объектов КИИ на основе метрик семантической близости текстовых описаний 74

3.3 Разработка метода и алгоритмов оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объектов КИИ 85

3.4 Построение сценариев реализации актуальных угроз БИ с помощью технологии трансформеров..... 92

3.5 Выводы по третьей главе..... 109

Глава 4. Разработка и применение исследовательского прототипа интеллектуальной системы поддержки принятия решений при оценке и анализе актуальных угроз БИ и уязвимостей ПО 111

4.1 Архитектура исследовательского прототипа ИСППР 111

4.2 Результаты применения ИСППР при решении задачи оценки и анализа актуальных угроз БИ АСУ ТП пункта приема, хранения и отпуска товарной нефти 124

4.3 Выводы по четвертой главе..... 144

ЗАКЛЮЧЕНИЕ 147

Список сокращений и условных обозначений..... 149

Список литературы 151

Приложение А. Акты о внедрении научных результатов..... 171

Приложение Б. Методика оценки актуальных угроз ИБ объектов АСУ ТП КИИ 177

Приложение В. Фрагмент модели угроз КИИ..... 181

Введение

Актуальность темы исследования. Масштабная цифровизация различных сфер экономики, связанная с активным развитием информационных технологий и переход на удаленный формат работы, вызванный пандемией коронавирусной инфекции в 2019 – 2021 гг., спровоцировали резкий рост активности киберпреступников. Чаще всего компьютерным атакам подвергаются предприятия, относящиеся к государственной, медицинской и промышленной отрасли и, как правило, являющиеся объектами критической информационной инфраструктуры (КИИ). Большую группу объектов КИИ составляют промышленные автоматизированные системы управления технологическими процессами (АСУ ТП). Обеспечение безопасности объектов КИИ стало, в соответствии с Доктриной информационной безопасности Российской Федерации, одним из приоритетных направлений в области информационной безопасности (ИБ). Требования к обеспечению ИБ закреплены в ряде нормативно-правовых документов, принятых в России в последние годы, таких как: Федеральный закон «О безопасности критической информационной инфраструктуры» №187-ФЗ (2017 г.), Приказы ФСТЭК России №№ 31 (2014 г.), 235 и 239 (2017 г.), «Методика оценки угроз безопасности информации» ФСТЭК России от 5 февраля 2021 г. Согласно последней Методике, одним из этапов оценки угроз безопасности информации (БИ) является оценка возможности реализации угроз БИ и определение их актуальности. Реализация данного этапа связана с необходимостью определения источников угроз, т.е. актуальных нарушителей, а также сценариев атак. В свою очередь, определение сценариев атак предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей посредством эксплуатации уязвимостей.

Вместе с тем, на практике при решении данной задачи специалисты по ИБ встречаются с необходимостью обращения к огромным массивам текстовых

описаний компонентов (угроз, уязвимостей, тактик, техник), размещенных в открытых базах данных (БД). Так, на момент проведения исследования только Банк данных угроз безопасности информации (БДУ) ФСТЭК России содержал текстовые описания более 220 угроз, свыше 36 500 уязвимостей, 10 тактик и от 7 до 29 соответствующих им техник. Работа с указанными БД предполагает поиск и анализ угроз и уязвимостей в «ручном» режиме, что требует больших временных затрат и сопровождается ошибками обработки, обусловленными человеческим фактором, в связи с чем закономерно желание специалистов по ИБ автоматизировать процесс сопоставления угроз, уязвимостей, тактик и техник их эксплуатации. Однако существующие на данный момент разработки в области автоматизации процесса оценки угроз БИ не учитывают в полной мере требований Методики относительно определения сценариев атак. В известных работах отсутствует возможность выявления соответствия между такими компонентами сценария атаки, как угрозы, уязвимости, тактики (техники). Как правило, происходит сопоставление только двух компонентов: уязвимости и сопутствующие им угрозы. В связи с этим тема диссертационной работы, посвященная вопросам автоматизации оценки и приоритизации актуальных угроз, уязвимостей, тактик (техник) и построения сценариев возможных атак с использованием методов интеллектуального анализа текстов, является актуальной.

Степень разработанности темы исследования. В настоящее время в данной предметной области ведутся активные исследования, о чем свидетельствуют работы ряда отечественных и зарубежных ученых: Аникина И.В., Бондарчука Д.В, Болодуриной И.П., Васильева В.И., Вульфина А.М., Жук Р.В, Зегжды П.Д., Катасёва А.С., Котенко И.В., Лаврентьева А.М., Макарян А.С., Машкиной И.В., Остапенко А.Г., Петренко В.И., Рагозина А.И., Рябова Д.М., Селифанова В.В., Сычугова А.А., Тебуева Ф.Б., Alfaycz F., de Boer M.H., Hemberg E., Lee Y., Liu Z.Q., Mendsaikhan O., Noel S., Shin S., Smyth V., Xiao H., Zhang J.Y. и др.

Анализ результатов проведенных исследований показал, что при всей их значимости, проблема оценки и анализа актуальных угроз БИ и уязвимостей ПО

объектов КИИ нуждается в дальнейшей проработке. Существующие подходы ориентированы в основном на установление связей между выявленными уязвимостями ПО и соответствующими им угрозами БИ, оценку степени опасности этих уязвимостей, необходимость использования для этих целей различных источников информации, и в первую очередь, открытых текстовых БД, регулярно пополняемых новыми данными об угрозах и уязвимостях. Вместе с тем, сегодня остаются открытыми вопросы комплексной оценки угроз БИ, уязвимостей ПО, тактик и техник их использования, построения сценариев реализации атак на объекты КИИ, а также задачи автоматизации соответствующих процедур, решение которых позволило бы значительно снизить трудоемкость обработки текстовых данных, используемых на этом этапе, повысить достоверность и оперативность принимаемых решений в процессе оценки рисков ИБ и уровня защищенности объектов КИИ.

Объектом исследования в диссертационной работе являются объекты критической информационной инфраструктуры (КИИ).

Предметом исследования являются методы и алгоритмы оценки актуальных угроз безопасности информации и уязвимостей ПО объектов КИИ.

Целью диссертационной работы является повышение достоверности и оперативности оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ на основе открытых баз данных и технологий интеллектуального анализа текстов (Text Mining).

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

1. Анализ современного состояния в области автоматизации процесса оценки и анализа актуальных угроз БИ и уязвимостей ПО объектов КИИ.

2. Разработка алгоритмов автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области информационной безопасности.

3. Разработка метода и алгоритма оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО АСУ ТП с использованием технологии

семантического анализа текстов.

4. Разработка алгоритма построения графовой модели сценария реализации угроз БИ на основе алгоритмов векторного вложения и технологии трансформеров.

5. Разработка архитектуры и ПО исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) в процессе оценки угроз БИ и уязвимостей ПО объектов КИИ, исследование эффективности ее применения при решении практических прикладных задач.

Научная новизна

1. Разработаны алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ, основанные на совместном применении алгоритмов кластеризации и извлечения признаков в виде векторов вложений, отличающиеся от известных алгоритмов возможностью осуществлять автоматизированную предобработку больших корпусов слабоструктурированных русскоязычных текстов и их последующий семантический анализ в соответствии с поставленной задачей выделения тематических направлений текстов и их автоматического реферирования на основе технологий трансформеров.

2. Разработаны метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов, отличающиеся использованием предложенного алгоритма кластеризации и оценки семантической близости текстовых описаний угроз БИ и уязвимостей ПО в многомерном векторном пространстве, применение которых позволяет сделать более содержательной работу эксперта, сократив время на поиск актуальных угроз БИ, обеспечивая при этом более высокую наглядность, полноту и достоверность результатов такого поиска.

3. Разработан алгоритм построения графовой модели сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, отличающийся использованием алгоритмов векторного вложения и

технологии трансформеров, что позволяет автоматизировать процесс построения графовой модели, снизить трудоемкость и когнитивную нагрузку на специалистов по ИБ, предоставляя им дополнительную информацию для формирования перечня актуальных угроз и уязвимостей объектов КИИ.

4. Предложены архитектура и состав программных модулей ИСППР, реализующих предложенные в работе метод и алгоритмы, применение которых позволяет снизить временные затраты и повысить достоверность решений, принимаемых специалистом по ИБ при оценке и анализе актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Практическая значимость

Практическая значимость полученных результатов заключается в разработке алгоритмов автоматической классификации и суммаризации специализированных текстов в области ИБ, метода и алгоритмов оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО объектов КИИ, архитектуры и программных модулей исследовательского прототипа ИСППР, применение которых позволяет сократить на 40-50 % временные затраты, повысить достоверность и объективность оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ и обеспечить в конечном итоге более обоснованный выбор организационных и технических мер, направленных на обеспечение нормативных требований к защищенности объектов КИИ.

Методы и методология исследования. Для решения поставленных в работе задач были использованы методы интеллектуального анализа данных и защиты информации, методы экспертных оценок, теории искусственных нейронных сетей, методология функционального моделирования (IDEF0), методы объектно-ориентированного анализа и проектирования, модели теории графов, методы имитационного моделирования.

Положения, выносимые на защиту:

1. Алгоритмы автоматической классификации и суммаризации специализированных текстов в области ИБ на основе технологий автоматизированной обработки слабоструктурированных текстовых данных.

2. Метод и алгоритм оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО объектов КИИ с использованием технологии семантического анализа текстов.

3. Алгоритм построения графовой модели сценария реализации угроз БИ с использованием алгоритмов векторного вложения и технологии трансформеров.

4. Архитектура и программная реализация модулей исследовательского прототипа ИСППР, предназначенной для оценки и приоритизации актуальных угроз БИ и уязвимостей ПО объектов КИИ, а также результаты ее применения при решении ряда практических прикладных задач.

Достоверность и обоснованность научных положений и выводов, полученных в диссертационной работе, подтверждается корректной постановкой задач, применением известных технологий и методов, успешно используемых в других прикладных областях, апробацией разработанного метода, алгоритмов и исследовательского прототипа ИСППР при решении практических прикладных задач.

Апробация результатов диссертации. Результаты работы были представлены на обсуждение на следующих конференциях: Международная научная конференция «Безопасность: информация, техника, управление» (Санкт-Петербург, 2018 г.); Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых «Безопасность информационного пространства» (г. Уфа, 2019 г.); XVIII Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых «Безопасность информационного пространства» (г. Магнитогорск, 2019 г.); VII Всероссийская научная конференция «Информационные технологии интеллектуальной поддержки принятия решений» (г. Уфа, 2019 г.); Всероссийская молодежная научная конференция «Мавлютовские чтения» (г. Уфа, 2020 г.); IV Всероссийская молодежная научно-практическая конференция с международным участием «Информационные технологии обеспечения комплексной безопасности в цифровом обществе» (г. Уфа, 2021 г.); XXVIII международная научно-практическая конференция «Приоритетные направления развития науки и технологий» (г. Тула, 2021 г.); Межвузовская

научная школа-семинар «Современные тенденции развития методов и технологий защиты информации» (Москва, 2022 г.).

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют следующим пунктам паспорта научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»:

п.1 «Теория и методология обеспечения информационной безопасности и защиты информации»;

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

п.8 «Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения»;

п.15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Публикация результатов работы. Основные результаты диссертации опубликованы в 14 работах, в том числе в 4 статьях в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, в 8 статьях в других изданиях. Получено 2 свидетельства о государственной регистрации программ для ЭВМ.

Структура и объем диссертации. Диссертация включает в себя введение, четыре главы, заключение, список используемой литературы и приложения. Основной текст работы изложен на 170 страницах, содержит 58 рисунков, 32 таблицы, 3 приложения. В список используемой литературы включено 159 наименований.

Глава 1. Анализ современного состояния в области автоматизации процесса оценки и анализа угроз БИ и уязвимостей ПО

В данной главе дается краткий анализ нормативно-правовой базы в области обеспечения ИБ объектов КИИ, обзор общедоступных баз данных, содержащих текстовые описания угроз БИ и уязвимостей ПО этих объектов. Рассмотрены существующие подходы к автоматизации процесса оценки и анализа текстовых описаний угроз БИ и уязвимостей ПО, сделаны выводы об актуальности проводимого исследования.

1.1 Анализ существующих стандартов и нормативной базы в области обеспечения ИБ объектов КИИ

Последние десятилетия характеризуются масштабной цифровизацией, связанной с активным внедрением новых информационных технологий (IT) во все отрасли экономики [35], расширением сферы Интернета вещей (IoT) [67] и промышленного Интернета вещей (IIoT). Цифровизация напрямую затронула и объекты КИИ, к которым, в частности, относятся АСУ ТП промышленных объектов [65]. В начале прошлого столетия АСУ ТП представляли собой автономные управляющие системы. Однако с приходом нового тысячелетия АСУ ТП преобразовались в развитые промышленные сетевые комплексы, функционирующие на базе стандартных сетевых протоколов, схожих с используемыми в корпоративных сетях. Соответственно, АСУ ТП, как и другие классы объектов КИИ, приобрели уязвимости, характерные для корпоративных сетей [64, 79]. По данным авторитетных источников [15,50], количество кибератак на объекты КИИ в последние годы резко возросло. Атаки на промышленные объекты КИИ способны нанести ущерб устойчивому функционированию предприятия, привести к крупным финансовым и имиджевым потерям, вызвать экологическую катастрофу, причинить ущерб жизни и здоровью граждан.

Обеспечение безопасности объектов КИИ требует комплексного подхода, учитывающего особенности промышленных систем, основанного на требованиях и рекомендациях международных стандартов и российских нормативных документов по обеспечению их ИБ [27, 45, 48].

Федеральный закон № 187-ФЗ [14] от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации». К объектам КИИ, в соответствии с данным законом, относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. В законе определяются основные требования к категорированию объектов КИИ, обеспечению безопасности значимых объектов (ЗО) КИИ, вводится государственный контроль в области обеспечения безопасности ЗО КИИ.

На основании закона № 187-ФЗ разработан **Приказ ФСТЭК России № 235** [10] от 21 декабря 2017 г. «Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». В этом приказе определяются требования, предъявляемые к:

– силам обеспечения безопасности ЗО КИИ;
– программным и программно-аппаратным средствам, применяемым для обеспечения безопасности ЗО КИИ;
– организационно-распорядительным документам по безопасности ЗО;
– функционированию системы безопасности в части организации работ по обеспечению безопасности ЗО.

В числе требований к силам обеспечения безопасности ЗО КИИ указана необходимость проведения анализа угроз БИ в отношении ЗО КИИ и выявление уязвимостей в них.

Уточнение требований, введенных федеральным законом № 187, описано в Приказе ФСТЭК России № 239.

Приказ ФСТЭК России № 239 [12] от 25 декабря 2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Действие данного приказа распространяется на информационные системы (ИС), автоматизированные системы управления (АСУ), информационно-телекоммуникационные сети, которые отнесены к значимым объектам КИИ. Документ устанавливает требования к обеспечению безопасности ЗО, устанавливает правила к разработке организационных и технических мер по обеспечению безопасности ЗО, включая анализ угроз БИ и выявление уязвимостей программных и программно-аппаратных средств ЗО, описание возможных сценариев реализации угроз БИ. Этот документ содержит также требования по внедрению организационных и технических мер по обеспечению безопасности ЗО, вводу его в действие и обеспечению безопасности ЗО при вводе и выводе его из эксплуатации. Приводится состав мер по обеспечению безопасности для ЗО соответствующей категории значимости.

Серия стандартов ISA/IEC 62443 была разработана техническим комитетом ISA99 в качестве американского национального стандарта и затем принята международной электротехнической комиссией (IEC) для использования по всему миру. Первые **национальные стандарты серии 62443/56205 («Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы». Части 1-1, 2-1, 3-3)** [1, 2, 6] введены на территории Российской Федерации в 2016 году. В настоящий момент переведено и принято 3 документа из этой серии. Данные стандарты представляют собой гибкий шаблон для исправления существующих и будущих уязвимостей в промышленных АСУ ТП. В основе предложенной концепции используется разбиение защищаемого объекта на зоны безопасности (в зависимости от уровня безопасности, который необходимо обеспечить), обеспечение эшелонированной защиты и риск-ориентированный подход к обеспечению ИБ.

Приказ ФСТЭК России №31 [11] от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически

важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». В документе изложены требования к организации защиты информации в АСУ, в соответствии с которыми АСУ ТП, как правило, имеет 3-уровневую структуру, однако количество уровней может меняться и зависит от назначения АСУ и выполняемых ею целевых функций. В документе указан порядок определения угроз БИ, который осуществляется на каждом из уровней АСУ и должен включать: выявление источников угроз (нарушителей), анализ нарушителей, анализ возможных уязвимостей ПО АСУ ТП, определение сценариев реализации угроз БИ.

По результатам проведенного анализа нормативной базы в области обеспечения ИБ промышленных объектов КИИ можно сделать вывод о существенном её развитии в последнее десятилетие. В описанных выше документах устанавливаются термины и определения в области обеспечения ИБ объектов КИИ, рассмотрены общие требования к уровню защищенности этих объектов, организационные и технические меры, направленные на реализацию данных требований. Подчеркивается необходимость оценки и анализа актуальных угроз БИ и уязвимостей ПО объектов КИИ, моделирования сценариев реализации угроз БИ с целью оценки возможных последствий от их реализации посредством эксплуатации существующих уязвимостей.

1.2 Существующие источники информации об угрозах БИ и уязвимостях ПО объектов КИИ

Согласно [3] угроза БИ – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения БИ.

В соответствии с Методикой ФСТЭК (Разд. 5.3.3): «Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способы реализации угрозы

безопасности информации, а реализация угрозы может привести к негативным последствиям:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].»

Уязвимость [4] – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(-ая) может быть использован(-а) для реализации угроз БИ.

Существуют различные системы классификации угроз БИ и уязвимостей ПО. Так по аспекту ИБ, угрозы делятся на угрозы конфиденциальности, целостности и доступности, по степени воздействия на ИС на активные и пассивные и др.

Уязвимости ПО также можно классифицировать по различным признакам. Уязвимости ИС по области происхождения подразделяются на следующие классы: уязвимости кода, конфигурации, архитектуры, организационные уязвимости, многофакторные уязвимости; по месту возникновения (проявления) подразделяются на следующие: уязвимости в общесистемном ПО, прикладном ПО, в специальном ПО, технических средствах, сетевом оборудовании и др. [4, 29].

В работе [47] предложен вариант классификации уязвимостей по уровням структуры АСУ ТП в соответствии с Приказом ФСТЭК России №31 и ГОСТ Р МЭК 62443-1-1 (Рисунок 1.1). На каждом уровне структуры АСУ ТП существует определенное оборудование, для которого характерны те или иные уязвимости. Например, для диспетчерского уровня характерны уязвимости системного и прикладного ПО, для уровня автоматического управления и ввода/вывода данных исполнительных устройств – уязвимости аппаратного обеспечения и прикладного ПО, для уровня трактов (по ГОСТ Р МЭК 62443-1-1) – уязвимости протоколов взаимодействия.

Рисунок 1.1 – Классификация уязвимостей по уровням структуры АСУ ТП

Примеры описаний уязвимостей представленных в БДУ ФСТЭК для программируемых логических контроллеров (ПЛК) и SCADA-систем представлены на Рисунках 1.2, 1.3.

ГОСТ Р [3] 56545-2015 устанавливает правила описания уязвимостей. В документе вводится понятие «Паспорт уязвимости», которое предполагает наличие следующих элементов описания уязвимостей: идентификатор, наименование, класс уязвимости, наименование ПО и его версия, служба (порт), которая (который) используется для функционирования ПО, язык программирования ПО, тип недостатка и др.

В последнее время в области ИБ прочное место заняли такие понятия, как Threat Intelligence и Vulnerability Intelligence [59, 101, 154, 157]. – это систематизированные и знания об угрозах БИ, уязвимостях ПО и способах их реализации, группировках киберпреступников, рекомендации о стратегии защиты

BDU:2023-00228: Уязвимость микропрограммного обеспечения программируемых логических контроллеров Schneider Electric, связанная с недоста необычных или исключительных состояний, позволяющая нарушителю выполнить произвольный код или вызвать отказ в обслуживании

Описание уязвимости	Уязвимость микропрограммного обеспечения программируемых логических контроллеров Schneider Electric связана с недостаточной проверкой исключительн позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании с помощью специально созданного вредонс
Вендор	Schneider Electric
Наименование ПО	Modicon M580, EcoStruxure Control Expert, EcoStruxur Process Expert, Modicon M340 CPU BMXP34, Momentum Unity M1E Processor (171CBU)
Версия ПО	- (Modicon M580) - (EcoStruxure Control Expert) до V2020 включительно (EcoStruxur Process Expert) - (Modicon M340 CPU BMXP34) - (Momentum Unity M1E Processor (171CBU))
Тип ПО	Программное средство АСУ ТП, ПО программно-аппаратного средства АСУ ТП, Средство АСУ ТП, Микропрограммный код
Операционные системы и аппаратные платформы	Данные уточняются
Тип ошибки	Недостаточная проверка необычных или исключительных состояний
Идентификатор типа ошибки	CWE-754
Класс уязвимости	Уязвимость кода
Дата выявления	10.01.2023
Базовый вектор уязвимости	CVSS 2.0: AV:N/AC:H/Au:N/C:C/I:C/A:C CVSS 3.0: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Уровень опасности уязвимости	Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 7,5)

Рисунок 1.2 – Пример описания уязвимости BDU:2023-00228 для ПЛК Schneider Electric (фрагмент)

Главная / Список уязвимостей / BDU:2023-00072

BDU:2023-00072: Уязвимость SCADA-систем EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2019, связанная с позволяющая нарушителю вызвать отказ в обслуживании

Описание уязвимости	Уязвимость SCADA-систем EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2019 связана с ошибками разграничения д действующему удаленно, вызвать отказ в обслуживании
Вендор	Schneider Electric
Наименование ПО	EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021
Версия ПО	до 10.2022 (EcoStruxure Geo SCADA Expert 2019) до 10.2022 (EcoStruxure Geo SCADA Expert 2020) до 10.2022 (EcoStruxure Geo SCADA Expert 2021)
Тип ПО	Средство АСУ ТП, ПО программно-аппаратного средства АСУ ТП
Операционные системы и аппаратные платформы	Данные уточняются
Тип ошибки	Неправильная авторизация
Идентификатор типа ошибки	CWE-285
Класс уязвимости	Уязвимость кода
Дата выявления	10.01.2023
Базовый вектор уязвимости	CVSS 2.0: AV:N/AC:L/Au:N/C:N/I:C/A:C CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Рисунок 1.3 – Пример описания уязвимости BDU:2023-00072 для SCADA-систем EcoStruxure Geo SCADA Expert 2019, 2020 (фрагмент)

объекта и иная информация, которую специалисты по ИБ могут использовать для выполнения своих профессиональных обязанностей.

Пополнение Threat/Vulnerability Intelligence осуществляется вручную или автоматически из специальных баз знаний (данных), новостных лент IT-компаний, бюллетеней безопасности производителей оборудования и ПО, форумов, блогов специалистов по ИБ.

Систематизированная информации о различных типах угроз БИ и уязвимостях ПО содержится в таких открытых БД и классификаторах, как CVE, CWE, NVD, стандарт описания шаблонов атак CAPEC, OWASP-проект по обеспечению ИБ веб-приложений, БДУ ФСТЭК России. Сравнительный анализ функциональных возможностей отдельных баз данных приведен в Таблице 1.1 [48].

Таблица 1.1 – Сравнительный анализ функциональных возможностей баз данных угроз и уязвимостей

Базы данных уязвимостей / **Поисковые признаки уязвимости**	**ФСТЭК**	**CVE**	**NVD**	**VND от CERT**
Описание уязвимости	+	+	+	+
Вендор	+	-	+	+
Наименование ПО	+	-	+	-
Версия ПО	+	-	+	-
Тип ПО	+	-	-	+
Операционные системы и аппаратные платформы	+	-	-	-
Тип ошибки	+	-	+	-
Идентификатор типа ошибки	+	+	+	+
Класс уязвимости	+	-	+	-
Дата выявления/включения в реестр	+	-/+	+	+
Базовый вектор	+	-	+	+
Уровень опасности уязвимости	+	-	+	+
Возможные меры по устранению уязвимости	+	-	-	+
Статус уязвимости	+	+	-	-
Наличие эксплойта	+	-	-	-
Способ эксплуатации	+	-	+	+
Способ устранения	+	+	-	+

Базы данных уязвимостей / Поисковые признаки уязвимости	ФСТЭК	CVE	NVD	VND от CERT
Информация об устранении	+	-	-	-
Ссылки на источники	+	+	+	+
Ссылки на другие БД	+	+	+	-
Идентификаторы других систем	+	-	+	+
Прямая загрузка	+	+	+	+

NVD (NIST National Vulnerability Database) [137] – это правительственный репозиторий данных, содержащий описания уязвимостей на основе стандартов, представленных с использованием протокола автоматизации содержимого безопасности (SCAP). NVD включает в себя базы данных контрольных списков безопасности, недостатков ПО, связанных с безопасностью, неправильных конфигураций, названий продуктов и показателей воздействия. На момент проведения исследования содержит более 150 тыс. записей.

CWE (Common Weakness Enumeration) [100] – база данных недостатков (слабых мест) программного и аппаратного обеспечения, которые могут быть использованы нарушителями при проведении атак. На основе CWE возможно выявление слабых мест, их устранение и предотвращение. На момент проведения исследования содержит 927 записей.

MITRE ATT&CK Matrix [135] – общедоступная база знаний, разработанная и поддерживаемая корпорацией MITRE, содержащая структурированный набор тактик и техник, используемых нарушителями на основе реальных наблюдений. ATT&CK может использоваться в качестве основы для разработки конкретных моделей угроз БИ частными лицами, вендорами, госструктурами, а также в сообществе производителей услуг в области ИБ. Содержит около 40 тактик и 335 соответствующих им техник.

OWASP (Open Web Application Security Project) [142] – открытый проект обеспечения безопасности веб-приложений. Это международная некоммерческая организация, сосредоточенная на анализе и улучшении безопасности ПО. OWASP создал список из 10-и самых опасных векторов атак на Web-приложения, в котором

сосредоточены наиболее опасные уязвимости ПО.

Банк данных угроз безопасности информации (БДУ) ФСТЭК России – база данных уязвимостей ПО и угроз БИ. Содержит информацию об уязвимостях, состоящую из 20 разделов, таких как: описание уязвимости; наименование, версия, тип ПО, тип ошибки и др. (Рисунок 1.2). Информация об угрозах содержится в четырех разделах: описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы (Рисунок 1.3). Содержит описания 222 угроз и более 41 тыс. уязвимостей.

Обзор вышеописанных БД показал [69, 81, 82], что, с одной стороны, хорошо структурированная информация об уязвимостях ПО в совокупности с функциями поиска внутри каждой БД, ежедневного их обновления и возможности получения уведомлений о вновь появившихся уязвимостях оказывает существенную поддержку широкому кругу специалистов в области ИБ, но, с другой стороны, наличие открытого доступа к подобным БД еще не гарантирует эффективность их использования. Так, ввиду того что описанные базы независимы друг от друга, существует проблема совместного использования (сопоставления) информации, хранящейся в виде текста в различных форматах в разных БД. Специалисту по ИБ приходится «вручную» обрабатывать огромные массивы текстовых описаний [33, 128], так как отсутствует автоматизированный инструментарий, позволяющий упростить выполнение данной задачи. Выход из сложившейся ситуации возможен путем использования интеллектуальных технологий анализа текстов (Text Mining) и автоматизации с их помощью процесса обработки текстовых описаний угроз БИ и уязвимостей ПО.

1.3 Методики оценки и анализа угроз БИ и уязвимостей ПО объектов КИИ

В качестве исходных данных при оценке и анализе уязвимостей ПО объектов КИИ можно использовать данные, полученные, например, с помощью сканеров уязвимостей (Vulnerability scanners) или средств тестирования на проникновение (Penetration testing).

Сканеры уязвимостей [75], системы инвентаризации и управления уязвимостями позволяют провести инвентаризацию определяют, какое ПО и какой версии установлено на рабочих станциях и серверах и какие уязвимости выявлены в этом ПО, что, в свою очередь, позволяет своевременно установить патч, обновить ПО, изменить настройки конфигурации и многое другое. Российскими производителями представлены следующие наименования сканеров уязвимостей: MaxPatrol 8, RedCheck, XSpider, «Ревизор сети», ScanOVAL и др. Зарубежными производителями представлены такие продукты, как Nessus Professional, Vulnerability Control, Owasp ZAP и др.

Программный продукт ScanOVAL разработан ФСТЭК России [20] совместно с «АЛТЭКС-СОФТ» и предназначен для обнаружения уязвимостей ПО рабочих станций и серверов, информация о которых содержится в БДУ ФСТЭК? Этот продукт будет применен в экспериментальной части данного исследования.

Под тестированием на проникновение понимается процесс оценки защищенности информационной системы путем моделирования действий нарушителя, направленный на обнаружение уязвимостей ПО исследуемого объекта.

Разделяют внешние и внутренние тесты на проникновение (пентесты). В результате тестирования выявляются следующие виды уязвимостей ПО: организационные уязвимости и недостатки (слабости) в процессах обеспечения ИБ, уязвимости общесистемного ПО, уязвимости прикладного ПО, уязвимости сетевой инфраструктуры. Методики для проведения пентестов изложены в OWASP, OSSTMM (Open Source Security Testing Methodology Manual) и др.

К настоящему времени известны различные методики оценки и анализа угроз ИБ и уязвимостей ПО информационных систем. Это такие методики, как OWASP, OSSTMM, ISSAF, PTES, NIST SP 800-115, модели Cyber Kill Chain и Unified Kill Chain, подробный анализ которых приведен в [43, 52]. Данные методики содержат:

– порядок проведения тестирования на проникновение, рекомендации по анализу и обработке рисков, метрики для оценки уровня безопасности и

рекомендации по составлению отчётов (методики OSSTMM, PTES, NIST SP 800-115);

– набор техник (методов), которые можно использовать для поиска уязвимостей в системе безопасности, что особенно важно для типовых удаленных объектов КИИ (методика OWASP [52]);

– конкретные виды тестирования на проникновение для объектов КИИ, в частности: тестирование паролей; тестирование безопасности ОС и БД; тестирование безопасности беспроводных сетей и интернет-коммуникаций; тестирование безопасности средств защиты (межсетевых экранов, систем обнаружения вторжений, VPN, антивирусных систем и пр.) и др. Методика ISSAF может быть адаптирована для оценки ИБ в любой организации, включает [52];

– схематическое описание последовательных действий (этапов) нарушителя в виде взаимосвязанных звеньев. Предлагаемые подходы позволяют экспертам идентифицировать методы и средства, применяемые нарушителями на каждом этапе кибератаки (модели Cyber Kill Chain и Unified Kill Chain (CKC, «цепочка кибервторжений», UCK, «унифицированная цепочка кибервторжений» [43]);

– метрика CVSS для расчета показателя опасности уязвимости по десятибалльной шкале позволяет получить количественную оценку уровня опасности уязвимости и на основе этих оценок помогает определить какие уязвимости необходимо устранить в первую очередь. В настоящий момент вышла версия стандарта CVSS v.3.1. В стандарте используются 3 группы метрик: базовые, временные, контекстные. Временные и контекстные метрики опциональны и применяются для более точной оценки опасности, которую представляет данная уязвимость (методика CVSS [99]);

– унифицированные именования и регистрацию обнаруженных уязвимостей ПО. Это, с одной стороны, словарь известных уязвимостей и дефектов, с другой стороны, CVE позволяет связывать между собой БД уязвимостей и другие инструменты безопасности, репозитории и службы. Инструменты сканирования используют данный стандарт для классификации уязвимостей. CVE

функционирует с 1999 г. и на момент проведения исследования содержит более 181 тыс. записей. На Рисунке 1.4 представлено окно CVE с информацией об уязвимости CVE-2023-22807 (методика (стандарт анализа уязвимостей) CVE [98]).

CVE-ID

CVE-2023-22807 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

LS ELECTRIC XBC-DN32U with operating system version 01.80 does not properly control access to the PLC over its internal XGT protocol. An attacker could cont the PLC by sending the packets to the PLC over its XGT protocol.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.cisa.gov/uscert/ics/advisories/icsa-23-040-02
- URL:https://www.cisa.gov/uscert/ics/advisories/icsa-23-040-02

Assigning CNA

ICS-CERT

Date Record Created

20230106 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate wh was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Рисунок 1.4 – Рабочее окно CVE с информацией об уязвимости CVE-2023-22807 (фрагмент)

– каталог известных шаблонов кибератак, используемых нарушителями. Запись о шаблоне атак в CAPEC включает описание механизмов эксплуатации уязвимости, возможные последствия и методы противодействия. Кроме того, запись ссылается на используемые в шаблоне уязвимости в CVE и на приводящие к ним недостатки из CWE. CAPEC функционирует с 2007 г. и на момент проведения исследования содержит 559 записей о шаблонах атак. На рисунке 1.5 представлен фрагмент рабочего окна CAPEC (методика построения сценариев компьютерных атак на основе БД шаблонов атак CAPEC [97].

CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs

Attack Pattern ID: 1
Abstraction: Standard

View customized information: Conceptual | Operational | Mapping-Friendly | Complete

Description

In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framew
application's functionality; particularly URL's for web apps. In the case that the administrator failed to specify an ACL for a pa
An attacker with the ability to access functionality not properly constrained by ACLs can obtain sensitive information and poss
resources that must be available only to users at a higher privilege level, can access management sections of the application,

Likelihood Of Attack

High

Typical Severity

High

Relationships

Nature	Type	ID	Name
ChildOf	M	122	Privilege Abuse
ParentOf	D	58	Restful Privilege Elevation
ParentOf	D	679	Exploitation of Improperly Configured or Implemented Memory Protections
ParentOf	D	680	Exploitation of Improperly Controlled Registers
ParentOf	D	681	Exploitation of Improperly Controlled Hardware Security Identifiers
CanPrecede	B	17	Using Malicious Files

View Name	Top Level Categories
Domains of Attack	Software, Hardware
Mechanisms of Attack	Subvert Access Control

Execution Flow

Рисунок 1.5 – Фрагмент рабочего окна CAPEC

Описанные методики обладают неоспоримыми достоинствами: это систематизированные сведения об уязвимостях, угрозах ИБ, шаблонах атак; данные инструменты предоставляют возможность для конструктивного взаимодействия в области ИБ. Недостатками методик являются отсутствие возможности автоматизированной оценки и анализа угроз и уязвимостей конкретного объекта КИИ, а также отсутствие возможности обработки больших массивов текстовых данных на русском языке.

Важным шагом в развитии отечественной нормативной базы в области ИБ является принятие 5 февраля 2021 г. методического документа ФСТЭК России «**Методика оценки угроз безопасности информации»** [7] (далее – Методика). Целью Методики является определение актуальных угроз БИ. Работу по оценке угроз БИ предлагается разделить на 3 этапа, каждый из которых содержит подэтапы:

Этап 1. Определение негативных последствий:

– анализ документации систем и сетей и иных исходных данных;

– определение негативных последствий от реализации угроз.

Этап 2. Определение объектов воздействий:

– анализ документации систем и сетей и иных исходных данных;

– инвентаризация систем и сетей;

– определение групп информационных ресурсов и компонентов систем и сетей.

Этап 3. Оценка возможности реализации угроз и их актуальности:

– определение источников угроз;

– оценка способов реализации угроз;

– оценка актуальности угроз.

Источником исходных данных для решения поставленных задач, в первую очередь, является БДУ ФСТЭК России и модели угроз БИ, разработанные ФСТЭК России, а также различные БД, содержащие описания векторов атак, такик как: CAPEC, ATT&CK, OWASP и др. В соответствии с Методикой: *«При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной…»*, при этом, определение сценариев угроз БИ предусматривает установление последовательности возможных тактик и соответствующих им техник, которыми может воспользоваться нарушитель для достижения своей цели.

Ввиду необходимости обработки больших массивов текстовых данных Методикой отмечается возможность автоматизации процесса оценки угроз БИ. Так, в ходе инвентаризации с целью получения исходных данных для анализа, возможно применение специального ПО, повышающего качество данного процесса.

Проведённый выше анализ существующих методик оценки и анализа угроз БИ и уязвимостей ПО показал в целом их ориентированность на ручную обработку данных. Методики в достаточной степени разрознены, плохо приспособлены для работы с большими массивами текстовых данных; они в основном дают качественную оценку угроз БИ и уязвимостей ПО, не в полной мере учитывают специфику объекта защиты (в частности, рассматриваемых в работе объектов КИИ). Как следствие, имеется настоятельная необходимость разработки и

внедрения новых, более совершенных инструментальных средств для семантического анализа текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя с использованием современных технологий искусственного интеллекта.

1.4 Технологии интеллектуального анализа текстов (Text Mining)

Как уже отмечалось в разделе 1.2, традиционно используемые БД (классификаторы, реестры) содержат большое количество текстовых описаний угроз, уязвимостей и тактик (техник). Несмотря на несомненные достоинства указанных БД, работа, связанная с оценкой и анализом существующих на конкретном предприятии угроз БИ и уязвимостей ПО, предполагает экспертный характер, что требует больших временных затрат, существенной когнитивной нагрузки и глубоких профессиональных знаний. В работе [33] для построения искусственной НС в качестве входных сигналов предлагается использовать количественные факторы актуальности угроз БИ. В то же время современные методы искусственного интеллекта позволяют обрабатывать большие массивы текстовых данных на естественном языке (ЕЯ) с целью решения следующих задач:

– поиск нужной информации по запросу (по ключевым словам);

– классификация текстов (тематизация);

– суммаризация (автоматическое реферирование) текстов;

– кластеризация (разбиение на группы текстов, близких по содержанию);

– автоматическое составление текстов заданного содержания; и т.п.

Решению перечисленных выше задач посвящено значительное количество публикаций, например [17, 31, 42, 81, 84]. Данное направление исследований, посвященное анализу слабоструктурированных текстовых данных на ЕЯ, получило название интеллектуального анализа текстов (Text Mining). Существенные результаты в рамках данного направления получены в работах [90, 103, 105, 136, 140]. Следует отметить, что для перехода к непосредственному использованию методов обработки ЕЯ, необходимо, прежде всего, произвести предварительную

обработку (подготовку) корпуса текстовых данных, затем перейти к векторному представлению текстовых описаний в многомерном семантическом пространстве и только после этого в полученном семантическом пространстве решать конкретную прикладную задачу, связанную с семантическим анализом текста.

Более подробно указанные этапы обработки текстовых данных будут описаны ниже.

Анализ методов векторного представления слов и метрик оценки семантической близости. Использование методов векторного представления слов и метрик оценки их семантической близости является необходимым этапом анализа слабоструктурированных текстов на ЕЯ [23, 49, 57]. На современном этапе развития машинного обучения для решения подобных задач используются различные методы, которые можно отнести к классическим – это линейные методы классификации, модели на основе гауссовских распределений, деревья решений и др. Наряду с классическими существуют методы обработки последовательностей – скрытые марковские модели, модели на основе условных случайных полей. Большую популярность для этих целей в последние годы приобрели нейронные сети (НС) – многослойные перцептроны, сверточные НС, рекуррентные НС, для подготовки входных данных которых используются инструменты векторного представления слов (Word Embeddings), такие как TF-IDF, Word2vec, Doc2Vec, GloVe, FastText и др.

Прежде чем перейти непосредственно к рассмотрению методов машинного обучения, рассмотрим основные этапы предварительной обработки текстовых данных. Эти этапы заключаются в выполнении следующих процедур [22, 24]:

1. Нормализация – приведение текста к более простому виду, удаление знаков пунктуации, аббревиатур, стоп-слов, не несущих смысловой нагрузки союзов, предлогов, междометий.

2. Токенизация – разделение письменного языка на предложения (слова)-компоненты.

3. Стеммизация – приведение слова к его корню, путем устранения суффиксов, приставок, окончаний.

4. Лемматизация – приведение слова к смысловой канонической форме – инфинитив, именительный падеж единственного числа и т.д.

5. Фильтрация – удаление нерелевантных символов, слов.

Предобработанные таким образом тексты далее подвергаются обработке с помощью алгоритмов векторного представления слов (векторного вложения), которые описаны ниже.

TF-IDF (TF (от англ. term frequency – частота слова), IDF (inverse document frequency – обратная частота документа) [60] – это статистическая мера, используемая для оценки важности (значимости) слов в контексте документа, являющегося частью коллекции (корпуса) документов. Вес некоторого слова пропорционален частоте употребления этого слова в документе и обратно пропорционален частоте употребления слова во всех документах коллекции. Структура меры TF-IDF следующая:

– частота слова $tf(t,d)$ рассчитывается по формуле:

$$tf(t,d) = \frac{n_t}{\sum_k n_k}, \tag{1.1}$$

где n_t – число вхождений слова t в документ, а в знаменателе указывается общее число слов в данном документе;

– обратная частота документа $idf(t,D)$ рассчитывается по формуле:

$$idf(t,D) = log\frac{|D|}{|\{d_i \in D | t \in d_i\}|}, \tag{1.2}$$

где $|D|$ – число документов в коллекции; $|\{d_i \in D | t \in d_i\}|$ – число документов в коллекции D, в которых встречается t (когда $n_t \neq 0$). Учёт IDF уменьшает вес широкоупотребительных слов. Для каждого уникального слова в пределах конкретной коллекции документов существует только одно значение IDF. Таким образом, мера TF-IDF является произведением двух сомножителей:

$$tf - idf(t,d,D) = tf(t,d) \times idf(t,D). \tag{1.3}$$

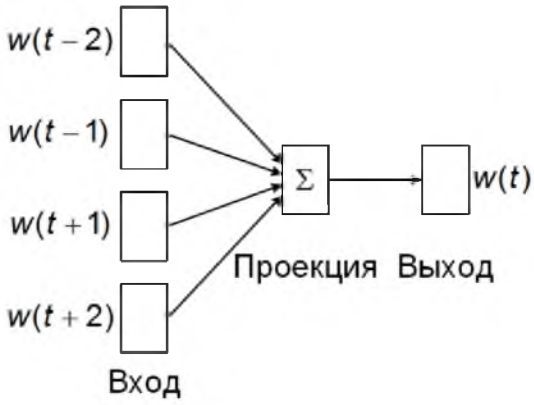
Недостаток данного алгоритма заключается в том, что он не учитывает порядок слов в предложении.

Мера TF-IDF часто используется в задачах анализа текстов и информационного поиска, например, как один из критериев релевантности

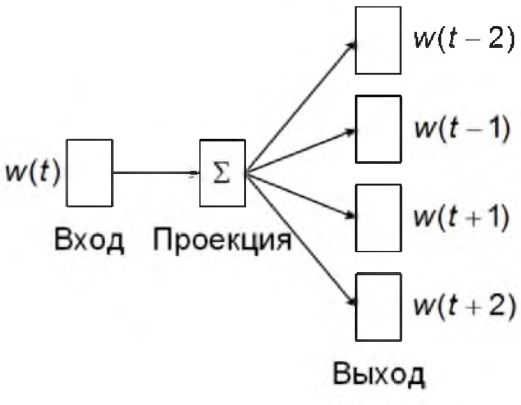
документа поисковому запросу, при расчёте меры близости документов при кластеризации.

Word2Vec [39, 114] – создан группой ученых компании Google во главе с Т. Миколовым в 2013 г. Это инструмент (набор алгоритмов) для расчета векторных представлений слов, где на вход подается корпус текста, а на выходе получается набор векторов слов. Данный инструмент обучается на огромном количестве текстов с запоминанием того, какое слово возникает в схожих контекстах. По окончании обучения формируется вектор в 300-мерном пространстве признаков (семантическом пространстве) для каждого слова в словаре. Главное требование: в искомом семантическом пространстве словам, близким по смыслу, соответствуют близко расположенные вектора. Word2Vec реализует две основные архитектуры – Continuous Bag of Words (CBOW) и Skip-gram.

CBOW и Skip-gram – это нейросетевые модели реализации алгоритма Word2Vec, описывающие процесс обучения НС и «запоминания» векторного представления слов. Принцип работы нейросетевых моделей следующий: CBOW предсказывает слова при данном контексте (Рисунок 1.6 а), а Skip-gram, наоборот, предсказывается контекст при данном слове (Рисунок 1.6 б).



а)



б)

Рисунок 1.6 – Архитектуры алгоритмов обучения Continuous Bag of Words (а) и Skip-gram (б)

Хотя Word2Vec хорошо справляется с предоставлением слов в векторы, но у него есть существенные недостатки: 1) при использовании данного алгоритма не

учитывается порядок слов в предложении; 2) он не учитывает смысловое значение слова (семантическое значение); 3) он не может создать вектор всего документа. Для решения этой задачи был разработан инструмент Doc2Vec.

Doc2Vec (paragraph2vec) [122, 133] был создан в 2014 г. на основе Word2Vec. Это инструмент, который позволяет получить из документов пространство признаков фиксированной длины. Полученный вектор можно использовать для анализа семантической близости между предложениями (абзацами, документами) с помощью определенной меры семантической близости. Также используется в задачах кластеризации, классификации, прогнозирования текстовых описаний.

Считается, что вышеперечисленные инструменты связаны с первой революцией по обработке естественного языка (Natural Language Processing, NLP). Вторая революция связана с появлением нейросетевых языковых моделей GPT, BERT и др. Это наиболее мощные на данный момент времени алгоритмы обработки текстовых данных, основанные на механизме внимания (Self-Attention). Данное поколение нейросетевых моделей получило название «трансформеров» (transformers).

Первая модель *GPT (Generative Pre-trained Transformer)* [107,146] – это генеративная языковая модель на архитектуре трансформера, выпущена в 2018 г. компанией Open AI (основатели – Илон Маск и Сэм Альтман). Третье поколение этой модели – GPT-3, вышедшая в 2020 г., была обучена более чем на 500 Гб текстовых данных. Русскоязычным проектом ruGPT-3 13B занимались компании SberDevices, SberCloud. Модель ruGPT обучена на 600 Гб текстовых данных. К сожалению, полноценная работа модели GPT возможна только при наличии серьезных вычислительных мощностей, недоступных для большинства научных исследователей.

Модель BERT (Bidirectional Encoder Representations from Transformers) [36, 37, 96] – двунаправленная модель с архитектурой трансформера, предназначенная для предобучения на больших объемах текстовых данных с целью их последующего применения в широком спектре задач обработки ЕЯ. Мультиязычные модели BERT уже предобучены на больших наборах данных и у

пользователей есть возможность скачать и встроить в свои проекты по обработке ЕЯ готовый инструмент, не тратя время на обучение НС с нуля. Саму НС можно запустить как на локальном компьютере, так и на бесплатном серверном GPU на Google Colab. В отличие от GPT, BERT более «легковесна», максимальная версия BERT-Large содержит 24-слойный трансформер с 240 млн. настраиваемых параметров. Так же, как и в случае с GPT, в модели BERT возможна тонкая настройка параметров для решения конкретных задач, в том числе в области ИБ. В отличие от Word2Vec и других классических языковых моделей, BERT обучает контексто-зависимые представления, что позволяет учитывать окружающий контекст предложения и генерировать различные векторные вложения (эмбеддинги) для омонимов в зависимости от контекста.

Архитектура трансформера (Рисунки 1.7, 1.8) состоит из двух частей – кодировщика (encoder) и декодеровщика (decoder), каждый из которых, в свою очередь, состоит из повторяющихся слоев, содержащих механизмы внутреннего внимания (Self-Attention) и НС прямого распространения (Feed-Forward NN).

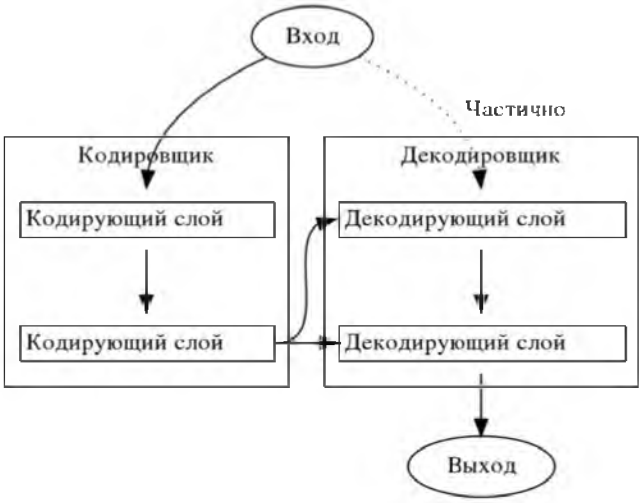


Рисунок 1.7 – Общая схема архитектуры трансформера

Кодировщик преобразует входную последовательность слов во множество векторов (эмбеддингов) в семантическом пространстве, декодировщик генерирует из этих векторов последовательность выходных слов в соответствии с запросом на решение конкретной прикладной задачи (классификация, поиск, перевод и т.п.).

Роль механизмов внимания в данном случае – выделить из текста наиболее важные, значимые слова, отражающие смысловое содержание текста, организовав с учетом этого процесс обработки информации в кодировщике и декодировщике. Особенностью построения трансформера является параллельная и независимая обработка входных слов, что сокращает вычислительные затраты и одновременно повышает качество обучения языковой модели.

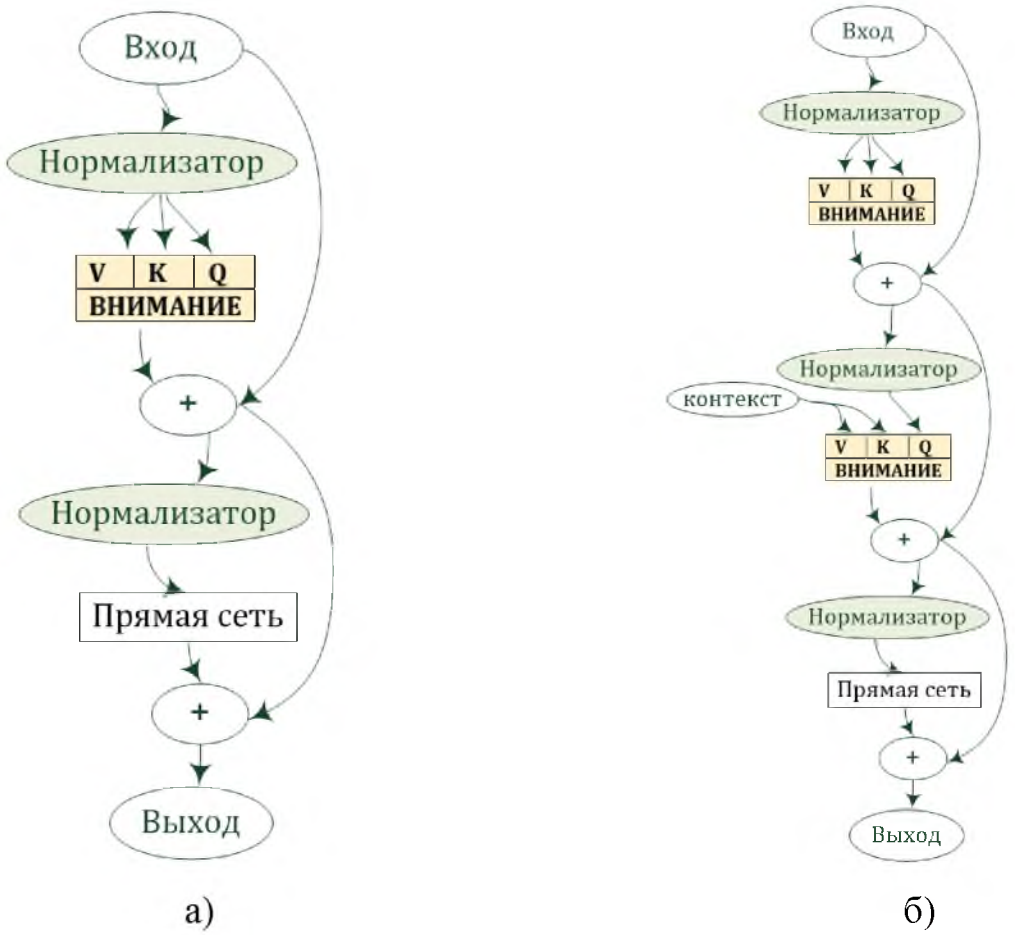


Рисунок 1.8 – Схема архитектуры трансформера: а) кодирующий слой; б) декодирующий слой

Такие методы векторизации слов, как TF-IDF, Word2Vec, Doc2Vec, относятся к статистическим. Они достаточно часто используются в задачах анализа ЕЯ, но имеют некоторые недостатки:

– не учитывают многозначность и контекст, в котором слова используются. Это значит, что для слов-омонимов будет создан один усредненный вектор, что может привести к некорректному анализу данных;

– плохо обрабатывают неизвестные и редкие слова.

От этих недостатков свободны контекстуализированные нейросетевые языковые модели, к которым относятся GPT и BERT, они позволяют вычислять векторное представление слова в зависимости от контекста, в котором он употреблен. В исследовании [34] проводился сравнительный анализ качества векторизации с использованием статистических моделей и одной из моделей трансформеров применительно к анализу текстов диалоговых чат-ботов. Эксперимент показал успешную работу комбинированной модели TF-IDF + Word2Vec и модели трансформеров.

Для анализа текстовых описаний и определения сходства между документами используют алгоритмы кластеризации, основная задача которых состоит в выявлении скрытой структуры в корпусах текстов с использованием определенных признаков, по которым текстовые данные можно отнести к той или иной группе. Центральное место при решении этой задачи занимает определение семантической близости между созданными при помощи моделей векторизации векторами текстовых описаний определенных документов, которые можно визуализировать в виде точек в пространстве признаков. Для этого используются метрики семантической близости, или метрики расстояний [22, 54, 95, 143]. Суть данных метрик заключается в определении расстояния между точками (векторами) в многомерном пространстве, причем чем меньше расстояние между точками, тем более схожими будут соответствующие текстовые описания. Ниже приведен краткий обзор метрик семантической близости, применяемых при решении задач анализа текстов [41, 55].

Манхеттенское расстояние (расстояние городских кварталов) измеряет расстояние не по кратчайшей прямой, а по блокам – это расстояние всех прямых линий пути:

$$dist(A, B) = \sum_{i=1}^{n} |x_{Ai} - x_{Bi}|, \tag{1.4}$$

где n – размерность векторного пространства.

Евклидово расстояние – это кратчайшее расстояние между двумя точками A и B (прямая линия). Расстояние между этими точками определяется формулой:

$$dist(A,B) = \sqrt{\sum_{i=1}^{n}(x_{Ai} - x_{Bi})^2}. \quad (1.5)$$

Расстояние Махаланобиса – это статистическая мера расстояния между двумя точками *A* и *B*, принадлежащими одному распределению вероятностей с ковариационной матрицей *COV*:

$$dist(A,B) = \sqrt{(X_A - X_B)\, COV^{-1}(X_A - X_B)^T}, \quad (1.6)$$

где *T* – операция транспонирования, COV^{-1} – матрица, обратная ковариационной. Если *COV* – единичная матрица, то расстояние Махалонобиса становится равным Евклидову расстоянию.

Косинусная мера семантической близости (косинусное расстояние) является мерой сходства между двумя векторами текстовых описаний. Определяется как косинус угла между ними, то есть как скалярное произведение векторов, деленное на произведение их длин:

$$dist(A,B) = cos(\theta) = \frac{X_A \cdot X_B}{|X_A| \cdot |X_B|} = \frac{\sum_{n=1}^{i} X_{Ai} X_{Bi}}{\sqrt{\sum_{n=1}^{i} X_{Ai}^2} \cdot \sqrt{\sum_{n=1}^{i} X_{Bi}^2}}. \quad (1.7)$$

Косинус угла между векторами можно интерпретировать как степень сходства документов, то есть, чем меньше угол между двумя векторами, тем более схожими будут документы (Рисунок 1.9).

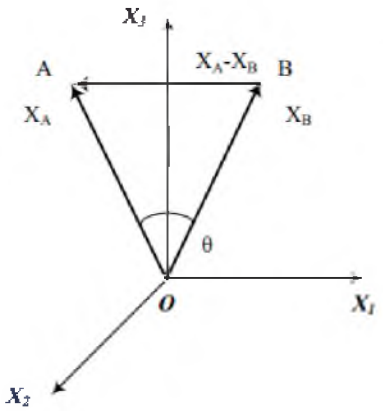


Рисунок 1.9 – Косинусная мера семантической близости

Часто в настройках параметров кластеризации по умолчанию указывается Евклидово расстояние, но многими экспериментами показано [91, 148], что

использование косинусной меры семантической близости позволяет добиться лучших результатов.

Анализ методов кластеризации и понижения размерности текстовых данных. Кластеризация является одним из важнейших этапов в задачах анализа текстовой информации. Суть методов кластеризации состоит в том, что полученные в результате предобработки текстовых данных векторы соответствующих им текстовых описаний необходимо разделить на несколько групп, объединенных по определенному признаку [80, 116].

Существуют различные способы построения алгоритмов кластеризации.

Иерархические алгоритмы кластеризации представляют собой совокупность алгоритмов систематизации данных, направленных на создание дендрограммы вложенных кластеров, т.е. новые кластеры строятся из уже образованных, создавая тем самым древовидную структуру. На каждом шаге работы данного алгоритма необходимо вычислить расстояние между кластерами и затем пересчитать расстояние между вновь появившимися кластерами. Для определения расстояния $R(U, V)$ между кластерами U, V, содержащими несколько элементов, используются различные функции (меры), выбираемые в зависимости от решаемой задачи.

В результате *плоской кластеризации* происходит разбиение объектов на кластеры сразу, причем один объект относится только к одному кластеру. Самым популярным представителем этого вида является алгоритм k-means (k-средних). Суть алгоритма заключается в том, что он случайно определяет центры кластеров и определяет ближайшие векторы данных к центру каждого кластера. Затем выполняется смещение центров кластеров и пересчет ближайших векторов к новому центру до тех пор, пока не перестанут меняться кластеры. Недостатки данного алгоритма: 1) необходимость задания количества кластеров вручную; 2) зависит от выбора начальных центров кластеров; 3) не выполняет задачу, когда элемент кластера принадлежит в равной степени к разным кластерам или не принадлежит ни к одному.

В алгоритме четкой кластеризации каждый объект множества принадлежит строго к одному кластеру.

В случае нечеткой кластеризации каждый объект множества принадлежит каждому кластеру с определенной долей вероятности. К данному виду алгоритмов относится алгоритм c-means (c-средних). Существенным недостатком алгоритма является невозможность корректного разбиения на кластеры в случае, когда кластеры имеют различный разброс значений по различным размерностям (осям) элементов.

При решении задач кластеризации одной из основных проблем является высокая размерность обучающих выборок [63], что сильно затрудняет процесс машинного обучения. Для решения этой проблемы используются алгоритмы снижения размерности выборок текстовых данных, рассматриваемые в работах ряда российских и зарубежных ученых [62, 144, 158]. В основе соответствующей процедуры используется определение наиболее значимых признаков из всей выборки, что позволяет:

– улучшить качество визуализации результатов;

– повысить точность классификации используемых алгоритмов;

– сократить ресурсы на проведение вычислительных операций;

– увеличить скорость вычислений (обучение моделей).

Таким образом, снижение размерности анализируемого векторного пространства является хорошим способом экономии ресурсов при сохранении информативности получаемых результатов [127].

Одним из наиболее популярных алгоритмов снижения размерности является алгоритм t-SNE (t-distributed stochastic neighbor embedding) [16, 71] – стохастическое вложение соседей с t-распределением (t-распределение Стьюдента). Это поэтапный итерационный процесс для представления вложений в плоскостях низкой размерности с сохранением информации об их расположении относительно друг друга, а также инструмент для визуализации многомерных переменных. Использование данного алгоритма позволяет упростить процесс поиска глобальных минимумов и повысить качество визуализации. t-SNE отличается невысокой скоростью работы, но при этом сохраняет базовую структуру данных.

UMAP (Uniform Approximation and Projection) [130] – эффективный алгоритм уменьшения размерности. В результате работы алгоритма происходит построение взвешенного графа путем соединения ближайших соседей (объектов) ребрами. Затем строится граф в низкоразмерном пространстве, который приближается к исходному графу путем минимизации дивергенции Кульбака-Лейблера между множествами в высоко- и низкоразмерном пространствах. У данного алгоритма нет ограничений на размерность исходного пространства признаков, и он превосходит t-SNE по быстродействию.

PCA (Principal Component Analysis) [38] – метод анализа главных компонент. Это статистический метод уменьшения размерности обучающей выборки. Суть метода состоит в линейном преобразовании исходных данных в новую систему координат, в которой вариации данных можно описать с меньшим количеством измерений, чем исходные данные. PCA отличается высокой скоростью вычислений, но достигается это за счет потери части данных.

Выделяются еще два популярных метода, нашедших применение в задачах тематической классификации текстов.

LSA (Latent semantic analysis) [51, 115] – это метод латентного семантического анализа ЕЯ. Метод дает возможность провести анализ скрытых взаимосвязей между документами (текстовыми описаниями) и терминами (словами), которые в них содержатся. LSA предполагает, что слова, близкие по значению, будут встречаться в похожих фрагментах текста. В процессе работы создается матрица, содержащая слова (*n*-граммы) в строках и текстовые описания в столбцах. При этом используется SVD (Singular Value Decomposition) – разложение матрицы по собственным значениям для уменьшения количества строк при сохранении структуры сходства между столбцами.

LDA (Latent Dirichlet allocation) [118] – скрытое распределение Дирихле. Также является одним из методов тематического моделирования. В отличие от LSA, предполагается, что документ может представлять вероятностный набор тем, при этом четко установлена взаимосвязь каждого слова документа с определенной темой.

В следующем разделе дан обзор практического применения моделей, методов и алгоритмов интеллектуального анализа текстов для решения задач, связанных с автоматизацией оценки и анализа текстовых описаний угроз БИ и уязвимостей ПО.

1.5 Существующие подходы к автоматизации анализа текстовых описаний угроз БИ и уязвимостей ПО

Как уже отмечалось, одним из перспективных путей решения проблем, связанных с обработкой больших объемов текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, является использование технологий интеллектуального анализа текстов (Text Mining). Использование данных технологий позволяет снизить трудоемкость и влияние человеческого фактора при обработке указанных текстовых описаний, хранящихся в БД.

Исследованиям в этой области посвящены работы большого числа отечественных и зарубежных ученых. Так, в работе [124] рассмотрена задача ранжирования (приоритизации) уязвимостей ПО с использованием алгоритма TextRank, основанного на оценке семантической близости текстовых описаний уязвимостей.

В [139] реализован поиск соответствующих определенным критериям запроса шаблонов атак, содержащихся в БД CAPEC. При этом в соответствии с технологией интеллектуального анализа текстов строится семантическое пространство векторов, содержащее представленные в векторной форме текстовые описания шаблонов атак. Далее происходит кластеризация текстовых описаний с использованием метода деревьев решений, т.е. вектора разбиваются на группы семантически близких по описанию шаблонов атак.

В исследовании [113] предложено связать тактики и техники из БД MITRE ATT&CK Matrix, CAPEC, CWE и CVE на основе существующих в гипертекстовых документах перекрестных ссылок. С этой целью стоится двудольный реляционный граф, описывающий взаимосвязь элементов из вышеперечисленных БД.

В работах [138, 159] представлены графы знаний, устанавливающие взаимосвязь с шаблонами атак (CAPEC) и классификаторами уязвимостей (CVE, CWE) не только с помощью гиперссылок документов, но и с использованием векторизованных с помощью алгоритма Word2Vec текстовых описаний этих документов.

В статье [102] на основе методов машинного обучения и обработки ЕЯ (TF-IDF и Doc2Vec) выполняется прогнозирование последствий кибератак. Предлагаемые инструменты упрощают информирование о последствиях атаки и позволяют снизить когнитивную нагрузку на исследователей в случае обнаружения новых атак. Предполагается, что предложенная система позволит успешно выполнять свои профессиональные обязанности даже специалистам с незначительным опытом работы в области ИБ.

Алгоритмам сопоставления угроз и уязвимостей, выявленных с помощью сканера, посвящена работа [85]. В исследовании предлагается модель автоматизированной генерации графа атак на основе данных, полученных из БД NVD. Модель реализована с использованием двух подходов на основе правил и методов машинного обучения (многослойный персептрон).

В работе [120] предлагается извлекать необходимые данные о способах устранения уязвимостей из существующих БД угроз и уязвимостей с целью прогнозирования способа устранения вновь обнаруженных уязвимостей. Это позволит оперативно ликвидировать новые уязвимости, не дожидаясь выхода патчей или обновления ПО. Предлагаемый авторами подход предполагает реализацию следующих этапов: 1) приоритизация источников данных с использованием метода MoSCoW; 2) извлечение признаков из текста с использованием Text Mining; 3) категоризация уязвимостей и способов их устранения (Overlapping clustering algorithms); 4) нахождение взаимосвязей между категориями с использованием взвешенного двудольного графа; 5) построение предиктора способов устранения новых уязвимостей ПО с использованием методов машинного обучения.

В работе [119] представлен автоматический метод прогнозирования оценки CVSS с использованием текстовых описаний уязвимостей, агрегированных из БД CVE и OSVDB (Open Source Vulnerability Database). В исследовании применены процедуры подготовки текстовых описаний для дальнейшей их обработки алгоритмами SVM и Random Forest и нечеткими системами для получения прогноза оценки CVSS. Точность прогноза с использованием нечетких систем составила 88 %, что выше показателей при использовании методов SVM и Random Forest.

В статье [155] решается задача оценки критичности уязвимостей по их текстовому описанию. С этой целью использовались методы анализа текстов и три различных метода классификации (деревья решений, НС и машины опорных векторов).

Работы ряда российских ученых также посвящены применению технологий Text Mining для решения задач обеспечения ИБ. Так, в статьях Селифанова В.В. и др. [72, 73] предложена методика выявления взаимосвязей между обнаруженными уязвимостями и угрозами БИ. Источником описаний угроз БИ и уязвимостей ПО является БДУ ФСТЭК России.

В диссертационной работе Полетаева В.С. [69] предложены модели и алгоритмы, решающие задачу прогнозирования угроз БИ и уязвимостей ПО информационной системы на основе правил нечеткого логического вывода. Источником данных являются тематические интернет-ресурсы.

Работа [77] посвящена выявлению актуальных угроз БИ информационной системы на основе данных о выявленных уязвимостях ПО. Автоматизация данного процесса осуществляется с использованием НС.

В ряде работ рассмотрены вопросы кластеризации текстовых данных в задачах обеспечения ИБ. Так, в работе [18] описан метод кластерного анализа пространственно-временной модели угроз БИ применительно к АСУ ТП транспортировки нефтегазового сырья. Особенностью предложенного подхода является исследование частных моделей угроз БИ для различных подсистем

распределенной АСУ, позволяющих снизить временные и стоимостные затраты на создание и модернизацию системы.

В работе [46] проведен кластерный анализ угроз БИ с помощью методов k-means и k-medoids. Реализация предложенного подхода позволяет выделить различные группы угроз БИ, схожих по определенным признакам, в том числе определить угрозы, наносящие существенный ущерб предприятию, что позволяет специалистам по ИБ своевременно принять меры по устранению данных угроз и, тем самым, сократить наносимый от реализации данных угроз ущерб.

В статье [66] освещена проблема кластеризации текстовых документов (в данном случае научных статей) с использованием алгоритмов Word2Vec, Paragraph2Vec. В этой работе рассмотрены и экспериментально исследованы методы кластеризации текстовых документов. Экспериментальное исследование показало, что лучшим методом (при условии оптимизации параметров с помощью внутренней меры эффективности) является k-means с векторизацией на основе алгоритма Paragraph Vectors для всех наборов данных, кроме Krapivin.

На основании проведенного анализа можно сделать вывод о том, что актуальность исследований в области автоматизации обработки текстовых данных обусловлена прежде всего необходимостью снижения трудоемкости и повышения эффективности работы специалистов в области ИБ, что особенно важно при решении задач анализа актуальных угроз БИ и уязвимостей ПО объектов КИИ.

1.6 Выводы по первой главе

По результатам проведенного анализа существующих стандартов и нормативной базы в области ИБ, а также методик и инструментальных средств оценки и анализа актуальных угроз БИ и уязвимостей ПО объектов КИИ выявлено, что, несмотря на широкий интерес специалистов и научной общественности к решению данной проблемы, сегодня отсутствуют решения, которые бы в полной мере удовлетворяли требованиям отечественной нормативной базы и, в частности, Методики ФСТЭК России от 05.02.2021 г. относительно необходимости детальной

оценки актуальных угроз БИ на основе моделирования сценариев их реализации в автоматизированном режиме. Задачи, связанные с оценкой и анализом актуальных угроз БИ и уязвимостей ПО, требуют дальнейших исследований. Обзор современных методов интеллектуального анализа текстов (Text Mining) показал перспективность применения данного направления искусственного интеллекта к решению указанной проблемы посредством разработки комплекса алгоритмов автоматизации оценки и анализа текстовых описаний угроз БИ, уязвимостей ПО и тактик (техник) действий нарушителя.

Исходя из вышеизложенного, была сформулирована цель исследования: повышение достоверности и оперативности оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ на основе открытых баз данных и технологий интеллектуального анализа текстов. А также сделаны выводы о необходимости дальнейшего проведения исследований в области оценки и анализа текстовых описаний угроз БИ, уязвимостей ПО и тактик (техник) действий нарушителя путем:

1. Разработки алгоритмов автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области информационной безопасности.

2. Разработки метода и алгоритма оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО АСУ ТП с использованием технологии семантического анализа текстов.

3. Разработки алгоритма построения графовой модели сценария реализации угроз БИ на основе алгоритмов векторного вложения и технологии трансформеров.

4. Разработки архитектуры и ПО исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) в процессе оценки угроз БИ и уязвимостей ПО объектов КИИ, исследование эффективности ее применения при решении практических прикладных задач.

Глава 2. Разработка и исследование алгоритмов автоматической классификации и суммаризации текстов из открытых источников в области ИБ

В данной главе описаны понятия классификации (тематического моделирования) и суммаризации. Перечислены основные методы, этапы классификации и суммаризации с использованием технологий NLP. Проведено экспериментальное исследование о возможности использования алгоритмов автоматической классификации и суммаризации проблемно-ориентированных текстов для специалистов в области ИБ.

2.1 Общие подходы к решению задачи автоматической классификации и суммаризации

Все более востребованной становится задача обработки большого объема текстовых данных, в том числе и в области ИБ. Специалист по ИБ для решения профессиональных задач может обратиться за информацией не только к соответствующим базам знаний (данных), но и к иным открытым источникам в области ИБ (научные статьи, специальные форумы и блоги). В процессе анализа этих данных появляется необходимость классифицировать информацию по определенным темам или сделать аннотацию большого корпуса текстов для ускорения их обработки. Качественная обработка вручную всего потока слабоструктурированной или неструктурированной информации представляет собой сложную задачу, с которой хорошо справляются инструменты интеллектуального анализа данных, в частности, алгоритмы Text Mining, о чем свидетельствует большое количество научных исследований на эту тему [24, 61, 153], в том числе в области ИБ [156].

Под классификацией (тематическим моделированием) информации в данном случае понимается тип интеллектуального анализа текста, в ходе которого выявляется устойчивая тематическая структура в больших текстовых коллекциях,

т.е., другими словами, тематическое моделирование – это разбиение документов на кластеры, причем каждый кластер представляет собой отдельную тему. При этом выполняется нечёткая кластеризация [56]. Как правило, для решения задач тематического моделирования используются такие методы как латентно-семантический анализ (LSA), вероятностный семантический анализ (pLSA), скрытое распределение Дирихле (LDA), метод k-средних (k-means) и др. [106,126].

Суммаризация текста – это генерация краткого содержания исходного текста (заголовка, резюме, аннотации) с использованием инструментов интеллектуального анализа текстовых данных. Методы суммаризации делят на экстрактивные и абстрактивные [109]. При экстрактивной суммаризации происходит извлечение их исходного текста наиболее значимых информационных элементов (например, предложений). Абстрактивный метод отличается тем, что в ходе его реализации генерируется новый текст, обобщающий информацию, изложенную в исходном тексте (по изложению похоже на краткий пересказ прочитанного текста). В исследованиях [21, 78, 109] проведен сравнительный анализ методов суммаризации, в которых авторы приходят к выводу о том, что абстактивные методы обеспечивают более качественную суммаризацию текстов (близкую к ручному составлению), вместе с тем являются более сложными и трудоемкими в процессе реализации. Также немаловажное значение имеет выбор метода суммаризации, так как он должен соответствовать поставленным задачам, например, методы, хорошо зарекомендовавшие себя с новостными лентами, могут плохо работать с литературными произведениями. Активное развитие абстрактивных методов суммаризации связано с разработкой алгоритмов машинного обучения, в том числе рекуррентных НС, сверточных НС, долгой краткосрочной памяти (Long short-term memory; LSTM), которая представляет собой особую разновидность архитектуры рекуррентных НС, способную к обучению долговременным зависимостям.

С приходом новых технологий глубокого обучения, в частности архитектуры трансформеров, начался следующий этап в развитии абстрактивных методов. О перспективности использования таких моделей трансформеров, как BERT, BART,

GPT-3, T5 в задачах классификации и суммаризации текстовых данных говорят исследования последних лет [21, 88, 110, 156].

Основными этапами при решении задач тематического моделирования и суммаризации с использованием инструментов интеллектуального анализа текстов являются: сбор и подготовка корпусов текстов, предобработка корпусов текстов, выделение тематических групп в корпусе текстов, векторизация, понижение размерности, кластеризация, далее, в зависимости от поставленной задачи, для тематического моделирования составляется список тем и для каждого текста определяется принадлежность к одной из тем, либо для суммаризации проводится выделение смысловых фрагментов и репрезентативных предложений.

Для автоматизации решения поставленных задач применяются следующие методы:

– Natasha – набор Python-библиотек для обработки текстов на естественном русском языке. Состоит из 9 репозиториев, объединенных одним интерфейсом (например, Razdel – система токенизации предложений и слов, основанная на правилах для русского языка). Решает задачи обработки русского языка: сегментация на токены и предложения, лемматизация, извлечение, нормализация именованных сущностей;

– pymorphy2 – морфологический анализатор для русского языка на Python, который позволяет склонять слова, определять часть речи, падеж и т.д.;

– SpaCy – библиотека ПО с открытым исходным кодом для расширенной обработки ЕЯ, написанная на языках программирования Python и Cython, которая позволяет склонять слова, выделения именованных сущностей, создавать собственные модели для анализа и т.д.;

– NLTK (Natural Language Toolkit) – это ведущая платформа для создания программ Python для работы с текстами на ЕЯ (русском, английском и др). NLTK предоставляет простые в использовании интерфейсы для более чем 50 корпусов и лексических ресурсов, таких как WordNet, а также набор библиотек для классификации, токенизации, выделения корней, тегов, синтаксического и семантического анализа, и т.д.

Для успешного использования методов машинного обучения необходимо провести предварительную обработку текстовых данных.

2.2 Построение корпуса текстов из открытых источников в области ИБ и векторное представление слов

Использование методов векторного представления слов и метрик оценки семантической близости является весьма перспективными способами анализа слабоструктурированных данных (текстов на ЕЯ) [23, 57]. На современном этапе развития машинного обучения для решения подобных задач используются различные методы, некоторые из них уже можно отнести к классическим – это линейные методы классификации, модели на основе гауссовских распределений, деревья решений и др. Вместе с тем существуют иные методы обработки последовательностей, например, скрытые марковские модели, модели на основе условных случайных полей. Наибольшую популярность в последние годы приобрели НС, для обучения которых используются инструменты векторного представления слов – word embeddings.

Для того чтобы перейти непосредственно к использованию методов машинного обучения, необходимо провести предварительную обработку текстовых данных. Авторы [22] предлагают в своей работе алгоритм предварительной обработки текстовых данных, состоящий из 5 этапов:

1) извлечение контента;
2) выделение абзацев;
3) выделение предложений;
4) выделение лексем;
5) маркировка лексем тегами частей речи.

Извлечение контента для создания полезного корпуса текста является одной из важнейших задач, от которой зависит качество дальнейшей обработки текста. Проблемой здесь является отсутствие четкой структуры обрабатываемых текстов. Существуют специальные инструменты (например, readability-lxml),

использующие регулярные выражения для удаления ненужных символов, тегов сценариев, рекламы и т.п.

Выделение абзацев необходимо для эффективного разделения документа на составляющие компоненты с сохранением первоначальной структуры документа. Абзацы, содержащие в себе законченные идеи, выполняют роль структурной единицы документа. Подобное исследование документа может существенно повлиять на то, как будет в дальнейшем классифицироваться статья.

Выделение предложений. По аналогии с абзацами, предложения можно считать смысловыми единицами, которые содержат законченную мысль. В письменном тексте предварительная сегментация упрощает маркировку лексем частями речи. С этой целью используют такой инструмент, как sent_tokenize из NLTK.

Выделение лексем (токенизация) – процесс извлечения лексем из текста путем разбиения потока текста на фразы, слова, символы или значимые элементы, называемые лексемами (токенами). Применение лексемизации ведет к формированию листа, содержащего лексемы в порядке их нахождения в документе. Каждая лексема содержит число с информацией о том, из какого общего модуля он был создан. С этой целью может быть использован инструмент RegexpTokenizer.

Маркировка лексем тегами частей речи. Маркировка частями речи заключается в добавлении к каждой лексеме соответствующего тега, несущего информацию об определении слова и его роли в текущем контексте. Средством маркировки из NLTK является инструмент pos_tag.

В других источниках [68] используются иные термины для описания, по сути, тех же процедур, они изложены в разделе 1.4 данного исследования.

Предобработанные таким образом текстовые описания далее подаются на вход алгоритмов векторизации текстовых данных.

Специалистам в области ИБ обработка больших объемов текстовых данных необходима как с тактической точки зрения для оценки актуальности уязвимостей и угроз, так и со стратегической точки зрения для оценки трендов в отношении используемых нарушителями путей (тактик/техник) реализации уязвимостей,

направления будущих атак. Для решения оперативной задачи по оценке актуальных угроз БИ и уязвимостей необходимо проанализировать около 40 тысяч описаний уязвимостей, 222 описания угроз, 10 тактик (и соответствующих им техник). Для оценки трендов и построения прогнозов в области ИБ возможен анализ текстовых данных статей журналов, специализированных сайтов, блогов в области ИБ. В разделе 2.3 данного исследования проводится анализ 438 научных статей (журнал «Вопросы кибербезопасности» за период с 2013 по 2022 годы).

Предлагаемая структура конвейера обработки текстовых данных представлена в Таблице 2.1. Основные этапы и применяемые фреймворки отражают накопленный ведущими специалистами по компьютерной лингвистике и интеллектуальному анализу текстов опыт, а также адаптированы для использования с русскоязычным корпусом текстов. Применение нейросетевых моделей вложений на уровне слов и параграфов требует предварительной предобработки для построения качественных векторов признаков. Здесь и далее предлагается использовать модульный принцип построения информационных систем и опираться на существующие библиотеки и фреймворки, интерфейс которых реализован на языке программирования Python. Подобные фреймворки (Natasha, Spacy, NLTK, pymorph) поддерживаются ведущими отечественными и зарубежными специалистами (DeepPavlov, Яндекс и т.д.) и отражают наиболее свежий «срез» инструментальных средств языковой обработки. Их применение позволяют существенно повысить эффективность анализа за счет возможности сравнения множества подходов и моделей и выбора оптимальной конфигурации итогового решения.

Таблица 2.1 – Структура конвейера обработки текстовых данных

Этап	**Шаги**	**Действия**	**Инструменты**
Предобработка	Символьная фильтрация	Удаление нерелевантных символов, HTML-тегов	Набор регулярных выражений
	Токенизация	Разбивка текста на токены с помощью предобученной для русского языка нейросетевой модели	Razdel (фреймворк Natasha), Spacy, Stanza, nltk

Этап	Шаги	Действия	Инструменты
	Фильтрация нерелевантных токенов	Удаление ссылок, нерелевантных сокращений	Регулярные выражения
Нормализация	Лемматизация	Приведение слов в исходную форму с помощью предобученной нейросетевой модели	Morph (фреймворк Natasha), pymorphy2, spacy
Постобработка	Частеречная фильтрация	Остаются только существительные, глаголы, прилагательные, наречия, местоимения	Morph (фреймворк Natasha)
	Извлечение именованных сущностей	Разметка тегами выделенных типов именованных сущностей	Natasha, spacy
	Фильтрация на основе стоп-словарей	Фильтрация нерелевантных лемм с помощью составного стоп-словаря, включающего наиболее часто встречающиеся слова корпуса текстов	NLTK-russian, english
	Формирование документа-строки	Объединение лемм в нормализованную строку-документ	

Далее для выявления основных тем (структуры) анализируемых научных статей проводится тематическое моделирование. Шаги алгоритма тематического моделирования и используемые при этом инструменты представлены в Таблице 2.2. Рассмотренные решения отражают текущее состояние методов, моделей и алгоритмов для тематического моделирования текстов в порядке возрастания сложности (вычислительной сложности, в том числе) применения и качества ожидаемых результатов. Заключительные шаги алгоритма основаны на применении актуальных моделей-трансформеров.

Таблица 2.2 – Основные шаги алгоритма тематического моделирования

№	Шаг алгоритма	Модель (инструмент)	Примечания
1	Предварительная обработка и нормализация текстов	конвейер обработки текстовых данных	см. табл. 2.1
2	Извлечение признаков из текста (формализация)	TF-IDF – построение взвешенного частотного словаря (TF) и разреженной матрицы встречаемости слов с последующим взвешиванием с помощью вектора обратной частоты документа (IDF) – матрица «термы-документ»	-

№	Шаг алгоритма	Модель (инструмент)	Примечания
		хеширование вхождений слов в пространстве фиксированного размера, нормализация векторов слов с помощью L_2-нормы	
		предобученная дистрибутивно-семантическая языковая модель FastText [149]– вектор предложения строится путем нормализации и усреднения векторов токенов	[93]
		предобученная модель-трансформер SBERT – вектор предложения и/или документа строится путем усреднения выходного слоя модели	[134] – нормализация не выполняется
3	Понижение размерности признакового пространства	сингулярное разложение матрицы (NMF) «термы-документ» TF-IDF согласно алгоритму скрытого семантического анализа (LSA)	[104,123]
4	Тематическое моделирование	кластеризация документов с помощью алгоритма K-Means с оценкой оптимального количества кластеров с помощью метрики «ширина силуэта»	[121, 152]
		неотрицательная матричная факторизация (пакетная реализация с различными целевыми функциями: нормой Фробениуса и обобщенной дивергенцией Кульбака-Лейблера)	-
		скрытое распределение Дирихле (LDA)	[92]
		представление на уровне документа, на уровне *n*-грамм ключевых слов и словосочетаний с помощью предобученной модели-трансформера на основе оценки семантической близости их векторов вложений	- модель Top2Vec [87]; - модель KeyBert; - модель BERTopic [108]

Для составления аннотаций (сжатия) анализируемых научных статей предлагается применить алгоритм суммаризации. Комплекс моделей и инструментов, используемых в ходе этой процедуры представлен в Таблице 2.3. Применение выбранных моделей обусловлено анализом результатов схожих исследований и серией проведенных экспериментов, подтвердивших выбор.

Таблица 2.3 – Комплекс моделей и инструментов, используемых в алгоритме суммаризации

№	Шаг алгоритма	Модель (инструмент)	Примечания
1	Предварительная обработка и нормализация текстов	Конвейер обработки текстовых данных	см. табл. 2.1

№	Шаг алгоритма	Модель (инструмент)	Примечания
2	Извлечение признаков из текста (формализация)	TF-IDF – каждое предложение входного текста рассматривается независимо, строится матрица «термы-документ»	-
		предобученная модель FastText – вектор предложения строится путем нормализаци и усреднения векторов токенов	[93]
		предобученная модель RuBERT и SBERT – вектор предложения строится путем усреднения выходного слоя модели	[139] – предобработка, фильтрация и нормализация не выполняется
3	Выделение наиболее важных предложений, раскрывающих смысловые фрагменты документа	$TextRank_1$ – алгоритм PageRank с оценкой близости предложений как количество совпадающих слов в них, нормированное их суммарной длиной	[93]
		$TextRank_2$ – алгоритм PageRank с оценкой семантической близости предложений на основе косинус-меры	[139] формальный вектор предложения строится с помощью модели SBERT
		Кластеризация предложений с помощью алгоритма K-Means с оценкой оптимального количества кластеров с помощью метрики «ширина силуэта»	[124, 139, 152,]
4	построение итогового реферата	Выбор наиболее важных узлов графа TextRank	-
		Включение в реферат предложений, наиболее близких к выделенным центроидам кластеров	-
		Генерация текста с помощью модели трансформера T5 на основе выделенных с помощью TextRank наиболее важных узлов графа	[112] Модель-трансформер mT5, обученная на датасете XL-Sum (более 1 млн. аннотированных статей на 44 языках)

В разделе 2.3 представлены экспериментальные исследования в области тематического моделирования и суммаризации анализируемых тестовых данных.

2.3 Шаблон решения задачи классификации и суммаризации текстов с использованием технологии трансформеров

Исходными данными для построения проблемно-ориентированного корпуса текстов послужили полнотекстовые статьи выпусков журнала «Вопросы кибербезопасности» за период с 2013 по 2022 гг., размещенные в сети Интернет.

Для автоматизации сбора и подготовки корпусов текстов был разработан модуль, представленный на Рисунке 2.1.

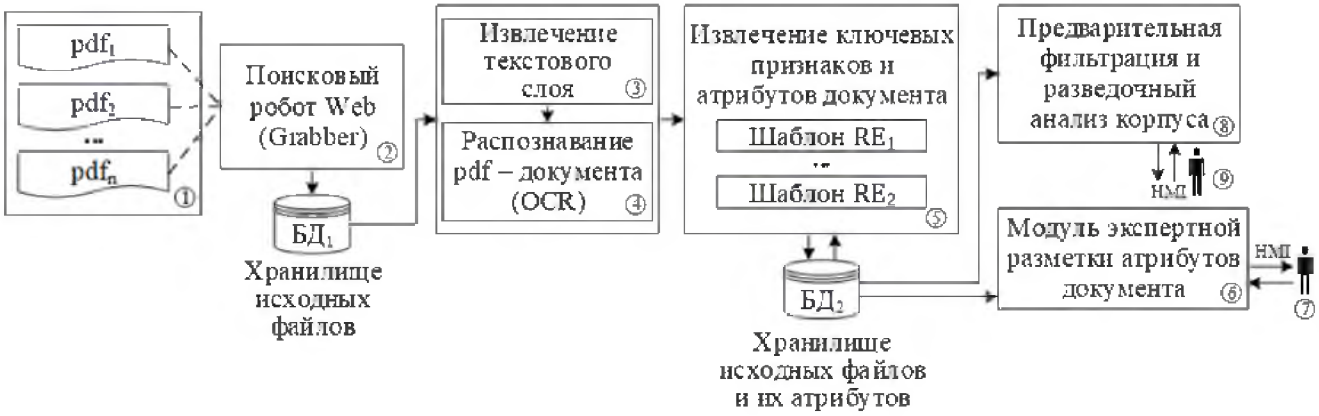


Рисунок 2.1 – Структура модуля сбора и подготовки корпуса документов

План проведения эксперимента представлен на Рисунке 2.2.

Данный модуль работает следующим образом. С помощью поискового робота (2) выполняется анализ стартовой HTML-страницы (1) с целью поиска и извлечения ссылок на документы формата pdf по схеме «обход в ширину». Собранные документы в формате pdf (всего найдено 438 документов) помещаются в хранилище исходных файлов ($БД_1$).

Следующий этап подразумевает получение текстовой информации из собранных pdf-документов с помощью модуля извлечения текстового слоя (3) для корректно созданных файлов или применения инструментов распознавания (OCR) pdf-файлов как набора изображений (4) для документов со сложной структурой и версткой.

Далее осуществляется извлечение с помощью набора разработанных регулярных выражений (5) основных атрибутов и ключевых признаков документа: название, авторы, аннотация, ключевые слова, DOI, номер журнала (локальный и глобальный), год выпуска, текст статьи, список литературы. Текстовый документ и его атрибуты размещаются в документ-ориентированном хранилище ($БД_2$). Модуль экспертной разметки атрибутов документа (6) с участием человека (7) позволяет откорректировать ошибочно выделенные значения, например разрыв строки в названии, пропуск блока литературы и т.п.

Рисунок 2.2 – План проведения эксперимента по классификации и суммаризации анализируемых научных статей

С помощью категоризации *n*-грамм, выделяемых из текста, и их частотного анализа определяется язык документа: русский или английский. Дальнейший анализ выполнен для 321 статьи на русском языке с непустой аннотацией.

Далее выполняется предварительная фильтрация и разведочный анализ (8) корпуса текстов, позволяющий оценить предварительное соотношение текстов документов и их аннотаций (Таблица 2.4).

Таблица 2.4 – Структура текстов и аннотаций

Статистика в разрезе	Параметр	Значение
Текстов	Максимальное количество слов	10488
	Минимальное количество слов	483
	Среднее количество слов	3381
	Среднее количество предложений	128
	Среднее количество уникальных слов	1149
	Среднее количество уникальных лемм	811
Аннотаций	Максимальное количество слов	340
	Минимальное количество слов	1
	Среднее количество слов	98,4
	Среднее количество предложений	4,57
	Среднее количество уникальных слов	67,2
	Среднее количество уникальных лемм	59,8
Пересечение текстов и аннотаций	Среднее по числу уникальных слов	67,8 %
	Среднее по числу уникальных лемм	59,8 %
	Среднее по числу слов	98,96 %
	Среднее по числу лемм	98,95 %
	Среднее по числу биграмм	93,97 %
	Среднее по числу триграмм	80,92 %

Особенностью построенного корпуса документов является следующее:

– и аннотации, и тексты документов достаточно объемны;

– вариабельность (длина, количество предложений) текстов – средняя;

– аннотации не являются экстрактивными.

Тематическое моделирование на основе кластеризации документов с предварительным понижением размерности признакового пространства (Таблица 2.5). Понижение размерности признакового пространства выполнено с помощью сингулярного разложения матрицы «термы-документы» TF-IDF согласно алгоритму латентно-семантического анализа (LSA).

Таблица 2.5 – Схема кластеризации корпуса текстов

Исходное признаковое пространство	Алгоритм понижения размерности	Алгоритм кластеризации	Оценка коэффициента «ширина силуэта» для выделенной структуры кластеров («больше – лучше»)
TF-IDF	-	Алгоритм k-средних (k-means, 5 проходов, 1000 итераций, 10 центров)	0,009 ± 0,012
	LSA		0,064 ± 0,007

Исходное признаковое пространство	Алгоритм понижения размерности	Алгоритм кластеризации	Оценка коэффициента «ширина силуэта» для выделенной структуры кластеров («больше – лучше»)
		Алгоритм k-средних для наборов (MiniBatchKMeans, 10 центров)	0,034 ± 0,028
Хешированное векторное представление	LSA	Алгоритм k-средних (k-means, 5 проходов, 1000 итераций, 10 центров)	0,059 ± 0,004
		Алгоритм k-средних для наборов (MiniBatchKMeans, 10 центров)	0,010 ± 0,021

Как показали эксперименты, кластеризация в LSA-представлении матрицы признаков выполняется значительно быстрее ввиду существенно меньшего их количества, а оценка качества кластеризации, наоборот, улучшилась. При инверсии матрицы признаков становится возможным идентификация центров кластеров как списка наиболее важных слов для каждого кластера:

```
Cluster 0: национальный российский защита год федерация организация технология
международный стандарт требование
Cluster 1: вероятность злоумышленник проникновение кабинет взлом канал утечка
функция схема блок
Cluster 2: модель защита атака объект воздействие управление сеть оценка угроза
процесс
Cluster 3: сеть пользователь код изображение алгоритм программный устройство
сигнал защита мобильный
Cluster 4: риск оценка угроза управление ущерб реализация защита нарушение уровень
этап
Cluster 5: ключ подпись схема алгоритм квантовый шифрование криптографический шифр
функция блочный
Cluster 6: метаданные аис эда элд документ электронный целостность запись
криптографический рекурсивный
Cluster 7: текст признак корпус словарь противоправный личностный именной группа
лексический психологический
Cluster 8: полином булев уравнение число матрица моном комбинаторный
алгебраический линейный нуль
Cluster 9: автомат клеточный ячейка обобщенный функция состояние параллельный
кольцо граф криптография
```

Автоматически выявленная структура кластеров частично отражает основные тематики, определяемые редакцией журнала. Например: Безопасность в сетях общего доступа, Анализ рисков информационной безопасности, Методы и средства кодирования информации, Методы и средства стеганографии, Методы анализа программ и верификации, Теоретические основы информатики. В то же время, достаточно сложно автоматически декомпозировать документы «сложных» тематических групп, таких как: Концептуальные вопросы кибербезопасности,

Киберпротивоборство и операции, Безопасность критической инфраструктуры и т.п.

Проецирование матрицы TF-IDF с установленными метками кластеров с помощью метода главных компонент (PCA) в двумерное признаковое пространство позволяет оценить взаиморасположение и плотность полученного разбиения на кластеры (Рисунок 2.3). В качестве наложенных подписей выделены наиболее близкие к центрам кластеров слова (термы).

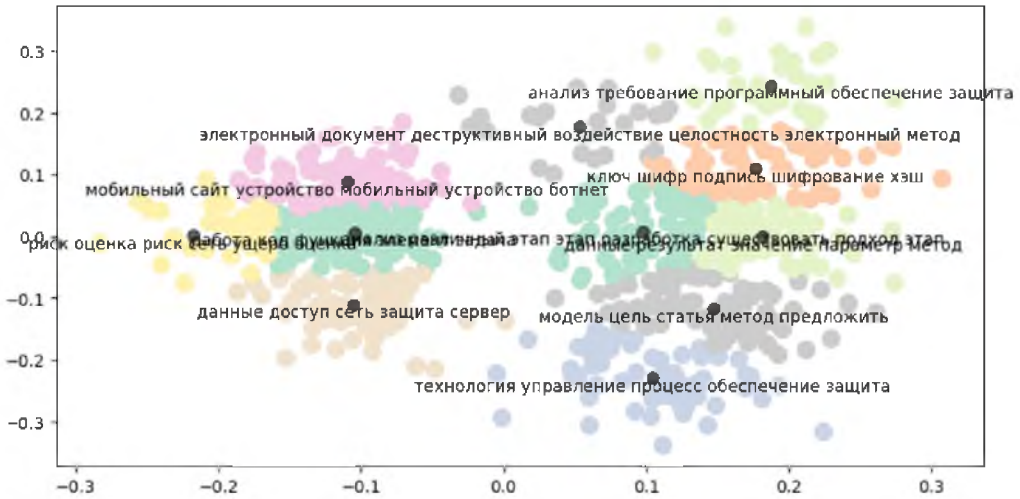


Рисунок 2.3 – Визуализация выделенных кластеров и наиболее важных слов для каждого из них

Анализ выделенной структуры позволяет оценить взаиморасположение тематических кластеров, их плотность и обособленность, а также принять решение о необходимости слияния или, наоборот, разделения тематических групп.

Тематическое моделирование с помощью скрытого распределения Дирихле (LDA) и неотрицательной матричной факторизации (NMF) (пакетная реализация с различными целевыми функциями: нормой Фробениуса и обобщенной дивергенцией Кульбака-Лейблера) позволяет построить альтернативный вариант аддитивных моделей тематической структуры корпуса и сравнить с построенной ранее кластерной моделью. Анализ выделенных тем (Таблица 2.6) показывает, что пакетная реализация с целевой функцией, определяемой обобщенной дивергенцией Кульбака-Лейблера, позволяет выделить

тематики документов с более сбалансированным количеством документов, а при использовании в качестве целевой функции нормы Фробениуса явно выделяет основные ключевые слова для каждой из тематик.

Таблица 2.6 – Сравнение выделенных тематик

Модель / Тема	MiniBatchNMF (Frobenius norm)	MiniBatchNMF (Kullback-Leibler norm)	LDA
1	Модель защиты	Модель защиты	Аппаратные и программные закладки
2	Криптография	Алгоритмы криптографии	Цифровая подпись
3	Криптография + управление	Национальная кибербезопасность	Моделирование сетей
4	Оценка рисков	Оценка рисков	Оценка рисков
5	Клеточные автоматы	Моделирование сетей	Модель объекта защиты + угроз
6	Цифровая подпись	Цифровая подпись	Не определена
7	Мобильные устройства	Мобильные и веб-приложения	Модель канала
8	Социальные сети	Социальные сети	Не определена
9	Сертификация специалистов ИБ	Модель доступа + Сертификация специалистов ИБ	Стеганография
10	Стеганография	Стеганография	Хеширование

Аддитивная модель на основе скрытого распределения Дирихле, напротив, акцентирует внимание на трех основных тематиках.

Тематическое моделирование на основе моделей векторных вложений. Для формирования гетерогенных моделей вложений использованы модель BERTopic (Рисунок 2.4) и модель Top2Vec.

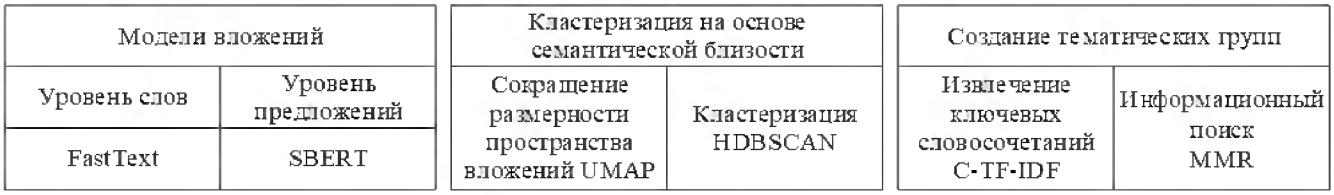


Рисунок 2.4 – Общая схема применения моделей-трансформеров для извлечения ключевых слов

В сочетании с моделью вложений на уровне документа предлагается использовать дистрибутивно-семантическую языковую модель FastText [93],

которая рассматривает каждое слово как композицию n-грамм символов и позволяет строить более качественные векторные вложения для редких и отсутствующих в обучающем корпусе слов при работе с флективными языками (в подобных языках доминирует словоизменение при помощи флексий – формантов, сочетающих сразу несколько значений) [19]. Для получения представления на уровне документа модель BERTopic формирует вложение (embedding) с помощью предобученного трансформера KeyBERT. Затем строятся вложения слов и слов/словосочетаний в виде n-грамм. Строится набор моделей векторизации, которые извлекают ключевые фразы с шаблонами частей речи из коллекции текстовых документов и преобразуют их в матрицу ключевых фраз документа [151] («ключевая фраза-документ»), позволяют проводить фильтрацию по «стоп-словарю» и адаптивное взвешивание векторов вложений ключевых фраз. Далее оценивается косинусное расстояние для поиска слов и словосочетаний, наиболее семантически близких к документу, понижение размерности с помощью алгоритма UMAP [135] и кластеризации (HDBSCAN) [129]. Метод максимальной граничной значимости (MMR) информационного поиска [94] позволяет повысить разнообразие получаемых ключевых слов, отсортированных в порядке убывания меры близости к исходному документу.

Одной из важнейших задач тематического моделирования является подбор количества выделяемых тем. Для собранного корпуса текстов подбор количества тем выполнен на основе анализа коэффициента согласованности (coherence) и коэффициента перекрытия кластеров для моделей SBERT и LDA (Рисунок 2.5).

Автоматическая оценка количества выделяемых тем показала, что для обеих моделей оптимальное количество тем составляет 26. Подобная оценка применима, если предварительно не заданы ключевые слова/словосочетания, используемые в качестве центров предполагаемых тематических групп. Ввиду ограниченного объема анализируемого корпуса такая детализация является излишней, т.к. отдельные темы содержат недостаточное количество документов, либо являются слишком близкими по содержанию. При увеличении количества документов автоматический выбор количества тем становится более обоснованным.

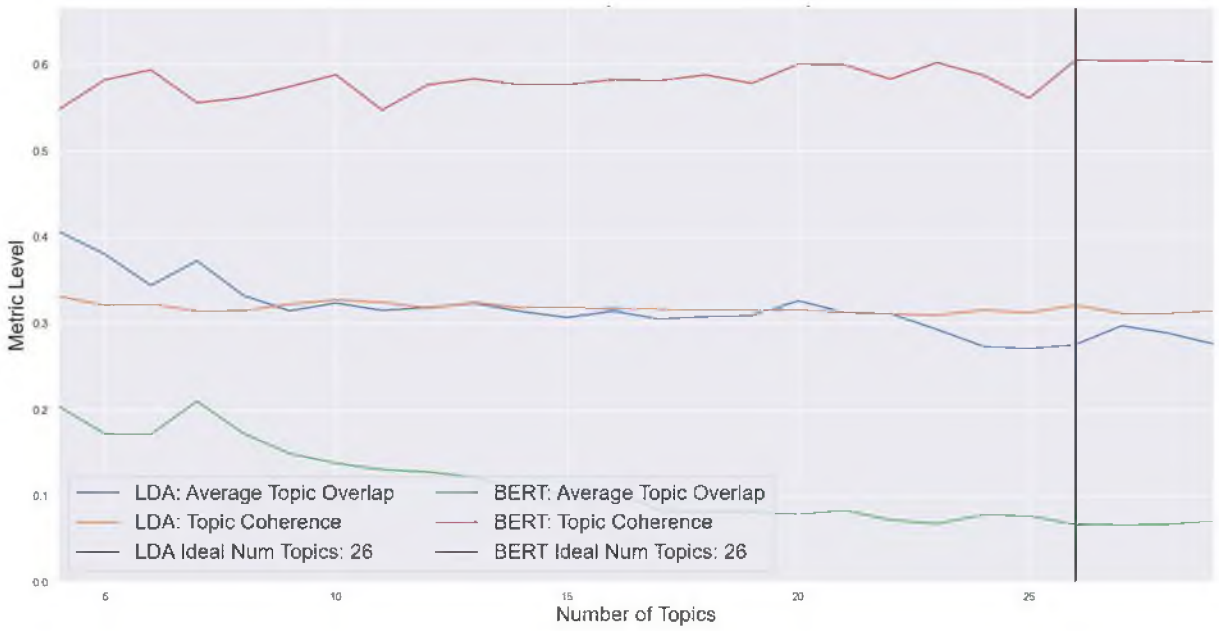


Рисунок 2.5 – Коэффициенты согласованности и перекрытия тем для моделей SBERT и LDA в зависимости от количества выбираемых тем (количество тем варьировалось от 4 до 35)

Основные результаты тематического моделирования в выявлении новых направлений исследований и применяемых инструментов в области ИБ представлены в Таблице 2.7. Из всего корпуса документов и для подмножеств документов по годам извлечены ключевые слова и словосочетания.

Таблица 2.7 – Ключевые слова и словосочетания для корпуса документов

Год	**Ключевые словосочетания**	**Оценка близости к документам за год**
2014	функционирование инфраструктуры управления противника, схема объект воздействия эффекты воздействия технологии защиты, числе применение кибероружия, ряд направлений толкования определения кибербезопасность, ходе исследования перечень угроз, перевод кибероружия,	0,5549 0,5321 0,5181 0,5138 0,5118 0,4893
2015	описание метода криптоанализа, реализации угроз безопасности информации содержание, внимание описание структуры канала передачи данных, основе известности видов кодирования сигналов, хранение базы данных подсистемы кэширования запросов, области безопасности информации взаимодействие,	0,6460 0,6132 0,6081 0,6026 0,5985 0,5972

Год	Ключевые словосочетания	Оценка близости к документам за год
2016	конкретизация порядка импортозамещения, описание этапов планирования состава средств защиты информации, механизмов реализации концепции, условиях усложнения проблем обеспечения кибербезопасности государства, концепция развития энергетики, решении проблемы импортозамещения,	0,6243 0,5700 0,5332 0,5326 0,5246 0,5198
2017	условии задания критерия вероятность нарушения конфиденциальности информации, случае представления авторами результатов анализа, пример представления вычислений уравнениями подобия, учете влияния множественности центров управления, примеры методики анализа рисков, вероятностей ошибок обоих типов,	0,5924 0,5780 0,5424 0,5338 0,5308 0,5197
2018	расчет коэффициента ущерба объекта информатизации органа, множество оценок эффективности использования средств защиты, пределы значимости уязвимости элементы защиты объекта информатизации, периодичности регистрации пакетов скорость динамики показателя тревоги, зашумление каналов передачи данных сигналами помех, исследовании задача классификации систем управления инцидентами безопасности,	0,5797 0,5782 0,5693 0,5607 0,5525 0,5516
2019	конкретизация моделей угроз безопасности информации, степени соответствия результатов защиты информации цели защиты информации, основе сравнения возможностей реализации угроз, результатом применения модели распределения механизмов защиты, базиса решетки решение задач теории решеток, практике исследования угроз безопасности информации,	0,6401 0,6044 0,5982 0,5907 0,5559 0,5490
2020	разработка методики оценки степени влияния системы защиты, каналы влияния источников угроз безопасности информации, гарантий корректности реализаций механизмов обеспечения защиты информации, алгоритмы адаптации интерфейсов пользователя, информации предотвращение передачи информации предотвращение применения, принцип декомпозиции процесса деятельности,	0,6177 0,6042 0,5974 0,5780 0,5743 0,5742
2021	определение матрицы вероятностей перехода, этапе разработка метода сравнения двух битов, уравнений метод решения систем, методах препроцессинга вектора, дефрагментация расшифрование обработка двух заголовков, отношении достижения задач тестирования,	0,6110 0,5977 0,5770 0,5553 0,5450 0,5355
2022	имя способа реализации угрозы копирования информации, угроз безопасности информации сопоставления описаний уязвимостей, выводов результатов криптоанализа схем,	0,6374 0,6344 0,6203

Год	Ключевые словосочетания	Оценка близости к документам за год
	статье метод контроля корректности функционирования программ, совершенствование методов определения пригодности криптосистем, суть алгоритма факторизации,	0,6148 0,6079 0,5873

С помощью выделенных наиболее релевантных ключевых слов можно проследить динамику распределения статей по тематикам, отражающим основные тренды в области обеспечения ИБ, затрагиваемой авторами.

Для выделения ключевых тем использована модель BERTopic [108], которая с помощью предобученной модели трансформера (построение вложений для отдельных предложений документов с взвешиванием – SBERT) и матрицы «термы-документ» TF-IDF с последующей кластеризацией позволяет формировать компактные кластеры – темы документов. С помощью модели SBERBANK_AI [83] и алгоритма кластеризации HDBSCAN [133] автоматически выделено 22 группы документов с последующим объединением в 8 ключевых тем, построен график зависимости количества документов каждой из тем по годам выхода журнала (Рисунок 2.6).

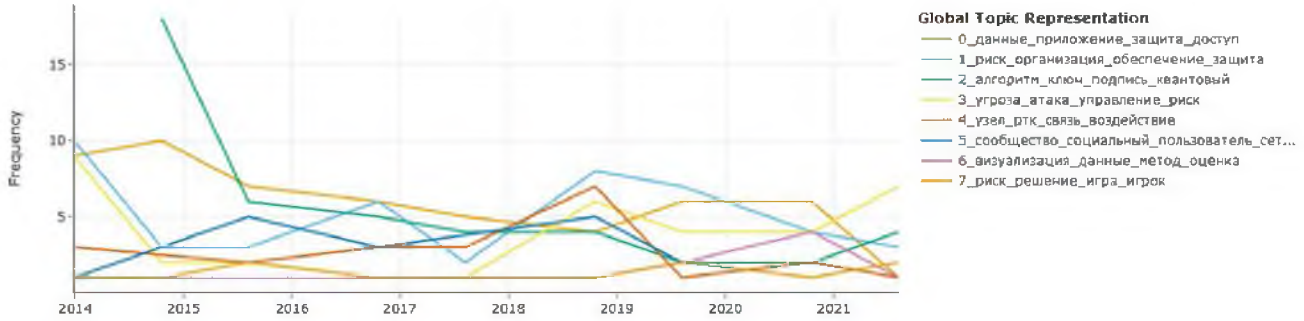


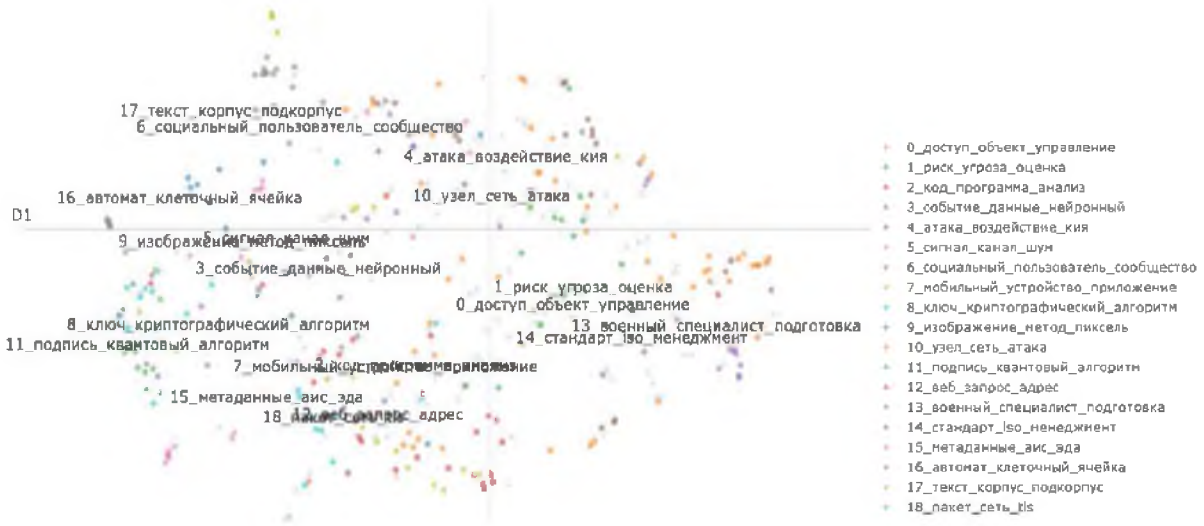
Рисунок 2.6 – Количество документов в выделенных темах по годам выхода журнала

Более информативным является анализ количества публикаций каждой из тематик по годам публикации. Заметно преобладание в количественном соотношении документов по тематикам «алгоритм_ключ_подпись_квантовый» («Криптография») и «данные_приложения_защита_доступ» («Обеспечение

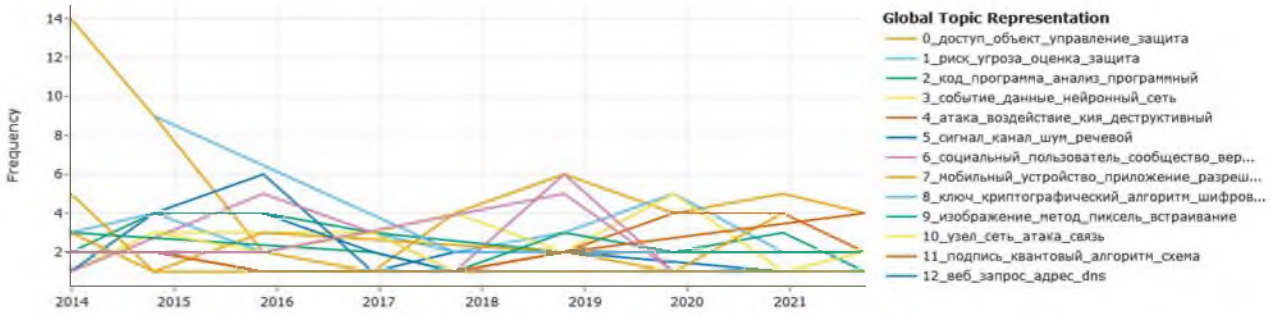
защиты данных в информационных системах») в период 2013-2016 гг. с последующим выравниванием по количеству публикаций других тематик.

Можно отметить повышательный тренд с 2021 г. по тематикам «алгоритм_ключ_подпись_квантовый» («Криптография») и «угроза_атака_управление_риск» («Обеспечение защиты данных в информационных системах»).

При использовании трансформера SBERT для создания вложений документов с векторизацией по ключевым фразам и модели FastText для создания вложений слов набор тематик более детализирован и включает 19 тем (Рисунок 2.7).



а)



б)

Рисунок 2.7 – а) Кластерная структура документов, полученная с помощью гетерогенных моделей вложений; б) динамика тематик по годам выхода журнала

Рассмотренные инструменты позволяют отслеживать количество документов определенной тематики и оценивать интересы исследователей к отдельным направлениям и задачам обеспечения кибербезопасности.

Отметим, что тематическое моделирование с использованием инструментов семантического анализа позволяет осуществлять гибкий поиск (семантический поиск) и оценку степени сходства документов с заданной темой (ключевым словом или словосочетанием), а не опираться только на указанные авторами ключевые слова.

Дальнейшие эксперименты связаны с суммаризацией корпусов текстов. Алгоритм суммаризации предложен в разделе 2.2 данного исследования и основан на моделях, предложенных в [111].

Для выделения наиболее важных предложений, раскрывающих смысловые фрагменты документа, предлагается использовать подходы на основе графового алгоритма Text Rank [132]:

1. Вершины взвешенного неориентированного графа сопоставляются с предложениями текста. Весовые коэффициенты ребер графа отражают степень сходства двух предложений, которая определяется как количество совпадающих в них слов, нормированное их суммарной длиной (TextRank_1), либо оценкой семантической близости на основе косинус-меры сходства формальных векторов предложений (TextRank_1).

2. С помощью алгоритма PageRank [89] каждой вершине сопоставляется коэффициент, определяемый рекуррентным выражением.

3. После стабилизации коэффициенты вершин упорядочиваются по убыванию значения веса и в реферат включаются первые n предложений.

Альтернативным вариантом определения наиболее значимых предложений для включения в реферат является алгоритм кластеризации [145]:

1. Для каждого предложения текстового документа строится вектор формальных признаков.

2. Рациональное количество кластеров определяется по методу «локтя» на основе оценки метрики качества кластеризации «ширина силуэта».

3. Реферат строится из предложений, наиболее близких к центроидам выделенных кластеров.

Вариант алгоритма абстрактивной суммаризации основан на последовательном применении алгоритма TextRank2 с последующим выделением набора предложений для преобразования «text-to-text» с помощью модели трансформера mT5, обученной на наборе данных XL-Sum (более 1 млн. аннотированных статей на 44 языках).

Итоговое сравнение для рассмотренных выше алгоритмов суммаризации представлено в Таблице 2.8.

Таблица 2.8 – Результаты суммаризации корпуса текстов

Модель	Экстрактивные методы						Абстрактивные методы
	TF-IDF + KMeans	SBERT + KMeans	Fast Text + KMeans	SBERT + Page Rank	Fast Text + Page Rank	Text Rank	Text Rank + T5
Метрика							
BLEU	0,115	0,110	0,069	0,022	0,002	0,082	0,107
ROUGE-1-F	0,250	0,234	0,185	0,092	0,037	0,254	0,257
ROUGE-2-F	0,126	0,110	0,068	0,017	0,003	0,141	0,130
ROUGE-L-F	0,206	0,194	0,143	0,074	0,027	0,194	0,204
Совпадение по леммам	0,356	0,320	0,338	0,354	0,522	0,512	0,501
Совпадение по парам лемм	0,092	0,068	0,091	0,129	0,302	0,202	0,267
Совпадения по тройкам лемм	0,042	0,029	0,047	0,082	0,217	0,116	0,154
Средняя длина	1066,84	1017,57	896,22	457,5	146,51	3043,99	768,28

Согласно полученным оценкам, наилучшими экстрактивными моделями реферирования являются TextRank, PageRank и TF-IDF+KMeans. Комплексная модель на основе трансформера T5 показала по отдельным метрикам сравнимый и в целом превосходящий результат. Однако, как отмечается в [114], автоматические

оценки работы алгоритмов реферирования на научных текстах имеют существенные ограничения, необходима экспертная оценка полученных рефератов (Таблица 2.9).

Таблица 2.9 – Фрагменты созданных рефератов

Алгоритм суммаризации	**Фрагмент реферата**
TF-IDF + KMeans	*Главными тенденциями развития угроз являются следующие : рост числа атак , многие из которых ведут к большим потерям ; возрастание сложности атак , которые могут включать несколько этапов и применять специальные методы защиты от возможных методов противодействия ; воздействие практически на все электронные (цифровые) устройства , в числе которых в последнее время все большую значимость приобретают мобильные устройства , а они в наибольшей степени подвержены рискам в области информационной безопасности ; …*
SBERT + KMeans	*В NUM г . Масштабные нарушения, затрагивающие все стороны жизни общества , в основе которых лежат новейшие методы осуществления атак на компьютерные сети , а также управление общественным сознанием требуют системного подхода к созданию комплексной системы безопасности , способной противостоять этим угрозам . …*
Text Rank	*Главными тенденциями развития угроз являются следующие : рост числа атак , многие из которых ведут к большим потерям ; возрастание сложности атак , которые могут включать несколько этапов и применять специальные методы защиты от возможных методов противодействия ; воздействие практически на все электронные (цифровые) устройства , в числе которых в последнее время все большую значимость приобретают мобильные устройства , а они в наибольшей степени подвержены рискам в области информационной безопасности ; …*

При решении задач суммаризации текста важную роль играет выбор критерия оценки качества результатов суммаризации. Для этих целей можно воспользоваться оценкой ROUGE (Recall-Oriented Understudy for Gisting Evaluation) [129], которая показывает, как сильно пересекаются два разных текста (в данном случае, это «правильное» краткое содержание текста и сгенерированное с помощью выбранного метода суммаризации). В общем виде оценка ROUGE-n вычисляется как среднее гармоническое между оценками точности ROUGE-n-Precision и полноты ROUGE-n-Recall, где:

ROUGE -n-Precision = (количество пересекающихся словосочетаний из *n*-слов) / (количество словосочетаний из n слов в сгенерированном тексте);

ROUGE -n-Recall = (количество пересекающихся словосочетаний из *n* слов) / (количество словосочетаний из n слов в правильном тексте).

Обычно при оценке эффективности по результатам экспериментов подсчитываются оценки ROUGE-1, ROUGE-2 и ROUGE-L, где L означает, что поиск пересечений идет не по фиксированному размеру словосочетаний (*n*-грамм), а по их наибольшему размеру.

Анализ полученных результатов показал следующее:

1. Формализация текстовых описаний с помощью моделей-трансформеров и SBERT не является удачным вариантом для последующего применения графовых алгоритмов реферирования, но хорошо подходит для тематического моделирования и выделения ключевых слов, словосочетаний и тематик с возможностью оценки семантической близости документов предметной области.

2. Наилучшие результаты реферирования продемонстрировал традиционный графовый алгоритм на основе TextRank, который не требует сложных лингвистических моделей, знаний предметной области или языка. Сочетание графовых алгоритмов и возможностей построения векторных вложений на уровне документа, предложений, слов и символов позволяет получить гибкий инструмент для выделения ключевой информации из анализируемых документов.

3. Для формализации признаков на уровне предложений и их дальнейшей кластеризации наиболее подходящей оказалась традиционная модель TF-IDF в задаче суммаризации и модель SBERT в задачах тематического моделирования.

4. Ручной анализ рефератов показал, что наилучшие результаты получены с помощью модели TextRank для текстовых документов, посвященных одной тематике. Модель SBERT + KMeans позволяет выделить в тексте несколько тематик и выбрать из них наиболее важные предложения для включения в реферат.

5. Модель формализации FastText продемонстрировала наихудшие результаты по автоматически определяемым метрикам в задаче реферирования, но позволяет повысить качество векторных вложений в сочетании с моделями-трансформерами в задаче тематического моделирования.

6. Для большинства нейросетевых моделей абстрактивного реферирования необходим большой предметно-ориентированный корпус для обучения (технология «переноса обучения»), скромные результаты работы моделей трансформеров «text-to-text» обусловлены, в первую очередь, малым размером собранного корпуса.

2.4 Выводы по второй главе

В данной главе изложены основные понятия, методы, этапы классификации и суммаризации с использованием технологий NLP. Проведено исследование о возможности использования алгоритмов автоматической классификации и суммаризации проблемно-ориентированных текстов для специалистов в области ИБ, показавшее перспективность использования инструментов интеллектуального анализа данных, в частности, алгоритмов Text Mining совместно с графовыми моделями применительно к анализу слабоструктурированной или неструктурированной информации на примере корпусов текстов, сформированных из научных статей журнала «Вопросы кибербезопасности». Использование данных алгоритмов позволяет повысить качество анализа документов и снизить когнитивную нагрузку на эксперта.

Результаты анализа проблемы тематического моделирования и реферирования (суммаризации) проблемно-ориентированных текстов для специалистов в области кибербезопасности показали следующее:

– проведенный эксперимент показал увеличивающийся с 2021 г. интерес научной общественности к таким тематикам, как «алгоритм_ключ_подпись_квантовый» («Криптография») и «угроза_атака_управление_риск» («Обеспечение защиты данных в информационных системах», внимание к последней тематике говорит об актуальности проводимого исследования в целом;

– применение моделей машинного обучения и интеллектуального анализа позволит на основе тонкой настройки (finetuning) существующих нейросетевых

языковых моделей, построенных на обобщенных корпусах текстов, в сочетании с классическими графовыми моделями, существенно повысить качество анализа исходных документов и снизить нагрузку на эксперта, в профессиональные обязанности которого входит анализ текстовых документов из различных источников в виде «сырых» слабоструктурированных данных, за счет их реферирования и автоматического выделения тем;

– для русскоязычного сегмента сегодня представлены лишь отдельные достаточно небольшие по размеру корпусы проблемно-ориентированных текстов по тематике кибербезопасности (до тысяч килобайт), что объясняется высокой трудоемкостью их сбора и отсутствием общепринятого протокола разметки, учитывающего структуру и номенклатуру отечественной документации;

– имеет место недостаточное количество полилингвальных языковых предметно-ориентированных моделей семейства BERT, T5 и др.;

– автоматически выявленная структура тематик (кластеров) частично отражает основные тематики, определяемые редакцией журнала, и является перспективным инструментом для анализа специализированных документов предметной области$

– тематическое моделирование с помощью гетерогенных моделей вложений позволяет выделять основные тематики документов и оценивать интересы исследователей к отдельным направлениям и задачам обеспечения кибербезопасности, расширяя возможности интеллектуального поиска и обработки текстовых данных с учетом семантики.

Глава 3. Разработка и исследование алгоритмов оценки угроз и уязвимостей информационной безопасности на основе технологий семантического анализа текстов в соответствии с требованиями Методики ФСТЭК России

В данной главе выполнено системное моделирование процесса оценки угроз БИ, изложенной в Методике ФСТЭК России, с целью выявления основных затруднений в работе при ее реализации. Разработаны алгоритмы векторизации и кластеризации, на их основе алгоритм оценки угроз и уязвимостей ИБ, метод оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объекта АСУ ТП на основе оценки их семантической близости с использованием БДУ ФСТЭК России. Разработана семантическая модель фрагмента сценария реализации угроз.

3.1 Функциональная модель процесса оценки и анализа актуальных угроз безопасности информации в соответствии с Методикой ФСТЭК России

Оценка угроз безопасности представляет собой сложную, многоэтапную задачу. Методика оценки угроз БИ ФСТЭК России определяет порядок и содержание работ, необходимых для определения угроз БИ различных информационных систем, в частности, для АСУ. Документ определяет как общий порядок работы при определении угроз БИ – определение негативных последствий, источников угроз, целей воздействий, так и детализирует порядок действий при определении актуальных угроз – определение сценариев угроз, который предусматривает установление последовательности возможных тактик и соответствующих им техник [7]. В рамках представленного исследования и в соответствии с [7] разработана методика оценки актуальных угроз ИБ объектов АСУ ТП КИИ (Приложение Б) и фрагмент модели угроз КИИ (Приложение В). Для проведения детального анализа Методики ФСТЭК предлагается применить методологию системного моделирования [8], одним из инструментов которого является IDEF-технологии (I-CAM DEFinition или Integrated DEFinition) – это

технологии семейства ICAM (Integrated Computer-Aided Manufacturing), предназначенные для решения задач моделирования сложных систем. В ходе системного моделирования процесса оценки актуальных угроз БИ проведена декомпозиция функций, реализуемых в ходе проведения оценки угроз БИ, выявлены процессы, предшествующие оценке актуальных угроз, и определен перечень документов (информации), необходимых для проведения этой процедуры, выявлены этапы непосредственно оценки актуальных угроз БИ, определена взаимосвязь между ними и также определен перечень документов (информации), необходимых для определения актуальных угроз БИ.

Использование IDEF-технологии позволит провести эффективный анализ процесса оценка угроз БИ и представить модель данного процесса в виде наглядной IDEF-диаграммы. Далее на Рисунках 3.1 ,3.2 и 3.3 представлены функциональные модели процесса оценки угроз БИ в нотации IDEF-0.

Согласно представленной на Рисунке 3.1 функциональной модели, процесс оценки угроз БИ включает в себя:

– анализ документации систем, сетей и иных документов (блок А1);

– определение негативных последствий от реализации угроз (блок А2);

– инвентаризацию систем и сетей, определение групп информационных ресурсов и компонентов систем и сетей (блок А3); (блок А2);

– определение источников угроз (блок А4);

– оценку способов реализации угроз (блок А5);

– оценку актуальных угроз (блок А6).

Функциональная модель оценки актуальных угроз (Рисунок 3.2) состоит из следующих блоков:

– сбор и анализ исходных данных для оценки актуальных угроз (блок А61);

– определение перечня возможных угроз БИ (блок А62);

– построение сценариев реализации угроз (блок А63);

– определение актуальных угроз (блок А64).

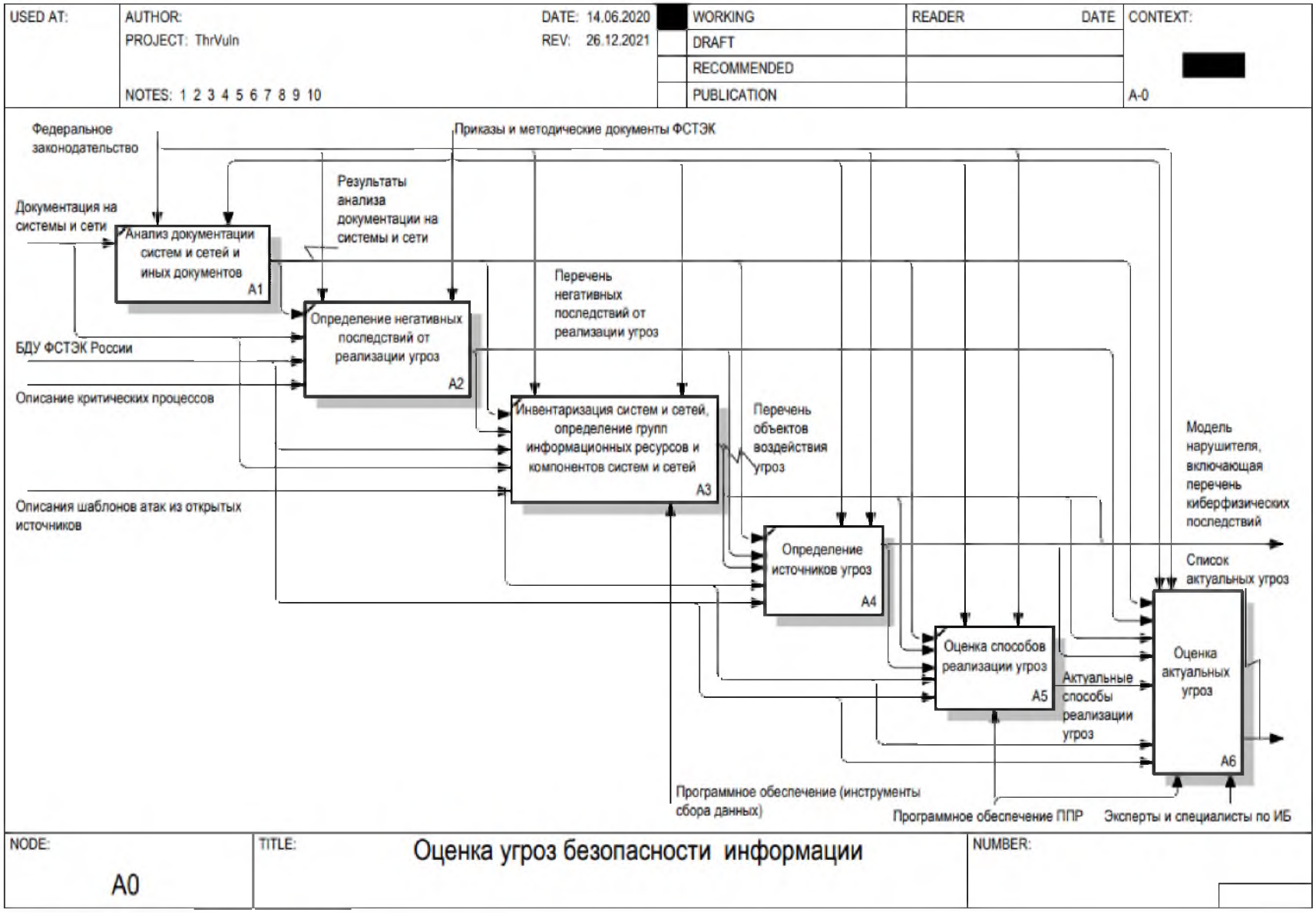


Рисунок 3.1 – Функциональная модель оценки угроз безопасности информации

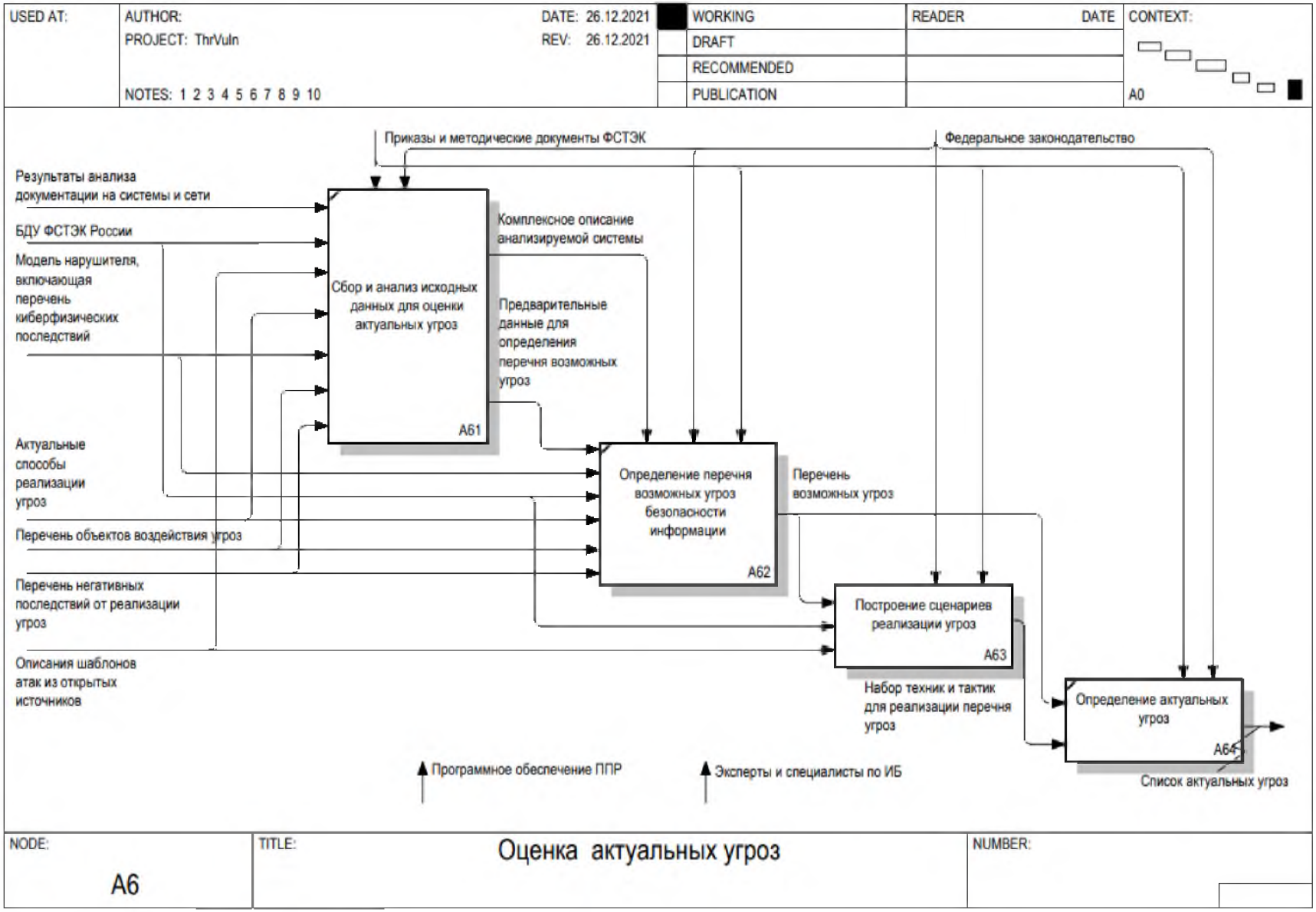


Рисунок 3.2 – Функциональная модель процесса оценки актуальных угроз

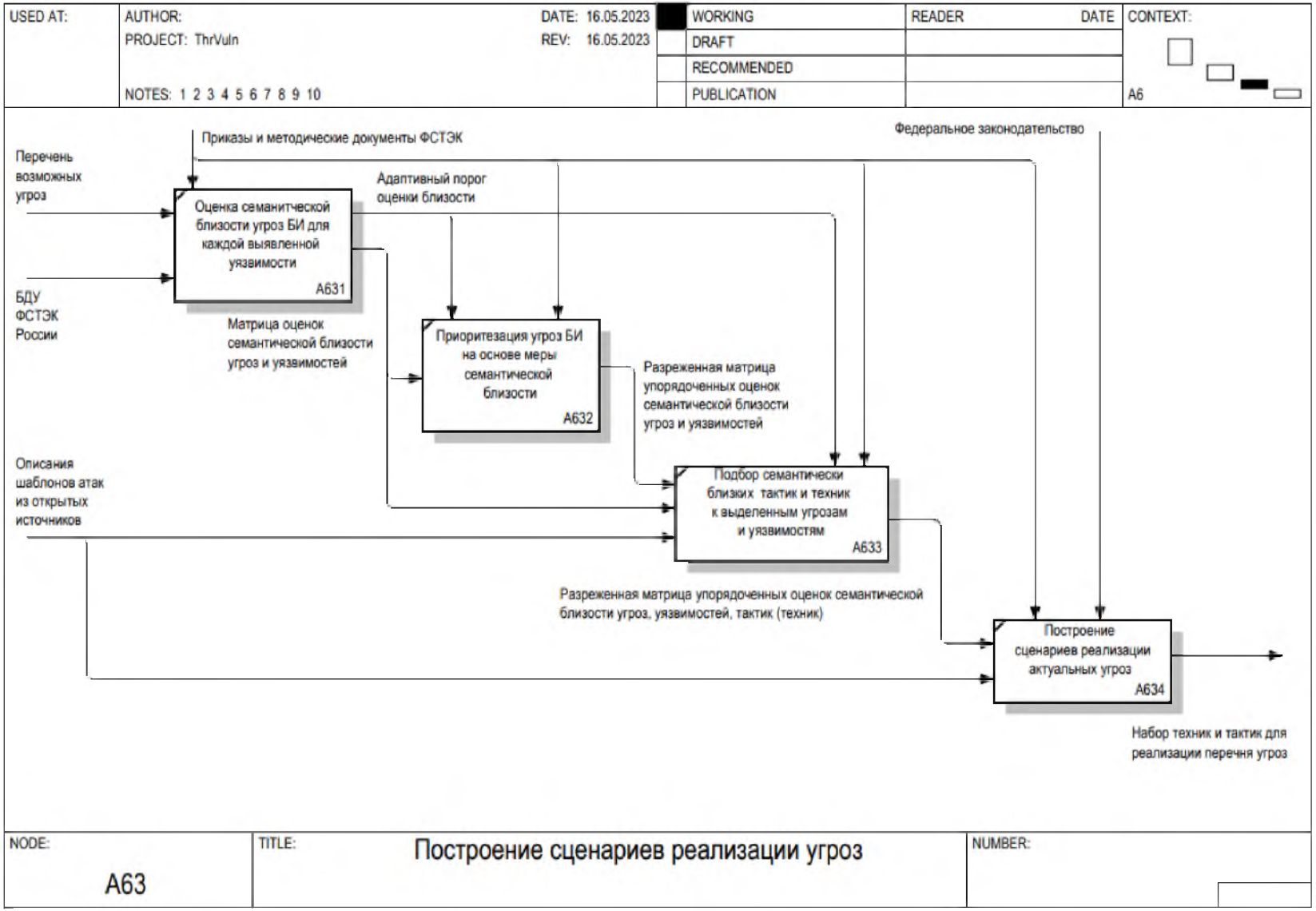


Рисунок 3.3 – Функциональная модель процесса построения сценариев реализации угроз

Процесс построения сценариев реализации угроз (рис.3.3) состоит из следующих этапов:

– оценка семантической близости угроз БИ для каждой выявленной уязвимости;

– приоритизация угроз БИ на основе меры семантической близости;

– подбор семантически близких тактик и техник к выделенным угрозам и уязвимостям;

– построение сценариев реализации актуальных угроз.

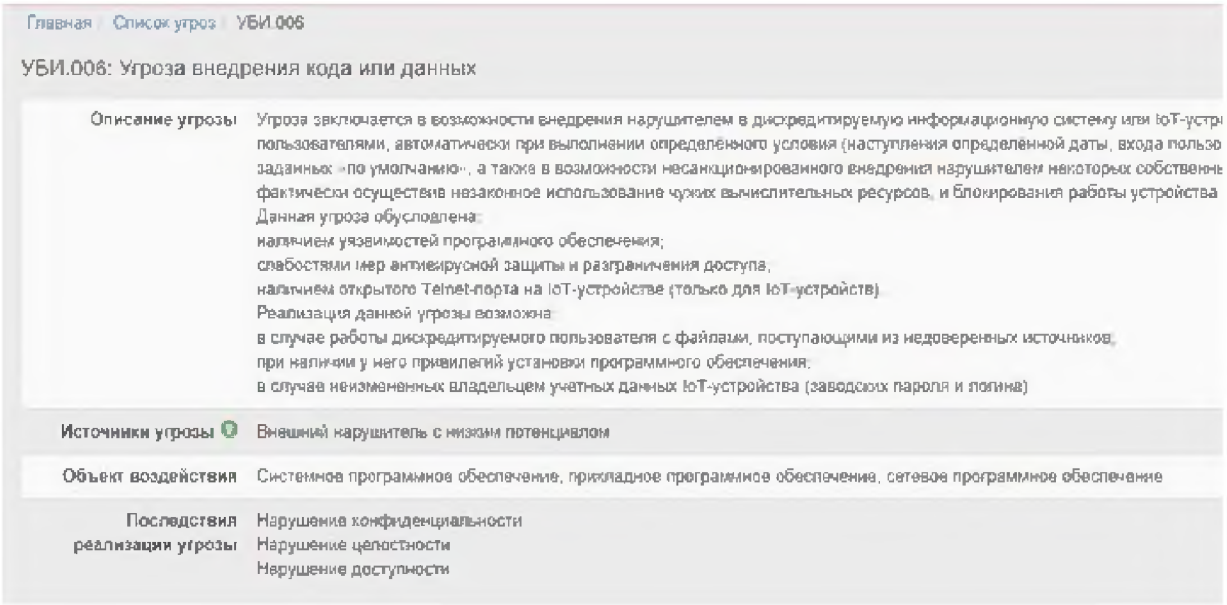
Основной сложностью при работе с данной методикой является определение сценариев реализации угроз (блок А63, Рисунок 3.2, 3.3) в связи с низкой степенью связанности с данными, полученными с предыдущих этапов (блоки А1-А4) (перечнями актуальных уязвимостей, типами доступа, типами нарушителей и т.п.), а также ввиду отсутствия автоматизированной системы, позволяющей упростить процесс сопоставления полученных данных (актуальных для данной системы уязвимостей, тактик (техник) и возможных угроз). Результаты проведенного анализа совпадают с мнением экспертов в области ИБ [82, 58].

Следовательно, актуальным является автоматизация процедуры построения сценариев эксплуатации уязвимостей и реализации угроз на основе текстовых описаний угроз, уязвимостей и тактик (техник), содержащихся в БДУ ФСТЭК. Для этого предлагается обобщить рассмотренные ранее подходы к построению семантических моделей. Далее описаны алгоритмы, позволяющие автоматизировать процесс оценки актуальных угроз и уязвимостей.

3.2 Разработка алгоритмов векторизации текстовых описаний угроз, уязвимостей, тактик (техник) и кластеризации угроз БИ и уязвимостей ПО объектов КИИ на основе метрик семантической близости текстовых описаний

В связи с необходимостью соответствия работы Методике ФСТЭК, в частности, этапу 3 «Оценка возможности реализации угроз и их актуальности»

требуется провести анализ текстовых данных, содержащихся в первую очередь в БДУ ФСТЭК России и, в случае необходимости, в зарубежных классификаторов угроз и уязвимостей, описанных в разделе 1.1 представленного исследования. На момент исследования БДУ ФСТЭК России содержала более 220 текстовых описаний угроз, свыше 34 тысяч описаний уязвимостей, 10 тактик и от 7 до 29 соответствующих им техник, образцы текстовых описаний представлены на Рисунках 3.4, 3.5, 3.6. В базе данных NDV содержалось свыше 135 тысяч описаний, в MITRE ATT&CK – 14 тактик и до 40 соответствующих им техник. В настоящее время для сопоставления уязвимостей, тактики (техник) и угроз специалисту по ИБ необходимо прочитать их текстовые описания и принять решение о том, насколько точно текстовые описания уязвимостей соотносятся с описаниями угроз, тактик и техник. То есть, по сути, построить сценарий реализации угроз в «ручном» режиме, что является трудоемкой задачей, требующей больших временных затрат, учитывая огромное количество узлов АСУ ТП, содержащихся на промышленных объектах. В связи с этим закономерно желание специалистов по ИБ автоматизировать данный процесс.



Главная / Список угроз / УБИ.006

УБИ.006: Угроза внедрения кода или данных

Описание угрозы	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устр пользователями, автоматически при выполнении определенного условия (наступления определенной даты, входа пользо заданных «по умолчанию», а также в возможности несанкционированного внедрения нарушителем некоторых собственны фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа; наличием открытого Telnet-порта на IoT-устройстве (только для IoT-устройств) Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения; в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина)
Источники угрозы	Внешний нарушитель с низким потенциалом
Объект воздействия	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

Рисунок 3.4 – Скриншот описания угрозы УБИ.006 БДУ ФСТЭК России (фрагмент)

BDU:2023-00949: Уязвимость ПЛК MKLogic-500, связанная с использованием скрытых функций, позв

Описание уязвимости	Уязвимость ПЛК MKLogic-500 связана с наличием скрытого функционала (SSH доступа). Эксплуата устройством
Вендор	АО «Нефтеавтоматика»
Наименование ПО	ПЛК MKLogic-500
Версия ПО	до 1.3.8.0
Тип ПО	Средство АСУ ТП, ПО программно-аппаратного средства АСУ ТП
Операционные системы и аппаратные платформы	Данные уточняются
Тип ошибки	Скрытые функции
Идентификатор типа ошибки	CWE-912
Класс уязвимости	Уязвимость архитектуры
Дата выявления	20.09.2022
Базовый вектор уязвимости	CVSS 2.0: AV:N/AC:L/Au:S/C:C/I:C/A:C CVSS 3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Рисунок 3.5 – Скриншот описания уязвимости BDU:2023-00949 БДУ ФСТЭК России (фрагмент)

№	Тактика	Основные техники
T1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		T1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок
		T1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		T1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера nmap
		T1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера

Рисунок 3.6 – Образец описания тактики и соответствующих ей техник Методики оценки угроз БИ ФСТЭК России

В Главе 1 данного исследования были сделаны выводы о перспективности применения методов интеллектуального анализа текстов в задачах анализа и

оценки актуальных угроз и уязвимостей. Далее подробно описаны алгоритмы, входящие в структуру метода оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объектов КИИ.

Технологии интеллектуального анализа текстов используются при решении таких задач как: машинный перевод текстов; аннотирование (суммаризация) текста (краткое содержание); классификация текстов; диалоговые системы (чат-боты, системы вопрос-ответ), распознавание именованных сущностей и т.д.

Для того, чтобы приступить к применению методов интеллектуального анализа текстов (машинного обучения) необходимо, прежде всего, провести предварительную обработку текстовых данных. Этапы данной процедуры описаны в разделе 1.4.1 Главы 1 представленной работы. Такие шаги предобработки текстовых описаний, как нормализация (удаление знаков пунктуации, аббревиатур, союзов междометий и т.п.) и токенизация, используются, как правило, во всех задачах интеллектуального анализа текстов, в то время как использование этапов удаления стоп-слов (расширенная нормализация), стеммизации, лемматизации зависит от поставленной задачи [22, 70, 86]. Т.е. количество этапов предобработки текстов и их порядок непосредственно зависит от формы корпуса (формата документов), поставленной задачи и языка, на котором изложена текстовая или речевая информация. Так что с уверенностью можно сказать, что каждый алгоритм векторизации, разработанный для решения конкретной прикладной задачи, будет уникальным.

Процедуры предварительной обработки текстовых данных являются одними из ключевых в задачах интеллектуального анализа текстов. От того, насколько качественно будут выполнены вышеописанные этапы, будет зависеть точность кластеризации обрабатываемых данных.

Далее описана функциональная схема предобработки текстовых описаний угроз, уязвимостей и тактик (техник) БДУ ФСТЭК России.

С помощью агрегации данных БДУ ФСТЭК России построен корпус русскоязычных текстов (описаний угроз, уязвимостей, тактик и техник).

Корпус текстов для анализа построен из более чем 34 000 агрегированных текстовых описаний уязвимостей, 222 описаний угроз и 10 техник (каждой технике соответствует от 9 до 29 тактик) на русском языке из БДУ ФСТЭК России. Составное текстовое поле включает данные о характеристике уязвимости и вариантах ее эксплуатации.

Для анализа корпуса разработан алгоритм построения векторного представления текстовых описаний угроз, уязвимостей, тактик (техник) и оценки их семантической близости (Рисунок 3.7).

Ключевыми этапами обработки являются:

Загрузка данных из локальной БД (1) – необходима для преобразования текстовых полей каждой записи в единое текстовое описание для последующей обработки.

Нормализация (2) текстовых описаний угроз и уязвимостей – включает шаги по символьной фильтрации, токенизации и фильтрации с использованием общего и специализированного (формируемого экспертами) «стоп-словарей». Заключительным шагом является лемматизация с применением инструментов pymystem3.

Экспертная структурно-семантическая разметка (3) текста на основе системы doccano [141] позволяет выделить семантические особенности текстовых описаний (ключевые слова, ключевые словосочетания, отношения между сущностями) и уточнить состав специализированного стоп-словаря. Ключевым является этап (4) построения формализованного вектора признаков текстовых описаний. Применяемые схемы частотного представления (Bag of Word, BoW), прямого кодирования, скоринга для частотного представления (BoW + TF-IDF). Созданная модель TF-IDF, позволяет оценить важность каждого слова в корпусе. Распределенное представление (с помощью моделей Word2Vec, Doc2Vec и FastText) позволяют сформировать гетерогенный вектор признаков, однозначно определяющий текстовое описание сущности в признаковом пространстве.

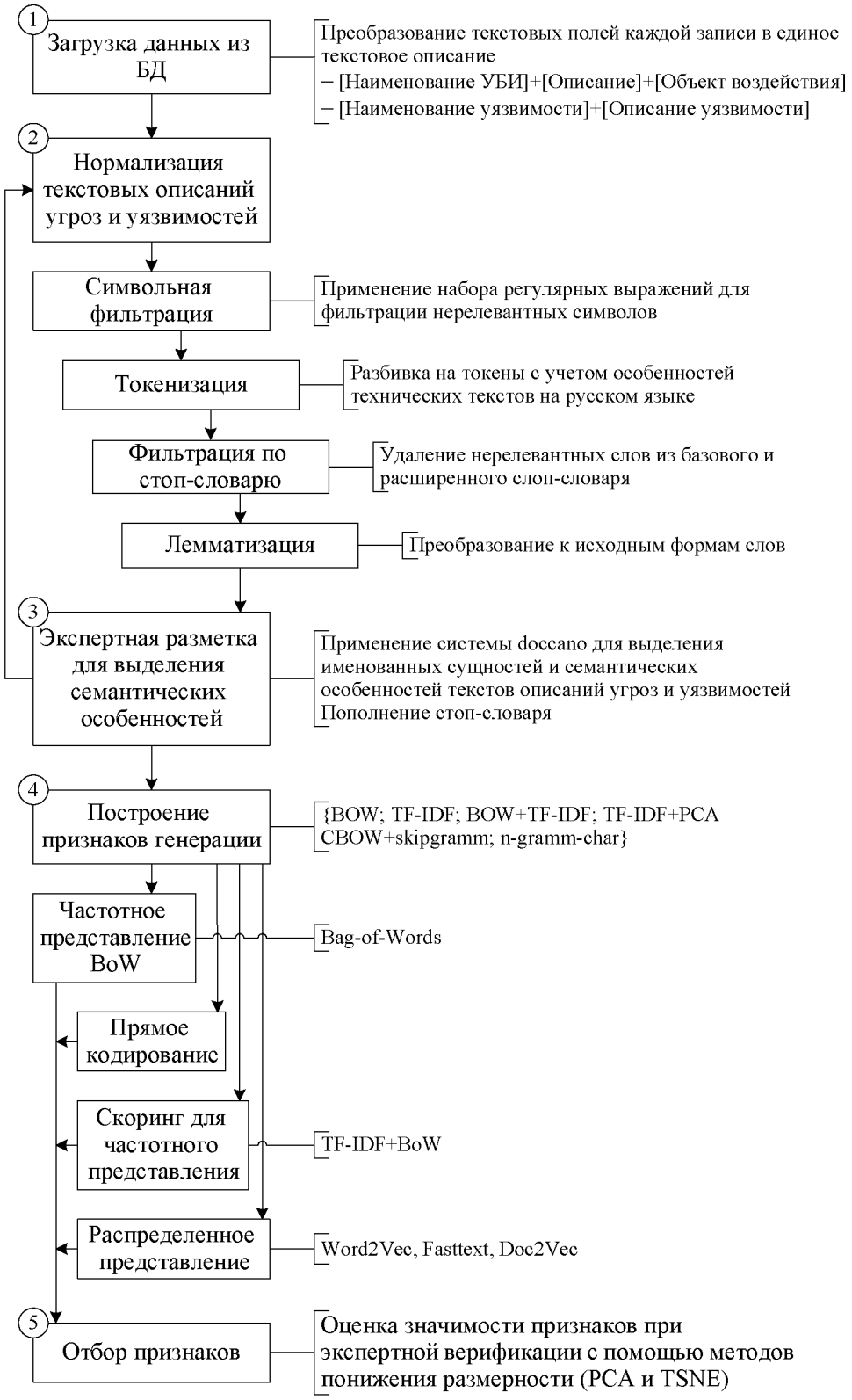


Рисунок 3.7 – Схема алгоритма построения векторного представления текстовых описаний угроз, уязвимостей, тактик (техник) и оценки их семантической близости на основе построения матрицы попарных расстояний (Алгоритм векторизации)

На следующем этапе (5) выполняется отбор наиболее значимых признаков с помощью экспертной оценки структуры двухмерной визуализации стохастического вложения соседей с t-распределением (t-SNE) редуцированного пространства признаков с помощью метода главных компонент (PCA) или сингулярного разложения (SVD) (Рисунок 3.8). Визуальная оценка при разной заданной избирательности модели векторизации позволяет оценить, насколько компактными и отделимыми являются формируемые группы текстовых описаний угроз и уязвимостей. Основная задача данного этапа – оценить, имеется ли структура в данном признаковом пространстве у данных, т.е. присутствует ли группировка семантически близких сущностей в отделимые кластеры.

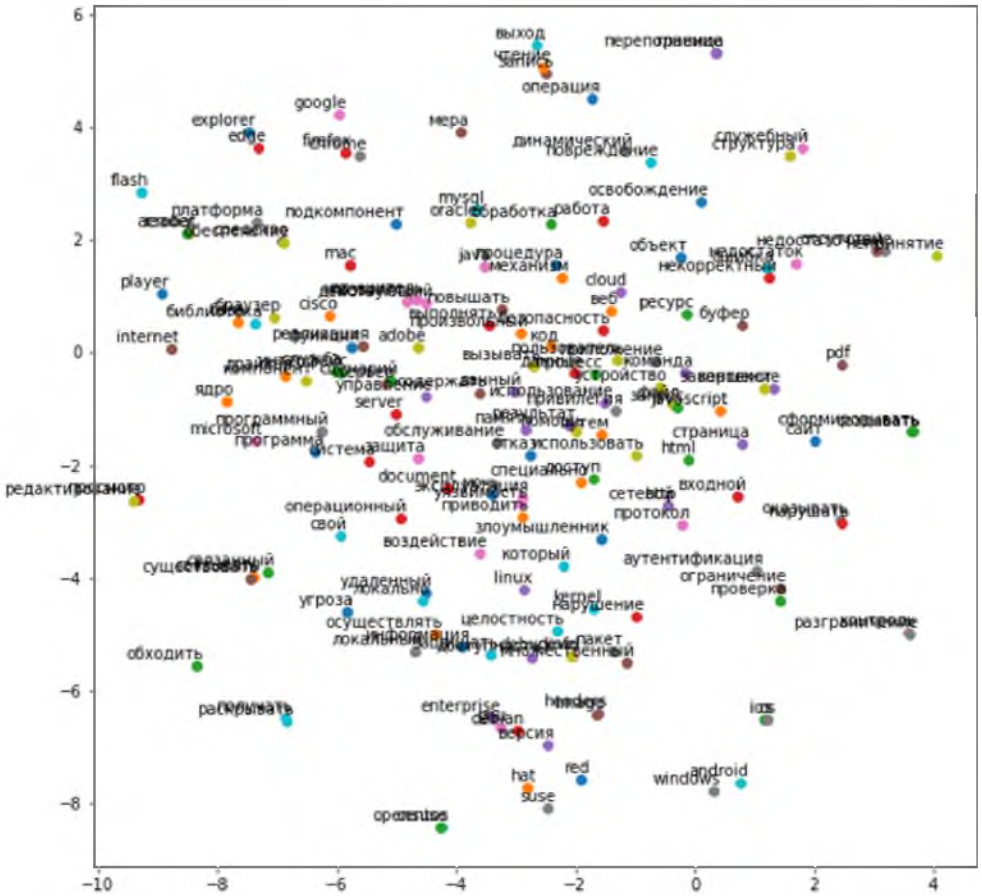


Рисунок 3.8 – Двухмерная визуализация стохастического вложения соседей с t-распределением (t-SNE) редуцированного пространства признаков распределенного векторного представления Doc2Vec

В Таблице 3.1 представлена процедура предобработки и подготовки текстовых данных, извлеченных из БДУ ФСТЭК России в виде конвейера NLP-pipe.

Таблица 3.1 – Структура конвейера предобработки текстовых описаний угроз и уязвимостей

Этап		**Методы и инструменты**
Предобработка	Токенизация	Токенизация на основе адаптивной модели на основе системы правил Razdel [72] (русский язык) и Gensim Simple Tokenizer (английский язык)
	Символьная фильтрация	Регулярные выражения формата regexp, 38 регулярных выражений для фильтрации URLs, HTML-tags и пр.
	Фильтрация токенов	NLTK словари русского и английского языка, дополненные выделенным вручную списком стоп-слов, 400 токенов
Нормализация	Лемматизация	Natasha (русский язык), spacy (английский язык)
Модель вложений	Doc2Vec Distributed Memory	Модель Gensim (минимальная частота встречаемости слова – 2, количество отбрасываемых слов – 5, размер вектора вложений – 100)
	Word2Vec	Модель Gensim (минимальная частота встречаемости слова – 2, количество отбрасываемых слов – 5, размер вектора вложений – 100)
Вектор признаков дескриптора	Композиция	Агрегированный вектор: Doc2Vec и нормированный TF-IDF Word2Vec для лексем в тексте

Параметры нейросетевой модели векторного вложения для текстовых документов Distributed memory (PV-DM) Doc2Vec приведены в Таблице 3.2.

Таблица 3.2 – Параметры Distributed memory (PV-DM) Doc2Vec Model

Параметр	**Значение**
Размерность вектора признаков	100
Размер окна анализа	5
Минимальная частота встречаемости слова для включения в модель	2
Количество эпох обучения	100

Разработанный алгоритм отличается от иных алгоритмов векторизации построением результирующего вектора признаков в виде взвешенного с помощью коэффициентов TF-IDF кортежа векторов вложений, полученных с помощью моделей Doc2Vec, Word2Vec, BERT.

Разработка алгоритма кластеризации текстовых описаний угроз, уязвимостей, тактик и техник на основе оценки их семантической близости.

Использованию алгоритмов кластеризации посвящен ряд научных исследований. Вопросам анализа текстовой информации посвящена работа [40, 74, 76]. Вопросам анализа угроз, уязвимостей посвящены статьи [30, 46]. Работа [53] посвящены использованию кластерного анализа в задачах оценки рисков и менеджмента ИБ. В работе [18] описан метод кластерного анализа пространственно-временной модели угроз позволяющий реализовать дифференцированный подход к защите распределенного объекта АСУ ТП транспортировки нефтегазового сырья.

Автором предлагается алгоритм кластеризации текстовых описаний угроз, уязвимостей, тактик и техник, позволяющий оценить наличие устойчивой структуры текстовых описаний в пространстве признаков векторных вложений в виде устойчивых групп, образованных на основе оценки их семантической близости (Рисунок 3.9). Работа алгоритма начинается с выбора модели формализации, при помощи которой в дальнейшем текстовые описания будут преобразованы в вектора. Далее применяется алгоритм векторизации – происходит предобработка и векторизация (формализация) текстовых описаний, после чего определяются параметры кластеризации (метрики качества кластеризации, центры кластеров, их количество, количество итераций) и запускается сам алгоритм кластеризации. Происходит преобразование пространства признаков. Как правило, из-за огромного размера словаря (корпуса текстов) сгенерированные векторы обладают большой размерностью, что затрудняет работу с ними. Вследствие чего для улучшения качества модели и снижения вычислительных затрат используют алгоритмы понижения размерности, такие как PCA, T-SNE, UMAP. Затем выбирают один из алгоритмов кластеризации, и с помощью выбранного алгоритма происходит разделения векторов текстовых описаний на группы, схожие по описанию. После чего эксперт оценивает качество сформированной структуры, если качество структуры эксперта удовлетворило, то оценивается состав

выделенных кластеров, если нет, то необходимо откорректировать параметры кластеризации.

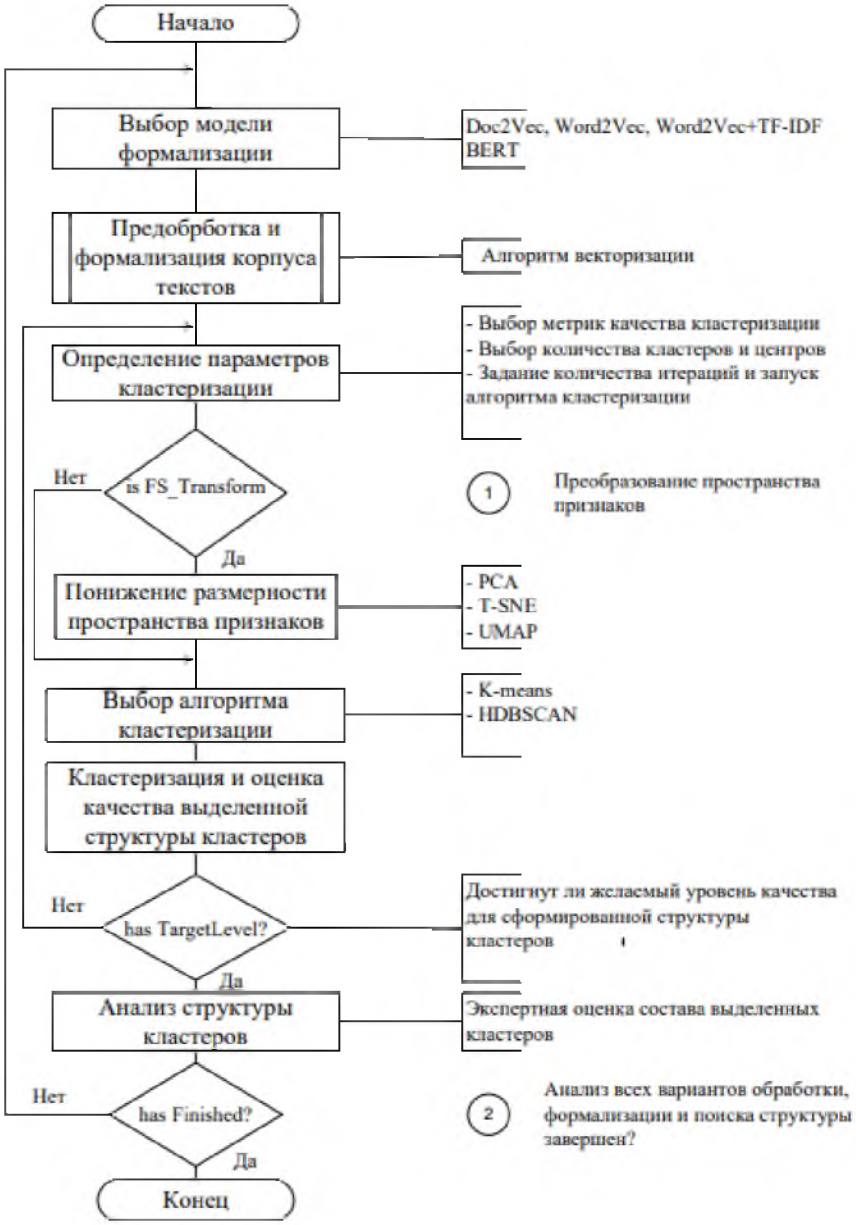


Рисунок 3.9 – Схема алгоритма кластеризации текстовых описаний угроз, уязвимостей, тактик и техник (алгоритм кластеризации)

Для выбора оптимального значения k – количества кластеров для алгоритма k-means был использован «метод локтя» (Elbow). Из Рисунка 3.10 видно, что оптимальное количество кластеров находится в районе значения 20, после которого изменение графика минимально.

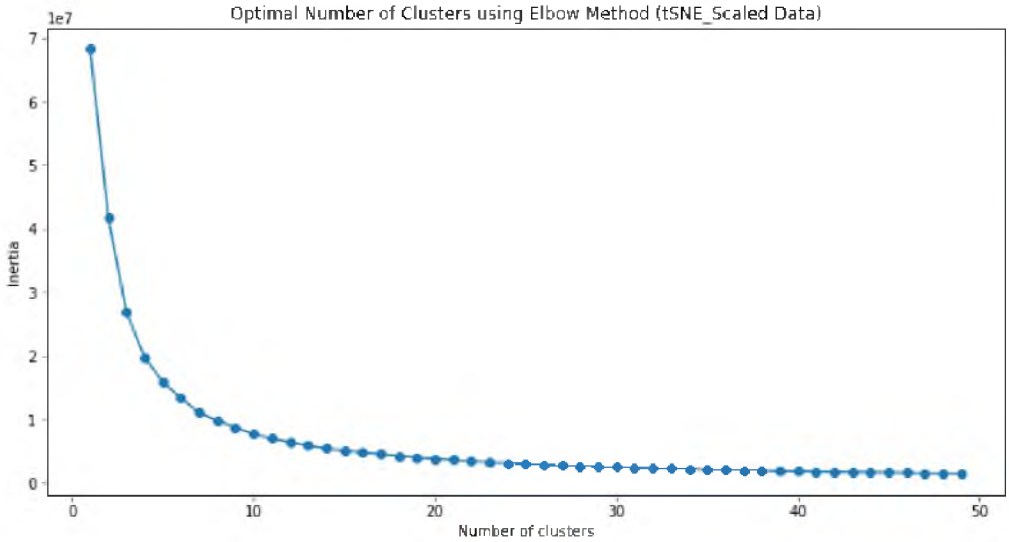


Рисунок 3.10 – Выбор количества кластеров с использованием метода Локтя

Выполнена кластеризация корпуса (Рисунок 3.11) с предварительно заданными центрами кластеров, полученных из векторного представления текстовых описаний БДУ ФСТЭК (22 объекта воздействия согласно Методике) методом k-means в признаковом пространстве, размерность которого снижена с помощью преобразования t-SNE (t-distributed stochastic neighbor embedding, стохастическое вложение соседей с распределением Стьюдента).

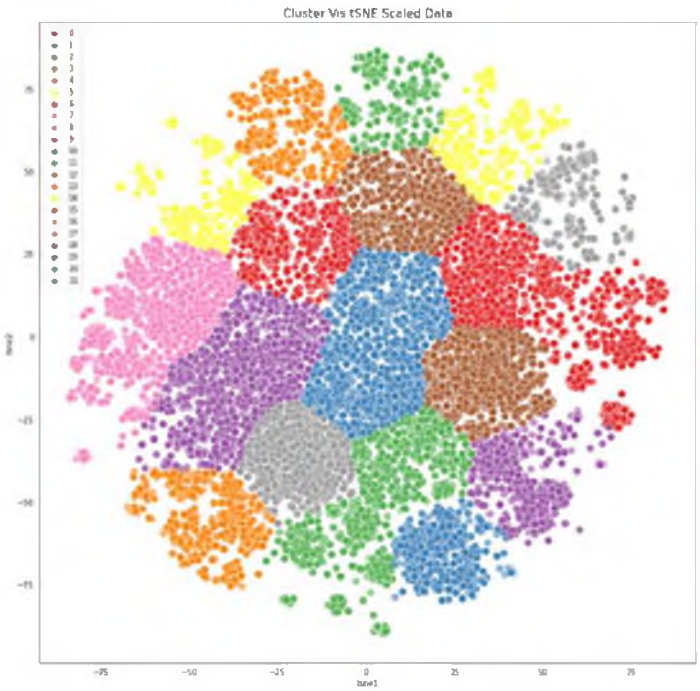


Рисунок 3.11 – t-SNE визуализация кластерной структуры с предварительно заданными центрами

Визуализация сформированных кластеров с использованием алгоритма t-SNE свидетельствует о наличии структуры компактных групп текстовых описаний и подтверждает возможность применения технологии Text Mining для структуризации текстовых описаний угроз и уязвимостей на основе оценки их семантической близости.

Результат работы алгоритма кластеризации показал возможность использования технологии Text Mining для структуризации текстовых описаний, что позволяет перейти к разработке алгоритма оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО.

3.3 Разработка метода и алгоритмов оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объектов КИИ

На сегодняшний день требование по построению сценария реализации угроз в соответствии с Методикой ФСТЭК трудноосуществимо, в том числе ввиду отсутствия автоматизированных систем, позволяющих реализовать эту задачу [32]. В настоящий момент для построения сценария реализации угроз используются: экспертный способ сопоставления уязвимостей тактик (техник) и угроз, методы автоматизации, описанные в [72, 73], а также автоматизированная система ФСТЭК России, находящаяся в процессе разработки. Недостаток экспертного способа построения сценариев реализации угроз связан с необходимостью обработки специалистом по ИБ больших массивов текстовых данных. Эта процедура требует значительных временных затрат и может сопровождаться ошибками. В работах [72, 73] предлагается автоматизировать процесс сопоставления угроз и уязвимостей с использованием, разработанного авторами исследований программного продукта «ThreVulSec». Данных подход частично решает проблему построения сценария реализации угроз, но, тем не менее, полностью не соответствует требованиям Методики, поскольку не позволяет выявить тактики и техники, при помощи которых эксплуатируются выявленные уязвимости. Новый раздел угроз, предлагаемый ФСТЭК России и находящийся в процессе разработки на момент

написания диссертации, не отображает тактики и техники и, соответственно, не позволяет построить сценарий реализации угроз в автоматизированном режиме.

В отличие от существующих на данный момент способов, предлагаемый в данном научном исследовании метод оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объекта АСУ ТП на основе оценки их семантической близости позволяет построить сценарий реализации атак в автоматизированном режиме, что значительно сокращает время на обработку текстовых данных с более чем 1 часа до 20 минут, снижает трудоемкость работы, а также уменьшает когнитивную нагрузку на специалиста по ИБ (эксперта). Далее представлено описание Метода.

На основании вышеизложенного и в рамках рекомендаций Методики предлагается решение задач, связанных с оценкой угроз БИ, т.е. инвентаризацией объекта исследования, определением источников угроз, оценкой способов реализации угроз, предполагающей оценку уязвимостей, определение тактики и техник, позволяющих эксплуатировать выявленные уязвимости, определение сценариев реализации угроз БИ исследуемого объекта, а также разработкой ИСППР для решения вышеописанных задач. На Рисунке 3.12 представлена схема оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объекта АСУ ТП на основе оценки их семантической близости (далее Метод).

Суть метода заключается в последовательном использовании совокупности представленных на Рисунке 3.12 алгоритмов, предназначенных для обработки данных (текстовых описаний) об уязвимостях ПО объекта исследования, угрозах, тактиках (техниках), загруженных из БДУ ФСТЭК. Обработка вышеупомянутых данных происходит в разработанной ИСППР с возможностью предоставления полученных результатов в виде возможных вариантов сценариев реализации угроз специалисту по ИБ для дальнейшей оценки их достоверности и принятия решения об актуальности угроз, выявленных на объекте исследования. Далее дано краткое описание элементов схемы.

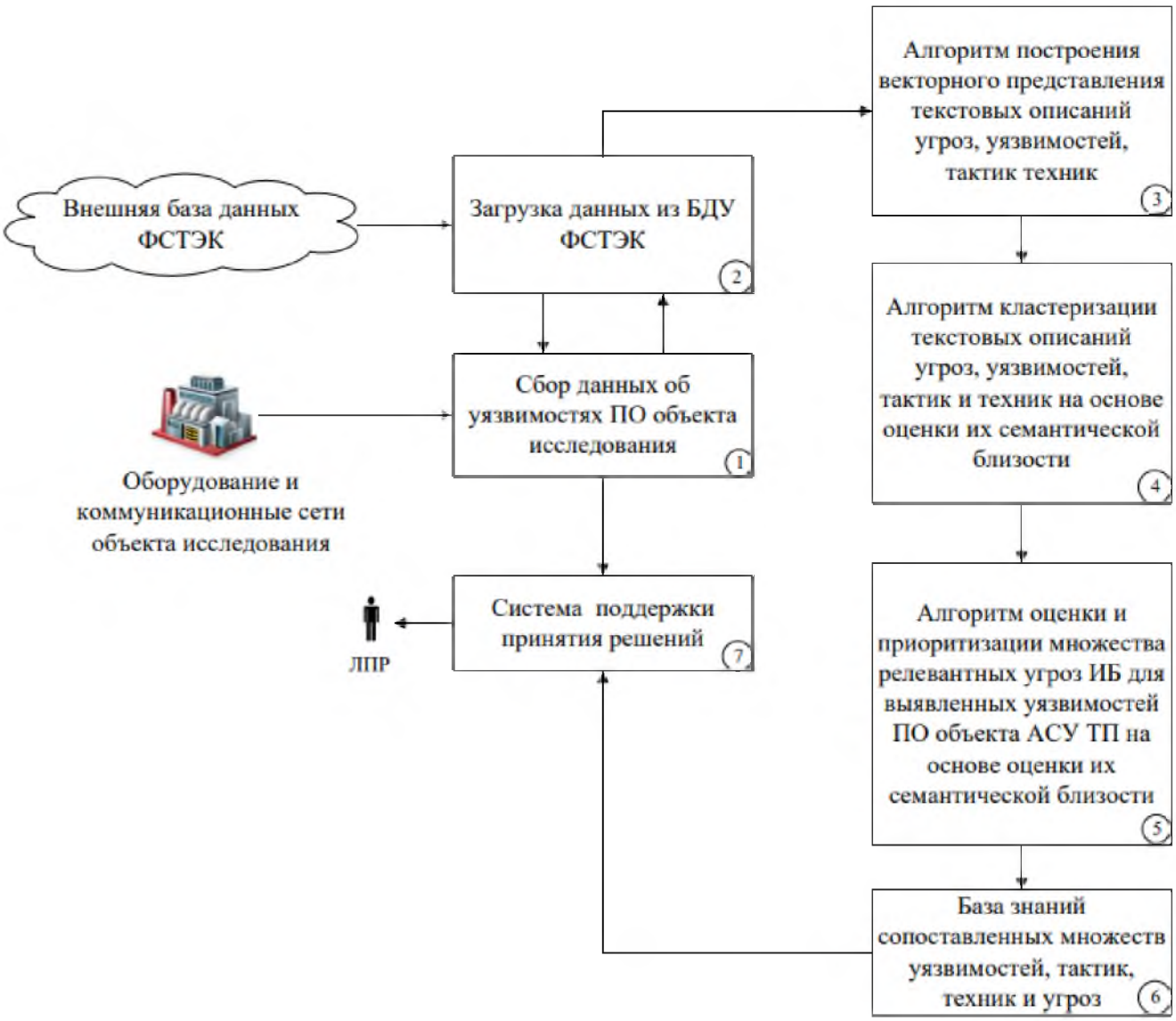


Рисунок 3.12 – Схема оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объектов КИИ

Прежде всего происходит сканирование оборудования и коммуникационных сетей объекта исследования с целью сбора данных об уязвимостях ПО (1) и загрузка данных из внешней БДУ ФСТЭК (2).

Алгоритм построения векторного представления текстовых описаний угроз, уязвимостей, тактик и техник (далее алгоритм векторизации) (3). Необходимость разработки алгоритма векторизации связана с тем, что вычислительная техника на сегодняшний день не способна работать непосредственно со словами, т.е. если существует необходимость анализа и

обработки текстовых данных, то их прежде всего необходимо формализовать. Таким образом, алгоритм предназначен для предварительной обработки и формализации (векторизации) текстовых описаний угроз и уязвимостей, загруженных из БДУ ФСТЭК. Работа алгоритма начинается с загрузки данных (текстовых описаний) из БДУ ФСТЭК (примеры текстовых описаний угроз, уязвимостей, содержащихся в БДУ ФСТЭК, представлены в разделе 3.2, Рисунки 3.4-3.6), затем происходит нормализация (предобработка) текстовых описаний (этапы предобработки подробно описаны в разделе 1.3.1. данной работы). После чего создаются векторы текстовых данных, т.е. происходит построение семантического пространства, состоящее из векторов, соответствующих каждому текстовому описанию.

Алгоритм кластеризации текстовых описаний угроз, уязвимостей, тактик и техник на основе оценки их семантической близости (алгоритм кластеризации) (4). Алгоритмы кластеризации используются в случаях, когда необходимо обобщить информацию о выборке объектов и упорядочить объекты в группы, объединенные по определенному признаку. Т.е. в случае обработки текстовых описаний уязвимостей и угроз разработка алгоритма кластеризации обусловлена необходимостью выявления устойчивых групп векторных вложений, соответствующих определенным текстовым описаниям, образованных в результате оценки их семантической близости. В работе алгоритма кластеризации задействован в первую очередь алгоритм векторизации, затем определяются параметры кластеризации. Ввиду высокой размерности пространства признаков используются инструменты понижения размерности, далее происходит кластеризация векторных вложений и оценка качества полученных групп текстовых описаний.

Алгоритм оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объекта АСУ ТП на основе оценки их семантической близости (далее алгоритм оценки и приоритизации) (5) непосредственно обеспечивает возможность сопоставления текстовых описаний уязвимостей и угроз. Первые шаги работы данного алгоритма связаны с

инициализацией работы алгоритмов векторизации и кластеризации, далее строится матрица сопоставления уязвимостей и угроз на основе оценок их семантической близости, а также отбираются ближайшие по описанию выявленным уязвимостям угрозы (Рисунок 3.13).

Результаты анализа текстовых описаний уязвимостей тактик (техник) и угроз заносятся в базу знаний сопоставленных множеств уязвимостей и угроз (6) после чего, посредством автоматизированной системы передаются специалисту по ИБ для принятия окончательного решения о корректности построения сценария и актуальности выявленных угроз объекта исследования.

Проведена апробация предложенного метода и алгоритма оценки и приоритизации актуальных угроз и уязвимостей ПО. Анализировались текстовые данные БДУ ФСТЭК, содержащего на момент эксперимента 27085 текстовых описаний уязвимостей и 217 – угроз. Из текстовых описаний объемом 740634 слова был сформирован словарь, содержащий 12884 слов. После процедуры предобработки и нормализации построена модель Doc2Vec с помощью фреймворка Gensim.

В качестве иллюстрации работы предложенного метода и алгоритма рассмотрены выявленные хостовым сканером безопасности уязвимости BDU:2015-00285 «Уязвимость программного обеспечения Flash Player, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации» и BDU:2015-00513 «Уязвимость браузера Internet Explorer, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации». Данным уязвимостям эксперт в ручном режиме сопоставил угрозы соответственно: УБИ.192 и УБИ.94.

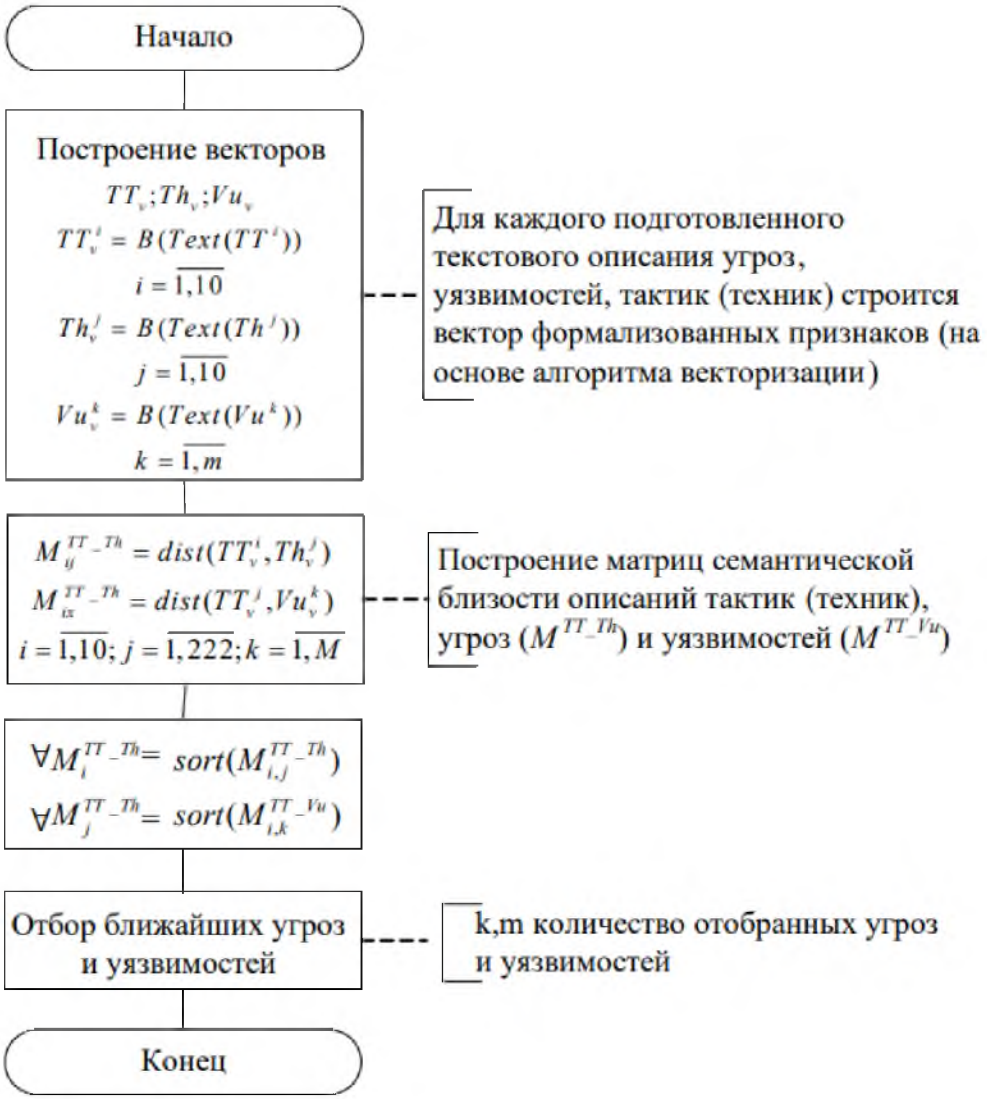


Рисунок 3.13 – Схема алгоритма приоритизации множества угроз ИБ для выявленных уязвимостей ПО, на основе анализа формализованных признаков текстовых описаний угроз (Th), уязвимостей (Vu), техник (тактик) (TT) (Алгоритм оценки и приоритизации)

Используя текстовое описание выбранных уязвимостей, с помощью разработанного алгоритма проведен выбор релевантных угроз. Под «релевантными угрозами» понимаются угрозы, семантически близкие по описанию уязвимостям, обнаруженным на исследуемом объекте. При этом критерием приоритизации является значение метрики семантической близости, равной значению косинуса угла между двумя векторами текстовых описаний определенной уязвимости и сопоставляемой ей угрозы. Пороговое значение косинуса данного угла равно 0,7.

На Рисунках 3.14 и 3.15 показаны результаты подбора 10 релевантных угроз, отсортированных в порядке убывания метрики семантической близости.

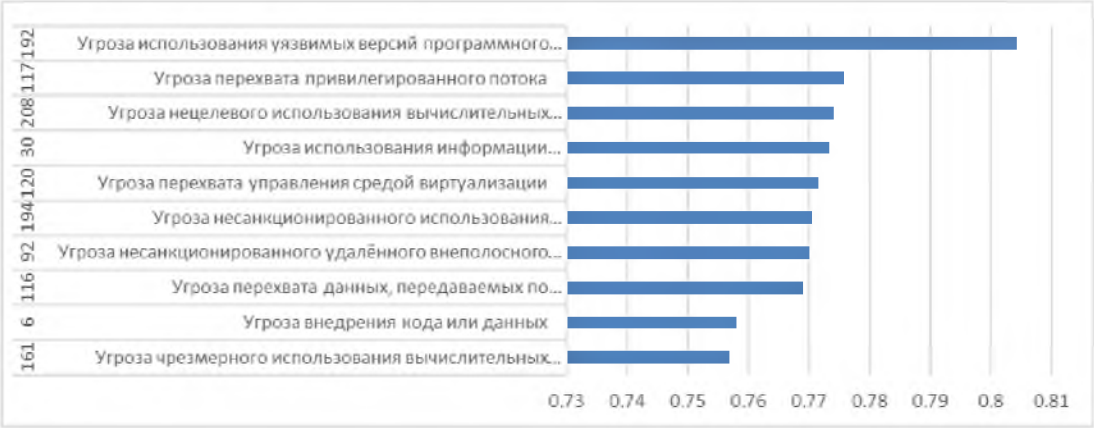


Рисунок 3.14 – Релевантные угрозы, отсортированные в порядке убывания нормированной метрики семантической близости (score) к данной уязвимости BDU:2015-00285

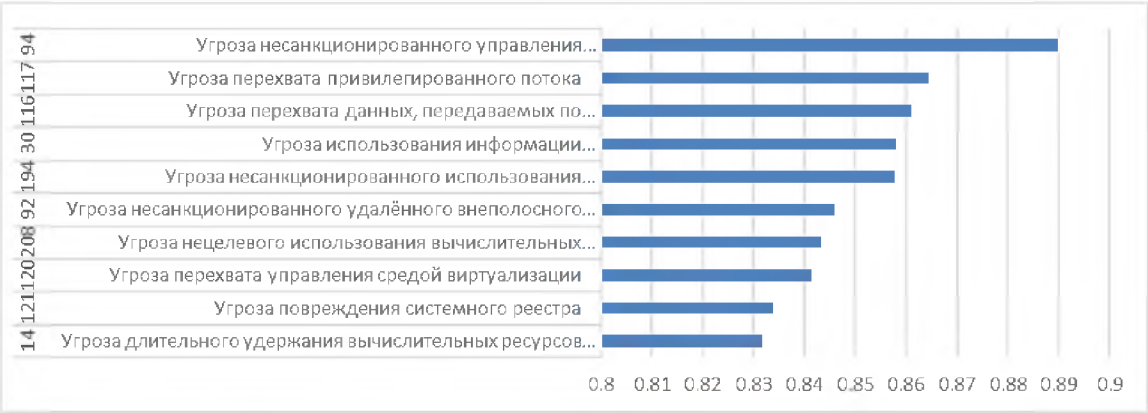


Рисунок 3.15 – Релевантные угрозы, отсортированные в порядке убывания нормированной метрики семантической близости (score) к данной уязвимости BDU:2015-00513

Как видно из Рисунков 3.14 и 3.15, угрозы УБИ.192 и УБИ.94 попадают в данный перечень, что совпадает с результатом предварительного экспертного оценивания. Аналогичным образом для выбранных в процессе экспертного анализа и сбора данных сканерами уязвимостей (поиск установленных версий ПО с имеющимися уязвимостями по БДУ ФСТЭК) производится подбор соответствующих угроз. Финальная стадия анализа позволяет упростить поиск и

сопоставление актуальных угроз и уязвимостей для конкретных версий ПО и сократить количество просматриваемых экспертом угроз для отдельной уязвимости более чем в 10-15 раз.

Применение предложенных моделей и алгоритмов позволит снизить трудоемкость и когнитивную нагрузку на специалистов по ИБ при формировании перечня актуальных угроз и уязвимостей.

Результаты исследований, представленных выше, указывают на возможность построения семантической и графовой модели фрагмента сценария реализации угроз объекта АСУ ТП с использованием алгоритмов Word2Vec, Doc2Vec и технологии трансформера.

Разработки, описанные в данном разделе опубликованы в [39, 40].

3.4 Построение сценариев реализации актуальных угроз БИ с помощью технологии трансформеров

Главной задачей технологий семантического моделирования является аналитика, т.е. извлечение знаний из больших наборов неструктурированной информации. Использование семантического моделирования в задачах оценки актуальных угроз означает построение всех возможных взаимосвязей между сущностями – текстовыми описаниями уязвимостей, тактик, техник и угроз. Согласно Методике ФСТЭК России п.5.3.4. «…Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник».

Проведенное в разделе 3.1 Главы 3 системное моделирование процесса оценки актуальных угроз БИ на основе IDEF-технологий и декомпозиция блока А6 «Оценка актуальных угроз» выявило, что наиболее трудоемкой задачей для специалиста по ИБ является оценка перечня актуальных угроз и построение сценариев их реализации, включающее сопоставление выявленных уязвимостей, совокупности тактик и техник, через которые последние были эксплуатированы, и угроз. Проблемой в данном случае является отсутствие инструментов,

позволяющих автоматизировать данный процесс, тем самым сократив его трудоемкость.

С помощью предложенного в разделе 3.3. Главы 3 метода строится граф соответствия (Рисунок 3.16).

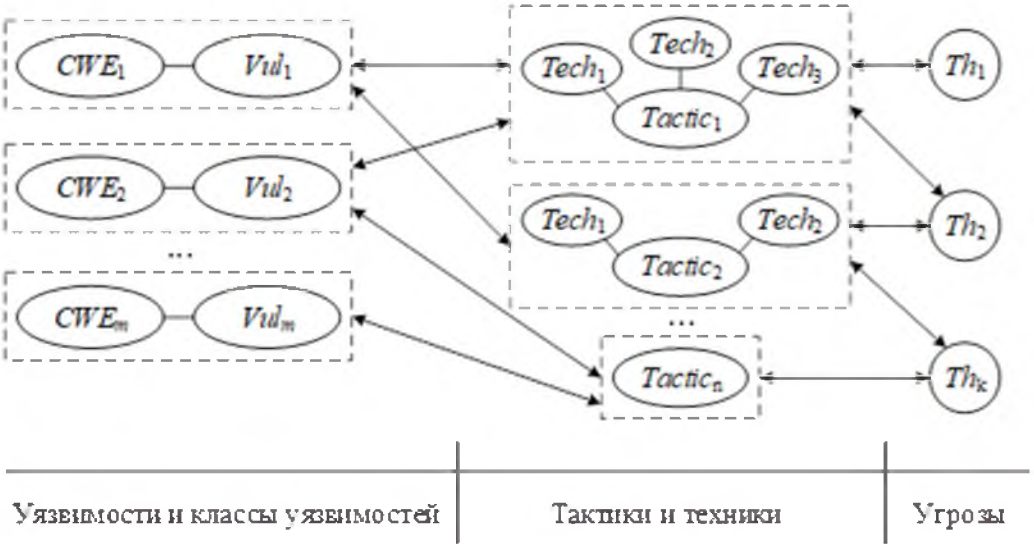


Рисунок 3.16 – Граф соответствия множеств угроз, уязвимостей, тактик и техник их эксплуатации

Схема алгоритма построения графа соответствия множеств угроз, уязвимостей, тактик и техник их эксплуатации (далее граф соответствия) представлена на Рисунке 3.17. На вход алгоритма подается корпус текстов, далее происходит выбор модели векторного представления корпуса текстов, предобработка и векторизация корпуса текстов. Далее, в несколько этапов, строится граф соответствия, т.е. происходит соотнесение множеств выявленных уязвимостей и слабостей ПО, затем уязвимостей – слабостей ПО с тактиками и техниками и, в заключении, тактики и техники соотносятся с угрозами на основе оценки семантической близости. На выходе алгоритма экспертами анализируется качество графовой модели.

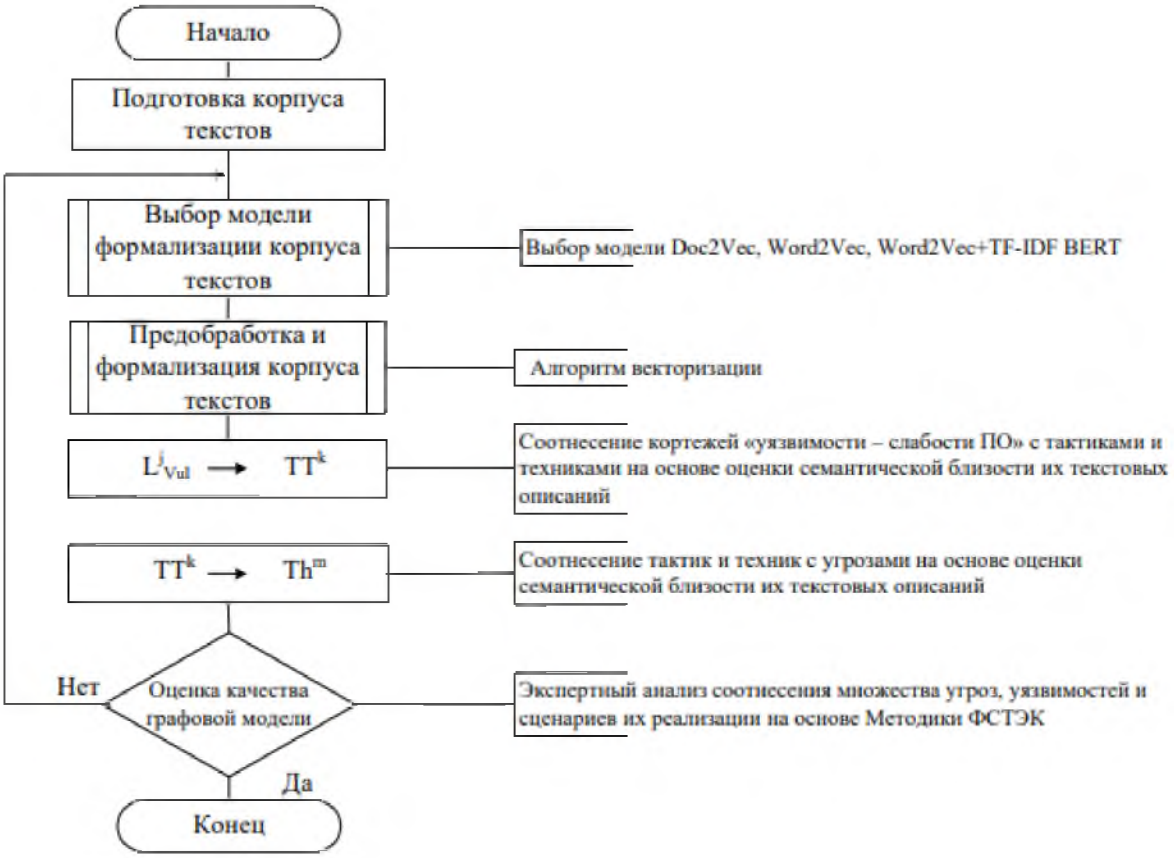


Рисунок 3.17 – Схема алгоритма построения графа соответствия множеств угроз, уязвимостей, тактик и техник их эксплуатации (Алгоритм определения соответствия множеств угроз, уязвимостей тактик и техник)

Для определения соответствия множеств угроз, уязвимостей тактик и техник их реализации можно воспользоваться оценкой метрик семантической близости имеющихся текстовых описаний методом Text Mining. Схема алгоритма оценки и приоритизации множества угроз ИБ для выявленных уязвимостей ПО и текстовых описаний угроз, тактик (техник) представлена на Рисунке 3.13

В основе алгоритма оценки и приоритизации множества угроз ИБ для выявленных уязвимостей ПО лежит построение матриц попарной семантической близости объектов двух множеств: M^{TT_Th} – тактик (техник) (TT) и угроз (Th) (Рисунок 3.18, а), M^{TT_Vu} – тактик (техник) (TT) и уязвимостей (Vu) (Рисунок 3.18, б)

TT_v \ Th_v	Th_v^1	Th_v^2	Th_v^3	...	Th_v^{221}	Th_v^{222}
TT_v^1						
TT_v^2						
...				...		
TT_v^{10}						

а)

TT_v \ Vu_v	Vu_v^1	Vu_v^2	Vu_v^3	...	Vu_v^k
TT_v^1					
TT_v^2					
...				...	
TT_v^{10}					

б)

Рисунок 3.18 – Матрицы попарной семантической близости объектов двух множеств

Далее матрицы сортируются построчно в порядке убывания семантической близости текстовых описаний с обрезкой по количеству элементов в строке: для угроз остается $p = 10$ наиболее схожих, для уязвимостей – $q = 25$ наиболее схожих с текстовым описанием тактик (техник). B – модель векторного представления текстовых описаний; функция *dist* – косинусная мера оценки семантической близости, позволяющая вычислить расстояние между двумя векторами (3.1):

$$similarity = cos(\theta) = \frac{A \cdot B}{\|A\| \cdot \|B\|} = \frac{\sum_{i-1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2} \cdot \sqrt{\sum_{i=1}^{n} B_i^2}}, \quad (3.1)$$

где, A и B – векторные представления текстовых описаний сопоставляемых пар: уязвимостей ПО, тактик, техник и угроз; функция *sort* – функция сортировки, сортирует элементы списка в порядке возрастания.

Методикой предполагается стратегический и тактический уровни построения модели угроз. Стратегический уровень включает в себя определение нарушителя, цели воздействия, негативные последствия, а тактический – применяемые тактики и техники эксплуатации уязвимостей (возможные сценарии реализации угроз). Семантическая модель фрагмента сценария реализации угроз (Рисунок 3.19) представляет собой граф:

$$G = \{V, E, D\},$$

где V – множество вершин графа – текстовые описания угроз, уязвимостей, тактик и техник:

$$V = V_1 \cup V_2 \cup V_3 \cup V_4, \tag{3.2}$$

V_1 – множество вершин, соответствующих идентификаторам выявленных уязвимостей для каждого компонента ИС;

V_2 – множество вершин, соответствующих техникам реализации атаки, которые описывают инструменты, технологии, утилиты и т.д., используемые нарушителями;

V_3 – множество вершин, соответствующих тактикам, т.е. действиям на разных этапах реализации атаки;

V_4 – множество вершин, соответствующих актуальным угрозам ИБ.

E – множество взвешенных ориентированных ребер, устанавливающих отношения между дескрипторами:

$$E \subseteq V \times V, \;\; e(v_i, v_j), \;\; v_i, v_j \in V. \tag{3.3}$$

D(e) – функция, определяющая степень семантической близости для концептов $v_i, v_j \in V$.

$w = dist(v_i, v_j)$ – весовой коэффициент, характеризующий метрику семантической близости текстовых описаний смежных вершин.

На основе построенной семантической модели в разделе 3.3 предложена графовая модель сценария реализации угроз с использованием Word2Vec, Doc2Vec и технологии трансформера.

Семантическая модель фрагмента сценариев реализации угроз G объектов строится на основе перекрестных ссылок в гипертекстовых документах (текстовых описаний угроз, уязвимостей и тактик (техник) их реализации ИС – V графа). Ребра модели нагружаются весовым коэффициентом $w^{i,j}$, характеризующим метрику семантической близости текстовых описаний смежных вершин, полученную с помощью моделей машинного обучения для векторного представления текстов отдельных документов (Word2Vec, Doc2Vec и технологии трансформера).

Далее предложен алгоритм построения графовой модели фрагмента сценария реализации угроз на основе технологии Text Mining с использованием БДУ ФСТЭК.

При построении графовой модели используются данные сканера безопасности об уязвимостях *i*-ого узла АСУ ТП, а также агрегированных текстовых описаний тактик (техник) и угроз.

Построение графовой модели начинается с подготовки текстовых описаний угроз, уязвимостей, тактик и техник. Затем, на основе ссылочных описаний устанавливаются связи между вершинами V_{Vul}, V_{Techs}, V_{Tacks} , несуществующие прореживаются.

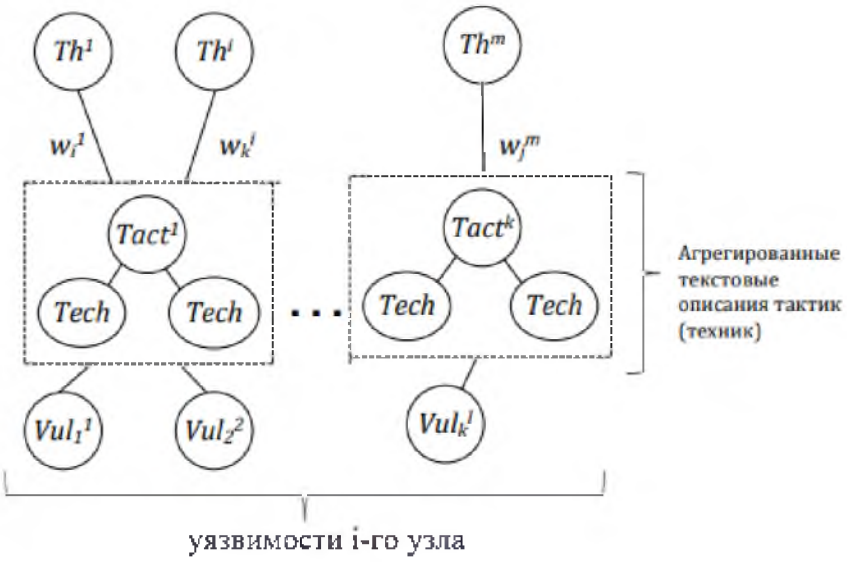


Рисунок 3.19 – Графовая модель фрагмента сценария реализации угроз

Далее строится матрица семантической близости описаний угроз, уязвимостей, тактик и техник, несуществующие связи прореживаются на основе порогового значения. В заключении проводится оценка и приоритизация множества угроз и уязвимостей.

Алгоритм построения графовой модели фрагмента сценария реализации угроз с использованием Word2Vec, Doc2Vec и технологии трансформера представлена на Рисунке 3.20.

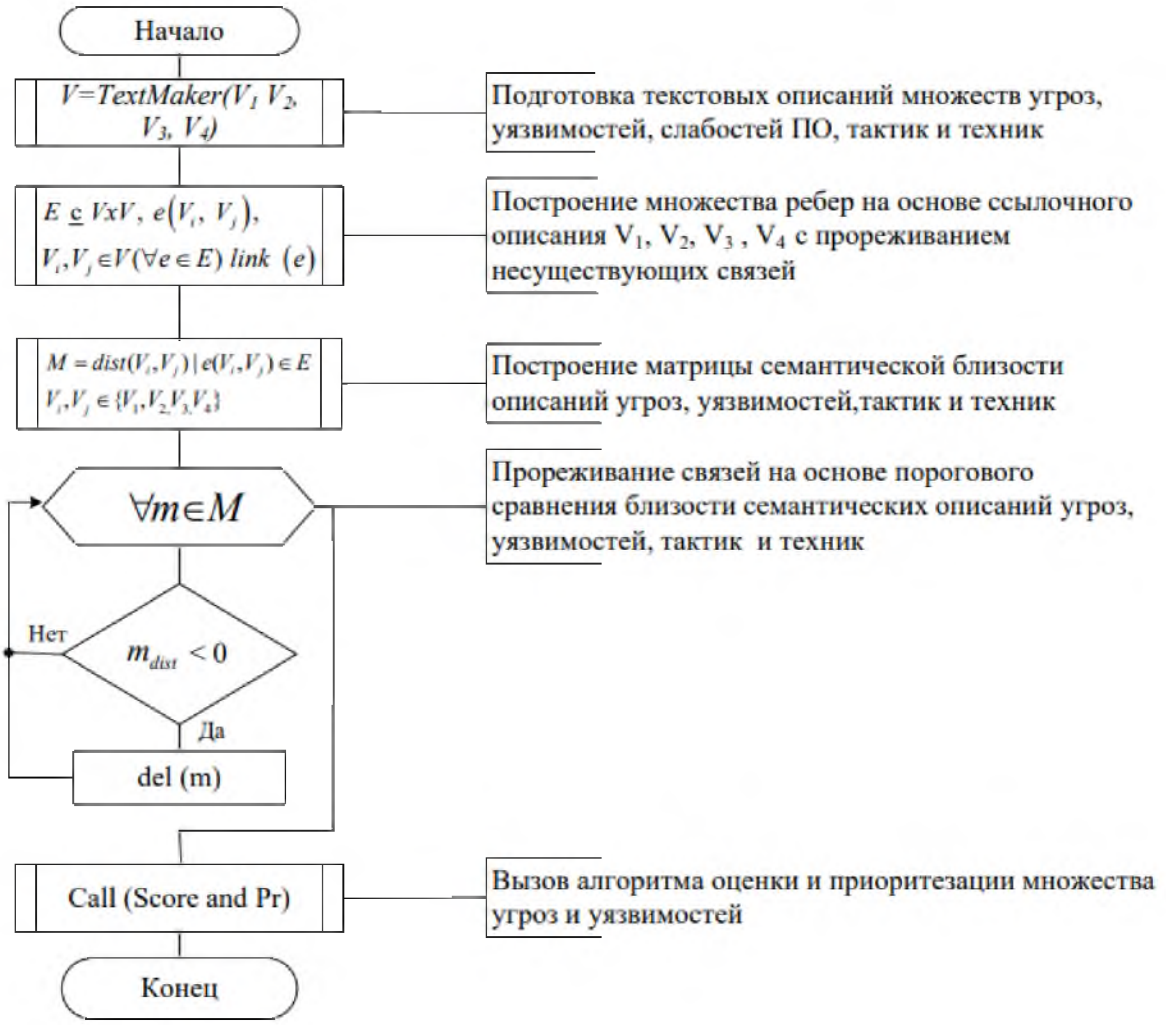


Рисунок 3.20 – Алгоритм построения графовой модели фрагмента сценария реализации угроз на основе алгоритма векторизации (Word2Vec, Doc2Vec и технологии трансформера)

Работа алгоритма начинается с подготовки текстовых описаний множеств угроз, уязвимостей и тактик (техник) их эксплуатации с использованием алгоритмов, описанных в разделе 3.2 диссертационного исследования. Далее на основе ссылочных описаний БДУ ФСТЭК множеств вершин, соответствующих идентификаторам выявленных уязвимостей, техник и тактик реализации атаки, актуальным угрозам строится множество рёбер с последующим прореживанием связей. Затем строится матрица семантической близости текстовых описаний дескрипторов безопасности на основе косинусной меры оценки семантической близости (Глава 2, раздел 2.4 данного исследования), после чего сравнивается

весовой коэффициент $w^{i,j}$ связи (ребра) с пороговым значением θ, если весовой коэффициент меньше порогового значения, то связь прореживается. В заключении выполняется алгоритм оценки и приоритизации, описанный в разделе 3.3.

Попытки сопоставления уязвимостей (CVE) и шаблонов атак для англоязычных баз знаний (CAPEC, ATT&CK, NVD) на основе семантического анализа их текстовых описаний предприняты в работах [117,118]. Проведено сравнение возможностей различных языковых моделей векторных вложений (SBERT, USE, TF-IDF) для сопоставления множеств текстовых описаний и показано, что специализированная модель TF-IDF показывает лучший результат по сравнению с более сложными моделями.

В данном исследовании предлагается для подготовленных русскоязычных текстовых описаний угроз и уязвимостей, полученных из БДУ ФСТЭК, применить методы построения векторных вложений в многомерном семантическом пространстве признаков (Word2Vec + TF-IDF, Doc2Vec, модели трансформеров). Отличительной особенностью данного подхода от предложенных ранее [25] является сопоставление множеств угроз, уязвимостей, техник (тактик) с использованием моделей трансформеров, что повышает качество результатов сопоставления за счет оценки контекста текстовых описаний не только на уровне отдельных слов, как это принято в моделях Word2Vec и Dov2Vec, но и на уровне предложений и фрагментов текстов. При этом используются модели трансформеров, обученные на значительном объеме (корпусе) русскоязычных текстов. Результаты данного исследования описаны в работе [26].

Далее для реализации графовой модели, описывающей отношения множеств угроз, уязвимостей, тактик и техник их эксплуатации предлагается применить технологию трансформеров, в частности метод BERT (Bidirectional Encoder Representations from Transformers) – это метод ЕЯ, основанный на использовании стека нейросетевых кодировщиков с механизмом внутреннего внимания (Self-Attention). Особенностью построения трансформера является двунаправленная обработка входных слов, что сокращает вычислительные затраты и повышает качество обучения языковой модели.

Обобщенная схема подготовки текстовых данных и формализации текстовых описаний на основе векторных вложений представлена на Рисунке 3.21. Специализированный корпус текстов для анализа данных включает в себя текстовые описания на русском языке 36752 уязвимостей, 222 угрозы, 10 техник и соответствующих тактик, взятые из БДУ ФСТЭК России.

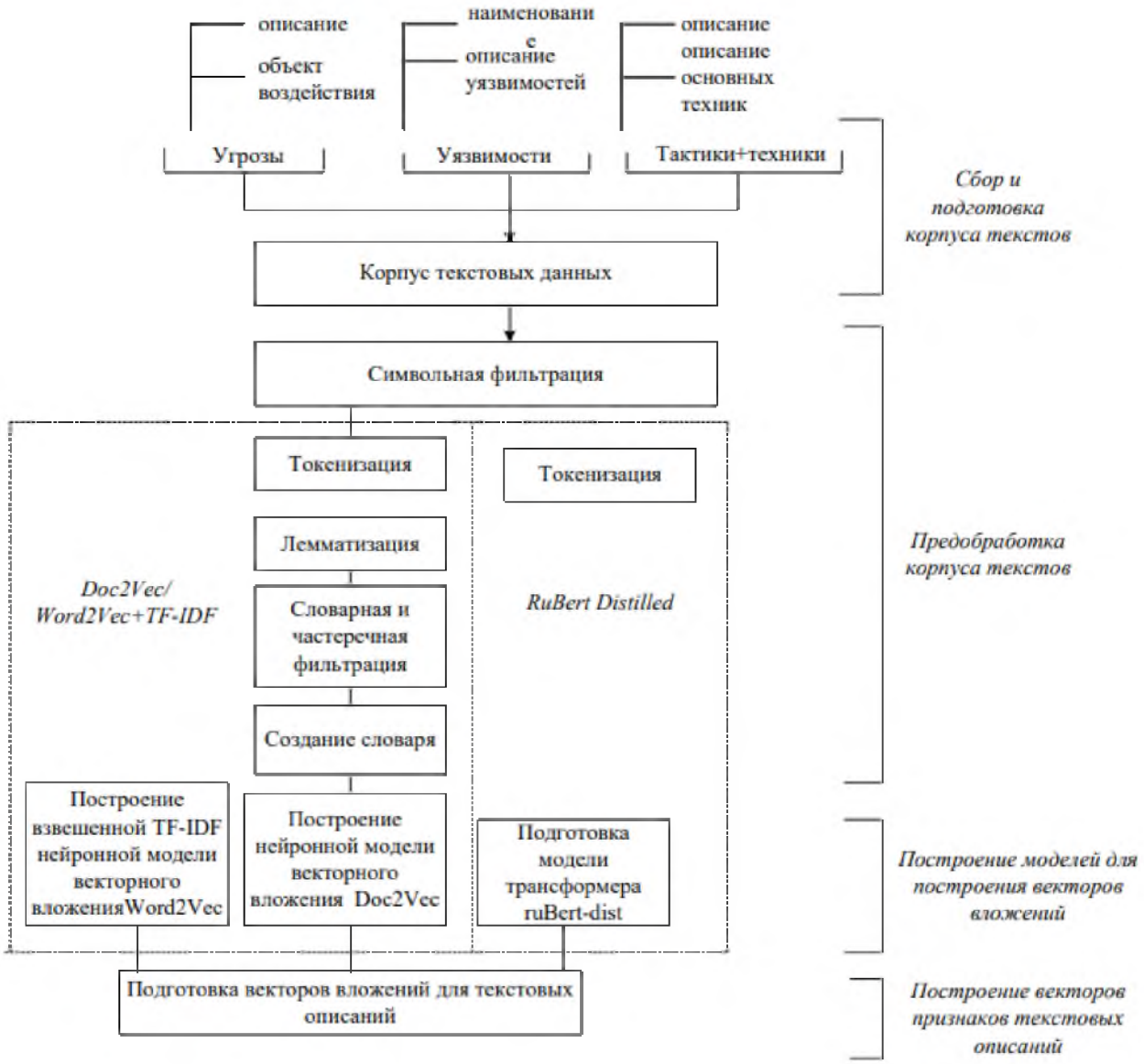


Рисунок 3.21 – Схема подготовки текстовых данных и формализации текстовых описаний

Применяемые на каждом этапе инструменты обработки текстовых данных представлены в Таблице 3.3.

Таблица 3.3 – Применяемые инструменты для предобработки данных

Этап	Шаги	Действия	Инструменты
Предобработка	Символьная фильтрация	Удаление нерелевантных символов, HTML-тегов	Набор регулярных выражений
	Токенизация	Разбивка текста на токены с помощью предобученной для русского языка нейросетевой модели	Razdel [150] (фреймворк Natasha)
	Фильтрация нерелевантных токенов	Удаление дат, цифр, чисел, ссылок, сокращений	Регулярные выражения
Нормализация	Лемматизация	Приведение слов в исходную форму с помощью предобученной нейросетевой модели	Morph (фреймворк Natasha)
Постобработка	Частеречная фильтрация	Остаются только существительные, глаголы, прилагательные, наречия, местоимения	Morph (фреймворк Natasha)
	Фильтрация на основе стоп-словарей	Фильтрация нерелевантных лемм с помощью составного стоп-словаря, включающего наиболее часто встречающиеся слова корпуса текстов	NLTK-russian
	Формирование документа-строки	Объединение лемм в нормализованную строку-документ	

Для формализации признаков текстовых описаний были использованы (Таблица 3.4):

– нейросетевая модель векторного вложения для текстовых документов Distributed memory (PV-DM) Doc2Vec [131];

– нейросетевая модель векторного вложения для текстовых документов Word2Vec, взвешенная коэффициентами частотности терминов-обратной частотности документов – TF-IDF [125, 147];

– модели трансформеры:

• BERT Large Model Multitask (cased) for Sentence Embeddings in Russian Language – предложенная специалистами RnD NLP SberDevices модель-трансформер многозадачного обучения для построения универсальной модели ЕЯ на основе модели SBERT;

• BERT Large Model (uncased) for Sentence Embeddings in Russian Language – также предложенная специалистами RnD NLP SberDevices модель-трансформер;

• ruBERT-tiny – дистиллированная модель BERT-Multilingual, обученная с помощью больших моделей RuBERT, LaBSE, Laser и USE.

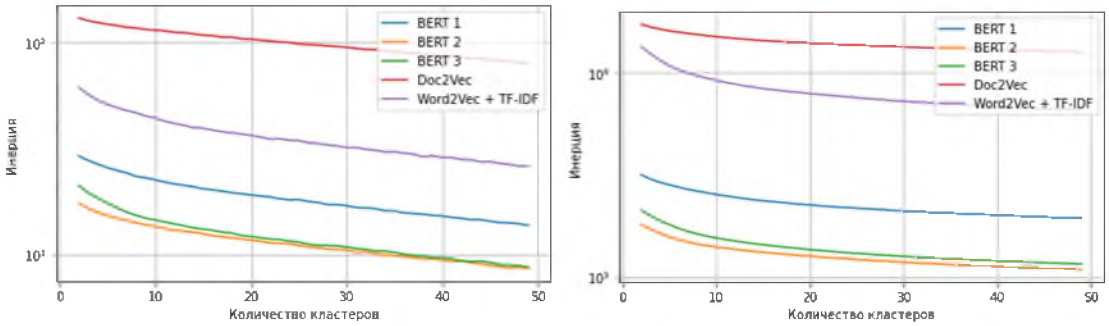
Таблица 3.4 – Модели построения векторных вложений текстовых описаний

Модель	Обозначение	Параметр	Значение
Distributed memory Doc2Vec Model	Doc2Vec	Размерность вектора признаков	100
		Размер окна анализа	5
		Минимальная частота встречаемости слова для включения в модель	2
		Количество эпох обучения	100
CBOW Word2Vec Model + TF-IDF	Word2Vec	Размерность вектора признаков	100
		Размер окна анализа	3
		Минимальная частота встречаемости слова для включения в модель	1
		Количество эпох обучения	150
BERT- Large Model Multitask	BERT1	Размерность вектора признаков	1000
		Количество слоев	12
		Дополнительные модели-адаптеры	NLI, NER, TOX
		Общее количество токенов	120 тыс.
		Общее количество параметров	427 млн.
BERT- Large Model	BERT2	Размерность вектора признаков	1000
		Количество слоев	12
		Дополнительные модели-адаптеры	Нет
		Общее количество токенов	120 тыс.
		Общее количество параметров	427 млн.
ruBERT-tiny	BERT3	Размерность вектора признаков	312
		Количество слоев	3
		Общее количество токенов	120 тыс.

Для каждого документа корпуса с помощью указанных моделей вычисляются векторы формализованных признаков, на основе которых может быть оценена семантическая близость документов как косинусная мера расстояния между векторами.

Дальнейший анализ (сопоставление) формализованных представлений текстовых описаний угроз, уязвимостей, техник (тактик) основан на применении методов кластеризации многомерных данных. С помощью алгоритма кластеризации k-средних оценим структуру формализованных описаний в признаковом пространстве, сформированном на основе пяти моделей вложений. В

качестве меры близости используется косинус-мера. Количество кластеров задается в пределах от 1 до 50, оценивается сумма внутрикластерных расстояний для определения оптимального числа кластеров. На Рисунке 3.22 показана зависимость суммы внутрикластерных расстояний (инерция) от числа кластеров для формализованных представлений текстовых описаний множества уязвимостей (а) и множества угроз (б).



а) б)

Рисунок 3.22 – Зависимость суммы внутрикластерных расстояний от числа кластеров для векторных представлений текстовых описаний уязвимостей (а) и угроз (б)

Из Рисунка 3.22 видно, что применение предобученных моделей-трансформеров позволяет получить более компактное представление структуры текстовых описаний, формируемой алгоритмом кластеризации k-средних в пространстве признаков векторов вложений. Наилучший результат демонстрирует модель BERT 2. Незначительно хуже дистиллированная модель-трансформер BERT 3, которая работает существенно быстрее (векторное представление текстового описания строится примерно в 20 раз быстрее). Взвешенная модель вложений на уровне слов (Word2Vec + TF-IDF) позволяет получить менее компактную структуру кластеров. В каждом из экспериментов модель Doc2Vec демонстрирует менее пригодное для кластеризации представление признакового пространства.

Проведен эксперимент с применением предобученной модели-трансформера BERT– Large Model для заданной уязвимости BDU:2021-02033, текстовое описание

уязвимости представлено в Таблице 3.5.

Таблица 3.5 – Описание заданной уязвимости

Параметр уязвимости	**Описание**
Идентификатор	BDU:2021-02033
Наименование уязвимости	Уязвимость сетевого программного обеспечения Siemens, связанная с неконтролируемым элементом пути поиска, позволяющая нарушителю выполнить произвольный код или вызвать отказ в обслуживании.
Описание уязвимости	Уязвимость сетевого программного обеспечения Siemens связана с неконтролируемым элементом пути поиска. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код или вызвать отказ в обслуживании

При помощи представленного в разделе 3.3 Главы 3 алгоритма приоритизации множества угроз ИБ для выявленных уязвимостей ПО были построены матрицы семантической близости для соотношений угрозы – тактики(техники) и тактики (техники) – уязвимости (Таблицы 3.6-3.9). Матрица ТН_ТТ (по строкам – техники (тактики) (индекс), по столбцам – 10 наиболее близких угроз (матрица содержит индекс угрозы)).

Таблица 3.6 – Матрица семантической близости для соотношений угрозы – тактики(техники) (матрица содержит индекс угрозы)

ТН / ТТ	0	1	2	3	4	5	6	7	8	9
0	105	15	41	121	44	9	156	10	76	25
1	73	105	10	166	15	203	189	127	55	65
2	105	72	133	109	52	10	149	193	94	141
3	203	81	102	186	55	111	205	15	1	145
4	15	105	55	73	203	33	10	142	121	81
5	129	74	44	171	10	111	105	56	50	72
6	105	10	33	127	118	162	182	15	104	203
7	129	50	24	41	68	16	15	44	56	105
8	68	120	50	105	13	127	44	182	34	155
9	139	41	156	96	105	15	146	121	44	9

Матрица ТН_ТТ – по строкам – техники (тактики) (индекс), по столбцам – 10

наиболее близких угроз (косинусная мера)).

Таблица 3.7 – Матрица семантической близости для соотношений угрозы – тактики(техники) (матрица содержит косинусную меру угрозы)

ТН / ТТ	0	1	2	3	4	5	6	7	8	9
0	0,878	0,871	0,871	0,869	0,868	0,868	0,868	0,867	0,865	0,862
1	0,834	0,826	0,823	0,821	0,820	0,820	0,818	0,818	0,818	0,817
2	0,900	0,892	0,891	0,890	0,888	0,888	0,888	0,886	0,885	0,885
3	0,828	0,821	0,819	0,816	0,814	0,810	0,810	0,809	0,809	0,808
4	0,856	0,855	0,853	0,852	0,849	0,843	0,843	0,838	0,838	0,838
5	0,873	0,866	0,865	0,865	0,863	0,863	0,863	0,860	0,859	0,859
6	0,881	0,869	0,866	0,866	0,862	0,862	0,861	0,861	0,860	0,860
7	0,829	0,819	0,817	0,814	0,811	0,810	0,809	0,809	0,808	0,805
8	0,886	0,867	0,866	0,857	0,857	0,855	0,854	0,854	0,854	0,851
9	0,853	0,851	0,844	0,843	0,842	0,842	0,842	0,841	0,840	0,838

Матрица VU_TT – по столбцам – 10 наиболее близких тактик (техник) (индекс)).

Таблица 3.8 – Матрица семантической близости для 10 наиболее близких тактики(техники) (матрица содержит индекс тактики (техники))

№ / ТТ	0	1	2	3	4	5	6	7	8	9
0	2	5	0	9	6	7	4	8	3	1

Матрица VU_TT – по столбцам – 10 наиболее близких тактик (техник) (косинусная мера близости)).

Таблица 3.9 – Матрица семантической близости для соотношений уязвимости – тактики(техники) (матрица содержит косинусную меру тактики (техники))

№ / ТТ	0	1	2	3	4	5	6	7	8	9
0	0,870	0,825	0,820	0,808	0,791	0,781	0,770	0,764	0,744	0,741

Построенный граф взаимосвязей тактики(техники) – угрозы – уязвимость (TT-TH-VU) включает 2452 узла. Визуальная интерпретация графовой модели представлена на рисунках 3.23, 3.24. Граф позволяет оценивать возможность эксплуатации уязвимости с помощью тактики (техники), что приводит к реализации угрозы (фрагмент сценария «уязвимость» – «тактика (техника)» – «угроза»).

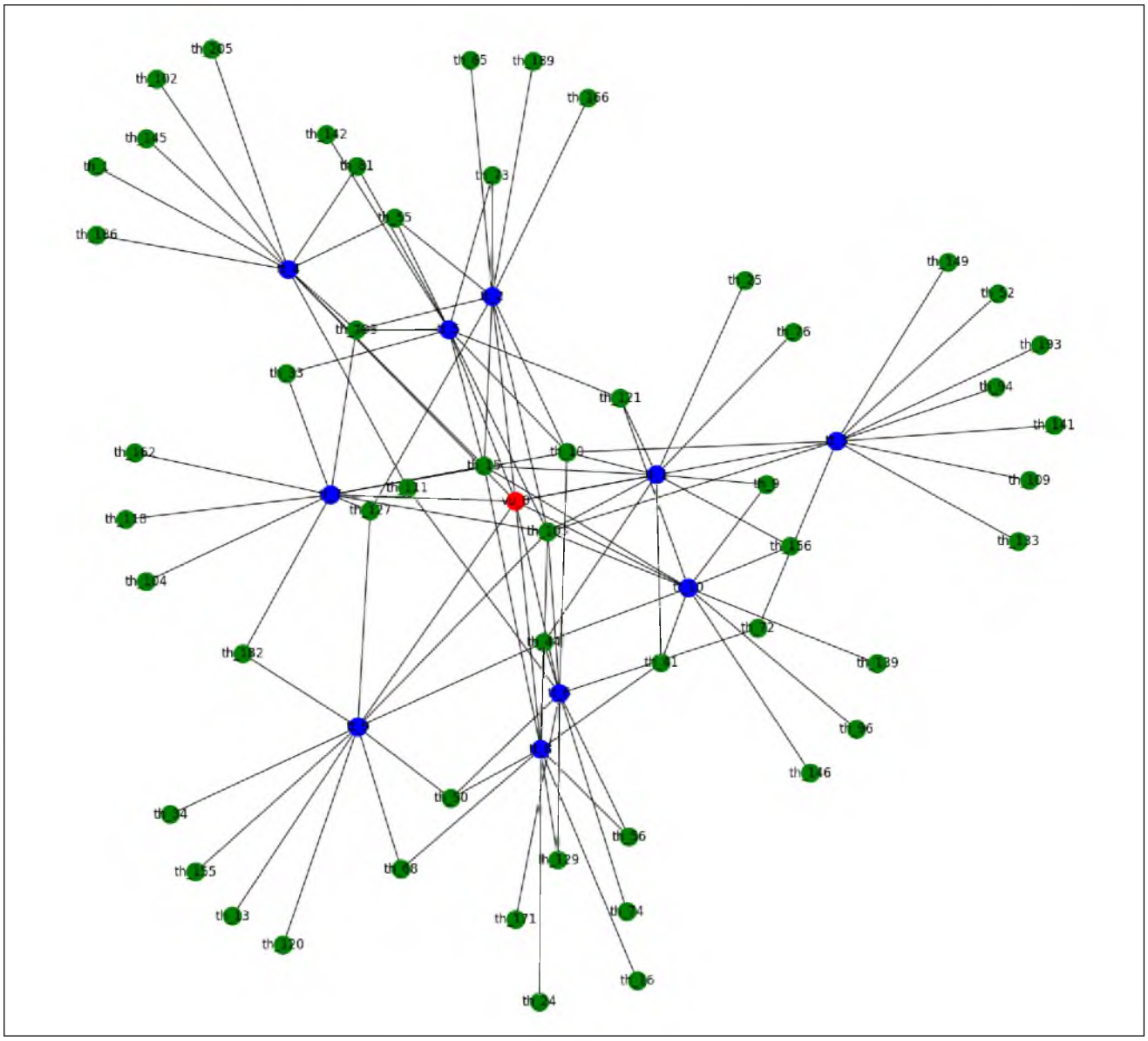


Рисунок 3.23 – Графовая модель связей между заданной уязвимостью (VU – красная вершина), множеством тактик (техник) (TT_i – синие вершины), множеством угроз (TH_j – множество угроз – зеленые вершины)

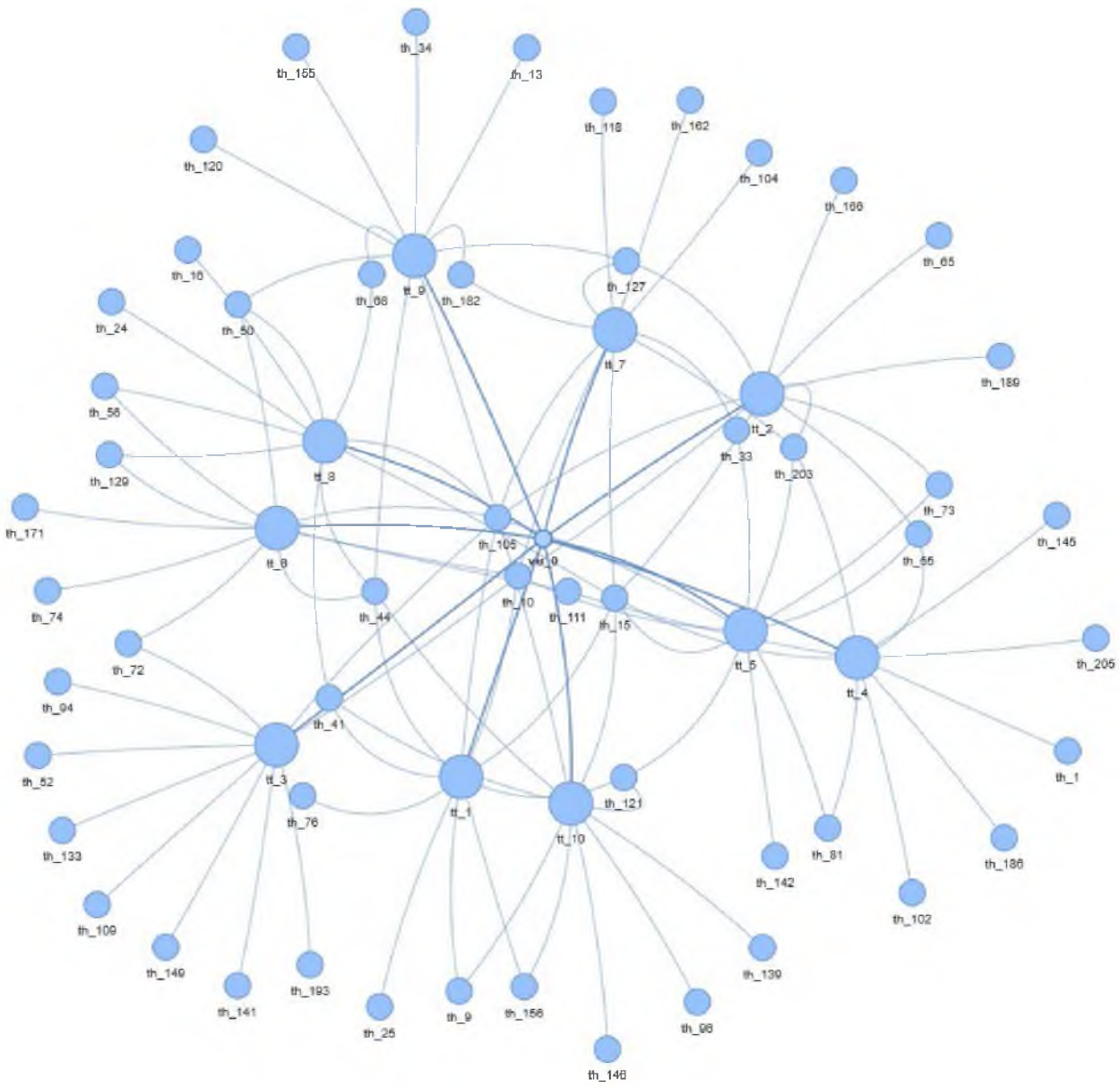


Рисунок 3.24 – Графовая модель связей между заданной уязвимостью (VU), множеством тактик (техник) (TT_i), множеством угроз (TH_j) с выделенными ребрами связей «уязвимость» – «тактика (техника)»

В Таблице 3.10 представлена оценка семантически близких угроз и тактик (техник) к заданной уязвимости с указанием совпадения с экспертной оценкой отбора угрозы.

Таблица 3.10 – Выборка семантически близких угроз и тактик (техник) к заданной уязвимости

	th_idx_2_vu_w	vu_idx_2_tt	vu_idx_2_tt_w	th_2_vu	th_2_vu_text	Оценка угрозы	vu_2_tt	vu_2_tt_text
0	0,901864	2	0,870782	134	Угроза потери доверия к поставщику облачных услуг	-	10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям
1	0,891837	5	0,825528	122	Угроза повышения привилегий	+	2	Получение первоначального доступа к компонентам систем и сетей
2	0,888747	0	0,820814	73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	+	3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях
3	0,885316	9	0,80824	77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	+	5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ
4	0,884451	6	0,791406	173	Угроза «спама» веб-сервера	-	9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз
5	0,882458	7	0,781376	175	Угроза «фишинга»	-	1	Сбор информации о системах и сетях
6	0,882449	4	0,770201	53	Угроза невозможности управления правами пользователей BIOS	-	8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям
7	0,881991	8	0,764556	95	Угроза несанкционированного управления указателями	+	7	Сокрытие действий и применяемых при этом средств от обнаружения
8	0,881384	3	0,744774	191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	+	6	Повышение привилегий по доступу к компонентам систем и сетей
9	0,878958	1	0,741071	21	Угроза злоупотребления доверием потребителей облачных услуг	-	4	Закрепление (сохранение доступа) в системе или сети

Анализ результатов моделирования показывает, что совпадение экспертных оценок и предложенных сценариев реализации составляет более 50 %. Время, затраченное на построение сценариев экспертным способом и при работе эксперта с применением ИСППР сокращено в 3 раза.

3.5 Выводы по третьей главе

1. Выполнено системное моделирование процесса оценки угроз БИ, изложенного в Методике ФСТЭК России с целью выявления основных затруднений в работе при его реализации.

2. На основе методов интеллектуального анализа текстов был разработан алгоритм построения векторного представления текстовых описаний угроз, уязвимостей, тактик (техник) и оценки их семантической близости, позволяющий провести предобработку текстовых описаний уязвимостей, тактик (техник) и угроз с целью их дальнейшей кластеризации.

3. Разработан алгоритм кластеризации текстовых описаний угроз, уязвимостей, тактик и техник на основе оценки их семантической близости, позволяющий оценить качество работы различных алгоритмов векторизации, путем определения наличия компактных групп текстовых описаний в пространстве признаков векторных вложений.

4. Разработаны метод и алгоритм оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО исследуемого объекта, позволяющие установить соответствие между множествами уязвимостей, тактик (техник) и угроз путем анализа матрицы попарных расстояний.

5. Проведен эксперимент, показывающий, что использование предложенных алгоритмов может снизить трудоемкость работы специалистов по ИБ в процессе оценки актуальных угроз. Время, затраченное на построение сценариев экспертным способом, составило более 0,5 часа, при работе эксперта с применением ИСППР затрачено менее 10 минут.

6. Разработанная семантическая модель фрагмента сценария реализации угроз позволила определить концепцию построения всех возможных взаимосвязей между текстовыми описаниями уязвимостей, тактик, техник и угроз, т.е. описать принцип построения сценария реализации угроз.

7. Реализация графовой модели, описывающей отношения множеств угроз, уязвимостей, тактик и техник их эксплуатации с использованием различных моделей векторных вложений совместно с алгоритмом кластеризации показал, что применение предобученных моделей-трансформеров позволяет получить более компактное представление структуры текстовых описаний. Наилучший результат продемонстрировала модель BERT 2.

В Главе 4 предложен прототип ИСППР, реализующий метод и алгоритм оценки и приоритизации множества релевантных угроз БИ для выявленных уязвимостей ПО объектов КИИ, алгоритм построения графовых моделей сценариев реализации актуальных угроз БИ Использование данных механизмов позволит упростить процесс выявления сценария реализации угроз.

Глава 4. Разработка и применение исследовательского прототипа интеллектуальной системы поддержки принятия решений при оценке и анализе актуальных угроз БИ и уязвимостей ПО

В данной главе рассмотрена архитектура исследовательского прототипа ИСППР, реализующей предложенные в работе метод и алгоритм оценки и приоритизации множества релевантных угроз БИ для выявленных уязвимостей ПО объектов КИИ, алгоритм построения графовых моделей сценариев реализации актуальных угроз БИ. Представлена методика оценки и анализа актуальных угроз БИ и уязвимостей ПО, а также результаты оценки и анализа актуальных угроз БИ для конкретного промышленного объекта – АСУ ТП приема, хранения и отпуска товарной нефти с использованием инструментальных средств разработанной ИСППР.

4.1 Архитектура исследовательского прототипа ИСППР

Как отмечалось в разделе 3.1, наиболее затруднительным и трудоемким этапом выполнения рекомендаций Методики ФСТЭК России является построение сценариев реализации угроз БИ ввиду отсутствия в настоящее время автоматизированной системы, позволяющей ускорить процесс обработки текстовых описаний выявленных уязвимостей ПО, релевантных угроз БИ и соответствующих им тактик (техник) реализации угроз БИ. Далее представлен исследовательский прототип ИСППР, предназначенной для оказания квалифицированной помощи специалистам по ИБ при определении перечня актуальных угроз БИ.

Ключевым элементом ИСППР является механизм сопоставления текстовых описаний уязвимостей ПО и связанных с ними угроз БИ, что позволяет определить для каждой выявленной уязвимости ПО множество релевантных (т.е. потенциально наиболее вероятных, ожидаемых) угроз БИ, с последующей их приоритизацией и

построением сценариев их реализации с использованием определенных тактик и техник.

Система включает в себя следующие основные модули:

– подсистему локального хранения актуальной копии записей БДУ ФСТЭК (I);

– подсистему сопоставления уязвимостей ПО, тактик (техник) и угроз БИ, на основе их текстовых описаний (II);

– подсистему оценки актуальных угроз БИ и уязвимостей ПО для исследуемого объекта КИИ (III).

Детализированная схема структурно-функциональной организаций системы представлена на Рисунке 4.1.

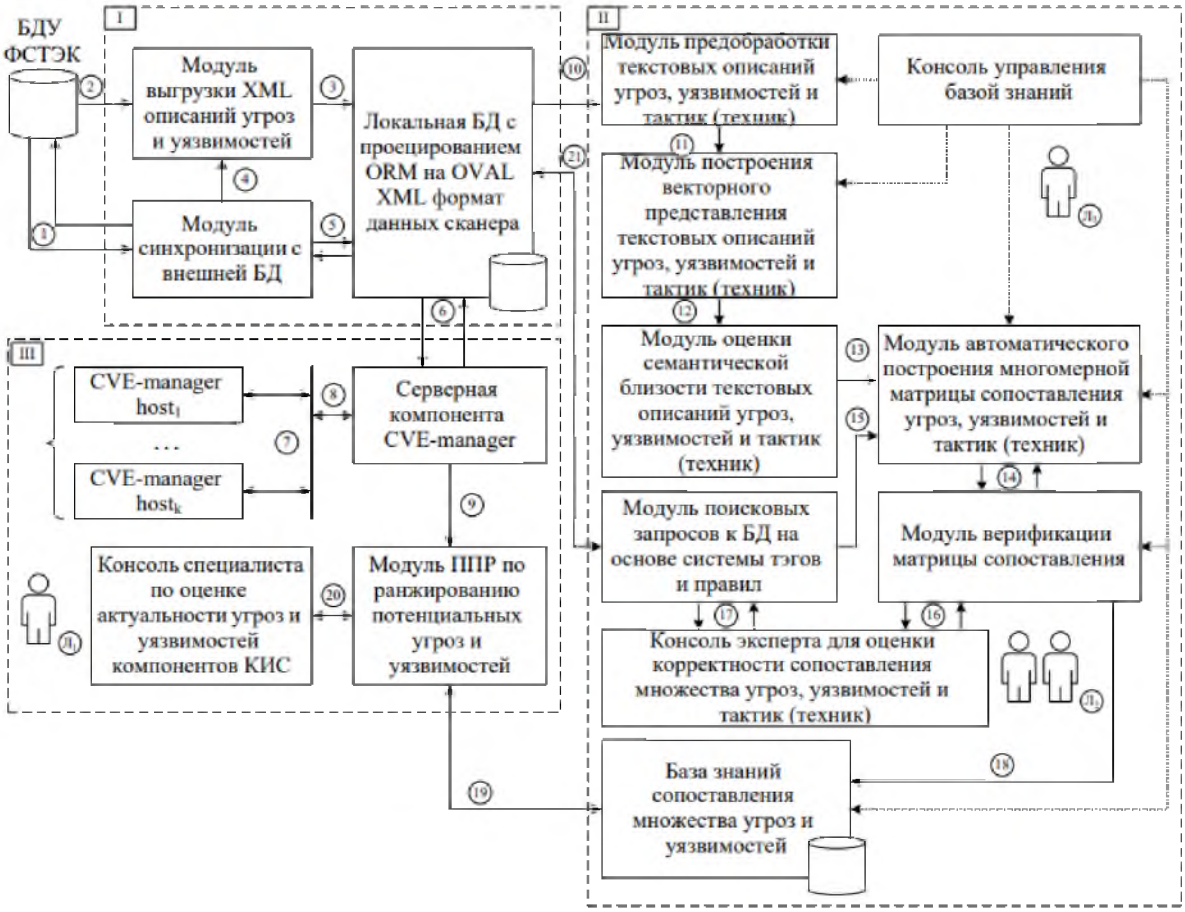


Рисунок 4.1 – Структурно-функциональная организация автоматизированной системы анализа актуальных угроз БИ и уязвимостей ПО на основе оценки семантической близости их текстовых описаний

Подсистема локального хранения актуальной копии БДУ ФСТЭК России (I) предназначена для построения СУБД с объектно-ориентированным проецированием (ORM) хранимых сущностей, характеризующих угрозы БИ и уязвимости ПО в формате открытого языка описания и оценки уязвимостей (OVAL) [110], на сериализуемые файлы в соответствии с выбранной XML-схемой. Модуль синхронизации с внешней БД сопоставляет (5) временные метки изменений данных внешнего хранилища БДУ ФСТЭК (1) и метки в локальном хранилище данных. По результатам сопоставления принимается решение о запуске (4) механизма синхронизации. Модуль выгрузки XML-описаний угроз БИ и уязвимостей ПО из внешней базы подключается (2) к серверу БДУ и выполняет импорт данных (3) в локальную СУБД в требуемом формате.

Подсистема сопоставления угроз и уязвимостей на основе их текстового описания (II) предназначена для построения базы знаний, описывающей отображение множества уязвимостей ПО на множество тактик (техник), а затем тактик (техник) на множество угроз БИ.

БДУ ФСТЭК, помимо формальных метрик, содержит текстовые описания уязвимостей ПО, тактик (техник) и угроз БИ, характеризующие особенности их проявления и возможности эксплуатации нарушителем. Модуль предобработки текстовых описаний угроз БИ, уязвимостей ПО и тактик (техник) извлекает (10) данные из локального хранилища и выполняет цепочку подготовительных преобразований текстовых описаний (фильтрацию и нормализацию) сущностей для передачи (11) в модуль построения их формализованных векторных представлений. Модуль оценки семантической близости текстовых описаний использует (12) формализованные векторы признаков каждой сущности для попарной оценки их близости на основе косинус-метрики. Далее модуль автоматизированного построения многомерной матрицы сопоставления уязвимостей ПО, тактик (техник) и угроз БИ на основе оценок семантической близости их описаний формирует (13) матрицу отображения множества уязвимостей ПО на множество тактик (техник), а затем тактик (техник) на множество угроз БИ (см. Рисунок 3.12, раздел 3.3 Главы 3).

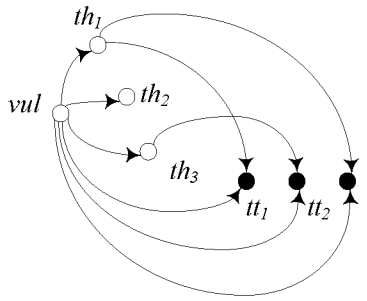
Эксперты (Л2) с помощью консоли доступа выполняют оценку (16) корректности сопоставления множества угроз БИ и уязвимостей ПО и, в случае необходимости, корректировку результатов. В процессе верификации (14) матрицы сопоставления эксперты опираются (17) на имеющийся механизм поисковых запросов к локальной БД на основе системы тегов и правил фильтрации (21, 15), предусмотренных БДУ ФСТЭК. Верифицированные результаты сопоставления уязвимостей ПО, тактик (техник) и угроз БИ помещаются в хранилище базы знаний для последующего использования экспертами в ходе аудита ИБ объекта КИИ. Специалист по знаниям (Л3) управляет работой модулей предобработки и векторизации текстовых описаний, а также следит за метриками качества базы знаний.

Подсистема оценки актуальных угроз БИ и уязвимостей ПО для объекта КИИ (III) – с помощью клиент-серверного сканера (CVE-manager) обеспечивается сбор (7, 8) данных об уязвимостях ПО рабочих станций и серверов объекта КИИ. Применяется связка ПО CVE-manager и ScanOVAL для ОС Linux и Windows, управляемое серверной компонентой, и взаимодействующее (6) с локальной БД. Результаты поиска уязвимостей ПО с помощью сканеров уязвимостей представляются в виде XML- документов с разметкой на языке OVAL. Применение графических интерфейсов работы с найденными уязвимостями ScanOVAL и WEB-интерфейс БДУ ФСТЭК позволяют выполнить фильтрацию найденных уязвимостей ПО по 15 параметрам. Однако, ввиду значительного количества выявляемых уязвимостей на отдельных хостах (более 200 уязвимостей для системы с систематическим обновлением минимального набора прикладного ПО), ручная фильтрация даже наиболее критических по оценкам уязвимостей ПО может занять длительное время. Существующие решения [32] позволяют несколько упростить поиск и сопоставление актуальных угроз БИ и уязвимостей ПО для конкретных версий ПО, но дальнейшая автоматизация процедуры подбора актуальных угроз БИ и уязвимостей ПО на основе данных интеллектуальной фильтрации и оценки семантической близости их текстовых описаний позволит значительно сократить

трудоемкость данной процедуры и масштабировать решение для крупных объектов КИИ.

С помощью консоли специалист по ИБ (Л1) выполняет оценку (20) актуальных угроз БИ и уязвимостей ПО для отдельных узлов объекта КИИ, руководствуясь рекомендациями модуля поддержки принятия решений по ранжированию и сопоставлению потенциальных угроз БИ и уязвимостей ПО, полученных (9) в результате сканирования ПО объекта КИИ, и механизмами интеллектуальной фильтрации (19) на основе извлекаемых из базы знаний данных.

Основная структура данных, использованная при проектировании алгоритмического обеспечения ИСППР, представляет собой списочное представление графа. На рисунке 4.2 «а» представлена визуализация фрагмента графа; на рисунке 4.2 «б» – графовое представление отношений между угрозами БИ, уязвимостями ПО, тактиками и техниками основано на построении списка кортежей $\mathbf{G} = \{src_i,\ dct_i, w_i\}$ с указанием в качестве весового коэффициента нормированного значения метрики семантической близости текстовых описаний соответствующих вершин, где типам вершин соответствуют: th_i – угроза, tt_i – тактика (техника), vul_i – уязвимость.



а)

src	***dst***	***w***
vul_i	th_j	w
vul_i	tt_k	w
th_j	tt_k	w

б)

Рисунок 4.2 – а) визуализация фрагмента графа; б) построение графа связей в виде списка кортежей

При реализации графового представления связей между угрозами БИ, уязвимостями ПО, тактиками и техниками, ключевой задачей является оценка семантической близости текстовых описаний не только двух смежных вершин (например, «угроза»-«уязвимость», «угроза»-«тактика (техники)», «угроза»-

«уязвимость», «уязвимость»-«тактика (техники)»), но и троек вершин типа «угроза»-«уязвимость»-«тактика (техники») для обеспечения смыслового сходства потенциальных действий нарушителя при эксплуатации уязвимости ПО с помощью определенных тактик с целью реализации той или иной угрозы БИ. Использование отдельных пар приводит к тому, что, например, связь между угрозой и уязвимостью через тактику (технику) может быть слишком слабо выражена (ниже заданного порога), тем самым не давая существенного сокращения списка рекомендаций для последующего ручного анализа экспертом.

Переход к тройкам вершин (Рисунок 4.3), между которыми мера близости выше заданных порогов для каждого типа пар (Рисунок 4.4), позволяет удалить из графа существенное количество избыточных связей и сократить количество анализируемых вариантов.

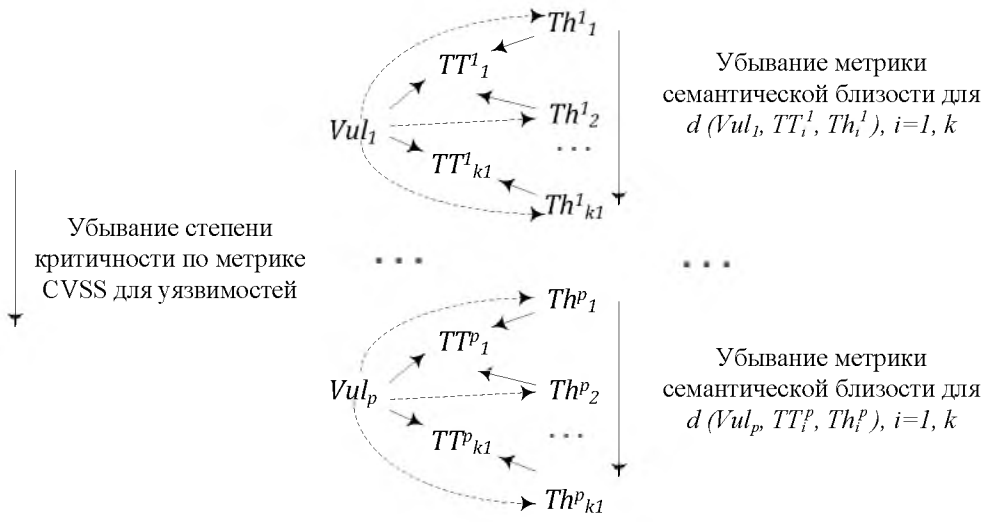


Рисунок 4.3 – Сопоставление угроз БИ, уязвимостей ПО и тактик (техник) их эксплуатации с учетом оценок семантической близости их текстовых описаний

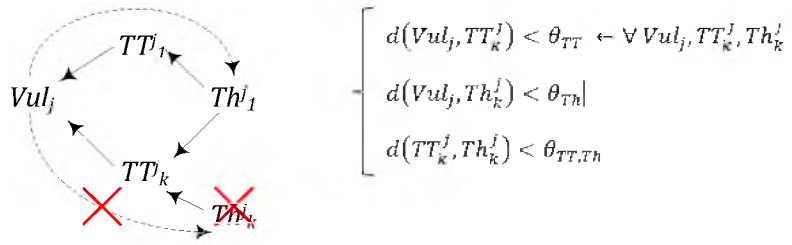


Рисунок 4.4 – Правило анализа семантической близости троек «*Vul-Th-TT*»

Алгоритм прореживания связей для формирования подобных троек вершин графа представлен на Рисунке 4.5.

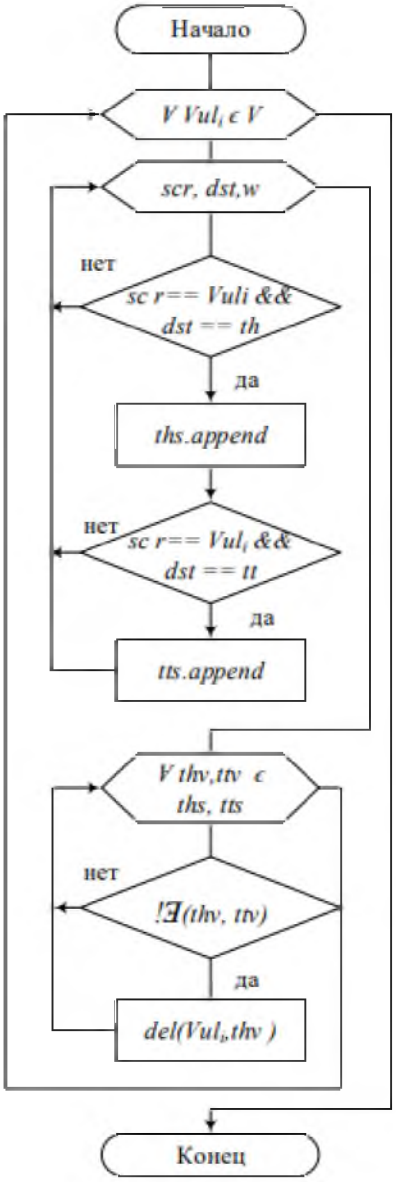


Рисунок 4.5 – Алгоритм прореживания связей для выделения сильно связанных троек *vul-th-tt*

На основе предложенного математического и алгоритмического обеспечения ИСППР последующая разработка ПО системы основана на применении парадигмы объектно-ориентированного анализа и проектирования. UML-диаграмма использования модулей ИСППР представлена на Рисунке 4.6. В проектируемом прототипе программной системы предусмотрены 2 роли: пользователь и

администратор. Администратор может выполнять те же функции, что и обычный пользователь и, помимо этого, он может создавать нового пользователя и назначать пользователям права на проект. Пользователь может создать проект, внести по нему различные данные, а также на каждом этапе оценки угроз БИ выгрузить табличные данные для дальнейшего формирования модели угроз БИ.

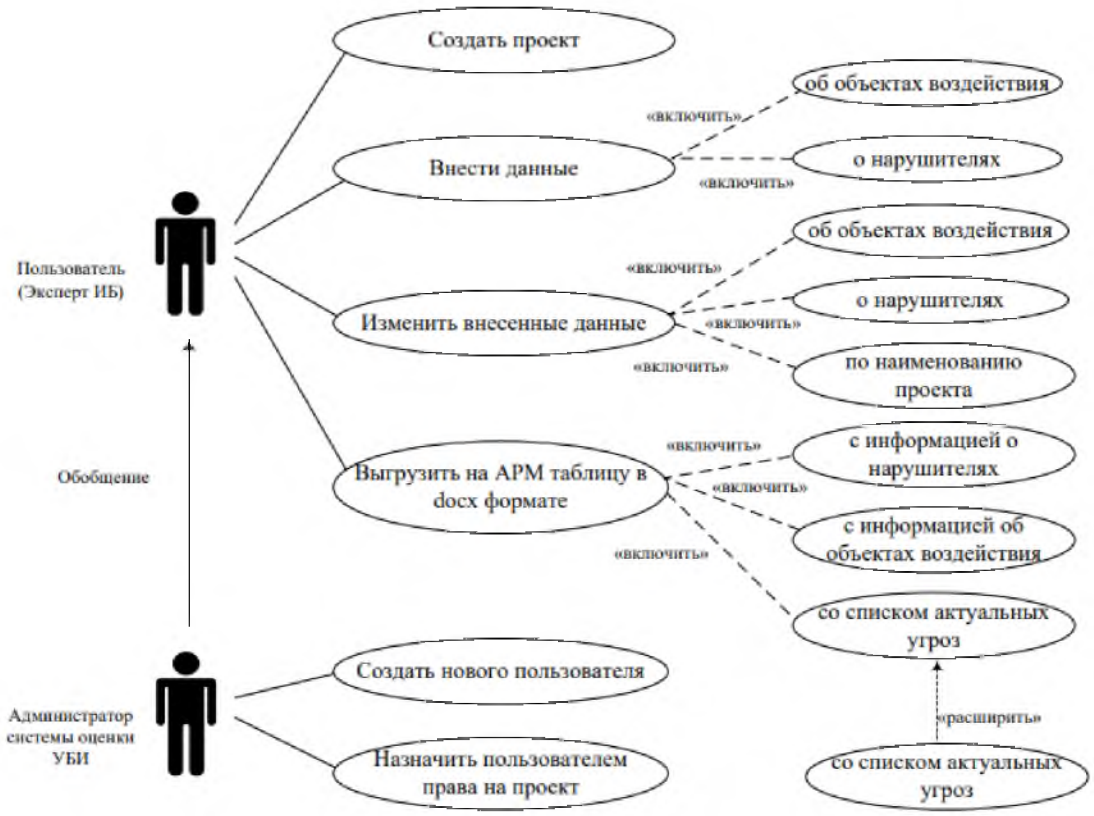


Рисунок 4.6 – UML-диаграмма использования модулей ИСППР

Информационная модель в нотации ERD (диаграммы «сущность-связь») для подсистемы I, обеспечивающей хранение сущностей, характеризующих угрозы БИ, уязвимости ПО, тактики и техники, представлена на Рисунке 4.7.

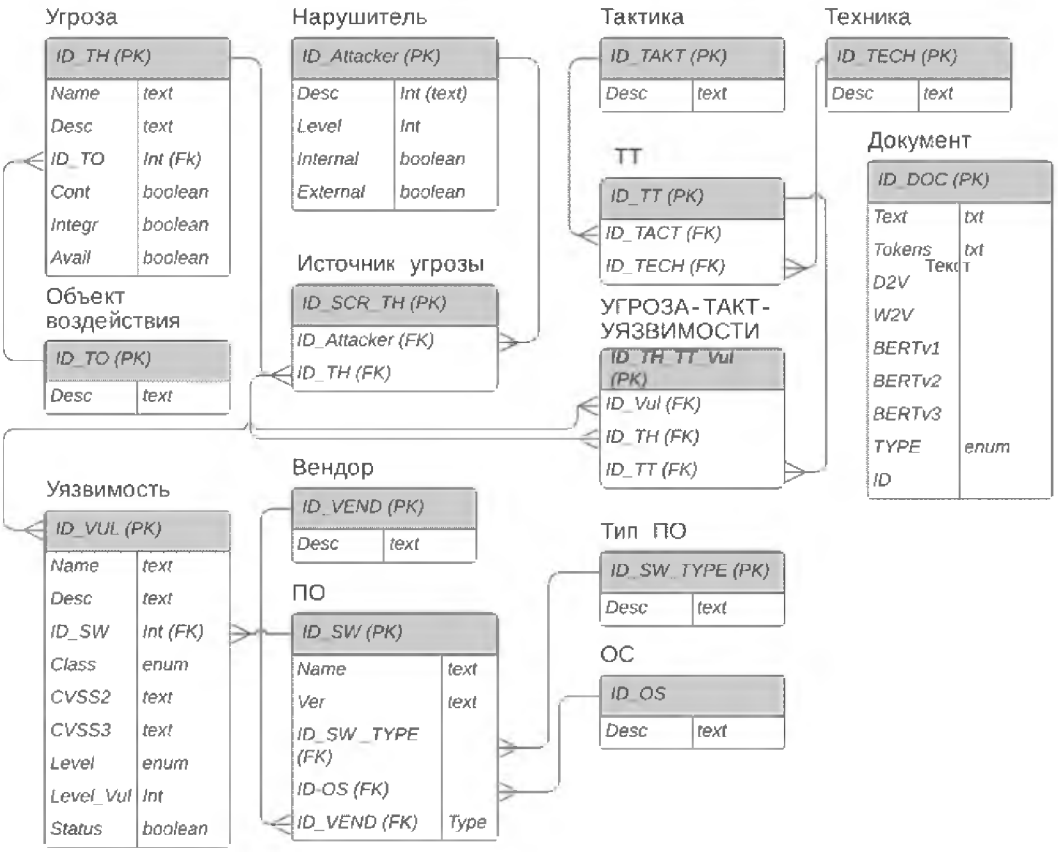


Рисунок 4.7 – Информационная модель в нотации ERD для подсистемы I ИСППР

Ключевые сущности и их характеристики приведены в Таблице 4.1.

Таблица 4.1 – Ключевые сущности, их параметры и тип

№	Сущность	Характеристика
1	Угроза	Описание угрозы безопасности информации, включая название, описание, ссылку на объект(ы) воздействия
2	Объект воздействия	Объект воздействия нарушителя в связи с угрозой БИ, уязвимостью и тактикой(техникой) эксплуатации уязвимости. Реализация отношения «многие ко многим»
3	Уязвимость	Описание уязвимости с основными характеристиками, метриками CVSS и текущим статусом в соответствии с БДУ ФСТЭК
4	Нарушитель	Описание нарушителя и его возможностей
5	Источник угрозы	Сущность для описания связей «многие ко многим» между угрозами БИ и нарушителями
6	Вендор	Поставщик ПО / оборудования
7	Тактика	Тактика эксплуатации уязвимостей
8	ТТ	Связь между тактиками и техниками
9	Техника	Техника эксплуатации уязвимости
10	Угроза Тактика Уязвимость	Отношение «многие ко многим» для описания связи между угрозами, уязвимостями и тактика (техниками)

№	Сущность	Характеристика
11	Программное обеспечение	Конкретные версии программного обеспечения
12	Тип программного обеспечения	Классификация типов ПО
13	Операционная система	Тип операционной системы
14	Документ	Сущность для хранения текстовых описаний основных описаний характеристик безопасности с учетом извлеченных векторов вложений

На основе информационной модели создана физическая модель БД для работы с СУБД MySQL. Для упрощения взаимодействия с созданной БД в составе разрабатываемого ПО ИСППР использована прослойка ORM с автоматической генерацией моделей из созданной БД.

В ходе объектно-ориентированного анализа и проектирования основных модулей подсистем ИСППР разработан ряд диаграмм в нотации UML. Диаграмма классов в нотации UML раскрывает организацию подсистемы I и III при построении матриц семантической близости для текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник для последующего формирования списка актуальных угроз БИ и способов их реализации (Рисунок 4.8).

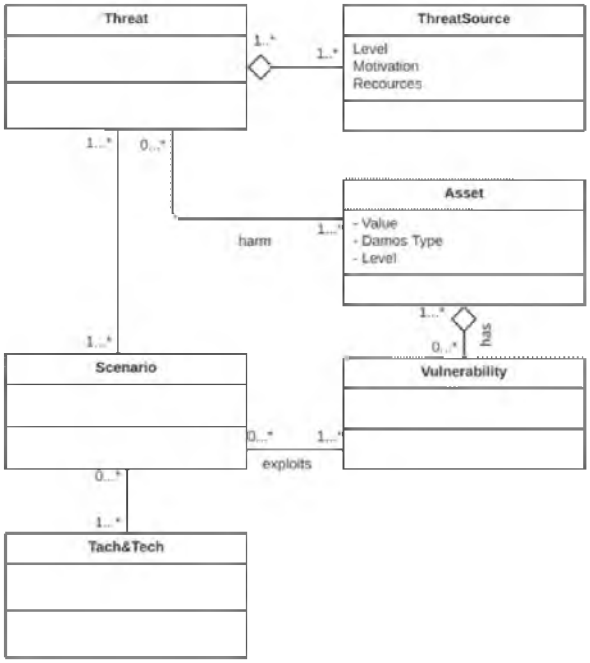


Рисунок 4.8 – Фрагмент диаграммы классов в нотации UML для подсистемы I и III

В Таблице 4.2 приведен перечень основных классов и интерфейсов фрагмента диаграммы на Рисунке 4.8.

Таблица 4.2 – Основные классы и интерфейсы фрагмента диаграммы классов подсистемы I и III

№	Сущность	Тип	Описание
1	Threat	Класс	Описание угрозы из БДУ ФСТЭК, включая поля состояния и методы сериализации
2	ThreatSource	Класс	Описание источника угрозы – логическая оболочка для представления сведений о нарушителе и его возможностях
3	Asset	Класс	Информационный актив, являющийся целью атаки нарушителя (реализации угрозы посредствам эксплуатации уязвимостей с помощью набора тактик и техник)
4	Vulnerability	Класс	Описание уязвимости программного и/или аппаратного обеспечения из БДУ ФСТЭК, включая поля состояния и методы сериализации
5	Scenario	Класс	Представление способа реализации угрозы для информационного актива
6	TacticTech	Класс	Описание тактик и техник из БДУ ФСТЭК, эксплуатация которых делает возможным нарушение конфиденциальности, целостности или доступности информации для выделенного актива

Фрагмент диаграммы классов для подсистемы II ИСППР в нотации UML приведен на Рисунке 4.9. Показаны основные сущности (классы и интерфейсы) для построения матриц семантической близости и фильтрации перечня уязвимостей ПО и угроз БИ (Таблица 4.3).

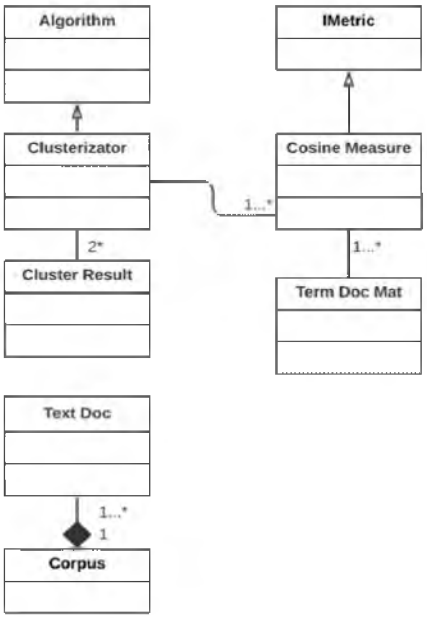


Рисунок 4.9 – Фрагмент диаграммы классов в нотации UML для подсистемы II

Таблица 4.3 – Основные классы и интерфейсы фрагмента диаграммы классов подсистемы II

№	Сущность	Тип	Описание
1	Algorithm	Абстрактный класс	Реализация паттерна «Стратегия»
2	IMetric	Интерфейс	Интерфейс для описания метода оценки семантической близости
3	Clusterizator	Реализация алгоритма кластеризации	Реализация конкретного алгоритма кластеризации для набора подготовленных текстовых описаний
4	CosineMeasure	Класс	Описание метрики семантической близости
5	ClustererResult	Класс	Описание структуры кластеров, полученной в результате применения алгоритма кластеризации (центры, разметка для образцов, оценки качества кластеризации)
5	TermDocMat	Класс	Матрица «терм-документ» для представления распределения токенов по текстовым описания
6	TextDoc	Класс	Текстовое описание, включая исходный фрагмент, предобработанный текст, список токенов, векторы вложений W2V, D2V, BERT1, BERT2, BERT3
7	Corpus	Класс	Описание корпуса текстов

Завершающим этапом разработки ПО, реализующего подсистемы ИСППР, является разработка диаграммы компонентов в нотации UML, позволяющей описать модульную структуру разработанного решения и общие интерфейсы их взаимодействия (Рисунок 4.10).

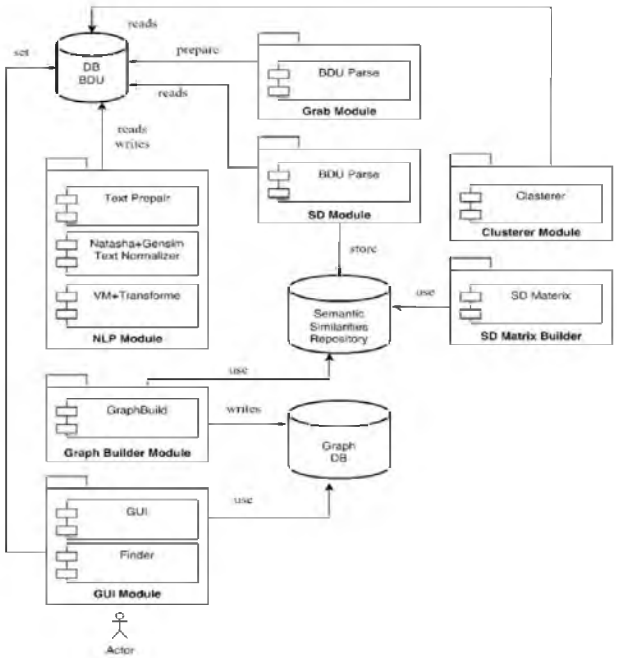


Рисунок 4.10 – Архитектура программного обеспечения ИСППР в нотации UML

Ключевые модули разработанного ПО представлены в Таблице 4.4.

Таблица 4.4 – Ключевые модули разработанного ПО

№	Модуль	Характеристика
1	NLP	Модуль для обработки текстовых описаний на естественном языке
2	Graph Builder	Модуль построения графа связей угроз, уязвимостей, тактик и техник на основе оценок семантической близости их описаний
3	Grab	Модуль для взаимодействия с внешней БДУ ФСТЭК и периодического инкрементного импорта данных в формате XML
4	SD	Модуль для разбора и структурирования собранных из БДУ данных
5	Clusterer	Модуль кластеризации формализованных текстовых описаний для предварительного анализа семантически близки сущностей
6	SD Matrix Builder	Модуль построения матриц семантической близости текстовых описаний угроз, уязвимостей, тактик и техник для последующего ранжирования по степени опасности
7	GUI	Графический интерфейс системы для работы с импортом-экспортом данных из внешних баз, задания параметров задачи и представления промежуточных результатов анализа
8	Semantic Similarities Repository	База хранения матриц семантической близости (файловое бинарное хранилище)
9	Graph DB	База хранения результатов построения графа семантической близости текстовых описаний в виде матриц смежности с соответствующими весовыми коэффициентами

Программное обеспечение ИСППР на этапе работы с уязвимостями ПО объекта КИИ реализовано как диалоговое веб-приложение, некоторые из экранных форм которого приведены на Рисунках 4.11, 4.12. Поэтапный ввод информации, согласно разработанной методике, позволяет сформировать список актуальных угроз БИ и возможных сценариев их реализации – набор тактик (техник) эксплуатации уязвимостей ПО элементов объекта КИИ.

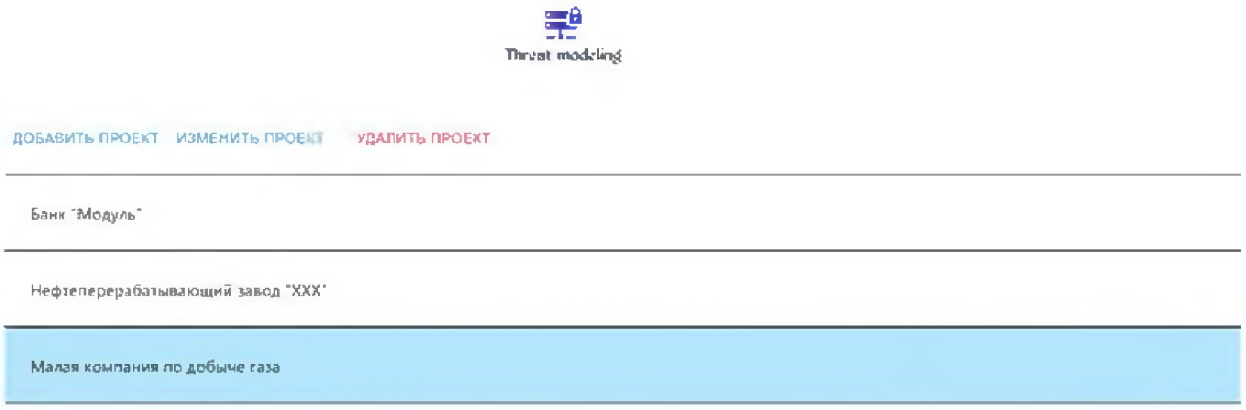


Рисунок 4.11 – Главное меню Web-приложения

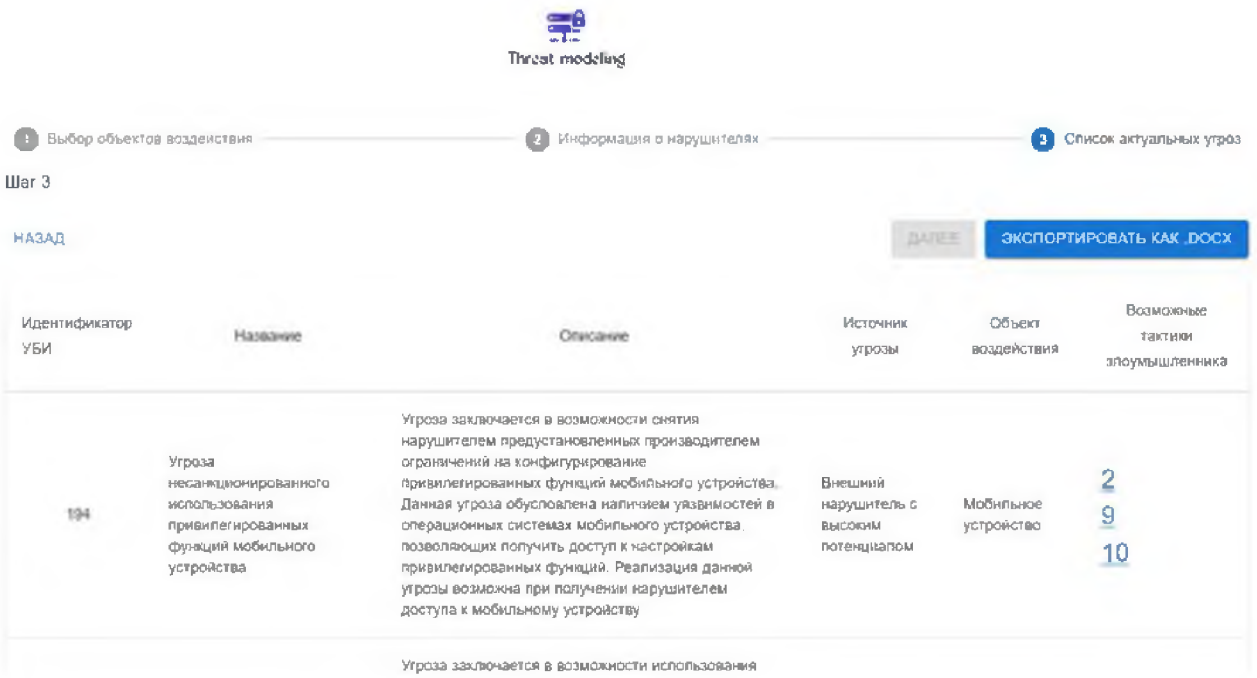


Рисунок 4.12 – Окно формирования списка актуальных угроз БИ

Для оценки угроз БИ для нового объекта КИИ необходимо создать новый проект. На завершающем этапе приложение автоматически формирует список актуальных угроз БИ на основе введенных пользователем данных и анализа семантических связей, а также выводит список возможных тактик (техник), которыми может воспользоваться нарушитель (Рисунок 4.12).

4.2 Результаты применения ИСППР при решении задачи оценки и анализа актуальных угроз БИ АСУ ТП пункта приема, хранения и отпуска товарной нефти

В соответствии с [5, 9], пункт сдачи-приемки нефти (ПСП) – это пункт по учету количества и оценке качества нефти, на котором подразделения принимающей и сдающей нефть сторон выполняют операции приема-сдачи нефти. Основной задачей ПСП является обеспечение достоверности учета и контроля качества нефти, организационно-техническое обеспечение приемо-сдаточных операций.

Средствами АСУ ТП ПСП обеспечивается измерение таких показателей

нефти, как: объем, плотность, температура, давление, массовая доля примесей; кроме этого, обеспечивается инвентаризация нефти в резервуарах и трубопроводах, контроль технологической схемы перекачки нефти через системы учета и многое другое. В составе АСУ ТП ПСП выделим АСУ ТП приема, хранения и отпуска товарной нефти. Данная система предназначена для контроля и управления оборудованием резервуарных парков нефтепродуктов и эстакад слива-налива в железнодорожные цистерны и предназначена для оперативного контроля, учета хранения нефти и нефтепродуктов и управления ТП перекачки, хранения и отгрузки нефтепродуктов.

Ввиду сложности анализируемого объекта, рассмотрим фрагмент базовой модели АСУ ТП приема, хранения и отпуска товарной нефти (Рисунок 4.13).

Рисунок 4.13 – Фрагмент базовой модели АСУ ТП (УПП – установка подогрева продукта; НО – насосное оборудование, ТН – товарная нефть, СКУД – система контроля и управления доступом)

Далее на основе [1, 11] разработана серия моделей, которые используются для оценки состояния ИБ АСУ ТП. Основной целью разработки этих моделей является определение необходимых требований к ИБ и выявлении ключевых характеристик инфраструктуры АСУ ТП на детальном уровне. В работе разработаны базовая модель, базовая архитектура и зональная модель комплексной исследуемой АСУ ТП приема, хранения и отпуска товарной нефти.

Базовая модель отражает общую структуру АСУ ТП, разделенную на несколько уровней (Рисунок 4.14):

– Уровень 4 – включает в себя системы масштаба предприятия, в том числе и технические;

– Уровень 3 – предполагает управление рабочими процессами, в том числе сбор и хранение данных о ходе производства, имеющемся оборудовании и др.;

– Уровень 2 – диспетчерское управление, включает в себя:

  – АРМ операторов, человеко-машинные интерфейсы для операторов;

  – SCADA – систему управления и сбора данных, необходимую для мониторинга и контроля процессов и устройств, таких как насосы, клапаны, трубопроводы, компрессоры и другие. Она позволяет операторам и инженерам наблюдать состояние и параметры работающих устройств, а также управлять ими из центрального управляющего пункта, что повышает качество работы и обеспечивает безопасность производства;

  – Сервер ввода/вывода – позволяет управлять потоками данных, включая прием информации с внешних устройств ввода, отправку информации на внешние устройства вывода, обработку операций чтения и записи на диски и другие устройства хранения данных, а также управление сетевыми соединениями.

– Уровень 1 – включает в себя подсистемы измерения и сбора данных. Они предназначены для сбора данных с датчиков, обработки и хранения информации о динамике процессов. Примерами таких систем на исследуемой АСУ ТП являются системы измерения параметров в резервуарах, системы индикации температуры и др. Оборудование управления считывает информацию с датчиков, приводит в исполнение управляющий алгоритм и подает выходной сигнал на исполнительный элемент (например, контрольные клапаны или приводы задвижек). Контроллеры уровня 1 непосредственно связаны с датчиками и исполнительными механизмами, участвующими в процессе, что позволяет

контролировать процессы, повышать эффективность производства и уменьшать количество аварийных ситуаций.

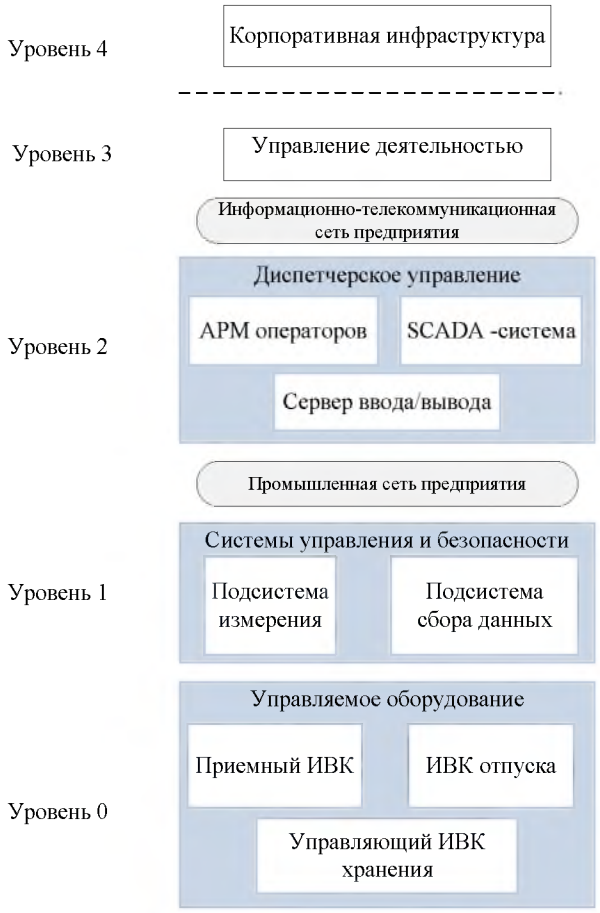


Рисунок 4.13 – Базовая модель комплексной АСУ ТП приема, хранения и отпуска товарной нефти

– Уровень 0 – включает в себя непосредственно управляемое оборудование (датчики и исполнительные механизмы). Для исследуемого объекта – это измерительно- вычислительные комплексы: приемный, хранения и отпуска.

Кроме того, базовая модель отражает расположение информационно-телекоммуникационной и промышленной сетей предприятия. Информационно-телекоммуникационная сеть играет ключевую роль в обеспечении эффективного функционирования бизнес-процессов. Она позволяет:

– обмениваться данными и информацией между сотрудниками предприятия;

– управлять доступом к информации и контролировать ее использование;

– создавать единое пространство для хранения и обработки информации;

– осуществлять мониторинг процессов и оперативно реагировать на изменения ситуации внутри предприятия и др.

Промышленная сеть предприятия необходима для обеспечения эффективного и быстрого обмена информацией между разными устройствами и системами на производстве. Она позволяет автоматизировать и управлять наиболее важными системами, такими как управление оборудованием и производственными процессами, например, отслеживать и контролировать качество принимаемой и отгружаемой нефти. Кроме того, промышленная сеть и её компоненты (коммутаторы, маршрутизаторы, контроллеры, сенсоры и др.) обеспечивают безопасность производства, контроль процессов и управление ресурсами.

Далее разработана базовая архитектура комплексной АСУ ТП приема, хранения и отпуска товарной нефти (Рисунок 4.14). Базовая архитектура содержит детализированные подсистемы, представленные в базовой модели.

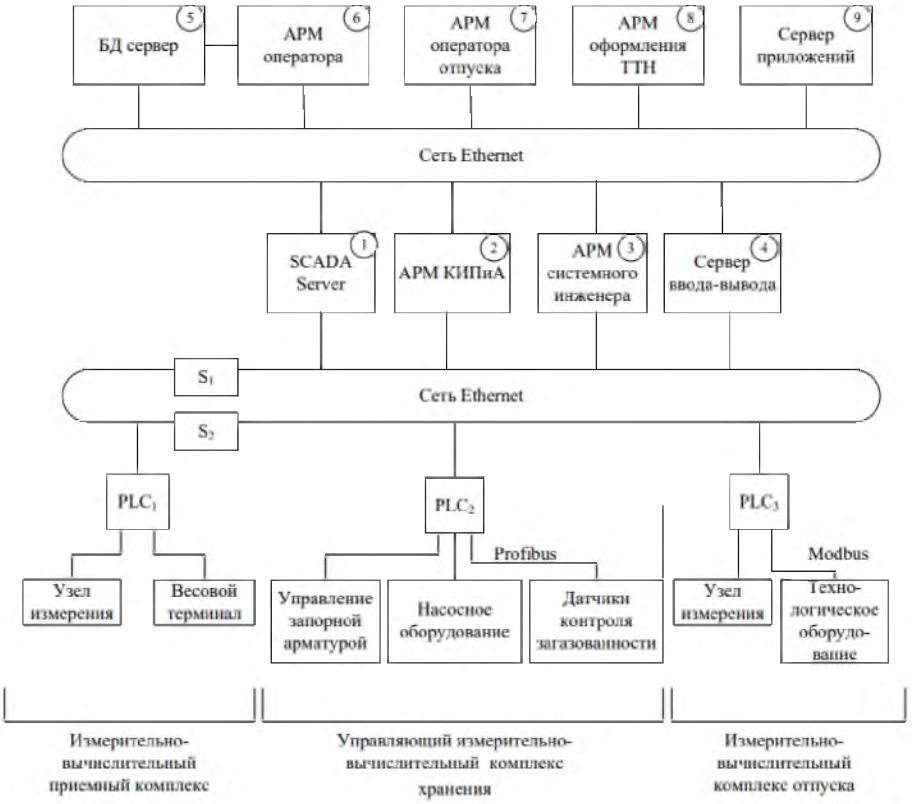


Рисунок 4.14 – Базовая архитектура АСУ ТП приема, хранения и отпуска товарной нефти

На основе базовой архитектуры разработана зональная модель комплексной АСУ ТП приема, хранения и отпуска товарной нефти, содержащая следующие подсистемы (Рисунок 4.15):

– SCADA-сервер (1) системы управления и сбора данных;

– АРМ КИПиА (2) – используется для контроля и управления ТП приема, хранения и отпуска товарной нефти;

– АРМ системного инженера (3) – комплекс программных средств, включающий в себя широкий спектр инструментов для управления инфраструктурой, настройки и конфигурирования сетевых соединений и серверов т.д.;

– сервер ввода/вывода (4) – позволяет управлять потоками данных, включая прием информации с внешних устройств ввода, отправку информации на внешние устройства вывода, обработку операций чтения и записи и т.п;

– БД сервер (5) сервер базы данных – необходим для хранения, управления и доступа к накапливаемы технологическим данных;

– АРМ оператора (6) – предназначен для обеспечения экспорта данных в MES/ERP вышестоящих систем управления;

– АРМ оператора отпуска (7) – предназначен для обеспечения эффективного контроля и управления процессом отпуска нефтепродуктов со складов и терминалов;

– АРМ оформления ТТН (8) – предназначен для контроля и управления транспортировкой нефти. С его помощью возможно автоматическое формирование документации по перевозкам нефти, отслеживание маршрута перемещения транспорта и т.п;

– сервер приложений (9) – предназначен для взаимодействия промышленной сети и сегмента диспетчерского управления.

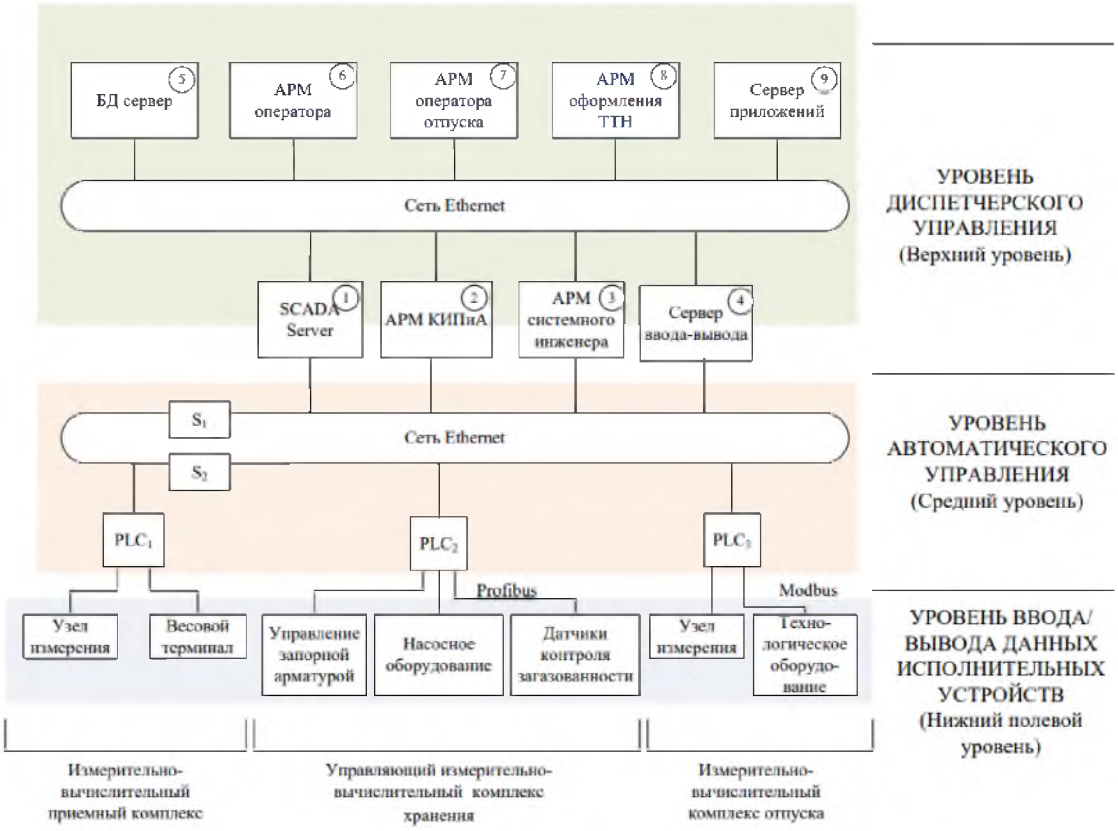


Рисунок 4.15 – Зональная модель комплексной АСУ ТП приема, хранения и отпуска товарной нефти

В соответствии с Методикой [7] была проведена инвентаризация активов АСУ ТП приема, хранения и отпуска товарной нефти, в ходе которой был определен состав программно-аппаратного обеспечения данной АСУ ТП, а также выявлены уязвимости, присущие выявленному программно-аппаратному обеспечению (Таблица 4.5). Всего на исследуемом объекте было обнаружено 66 уязвимостей (обозначения даны в соответствии с БДУ ФСТЭК).

Таблица 4.5 – Состав программно-аппаратного обеспечения и уязвимостей комплексной АСУ ТП приема, хранения и отпуска товарной нефти.

№	Обозначение	Название	Тип	Список уязвимостей
1	PLC_1	Schneider Electric PLC Modicon	ПЛК	BDU:2018-01587; BDU:2019-00122 BDU:2019-00126; BDU:2019-00127
2	PLC_2	Siemens SIMATIC S7-400 PN включая F	ПЛК	BDU:2017-02585; BDU:2019-01782 BDU:2019-00767; BDU:2019-01861 BDU:2021-02031; BDU:2021-02032 BDU:2021-02033

№	Обозначение	Название	Тип	Список уязвимостей
3	S_1, S_2	Промышленные коммутаторы Scalance X	Сетевое оборудование	BDU:2019-00764; BDU:2019-00766 BDU:2019-01539
4	2, 3, 6, 7, 8	АРМ Win7 + Client-based ПО HMI/ WinCC Client	SCADA Client + HMI	BDU:2019-01782; BDU:2019-01858 BDU:2019-01859; BDU:2019-01860 BDU:2019-01861; BDU:2019-01862 BDU:2019-01863; BDU:2019-01864 BDU:2019-04212; BDU:2019-04229 BDU:2020-02442; BDU:2021-02031 BDU:2018-00540; BDU:2018-01125 BDU:2019-00765; BDU:2019-00766 BDU:2019-01778 BDU:2015-11153; BDU:2019-00515 BDU:2019-00516; BDU:2019-00765 BDU:2019-01778; BDU:2019-01782 BDU:2019-01862; BDU:2019-01863 BDU:2019-01864; BDU:2019-04219
5	5	MS Win Server 2016 БД MS SQL Server 2016	Сервер локальной БД	BDU:2018-01029, BDU:2021-03092 BDU:2021-03223, BDU:2021-03322 BDU:2021-03578, BDU:2021-03828 BDU:2021-03999, BDU:2021-04033 BDU:2021-04045, BDU:2021-04118 BDU:2021-04123, BDU:2021-04156 BDU:2021-04157, BDU:2021-04158 BDU:2021-04160, BDU:2021-04161 BDU:2021-04164, BDU:2021-04165 BDU:2021-04166, BDU:2021-04167 BDU:2021-04380, BDU:2021-04381 BDU:2021-04382, BDU:2021-04383 BDU:2021-04384, BDU:2021-04385 BDU:2021-04434, BDU:2021-04435 BDU:2021-04438, BDU:2021-04440 BDU:2021-04441
6	9	Сервер приложений MS Win 2016 + MS Server App-V	Сервер приложений HMI и СУБД	BDU:2021-03092, BDU:2021-03223 BDU:2021-03322, BDU:2021-03578 BDU:2021-03828, BDU:2021-03999 BDU:2021-04033, BDU:2021-04045 BDU:2021-04118, BDU:2021-04123 BDU:2021-04156, BDU:2021-04157 BDU:2021-04158, BDU:2021-04160 BDU:2021-04161, BDU:2021-04164 BDU:2021-04165, BDU:2021-04166 BDU:2021-04167, BDU:2021-04380 BDU:2021-04381, BDU:2021-04382 BDU:2021-04383, BDU:2021-04384 BDU:2021-04385, BDU:2021-04434 BDU:2021-04435, BDU:2021-04438 BDU:2021-04440, BDU:2021-04441

№	Обозначение	Название	Тип	Список уязвимостей
7	1	Win CC V7.2 + Win 2008R2	SCADA сервер	BDU:2019-01782, BDU:2019-01858 BDU:2019-01859, BDU:2019-01860 BDU:2019-01861, BDU:2019-01862 BDU:2019-01863, BDU:2019-01864 BDU:2019-04212, BDU:2019-04229 BDU:2020-02442, BDU:2021-02031 BDU:2018-00540, BDU:2018-01125 BDU:2019-00765, BDU:2019-00766 BDU:2019-01778
8	4	Сервер ввода-вывода на основе Wonderware	Сервер ввода-вывода	BDU:2017-02105 BDU:2017-02595 BDU:2018-01123 BDU:2018-01124
9	2	Win7+ Simatic PDM	АРМ	BDU:2018-01125 BDU:2019-04229 BDU:2020-02442

В рамках первой серии экспериментов для анализируемого объекта был сформирован список из 22 наиболее критичных уязвимостей ПО промышленной сети АСУ ТП. В ходе ручного анализа экспертом были выявлены четыре потенциальные угрозы БИ для целевых активов АСУ ТП, время разработки сценариев их реализации составило более часа. Семантический анализ с помощью предложенных технологий интеллектуального анализа текстов (Text Mining) позволил автоматизировать процедуру префильтрации множества релевантных угроз БИ и способов их реализации, тем самым существенно сократив затраты времени эксперта. Сравнение выполнения процедуры анализа уязвимостей ПО, угроз БИ и сценариев их реализации, проведенного экспертом, с результатами анализа, проведенного автоматизированным способом, приведены в Таблице 4.6.

Таблица 4.6 – Сравнение выполнения процедуры анализа уязвимостей ПО, угроз БИ и сценариев их реализации

Параметр	Экспертное сопоставление по тегам в БДУ ФСТЭК	Автоматизированная система на основе технологий Text Mining	
		Сопоставление уязвимостей и угроз [73]	Сопоставление уязвимостей, угроз и тактик (техник)
Ввод информации	Вручную, графический WEB-интерфейс БДУ	Автоматизированная обработка результатов работы сканеров уязвимостей	

Параметр	**Экспертное сопоставление по тегам в БДУ ФСТЭК**	**Автоматизированная система на основе технологий Text Mining**			
		Сопоставление уязвимостей и угроз [73]		**Сопоставление уязвимостей, угроз и тактик (техник)**	
Тип сопоставления угроз	Ручное	Задается пороговыми и количественными метриками, определяющими чувствительность фильтра на основе сформированной матрицы			
Количество сопоставленных угроз	4	10		8	
Экспертная оценка корректности сопоставления угроз (техник и тактик)	-	Модель	оценка	Модель	оценка
		Word2Vec + TF-IDF	6 из 10	Word2Vec + TF-IDF	6 из 8
		Doc2Vec	5 и 10	Doc2Vec	5 из 8
				BERT 3	7 из 8
Затраченное время на сопоставление угроз и уязвимостей	Более 15 минут	< 5 с		< 10 с	
Возможность подбора техник и тактик реализации угроз	Да	Нет		Да	
Затраченное время на построение сценариев реализации угроз	Более 1 часа	-		Менее 20 минут (включая работу эксперта)	

Визуализация графа семантической близости текстовых описаний тактик (техник), угроз БИ и уязвимостей ПО представлена на рисунке 4.16. Центрами сформированных групп («цветков») являются тактики (техники) tt_i, которые связывают угрозы th_j с соответствующими им по описанию уязвимостями vu_k.

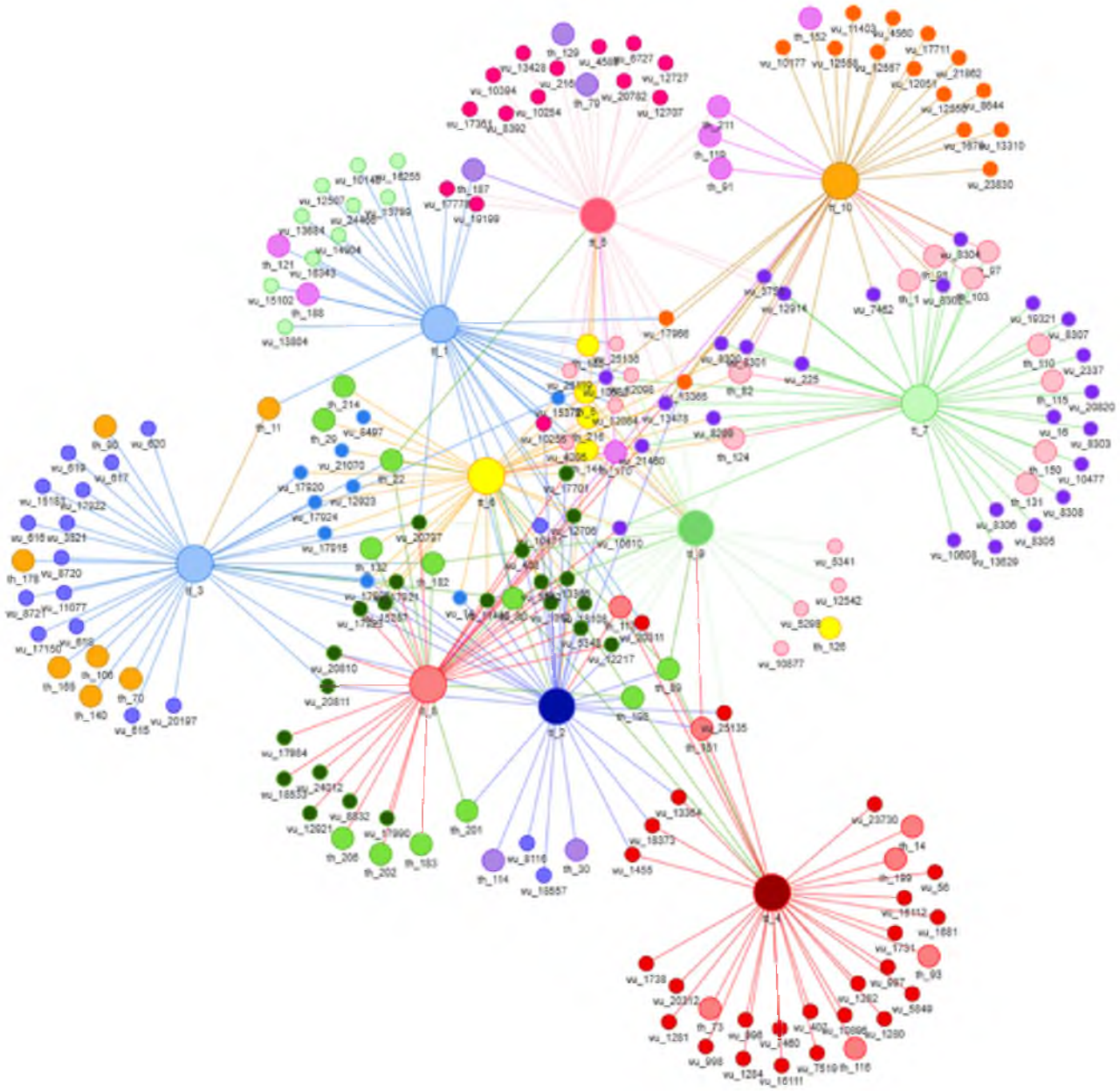


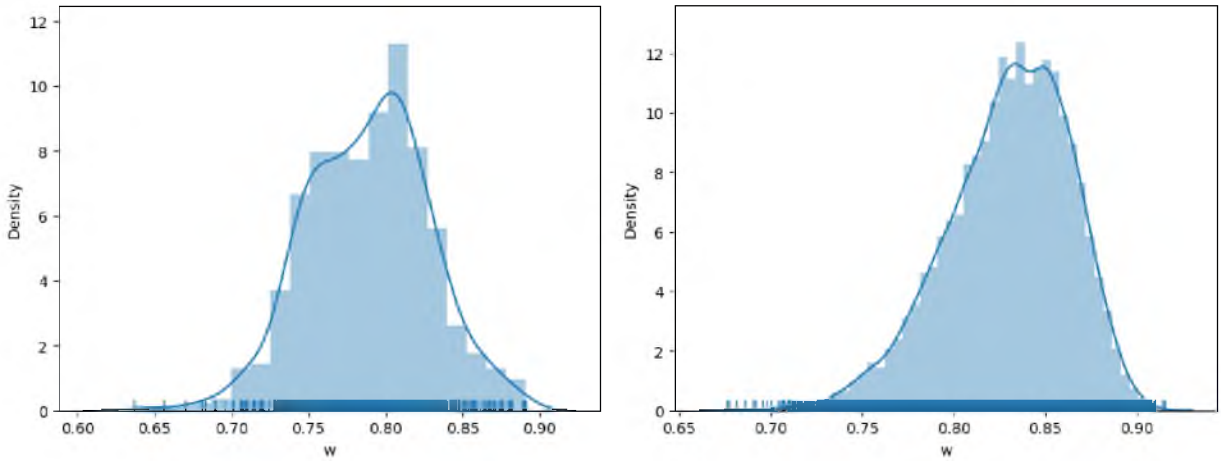
Рисунок 4.16 – Граф семантической близости текстовых описаний тактик (техник) tt_i, угроз th_j и уязвимостей vu_k

Результаты экспериментов, проведенных для исследуемой АСУ ТП, представлены в виде таблицы сопоставления тактик (техник), наиболее схожих угроз БИ и уязвимостей ПО, выявленных в ходе анализа ПО АСУ ТП с помощью сканеров уязвимостей или определенных экспертом (Таблица 4.7).

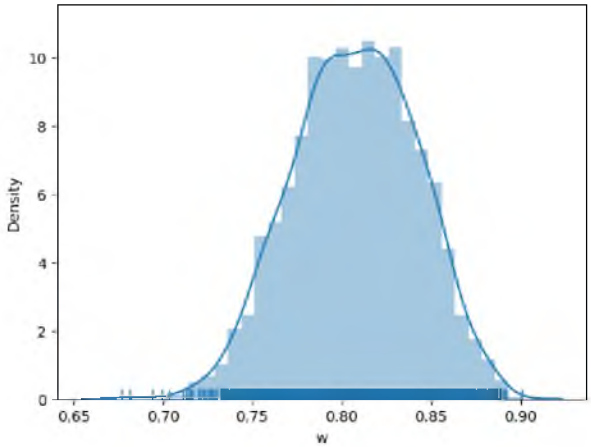
Таблица 4.7 – Фрагмент таблицы сопоставления тактик (техник), угроз БИ и уязвимостей ПО

№ тактики	Текстовое описание тактики и техник	Индексы семантических близких угроз	Текстовое описание семантически близких угроз	Индексы семантических близких уязвимостей	Текстовые описания семантических близких уязвимостей
8	Получение доступа (распространение доступа) к ...	[140, 98, 81, 23, 171, 84, 116, 27, 115, 80]	[Угроза приведения системы в состояние «отказ ...	[BDU:2019-02466, BDU:2019-02818, BDU:2020-0189...	[Уязвимость программного средства централизова...
2	Получение первоначального доступа к компонента...	[171, 203, 140, 80, 23, 84, 92, 77, 81, 116]	[Угроза скрытного включения вычислительного ус...	[BDU:2017-02265, BDU:2017-02264, BDU:2017-0226...	[Уязвимость протокола WPA2, связанная с ошибка...

В рамках второй серии экспериментов был использован полный список из 66 уязвимостей ПО (по группам устройств) (Таблица 4.5). Подбор пороговых значений для оценки семантической близости троек «угроза-уязвимость-тактика(техника)» показан на Рисунке 4.17, где а) гистограмма распределения весов между парами вершин графа «уязвимость»-«угроза» (vu -> th); б) гистограмма распределения весов между парами вершин графа «уязвимость»-«тактика(техника)» vu -> tt; в) гистограмма распределения весов между парами вершин графа «угроза»-«тактика(техника)» th -> tt.



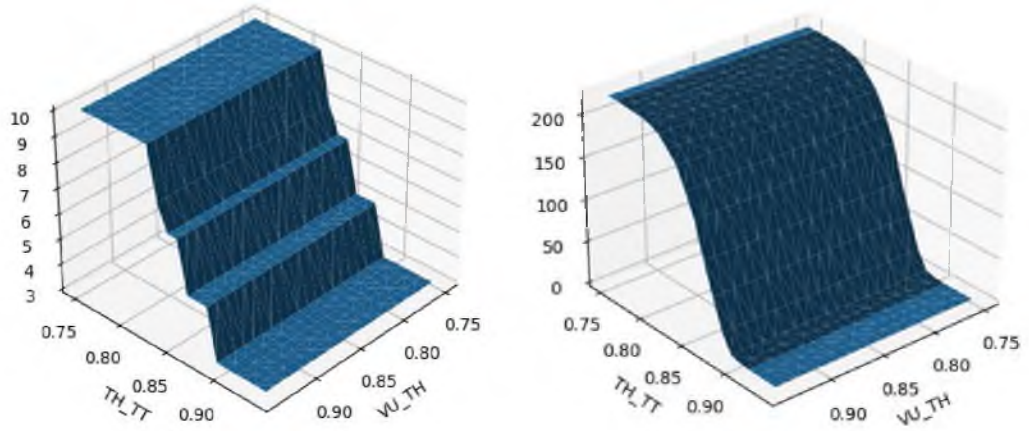
а) Θ_{vu} -> th б) Θ_{vu} -> tt



в) $\Theta_{th \text{ -> } tt}$

Рисунок 4.17 – Подбор пороговых значений для оценки семантической близости троек «угроза-уязвимость-тактика(техника)» на основе анализа гистограмм распределения весов связей (оценок семантической близости) между парами сущностей (по оси абсцисс – оценка семантической близости, по оси ординат – количество образцов, попавших в соответствующий диапазон значений по оси абсцисс)

Анализ Рисунка 4.17 позволяет подобрать пороговые значения для отсечения существенного количества связей с недостаточно выраженным семантическим сходством. Задание пороговых величин для соответствующих отношений «уязвимость»-«угроза» (vu -> th), «уязвимость»-«тактика(техника)» (vu -> tt), «угроза»-«тактика(техника)» (th -> tt) находится в правом «хвосте» распределений и может быть подобрано на основе оценки семантической близости троек «угроза»-«уязвимость»-«тактика(техника)». Зафиксируем порог отношения vu-tt на уровне $\Theta_{VU-TT} = 0{,}85$ и оценим количество соответствующих угроз и тактик (техник) в усеченном графе (после удаления связей, меньших заданного порога, и изолированных вершин) в зависимости от задаваемых порогов Θ_{TH-TT} и Θ_{VU-TT}, заданных на прямоугольной сетке в диапазоне значений [0,75; 0,95] (Рисунок 4.18, а и б).



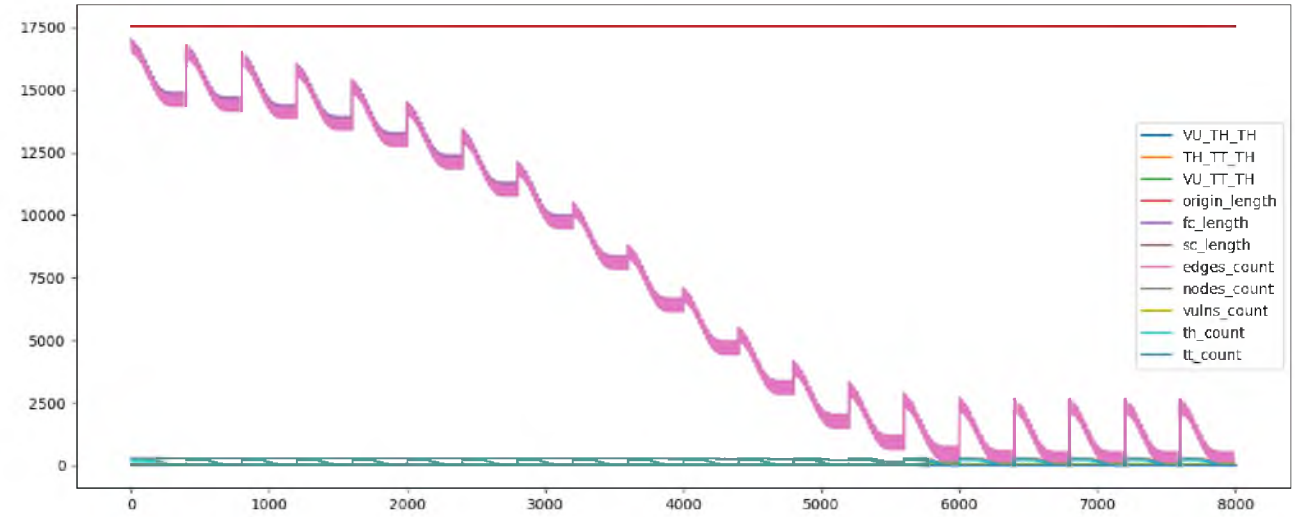
а) б)

Рисунок 4.18 – Зависимость количества соответствующих угроз (а) и тактик (техник) (б) в усеченном графе (после удаления связей, меньших заданного порога, и изолированных вершин) в зависимости от задаваемых порогов Θ_{TH-TT} и Θ_{VU-TT}, заданных на прямоугольной сетке в диапазоне значений [0,75; 0,95] при фиксированном значении $\Theta_{VU_TT} = 0{,}85$

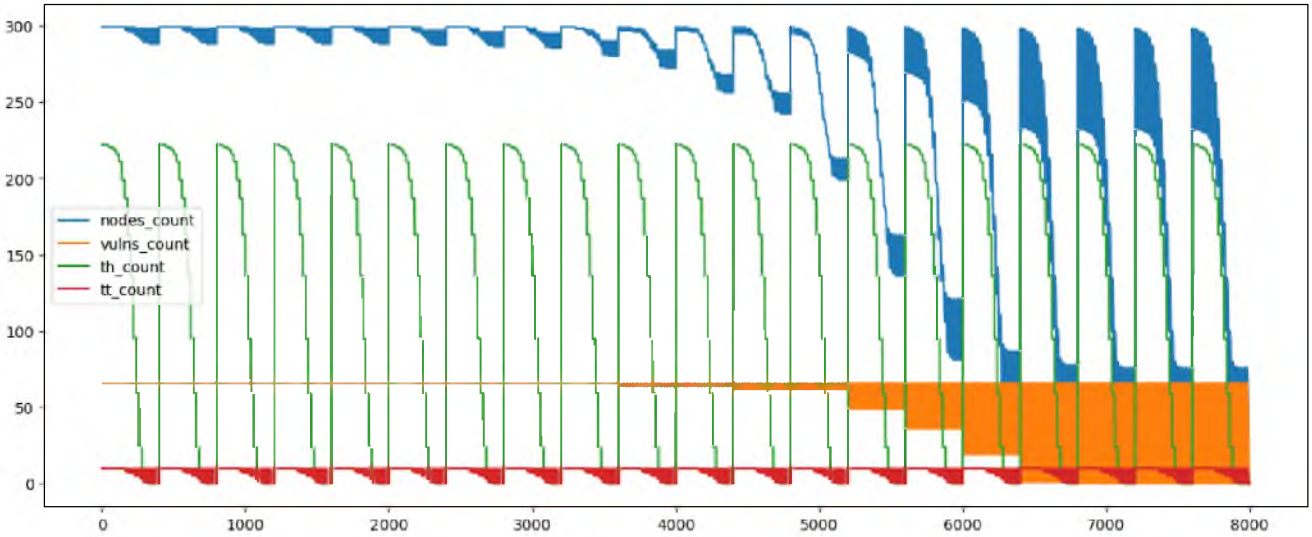
Анализ Рисунка 4.18 показывает, что искомые значения порогов Θ_{TH-TT} и Θ_{VU-TT} для отсечения ребер в графе G находятся в диапазоне [0,85; 0.90], т.к. количество вершин угроз и тактик (техник) остается на достаточном уровне (Таблица 4.8).

На Рисунке 4.19 приведены зависимости количества связанных троек «угроз»-«уязвимость»-«тактика (техника)», для которых выполняется пороговое условие оценки семантической близости. Проведено 8000 экспериментов при табулировании пороговых значений Θ_{VU-TH}, Θ_{TH-TT} и Θ_{VU-TT} в диапазоне [0,75; 0,95] с шагом 0.01 (декартово произведение кортежей пороговых значений в заданных пределах). На рисунок 4.19 а) представлены зависимости порогов (VU_TH, TH_NN, VU_TT), исходного количества ребер (origin_length) графа G, количества ребер после первого (fc_length) и второго (sc_length) этапов прореживания графа G, количества узлов (nodes_count) и ребер (edges_count), количества неизолированных вершин уязвимостей (vulns_count), угроз (th_count) и тактик (техник) (tt_count) в полном графе G от номера кортежа в декартовом

произведении множеств Θ_{VU-TH}, Θ_{TH-TT} и Θ_{VU-TT}; на рисунке б) зависимости количества узлов (nodes_count), количества неизолированных вершин уязвимостей (vulns_count), угроз (th_count) и тактик (техник) (tt_count) в полном графе G от номера кортежа в декартовом произведении множеств Θ_{VU-TH}, Θ_{TH-TT} и Θ_{VU-TT}



а)



б)

Рисунок 4.19 – а) зависимости порогов; б) зависимости количества узлов

Таблица 4.8 – Количество вершин графа связей между угрозами, уязвимостями и тактиками (техниками) при заданном значении порога $\Theta_{VU_TT} = 0{,}85$

VU_TH_TH	TH_TT_TH	edges_count	nodes_count	vulns_count	th_count	tt_count
0,8	0,75	14008	299	66	222	10
0,8	0,76	13910	299	66	222	10
0,8	0,77	13779	299	66	221	10

VU_TH_TH	TH_TT_TH	edges_count	nodes_count	vulns_count	th_count	tt_count
0,8	0,78	13630	299	66	220	10
0,8	0,79	13415	299	66	219	10
0,8	0,8	13181	299	66	216	10
0,8	0,81	12963	299	66	211	10
0,8	0,82	12729	299	66	199	10
0,8	0,83	12511	297	66	187	8
0,8	0,84	12309	296	66	163	7
0,8	0,85	12152	296	66	136	7
0,8	0,86	12023	294	66	95	5
0,8	0,87	11959	292	66	59	5
0,8	0,88	11922	292	66	24	5
0,8	0,89	11901	290	66	4	3
0,8	0,9	11898	290	66	1	3
0,8	0,91	11897	290	66	0	3
0,8	0,92	11897	290	66	0	3
0,8	0,93	11897	290	66	0	3
0,8	0,94	11897	290	66	0	3

При заданных условиях отбора из уточненного диапазона пороговых значений и серии экспериментов: количество угроз TH = 24, возможное количество тактик (техник) TT = {3, 5, 6}, непустое множество уязвимостей (VU! = 0), получено 715 расстановок пороговых величин: Θ_{VU_TH} = {0,75-0,94}, Θ_{TH_TT} = 0,88, Θ_{VU_TT} = {0,84-0,94}, следовательно, определяющим является порог для отношений «угроза»-«тактика(техника)».

Визуализация графа семантической близости текстовых описаний тактик (техник), угроз БИ и уязвимостей ПО представлена на Рисунке 4.20. Центром сформированной группы («цветка») являются тактики (техники) tt_i, которые связывают угрозы th_j с соответствующими им по описанию уязвимостями vu_k.

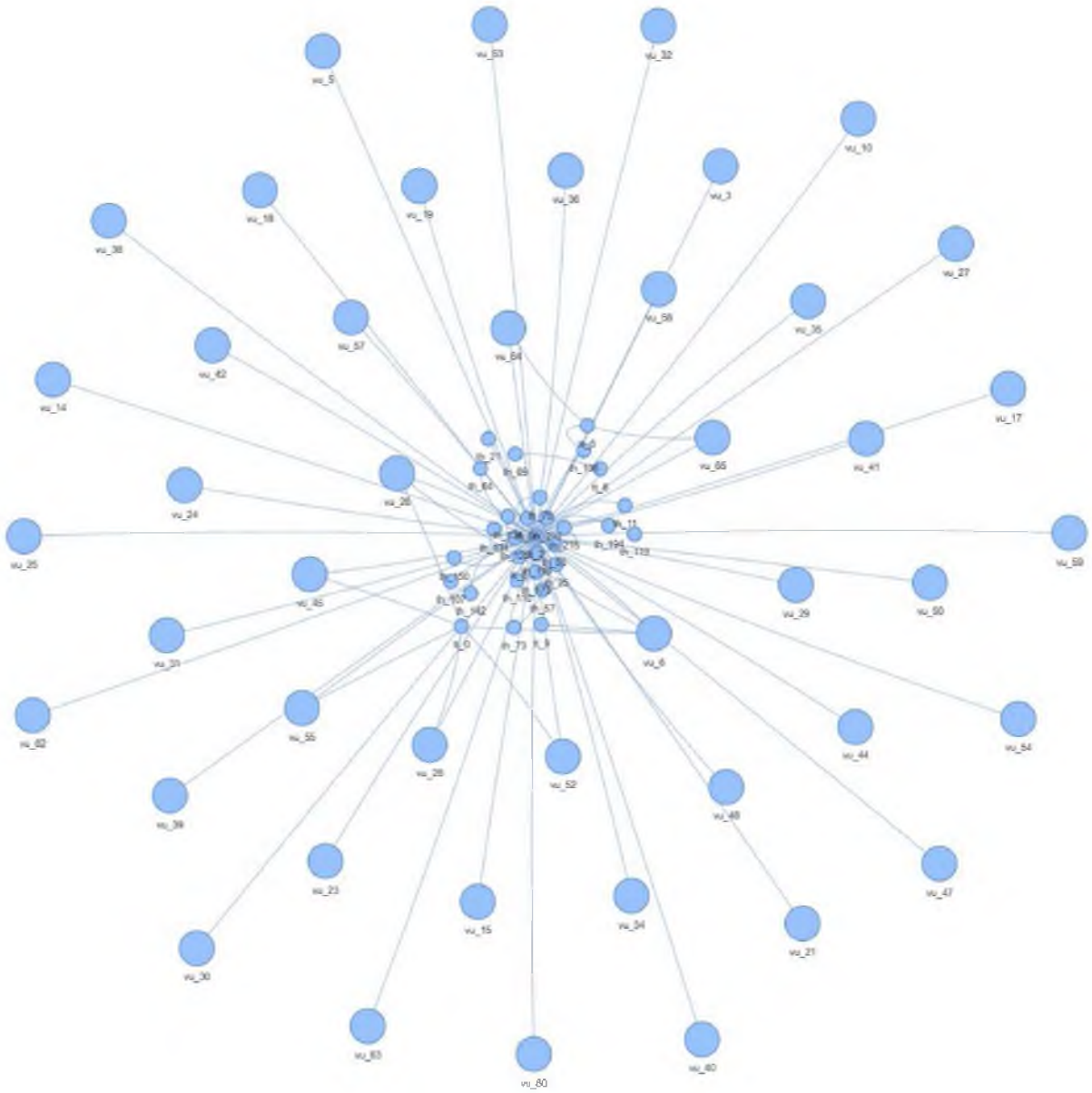


Рисунок 4.20 – Граф семантической близости текстовых описаний тактик (техник) tt_i, угроз th_j и уязвимостей vu_k при значениях порогов $\Theta_{VU_TH} = 0{,}88$, $\Theta_{TH_TT} = 0{,}88$, $\Theta_{VU_TT} = 0{,}84$

Результаты второй серии экспериментов, проведенных для АСУ ТП по сопоставлению уязвимостей ПО, угроз БИ, тактик (техник) представлены в виде Таблицы 4.9.

Таблица 4.9 – Результаты сопоставления уязвимостей ПО, угроз БИ, тактик (техник)

	Идентификатор	Идентификатор УБИ	№ тактики
3	BDU:2017-02595	[11, 21, 25, 53, 57, 64, 73, 75, 95, 106, 107, 110, 116, 119, 122, 131, 134, 142, 150, 173, 194, 210, 215]	[2]
5	BDU:2018-01029		[2, 1]
6	BDU:2018-01123		[2, 5, 1, 9, 6]
10	BDU:2019-00122		[2]
14	BDU:2019-00516		[2]
15	BDU:2019-00764		[2]
17	BDU:2019-00766		[2]
18	BDU:2019-00767		[2]
19	BDU:2019-01539		[2]
21	BDU:2019-01782		[2]
23	BDU:2019-01859		[2]
24	BDU:2019-01860		[2]
25	BDU:2019-01861		[2]
26	BDU:2019-01862		[2, 1, 5]
27	BDU:2019-01863		[2]
28	BDU:2019-01864		[2, 1]
29	BDU:2019-04212		[2]
30	BDU:2019-04219		[2]
31	BDU:2019-04229		[2]
32	BDU:2020-02442		[2]
34	BDU:2021-02032		[2]
35	BDU:2021-02033		[2]
36	BDU:2021-03092		[2]
38	BDU:2021-03322		[2]
39	BDU:2021-03578		[2]
40	BDU:2021-03828		[2]
41	BDU:2021-03999		[2]
42	BDU:2021-04033		[2]
44	BDU:2021-04118		[2]
45	BDU:2021-04123		[2, 1]
47	BDU:2021-04157		[2]
48	BDU:2021-04158		[2]
50	BDU:2021-04161		[2]
52	BDU:2021-04165		[2, 1]
53	BDU:2021-04166		[2]
54	BDU:2021-04167		[2]
55	BDU:2021-04380		[2, 1]
57	BDU:2021-04382		[2]
58	BDU:2021-04383		[2]
59	BDU:2021-04384		[2]
60	BDU:2021-04385		[2]
62	BDU:2021-04435		[2]

	Идентификатор	Идентификатор УБИ	№ тактики
63	BDU:2021-04438		[2]
64	BDU:2021-04440		[2, 6]
65	BDU:2021-04441		[2, 6]

Вручную экспертом также был сформирован список актуальных угроз БИ для выбранного набора уязвимостей ПО с учетом возможного применения тактик (техник) их эксплуатации. Сравнение данного набора угроз БИ с выбранным с помощью ИСППР приведено в Таблице 4.10.

Таблица 4.10 – Анализ выбранного с помощью ИСППР перечня угроз БИ и тактик (техник) их эксплуатации

№	Угроза	Экспертная разметка
1	Угроза деавторизации санкционированного клиента беспроводной сети.	
2	Угроза изменения системных и глобальных переменных.	+
3	Угроза невозможности управления правами пользователей BIOS.	+
4	Угроза неконтролируемого копирования данных внутри хранилища больших данных.	−
5	Угроза некорректной реализации политики лицензирования в облаке.	
6	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.	+
7	Угроза несанкционированного доступа к виртуальным каналам передачи.	
8	Угроза несанкционированного управления указателями.	+
9	Угроза отказа в обслуживании системой хранения данных суперкомпьютера.	
10	Угроза отключения контрольных датчиков.	+
11	Угроза перегрузки грид-системы вычислительными заданиями.	
12	Угроза перехвата данных, передаваемых по вычислительной сети.	+
13	Угроза повышения привилегий.	+
14	Угроза подмены субъекта сетевого доступа.	+
15	Угроза потери доверия к поставщику облачных услуг.	
16	Угроза приостановки оказания облачных услуг вследствие технических сбоев.	
17	Угроза сбоя процесса обновления BIOS.	+
18	Угроза «спама» веб-сервера.	

№	Угроза	Экспертная разметка
19	Угроза несанкционированного использования привилегированных функций мобильного устройства.	
20	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения.	+
21	Угроза несанкционированного доступа к системе при помощи сторонних сервисов.	+

Описание отобранных с помощью ИСППР в ходе экспериментов тактик/техник представлено в Таблице 4.11.

Таблица 4.11 – Фрагмент описания подобранных в ходе экспериментов тактик/техник

№	Тактика	Техники
2	Получение первоначального доступа к компонентам систем и сетей	Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке…
5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств…
6	Повышение привилегий по доступу к компонентам систем и сетей	Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике…
9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы…

Для оценки эффективности работы ИСППР был проведен анализ результатов, полученных от ИСППР на несоответствие мнению эксперта. Данные приведены в Таблице 4.12.

Таблица 4.12 – Оценки несоответствия выданных ИСППР результатов мнению эксперта

		экспертная оценка		сумма
		положительная	отрицательная	
Оценка ИСППР	положительная	11	10	21
	отрицательная	5	196	201
	сумма	16	206	222
Accuracy (точность, правильность измерения)	0,932			
Precision (доля объектов, названных классификатором положительными и при этом действительно являющимися положительными)	0,524			
Recall (доля объектов положительного класса из всех объектов положительного класса, найденные алгоритмом)	0,688			

Время, затраченное на построение сценариев экспертным способом, составило более 4 часов, при работе эксперта с применением ИСППР затрачено менее 40 минут, согласованность экспертной оценки и ИСППР F1 составила 0,59.

4.3 Выводы по четвертой главе

1. Разработана архитектура исследовательского прототипа ИСППР, предназначенной для автоматизации процесса оценки актуальных угроз БИ для объектов КИИ. Ключевым элементом системы является механизм сопоставления текстовых описаний уязвимостей ПО, тактик (техник) и связанных с ними угроз БИ. Предложенная интеллектуальная система позволяет ускорить процесс формирования сценария реализации угроз БИ более чем в 2 раза, кроме того, осуществить приоритизацию указанных угроз БИ с учетом наличия дополнительной информации о существовании зависимостей между угрозами БИ и уязвимостями ПО. Разработана схема структурно-функциональной организации автоматизированной системы анализа актуальных угроз БИ для выявленных уязвимостей ПО объекта КИИ на основе оценки семантической близости их

текстовых описаний. Предложена UML-диаграмма использования модулей ИСППР, раскрывающая функциональные возможности системы для пользователя и администратора. Разработана информационная модель в нотации ERD (диаграммы «сущность-связь») для подсистемы I, обеспечивающей хранение сущностей, характеризующих угрозы БИ, уязвимости ПО, тактики и техники эксплуатации уязвимостей. Построены диаграммы классов в нотации UML, раскрывающие организацию подсистем I, II и III при построении матриц семантической близости для текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник для последующего формирования списка актуальных угроз БИ и способов их реализации. Кроме того, разработана диаграмма компонентов в нотации UML, позволяющая описать модульную структуру разработанного решения и общие интерфейсы их взаимодействия.

2. Разработана методика оценки и анализа актуальных угроз БИ и уязвимостей ПО с использованием ИСППР, устанавливающая единый подход к оценке и анализу актуальных угроз БИ объектов КИИ. Методика соответствует существующим нормативным документам в области обеспечения ИБ объектов КИИ.

3. Рассмотрены вопросы применения предложенной ИСППР для решения задачи оценки и анализа актуальных угроз БИ для промышленной АСУ ТП пункта приема, хранения и отпуска товарной нефти. Реализованы основные этапы анализа и моделирования данного объекта согласно ГОСТ Р 56205-2014: построены фрагмент базовой модели и базовой архитектуры исследуемого объекта, построена зональная модель АСУ ТП, определяющая требования к ИБ объекта. В соответствии с предложенной в работе методикой проведена инвентаризация исследуемого объекта, в ходе которой был определен состав программно-аппаратного обеспечения АСУ ТП, а также выявлены уязвимости, присущие используемому на объекте программно-аппаратному обеспечению.

4. Всего на исследуемом объекте было обнаружено 66 уязвимостей. Проведены две серии экспериментов, в ходе первой серии было установлено, что при автоматизированном способе анализа угроз БИ и уязвимостей ПО время,

затрачиваемое на построение сценариев реализации угроз БИ, сокращается более чем в 2 раза, кроме того, увеличивается на 30 % точность определения актуальных угроз БИ. В ходе второй серии экспериментов были рассмотрены 23 актуальные угрозы БИ, 45 актуальных уязвимостей (из 66 обнаруженных сканером) и 4 тактики (техники), посредством которых могут быть реализованы эти уязвимости. При этом анализ выбранного с помощью ИСППР перечня угроз БИ и тактик (техник) их эксплуатации, показал, что около половины полученных результатов не соответствует мнению эксперта, что само по себе не является критичным, поскольку не приводит к исключению из списка рассматриваемых действительно актуальных угроз БИ.

ЗАКЛЮЧЕНИЕ

В диссертационной работе проведены исследования, позволяющие автоматизировать процесс сопоставления угроз и уязвимостей, определить возможные сценарии атак для выбранного объекта, сократить трудоемкость работы эксперта при оценки актуальных УБИ. В рамках диссертационной работы получены следующие научные и практические результаты:

– разработаны алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ, отличающиеся от известных алгоритмов возможностью осуществлять автоматизированную предобработку больших корпусов слабоструктурированных русскоязычных текстов и их последующий семантический анализ в соответствии с поставленной задачей выделения тематических направлений текстов и их автоматического реферирования;

– разработаны метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов, отличающиеся использованием предложенного алгоритма кластеризации и оценки семантической близости текстовых описаний угроз БИ и уязвимостей ПО в многомерном векторном пространстве, применение которых позволяет сделать более содержательной работу эксперта, сократив время на поиск актуальных угроз БИ, обеспечивая при этом более высокую наглядность, полноту и достоверность результатов такого поиска;

– разработан алгоритм построения графовой модели сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, отличающийся использованием алгоритмов векторного вложения и технологии трансформеров, что позволяет полностью автоматизировать процесс построения графовой модели, снизить трудоемкость и когнитивную нагрузку на специалистов по ИБ, предоставляя ему дополнительную информацию для

формирования перечня актуальных угроз и уязвимостей объектов КИИ;

– предложены архитектура и состав программных модулей ИСППР, реализующих предложенные в работе метод и алгоритмы, применение которых позволяет снизить временные затраты и повысить достоверность решений, принимаемых специалистом по ИБ при оценке и анализе актуальных угроз БИ и уязвимостей ПО объектов КИИ;

– результаты представленных разработок внедрены в производственные и бизнес-процессы предприятий г. Уфы. В ЗАО «РЦЗИ» осуществлено структурирование текстовых описаний бизнес-процессов, технологических процессов, производственных цепочек и совокупности организационно-распорядительной документации для оценок количественных значений показателей критериев значимости с использованием алгоритма автоматической классификации и суммаризации текстов из открытых источников в области информационной безопасности. В ФГБОУ ВО «УУНиТ» введен в учебный процесс для студентов по направлению подготовки 10.04.01 «Информационная безопасность», 09.04.01 «Информатика и вычислительная техника», профиль «Безопасность и защита информации» лабораторный практикум, использующий представленный в диссертации метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа. В ООО «УРАЛТЕХСИСТЕМЫ» проведены испытания алгоритма построения графовой модели сценария реализации угроз ИБ и ИСППР.

Проведенное исследование в области оценки актуальных УБИ позволит снизить трудоемкость оценки актуальных УБИ, а также улучшить качество построения сценариев атаки.

Список сокращений и условных обозначений

АРМ	–	автоматизированное рабочее место
АСУ ТП	–	автоматизированные системы управления технологическими процессами
БД	–	базах данных
БДУ	–	банк данных угроз
БИ	–	безопасности информации
ВПК	–	Военно-промышленный комплекс
ЗО	–	значимый объект
ИБ	–	информационной безопасности
ИС	–	информационная система
ИСППР	–	интеллектуальной системы поддержки принятия решений
КИИ	–	критической информационной инфраструктуры
ПО	–	программное обеспечение
ATT&CK	–	Adversarial Tactics, Techniques & Common Knowledge, общедоступная база знаний, содержащая структурированный набор тактик и техник
BERT	–	Bidirectional Encoder Representations from Transformers, языковая модель, основанная на архитектуре трансформер
CAPEC	–	Common Attack Pattern Enumeration and Classification, классификатор известных шаблонов атак
CBOW	–	Continuous Bag of Words, мешок слов, нейросетевые архитектуры алгоритмов обучения
CVE	–	Common Vulnerabilities and Exposures, база данных (стандарт) в области унификации именования и регистрации обнаруженных уязвимостей ПО
CVSS	–	Common Vulnerability Scoring System, общепринятый стандарт для определения степени опасности уязвимостей в прог
CWE	–	Common Weakness Enumeration, база данных недостатков программного и аппаратного обеспечения
DCS	–	Distributed Control System, распределенные системы управления
Doc2Vec	–	инструмент для расчета векторных представлений документов (предложений)
FastText	–	инструмент для расчета векторных представлений слов
GloVe	–	Global Vectors, инструмент для расчета векторных представлений слов
GPT	–	Generative Pre-trained Transformer, языковая модель, основанная на архитектуре трансформер, нейронная сеть для генерации текста

HMI	–	Human-machine interface, человеко-машинный интерфейс
IDEF	–	Integrated DEFinition, технологии, предназначенные для решения задач моделирования сложных систем
LDA	–	Latent Dirichlet allocation, скрытое распределение Дирихле
LSA	–	Latent semantic analysis, латентно-семантический анализ
NDV	–	National Vulnerability Database, репозиторий данных, содержащий описания уязвимостей
NLP	–	Natural language processing, обработка естественного языка
NLTK	–	Natural Language Toolkit, пакет библиотек и программ для символьной и статистической обработки естественного языка
OWASP	–	Open Web Application Security Project, открытый проект обеспечения безопасности веб-приложений
PCA	–	Principal Component Analysis, Анализ основных компонентов
PLC	–	programmable logic controller, программируемые логические контроллеры
RTU	–	Remote Terminal Unit, пульт дистанционного управления
SCADA	–	Supervisory Control And Data Acquisition, диспетчерское управление и сбор данных
Skip-gram	–	нейросетевые архитектуры алгоритмов обучения
STIX	–	Structured Threat Information eXpression, язык и формат данных, используемый для обмена информацией о киберугрозах
TF-IDF	–	term frequency-inverse document frequency, Статистическая мера, используемая для оценки важности слова в контексте документа
t-SNE	–	t-distributed stochastic neighbor embedding, алгоритм машинного обучения для визуализации
UMAP	–	Uniform Approximation and Projection, алгоритм уменьшения размерности
Word2vec	–	инструмент для расчета векторных представлений слов

Список литературы

1. ГОСТ Р 56205-2014 IEC/TS 62443-1-1-2009. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. – М.: Стандартинформ, 2020.
2. ГОСТ Р 56498 IEC 62443-3-3-2016 Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности. – М.: Стандартинформ, 2016.
3. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. – М.: Стандартинформ, 2018.
4. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – М.: Стандартинформ, 2018.
5. ГОСТ Р 58362-2019. Магистральный трубопроводный транспорт нефти и нефтепродуктов. Автоматизация и телемеханизация технологического оборудования. Основные положения, термины и определения. – М.: Стандартинформ, 2019.
6. ГОСТ Р МЭК 62443-2-1-2015. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики. – М.: Стандартинформ, 2015.
7. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения 25.09.2021).
8. Методология функционального моделирования IDEF0 Руководящий документ. – М.: ИПК Издательство стандартов, 2000.

9. РМГ 89-2010 Государственная система обеспечения единства измерений. Приемо-сдаточные пункты нефти. Метрологическое и техническое обеспечение. – М.: Стандартинформ, 2013.
10. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (утверждены приказом ФСТЭК России от 21.12.2017 № 235). – М., 2014 [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения 20.12.2021).
11. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды. [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения (дата обращения 20.12.2021).
12. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25.12.2017 г. № 239). – М.: 2017. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/1880 (дата обращения 20.12.2021).
13. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
14. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. – [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения 20.12.2021).

15. Актуальные киберугрозы: II квартал 2022 года // Отчет Positive Technologies [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения 08.01.2023).
16. Алгоритм машинного обучения t-SNE – отличный инструмент для снижения размерности в Python [Электронный ресурс]. – Режим доступа: https://medium.com/nuances-of-programming/ (дата обращения 15.10.2022).
17. Аникин, И.В. Нечеткая оценка уязвимостей, основанная на метриках CVSS V.2.0 / И.В. Аникин // Проблемы информационной безопасности. Компьютерные системы. – 2015. – № 3. – С. 111–117.
18. Аралбаев, Т.З. Кластерный анализ как инструмент построения и исследования пространственно-временных моделей угроз / Т.З. Аралбаев, Т.В. Абрамова, М.А. Гетьман // Университетский комплекс как региональный центр образования, науки и культуры: Материалы Всероссийской научно-методической конференции (с международным участием). – Оренбург, 23-25 января 2020. – Оренбург: Оренбургский государственный университет, 2020. – С. 1401–1405.
19. Бабина, О.И. Корпусный метод автоматического морфологического анализа флективных языков / О.И. Бабина, Н.Ю. Дюмин // Вестник Южно-Уральского государственного университета. Серия: Лингвистика. – 2012. – № 25. – С. 38–44.
20. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/scanoval (дата обращения 04.12.2022).
21. Белякова, А.Ю. Обзор задачи автоматической суммаризации текста / А.Ю. Белякова, Ю.Д. Беляков // Инженерный вестник Дона. – 2020. – № 10(70). – С. 142–159.
22. Бенгфорт, Б. Прикладной анализ текстовых данных на Python. Машинное обучение и создание приложений обработки естественного языка / Б. Бенгфорт, Р. Билбро, Т. Океда / Пер. с англ. – СПб.: Питер, 2019. – 368 с.
23. Бондарчук, Д.В. Векторная модель представления знаний на основе семантической близости термов / Д.В. Бондарчук // Вестник Южно-Уральского

государственного университета. Серия: Вычислительная математика и информатика. – 2017. – Т. 6. – № 3. – С. 73–83. – DOI 10.14529/cmse170305.

24. Болодурина, И.П. Автоматизированное машинное обучение: обзор возможностей современных платформ анализа данных / И.П. Болодурина, Д.И. Парфенов, А.Е. Шухман, Л.С. Забродина // Системная инженерия и информационные технологии. – 2021. – Т. 3. – № 1(5). – С. 50–57.
25. Васильев, В.И. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining / В.И. Васильев, А.М. Вульфин, Н.В. Кучкарова // Вопросы кибербезопасности. – 2020. – № 4(38). – С.22–31.
26. Васильев, В.И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В.И. Васильев, А.М. Вульфин, Н.В. Кучкарова // Вопросы кибербезопасности. – 2022. – № 2(48). – С. 27–38. – DOI 10.21681/2311-3456-2022-2-27-38.
27. Васильев, В.И. Методика определения актуальных угроз кибербезопасности АСУ ТП на основе стандарта ГОСТ Р 62443 / В.И. Васильев, Н.В. Кучкарова, К.И. Муслимова // Сборник избранных статей по материалам научных конференций ГНИИ "Нацразвитие". – Санкт-Петербург, 27-31 октября 2018. – 2018. – С. 122–126.
28. Васильев, В. И. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В.И. Васильев, А.М. Вульфин, Н.В.Кучкарова //Системы управления, связи и безопасности. – 2021. – №. 3. – С. 110-134.
29. Власенко, А.В. Информационная безопасность / А.В. Власенко, А.С. Макарян, В.А. Шарай, Б. Швырев. – Краснодар: Новация, 2020. – 190 с.
30. Грызунов, В.В. Выбор наиболее опасных уязвимостей для перспективных информационных систем критического применения / В.В. Грызунов, А.А. Гришечко, Д.Е. Сипович // Вопросы кибербезопасности. – 2022. – № 1(47). – С. 66–75. – DOI 10.21681/2311-3456-2012-1-66-75.

31. Гузаиров, М.Б., Машкина И.В. Управление защитой информации на основе интеллектуальных технологий / М.Б. Гузаиров, И.В. Машкина – М.: Машиностроение, 2013. – 241 с.
32. Дорошенко, И.Е. Вопросы описания возможных сценариев угроз при разработке моделей угроз безопасности информации / И.Е. Дорошенко, М.О. Максудов, В.В. Селифанов // Интерэкспо Гео-Сибирь. – 2021. – Т. 7. – № 1. – С. 16–21.
33. Жук, Р.В. Определение актуальности угроз информационной безопасности в информационных системах обработки персональных данных с использованием математического аппарата нейронных сетей / Р.В. Жук, П.И. Дзьобан, А.В. Власенко // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1(49). – С. 169–178. – DOI 10.21672/2074-1707.2020.49.4.169-178.
34. Жеребцова, Ю.А. Сравнение моделей векторного представления текстов в задаче создания чат-бота / Ю.А. Жеребцова, А.В. Чижик // Вестник Новосибирского государственного университета. Серия: Лингвистика и межкультурная коммуникация. – 2020. – Т. 18. – № 3. – С. 16–34. – DOI 10.25205/1818-7935-2020-18-3-16-34.
35. Зегжда, Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда, Ю.С. Васильев, М.А. Полтавцева, И.Ф. Кефели, А.И. Боровков // Вопросы кибербезопасности. – 2018. – № 2 (26). – С. 2–15.
36. Знакомство с трансформерами. Часть 1 [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/wunderfund/blog/592231/ (дата обращения 15.17.2022).
37. Знакомство с трансформерами. Часть 2 [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/wunderfund/blog/593713/ (дата обращения 15.17.2022).
38. Золотых, Н.Ю. Машинное обучение и анализ данных / Н.Ю. Золотых. – 2013. [Электронный ресурс]. – Режим доступа:

http://www.uic.unn.ru:8103/~zny/ml/Course/04.Principal%20Component%20analysis.pdf (дата обращения 15.10.2022).

39. Как работает Word2Vec: нейросети для NLP. [Электронный ресурс]. – Режим доступа: https://python-school.ru/blog/what-is-word2vec/ (дата обращения 26.06.2022).
40. Кириченко, К.М. Обзор методов кластеризации текстовой информации / К.М. Кириченко, М.Б. Герасимов // Труды Международного семинара «Диалог'2001 по компьютерной лингвистике и ее приложениям». – 2001. – Т. 2. Прикладные проблемы.
41. Кластерный анализ [Электронный ресурс]. – Режим доступа: http://statsoft.ru/home/textbook/modules/stcluan.html#d (дата обращения 11.10.2022).
42. Коноваленко, С.А. Выявление уязвимостей информационных систем / С.А. Коноваленко, И.Д. Королев // Инновации в науке. – 2016. – № 9 (58). – С. 12–20.
43. Котенко, И. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров // Вопросы кибербезопасности. – 2022. – № 4(50). – С. 52–79. – DOI 10.21681/2311-3456-2022-4-52-79.
44. Кучкарова, Н. В. Исследование возможности использования кластерного анализа данных при оценке сценариев реализации угроз безопасности / Н. В. Кучкарова // Мавлютовские чтения: материалы XV Всероссийской молодежной научной конференции: в 7 томах, Уфа, 26–28 октября 2021 года. Том 4. – Уфа: Уфимский государственный авиационный технический университет, 2021. – С. 436-440.
45. Кучкарова, Н.В. Сравнительный анализ систем классификаций АСУ ТП объектов критической информационной инфраструктуры / Н. В. Кучкарова, В. И. Васильев, А. М. Вульфин // Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2019): Труды VII Всероссийской научной конференции (с приглашением зарубежных ученых): в 3 томах, Уфа, 28–30 мая

2019 года. Том 2. – Уфа: Уфимский государственный авиационный технический университет, 2019. – С. 214-219.

46. Кучкарова, Н. В. Применение методов интеллектуального анализа текстов при решении задач обеспечения информационной безопасности / Н. В. Кучкарова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 21–22 мая 2021 года. – Уфа: Башкирский государственный университет, 2021. – С. 28-32. – DOI 10.33184/itokbco-2021-05-21.5.
47. Кучкарова, Н.В. Подход к определению актуальных уязвимостей при оценке уровня защищенности значимых объектов критической информационной инфраструктуры / Н.В. Кучкарова // Сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». – 2019. – С. 356–361.
48. Кучкарова, Н. В. Применение моделей интеллектуального анализа текстов при оценке угроз информационной безопасности / Н. В. Кучкарова // Современные проблемы цивилизации и устойчивого развития в информационном обществе: Сборник материалов VI Международной научно-практической конференции, Москва, 30 декабря 2021 года. – Москва: Общество с ограниченной ответственностью "Институт развития образования и консалтинга". – 2021 . – С. 178-184.
49. Лаврентьев, А.М. Сравнительный анализ специальных корпусов текстов для задач безопасности / А.М. Лаврентьев, Д.М. Рябова, Е.А. Тихомирова, А.И. Фокина, А.М. Чеповский, Т.Ю. Шерстинова // Вопросы кибербезопасности. – 2020. – № 3 (37). – С. 58–65.
50. Ландшафт угроз для систем промышленной автоматизации. Kaspersky ICS CERT. [Электронный ресурс]: – Режим доступа: https://ics-cert.kaspersky.ru (дата обращения 01.08.2022).
51. Латентно-семантический анализ: реализация [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/240209/ (дата обращения 15.10.2022).

52. Лившиц, И.И. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры / И.И. Лившиц, А.С. Бакшеев // Вопросы кибербезопасности. – 2022. – № 6 (52). – С. 40–52.
53. Лось, А.Б. Особенности использования кластерного анализа в системе менеджмента информационной безопасности / А.Б. Лось, А.С. Кабанов, В.И. Трунцев // Промышленные АСУ и контроллеры. – 2013. – №. 8. – С. 67–72.
54. Машинное обучение - сравнение нескольких методов измерения расстояния [Электронный ресурс]. – Режим доступа: https://russianblogs.com/article/7586220986/ (дата обращения 11.10.2022).
55. Метод измерения сходства в системе рекомендаций [Электронный ресурс]. – Режим доступа: https://russianblogs.com/article/7696266567/ (дата обращения 11.10.2022).
56. Милкова, М.А. Тематические модели как инструмент "Дальнего чтения" / М.А. Милкова // Цифровая экономика. – 2019. – № 1(5). – С. 57–70.
57. Минаев, В.А. Методы выявления латентной и негативной информации в текстовых документах / В.А. Минаев, И.Д. Королев, И.А. Кисленко // Технологии техносферной безопасности. – 2016. – № 5(69). – С. 241–248.
58. Моделирование угроз по новой методике ФСТЭК. В чем загвоздка? [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/blogi/aleksandr-astahov/modelirovanie-ugroz-po-novoi-metodike-fstek/view (дата обращения 20.12.2022).
59. Петренко, В.И. Метод реагирования на инциденты кибербезопасности в режиме реального времени / В.И. Петренко, Ф.Б. Тебуева, С.С. Рябцев, А.С. Павлов // FISP-2021: Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации: Сборник докладов III Всероссийской научной конференции (с приглашением зарубежных ученых). – Ставрополь, 30 ноября 2021 года. – Ставрополь: Северо-Кавказский федеральный университет, 2021. – С. 37–41.

60. Мультиклассовая классификация текста. Дисбаланс тренировочных данных и их генерация. Особенности взвешивания. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/677512/ (дата обращения 26.06.2022).
61. Мусаев, А.А. Обзор современных технологий извлечения знаний из текстовых сообщений / А.А. Мусаев, Д.А. Григорьев // Компьютерные исследования и моделирование. – 2021. – Т. 13. – № 6. – С. 1291–1315. – DOI 10.20537/2076-7633-2021-13-6-1291-1315.
62. Мясников, Е.В. Выбор способа декомпозиции пространства признаков для нелинейного снижения размерности / Е.В. Мясников // Компьютерная оптика. – 2014. – Т. 38. – № 4. – С. 790–797.
63. Об одной задаче Data Science [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/mlclass/blog/266727/ свободный (дата обращения: 15.09.2022).
64. Остапенко, А.Г. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск-анализ и оценка эффективности защиты / А.Г. Остапенко, Е.В. Ермилов, А.Н. Шершень, Е.С. Соколова, И.В. Шевченко // Информация и безопасность. – 2013. – Т.16. – № 2. – С. 167–178.
65. Отчет об атаках и инструментарии профессиональных кибергруппировок в 2021 году [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/analytics/reports/2270/] (дата обращения 04.01.2023).
66. Пархоменко, П.А. Обзор и экспериментальное сравнение методов кластеризации текстов / П.А. Пархоменко, А.А. Григорьев, Н.А. Астраханцев // Труды Института системного программирования РАН. – 2017. – Т. 29. – № 2. – С. 161–200. – DOI 10.15514/ISPRAS-2017-29(2)-6.
67. Петренко В. И. и др. Метод обнаружения нарушений информационной безопасности в роевых робототехнических системах с использованием технологий машинного обучения / В.И. Петренко, Ф.Б. Тебуева, С.С. Рябцев,

А.С. Павлов, М.М. Гурчинский //Вестник ВГУ. Серия: Системный анализ и информационные технологии. – 2022. – № 1. – С. 43–55.

68. Плавное введение в Natural Language Processing (NLP) [Электронный ресурс]. – Режим доступа: https://datastart.ru/blog/read/plavnoe-vvedenie-v-natural-language-processing-nlp (дата обращения 15.17.2022).
69. Полетаев, В.С. Информационно–аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет–ресурсов: специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность": диссертация на соискание ученой степени кандидата технических наук / Полетаев Владислав Сергеевич. – Уфа, 2020. – 149 с.
70. Правильный NLP: как работают и что умеют системы обработки естественного языка. [Электронный ресурс]. – Режим доступа: https://tproger.ru/articles/natural-language-processing/ свободный (дата обращения: 15.11.2022).
71. Препарируем t-SNE [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/267041/ (дата обращения 15.10.2022).
72. Селифанов, В.В. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных система с применением банка данных угроз ФСТЭК России / В.В. Селифанов, П.А. Звягинцева, Я.В. Юракова, И.С. Слонкина // Интерэкспо Гео-Сибирь. – 2017. – Т. 8. – С. 202–209.
73. Селифанов В.В. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах / В.В. Селифанов, Я.В. Юракова, И.Н. Картамов // Интерэкспо Гео-Сибирь. – 2018. – С. 271–276.
74. Семантический поиск: от простого сходства Жаккара к сложному SBERT [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/skillfactory/blog/566414/ (дата обращения 11.10.2022).

75. Сканеры уязвимостей – обзор мирового и российского рынков. [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets#part53 (дата обращения 04.12.2022).
76. Соколов, П.В. Сравнительный анализ методов кластеризации текстовой информации / П.В. Соколов, Е.Н. Каруна. [Электронный ресурс]. – Режим доступа: https://scm.etu.ru/assets/files/2021/scm21/papers/155-158.pdf свободный (дата обращения: 15.09.2022).
77. Соловьев, С.В. Применение аппарата нейросетевых технологий для оценки защищенности веб-приложений / С.В. Соловьев, В.В. Мамута // REDS: Телекоммуникационные устройства и системы. – 2016. – Т. 6. – № 4. – С. 575–579.
78. Суммаризация текста: подходы, алгоритмы, рекомендации и перспективы [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/514540/ (дата обращения 15.12.2022).
79. Сычугов, А.А. Методы и алгоритмы оперативного обнаружения опасных состояний промышленных объектов: автореферат на соискание ученой степени докт. техн. наук / А.А. Сычугов. – Тула: 2021. – 32 с.
80. Тюрин, А.Г. Кластерный анализ, методы и алгоритмы кластеризации / А.Г. Тюрин, И.О. Зуев // Вестник МГТУ МИРЭА. – 2014. – № 2(3). – С. 86–97.
81. Федорченко, А.В. Разработка сервиса доступа и управления интегрированной базой уязвимостей / А.В. Федорченко, И.В. Котенко, А.А Чечулин // Безопасность информационных технологий. – 2015. – Т. 22. – № 4. – С. 26–32.
82. Федорченко, А.В. Построение интегрированной базы уязвимостей / А.В. Федорченко, А.А. Чечулин, И.В. Котенко // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57. – № 11. – С. 62–67.
83. Электронная база знаний. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/sberbank/blog/567776/ (дата обращения 20.12.2022).
84. Яндыбаева, Э.Э. Оценка актуальности угроз информационной безопасности в информационной системе электронной торговой площадки / Э.Э. Яндыбаева,

И.В. Машкина // Безопасность информационных технологий. – 2014. – Т. 21. – № 1. – С. 41–44.

85. Aksu, M.U. Automated Generation of Attack Graphs Using NVD / M.U. Aksu, K. Bicakci, M.H. Dilek, A.M. Ozbayoglu, E.I. Tatli // Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. – 2018. – pp. 135–142.
86. All you need to know about text preprocessing for NLP and Machine Learning. [Электронный ресурс]. – Режим доступа: https://www.freecodecamp.org/news/all-you-need-to-know-about-text-preprocessing-for-nlp-and-machine-learning-bc1c5765ff67/ свободный (дата обращения: 20.11.2022).
87. Angelov, D. Top2vec: Distributed representations of topics // arXiv preprint arXiv:2008.09470. – 2020. – doi.org/10.48550/arXiv.2008.09470.
88. Automatic text summarization system using Transformers – Are you tired of reading a long paper? [Электронный ресурс]. – Режим доступа: https://neurondai.medium.com/automatic-text-summarization-system-using-transformers/ (дата обращения 20.12.2022).
89. Bar-Yossef, Z. Local Approximation of Pagerank and Reverse Pagerank / Z. Bar-Yossef, L.-T. Mashiach // Proceedings of the 17th ACM conference on Information and knowledge management, ACM. – 2008. – pp. 279–288. – DOI:10.1145/1458082.1458122.
90. Benjamin, V. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops / V. Benjamin, W. Li, T. Holt, H. Chen // 2015 IEEE international conference on intelligence and security informatics (ISI). – IEEE. – 2015. – pp. 85–90.
91. Berry, M.W. Survey of Text Mining / M.W. Berry // Computing Reviews. – 2004. – T. 45. – № 9. – pp. 548.
92. Blei, D.M. Latent Dirichlet Allocation / D.M. Blei, A.Y. Ng, M.I. Jordan // Journal of Machine Learning Research. – 2003. – Vol. 3. – pp. 993–1022. – DOI:10.1016/B978-0-12-411519-4.00006-9.

93. Bojanowski, P. Enriching Word Vectors with Subword Information / P. Bojanowski, E. Grave, A. Joulin, T. Mikolov// Transactions of the association for computational linguistics. – 2017. – Vol. 5. – pp. 135–146.
94. Carbonell, J. The use of MMR, diversity-based reranking for reordering documents and producing summaries / J. Carbonell, J. Goldstein J. // Proceedings of the 21st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, Melbourne, Australia. – 1998. – pp. 335–336. – DOI:10.1145/290941.291025.
95. Caron, M. Emerging properties in self-supervised vision transformers / M. Caron, H. Touvron, I. Misra, H. Jégou, J. Mairal, P. Bojanowski, A. Joulin // Proceedings of the IEEE/CVF international conference on computer vision. – 2021. – pp. 9650–9660.
96. Che, W. Towards better UD parsing: Deep contextualized word embeddings, ensemble, and treebank concatenation / W. Che, Y. Liu, Y. Wang, B. Zheng, T. Liu// arXiv preprint arXiv:1807.03121. – 2018.
97. Common Attack Pattern Enumeration and Classification [Электронный ресурс]. – Режим доступа: https://capec.mitre.org/ (дата обращения 01.10.2022).
98. Common Vulnerabilities and Exposures [Электронный ресурс]. – Режим доступа: https://cve.mitre.org/ (дата обращения 01.10.2022).
99. Common Vulnerability Scoring System [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/specification-document(дата обращения 04.12.2022).
100. Common Weakness Enumeration [Электронный ресурс]. – Режим доступа: https://cwe.mitre.org/ (дата обращения 01.10.2022).
101. Cyber Threat Intelligence and Monitoring [Электронный ресурс]. – Режим доступа: https://www.acronis.com/en-us/blog/posts/cyber-threat-intelligence/ (дата обращения 04.01.2023).
102. Datta, P. Cyber-Attack Consequence Prediction / P. Datta, N. Lodinger, A.S. Namin, K.S. Jones //arXiv preprint arXiv:2012.00648. – 2020.
103. de Boer, M.H. Text Mining in Cybersecurity: Exploring Threats and Opportunities / M.H. de Boer, B.J. Bakker, E. Boertjes, M. Wilmer, S. Raaijmakers, R. van der Kleij // Multimodal Technologies and Interaction. – 2019. – Vol. 3. – № 3. – pp. 62.

104. Deerwester, S.. Indexing by Latent Semantic Analysis / S. Deerwester, S.T. Dumais, G.W. Furnas, T.K. Landauer, R. Harshman // Journal of the American Society for Information Science. – 1990. – Vol. 41. – Issue 6. – pp. 391–407. – DOI:10.1002/(SICI)1097-4571(199009)41:6%3C391::AIDASI1%3E3.0.CO;2-9.

105. Epishkina, A. A Syllabus on data mining and machine learning with applications to cybersecurity / A. Epishkina, S. Zapechnikov // 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC). – IEEE. – 2016. – pp. 194–199.

106. Gambhir, M. Recent automatic text summarization techniques: a survey / M. Gambhir, V. Gupta //Artificial Intelligence Review. – 2017. – Vol. 47. – pp. 1–66.

107. GPT-2 в картинках (визуализация языковых моделей Трансформера). [Электронный ресурс]. – URL: https://habr.com/ru/post/490842/ (дата обращения 28.06.2022).

108. Grootendorst, M. BERTopic: Neural topic modeling with a class-based TF-IDF procedure / M. Grootendorst // arXiv preprint arXiv:2203.05794. – 2022. – doi.org/10.48550/arXiv.2203.05794.

109. Gupta, A. Automated news summarization using transformers / A. Gupta, D. Chugh, R. Katarya // Sustainable Advanced Computing: Select Proceedings of ICSAC 2021. – Singapore: Springer Singapore, 2022. – pp. 249–259.

110. Gupta, S. Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges / S. Gupta, B.B. Gupta // International Journal of Cloud Applications and Computing (IJCAC). – 2017. – Vol. 7. – № 3. – pp. 1–43.

111. Gusev, I. Dataset for Automatic Summarization of Russian News / I. Gusev // Conference on Artificial Intelligence and Natural Language. – Springer, Cham, 2020. – pp. 122–134. – DOI:10.1007/978-3-030-59082-6_9.

112. Hasan, T. XL-Sum: large-scale multilingual abstractive summarization for 44 languages / T. Hasan, A. Bhattacharjee, I. Md Saiful, K. Samin // Findings of the Association for Computational Linguistics: ACL-IJCNLP 2021. – 2021. – pp. 4693–4703.

113. Hemberg, E. Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting / E. Hemberg, J. Kelly, M. Shlapentokh-Rothman, B. Reinstadler, K. Xu, N. Rutar, U.M. O'Reilly // arXiv preprint arXiv:2010.00533. – 2020.
114. How to get started with Word2Vec – and then how to make it work. [Электронный ресурс]. – Режим доступа: https://translated.turbopages.org/ (дата обращения 26.06.2022).
115. Introduction to Topic Modeling [Электронный ресурс]. – Режим доступа: https://linis.hse.ru/data/2018/10/11/1155920858/TopicModeling.pdf (дата обращения 15.10.2022).
116. James, G. An Introduction to Statistical Learning / G. James, D. Witten, T. Hastie, R. Tibshirani. – New York: Springer, 2013. – Vol. 112. – pp. 18.
117. Kanakogi, K. Tracing CAPEC Attack Patterns from CVE Vulnerability Information using Natural Language Processing Technique / K. Kanakogi, H. Washizaki, Y. Fukazawa, S. Ogata, T. Okubo, T. Kato, N. Yoshioka. – 2021.
118. Kanakogi K. et al. Tracing CVE Vulnerability Information to CAPEC Attack Patterns Using Natural Language Processing Techniques / K. Kanakogi, H. Washizaki, Y. Fukazawa, S. Ogata, T. Okubo, T. Kato, N. Yoshioka //Information. – 2021. – Vol. 12. – № 8. – pp. 298.
119. Khazaei, A. An Automatic Method for CVSS Score Prediction Using Vulnerabilities Description / A. Khazaei, M. Ghasemzadeh, V. Derhami // Journal of Intelligent & Fuzzy Systems. – 2016. – Vol. 30. – № 1. – pp. 89–96.
120. Khazaei, A. Solution Prediction for Vulnerabilities Using Textual Data / A. Khazaei, M. Ghasemzadeh, C. Meinel // International conference applied computing. – 2016.
121. Layton, R. Evaluating Authorship Distance Methods Using the Positive Silhouette Coefficient / R. Layton, P. Watters, R. Dazeley // Natural Language Engineering. – 2013. – Vol. 19. – № 4. – pp. 517–535. – DOI: 10.1017/S1351324912000241.
122. Le, Q. Distributed Representations of Sentences and Documents / Q. Le, T. Mikolov // International Conference on Machine Learning. – PMLR, 2014. – pp. 1188–1196.

123. Lee, D.D. Learning the Parts of Objects by Non-Negative Matrix Factorization / D.D. Lee, H.S. Seung // Nature. – 1999. – Vol. 401. – № 6755. – pp.788–791. – DOI: 10.1038/44565.

124. Lee, Y. Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach / Y. Lee, S. Shin // CIKM Workshops. – 2018.

125. Li, J. The Weighted Word2Vec Paragraph Vectors for Anomaly Detection over HTTP Traffic / J. Li, H. Zhang, Z. Wei // IEEE Access. – 2020. – Vol. 8. – pp. 141787–141798.

126. Luhn, H.P. The automatic creation of literature abstracts / H.P. Luhn // IBM Journal of research and development. – 1958. – Vol. 2. – № 2. – pp. 159–165. – DOI.org/10.1147/rd.22.0159.

127. Maitra, S. Feature Reduction Strategy to Make Better Generalization Models / S. Maitra. [Электронный ресурс]. – Режим доступа: https://medium.com/swlh/feature-selection-techniques-to-make-better-generalization-models-6a19dd6dc9b1свободный (дата обращения: 25.11.2022).

128. Manzhosov, A.V. Method of constructing a visualization of threat model of information security / A.V. Manzhosov, I.P. Bolodurina // 2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT). – IEEE, 2020. – pp. 1–6.

129. McInnes, L. hdbscan: Hierarchical Density Based Clustering / L. McInnes, J. Healy, S. Astels // J. Open Source Softw. – 2017. – Vol. 2. – № 11. – pp. 205. – DOI:10.21105/JOSS.00205.

130. McInnes L. UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction / L. McInnes, J. Healy, J. Melville // arXiv preprint arXiv:1802.03426. – 2018.

131. Mendsaikhan, O. Identification of Cybersecurity Specific Content using the Doc2Vec Language Model / O. Mendsaikhan, H. Hasegawa, Y. Yamaguchi, H. Shimada // 2019 IEEE 43rd annual computer software and applications conference (COMPSAC). – IEEE. – 2019. – Vol. 1. – pp. 396–401.

132. Mihalcea, R. TextRank: Bringing Order into Texts. / R. Mihalcea, P. Tarau // Proceedings of the 2004 Conference on Empirical Methods in Natural Language Processing – 2004. – pp. 404–411.

133. Mikolov, T. Distributed representations of words and phrases and their compositionality / T. Mikolov, I. Sutskever, K. Chen, G.S. Corrado, J. Dean // Advances in neural information processing systems. – 2013. – Vol. 26.

134. Miller, D. Leveraging BERT for Extractive Text Summarization on Lectures / D. Miller // arXiv preprint arXiv:1906.04165. – 2019. – doi.org/10.48550/arXiv.1906.04165.

135. MITRE ATT&CK [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения 01.10.2022).

136. Mittal, S. Cybertwitter: Using Twitter to Generate Alerts for Cybersecurity Threats and Vulnerabilities / S. Mittal, P.K. Das, V. Mulwad, A. Joshi, T. Finin // 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). – IEEE. – 2016. – pp. 860–867.

137. National Vulnerability Database [Электронный ресурс]. – Режим доступа: https://https://nvd.nist.gov/ (дата обращения 01.10.2022).

138. Noel, S. Interactive Visualization and Text Mining for the CAPEC Cyber Attack Catalog / S. Noel // Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics. – 2015. – pp. 1–8.

139. Noel, S. Text Mining for Modeling Cyberattacks / S. Noel // Handbook of statistics. – Elsevier, 2018. – Vol. 38. – pp. 463–515. – DOI: 10.1016 / bs.host.2018.06.001.

140. Nunes, E. Darknet and deepnet mining for proactive cybersecurity threat intelligence / E. Nunes, A. Diab, A. Gunn, E. Marin., V. Mishra, V. Paliath, P. Shakarian // 2016 IEEE Conference on Intelligence and Security Informatics (ISI). – IEEE. – 2016.– pp. 7–12.

141. Open source annotation tool for machine learning practitioners. [Электронный ресурс]. – Режим доступа: https://github.com/doccano/doccano (дата обращения 27.12.2021).

142. Open Web Application Security Project [Электронный ресурс]. – Режим доступа: https://owasp.org/ (дата обращения 01.10.2022).

143. Panchenko, A. Extraction of semantic relations between concepts with KNN algorithms on Wikipedia / A. Panchenko, S. Adeykin, A. Romanov, P. Romanov // Concept Discovery in Unstructured Data Workshop (CDUD) of International Conference On Formal Concept Analysis. – 2012. – pp. 78–88.

144. Pramoditha R. Dimensionality reduction techniques you should know in 2021 /R. Pramoditha // Towards Data Science. [Электронный ресурс]. – Режим доступа: https://towardsdatascience.com/11-dimensionalityreduction-techniques-you-should-know-in-2021-dcb9500d388b. – 11 (дата обращения 01.10.2022).

145. Garc´ıa-Hern´andez, R.A. Text Summarization by Sentence Extraction Using Unsupervised Learning // R.A. Garc´ıa-Hern´andez, R. Montiel, Y. Ledeneva, E. Rend´on, A. Gelbukh, R. Cruz // Proceedings of the 7th Mexican International Conference on Artificial Intelligence: Advances in Artificial Intelligence/ Alexander Gelbukh and Eduardo F. Morales (Eds.) – Springer-Verlag, Berlin, Heidelberg, 2008. – pp. 133–143. – DOI:10.1007/978-3-540-88636-5_12.

146. Radford, A. Language Models are Unsupervised Multitask Learners. Technical Report OpenAi / A. Radford, J. Wu, R. Child, D. Luan, D. Amodei, I. Sutskever. – 2018. – [Электронный ресурс]. – Режим доступа: https://d4mucfpksywv.cloudfront.net/better-language-models/language_models_are_unsupervised_multitask_learners.pdf свободный (дата обращения: 01.09.2020).

147. Ramos, J. Using TF-IDF to Determine Word Relevance in Document Queries / S. Ramos // Proceedings of the first instructional conference on machine learning. – 2003. – Vol. 242. – № 1. – pp. 29–48.

148. Rei, M. Looking for Hyponyms in Vector Space / M. Rei, T. Briscoe // Proceedings of the Eighteenth Conference on Computational Natural Language Learning. – 2014. – pp. 68–77.

149. Repository of pretrained models. [Электронный ресурс]. – Режим доступа: http://docs.deeppavlov.ai/en/master/intro/pretrained_vectors.html. (дата обращения 20.12.2022).

150. Role and applications of NLP in Cybersecurity [Электронный ресурс]. – Режим доступа: https://medium.com/@ursachi/role-and-applications-of-nlp-in-cybersecurity-333d9280c737 (дата обращения 20.12.2022).

151. Schopf, T. PatternRank: Leveraging Pretrained Language Models and Part of Speech for Unsupervised Keyphrase / T. Schopf, S. Klimek, F. Matthes // Proceedings of the 14th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management KDIR. – 2022. – pp. 243–248. – DOI:10.20944/PREPRINTS201908.0073.V1.

152. See, A. Get to the Point: Summarization with Pointer-Generator Networks / A. See, P.J. Liu, C.D. Manning // Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). – 2017. – pp. 1073–1083.

153. Sethi, P. Automatic text summarization of news articles / P. Sethi, S. Sonawane, S. Khanwalker, R.B. Keskar // 2017 International Conference on Big Data, IoT and Data Science (BID). – IEEE. – 2017. – pp. 23–29.

154. Smyth, V. Vulnerability Intelligence / V. Smyth // ITNOW. – 2016. – pp. 26–27. – doi: 10.1093/itnow/bww100.

155. Spanos, G. Assessment of Vulnerability Severity using Text Mining / G. Spanos, L. Angeis, D. Toloudis // Proceedings of the 21st Pan-Hellenic Conference. – Sept.2017, Larissa, Greece. – 2017. – pp. 1–6.

156. Summarization with Transformers: Setting up for Success [Электронный ресурс]. – Режим доступа: https://www.sicara.fr/blog-technique/summarization-with-transformers-setting-up-for-success (дата обращения 20.12.2022).

157. Threat intelligence (данные о киберугрозах) [Электронный ресурс]. – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/threat-intelligence/ (дата обращения 04.01.2023).

158. Jia, W. Feature dimensionality reduction: a review / W. Jia, M. Sun, J. Lian, S. Hou // Complex & Intelligent Systems. – 2022 – Vol. 8. – pp. 2663–2693.

159. Xiao, H. Embedding and Predicting Software Security Entity Relationships: A knowledge graph-based approach / H. Xiao, Z. Xing, X. Li, H. Guo // Neural Information Processing: 26th International Conference, ICONIP 2019. – Sydney, NSW, Australia, December 12-15, 2019. – Proceedings, Part III 26. – Springer International Publishing, 2019. – pp. 50–63.

Приложение А. Акты о внедрении научных результатов

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
"УРАЛТЕХСИСТЕМЫ"

Юридический адрес: 450056 Республика Башкортостан, г.Уфа, д. Мокроусово, ул. Мокроусовская, д. 2/2, пом. 31
Банковские реквизиты: Поволжский филиал АО "РАЙФФАЙЗЕНБАНК", р/с № 40702810220000002829,
к/с № 30101810000000000847, БИК 042202847, ИНН 0278942325, КПП 027401001,
Почтовый адрес: 450056 Республика Башкортостан, г.Уфа, д. Мокроусово, ул. Мокроусовская, д. 2/2, пом. 31
E-mail: info@uraltsystem.ru, тел/факс (347) 2865210 / 2865220

УТВЕРЖДАЮ
Директор
ООО "УРАЛТЕХСИСТЕМЫ"
_____ Р.Ф. Хамзиханов
«13» мая 2023г.

АКТ

об внедрении в ООО "УРАЛТЕХСИСТЕМЫ" результатов диссертационной работы Кучкаровой Наили Вакилевны «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов»

Комиссия в составе:

Главный инженер	Трапезников А.Ф.
Начальник отдела автоматизации	Муллатагиров М.Р.
Зам. директора по безопасности	Хатильянов А.Р.

составили настоящий акт о том, что следующие научно-технические результаты диссертационной работы Кучкаровой Н.В. «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов», представленной на соискание ученой степени кандидата технических наук:

– алгоритм построения графовой модели сценария реализации угроз ИБ с использованием технологии трансформеров;

– архитектура и состав подсистем ПО ИСППР

были использованы на предприятии с целью решения задач по обеспечению информационной безопасности, в частности, выявлению уязвимостей ПО и актуальных угроз информационной безопасности, реализация которых может привести к нарушению штатной работы объектов АСУ ТП.

Испытания предложенных в диссертации алгоритма построения графовой модели сценария реализации угроз ИБ и ИСППР показали следующие результаты: упрощен поиск и сопоставление актуальных угроз и уязвимостей, сокращены временные затраты в 3-4 раза (с более 4 часов до 1 часа), повышена достоверность (на 20-40%, согласованность экспертной оценки и ИСППР составила F1=0,59) оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ. Данные результаты позволяют снизить трудозатраты и улучшить качество работы специалиста по защите

информации в ходе обеспечения информационной безопасности объектов АСУ ТП соответствии с нормативными требованиями к защищенности.

Главный инженер	_____	Трапезников А.Ф.
Начальник отдела автоматизации	_____	Муллатагиров М.Р.
Зам. директора по безопасности	_____	Хатипьянов А.Р.

«УТВЕРЖДАЮ»

Проректор по учебной работе

ФГБОУ ВО «Уфимский университет науки и технологий»

_____ Ю.В. Рахманова

«26» _____ 2023г.

АКТ

о внедрении результатов диссертационной работы
Кучкаровой Наили Вакилевны
«Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов», представленной на соискание ученой степени кандидата технических наук

Комиссия в составе: заведующий кафедрой «Вычислительная техника и защита информации» (ВТиЗИ), д.ф.-м.н., профессор Картак В.М.; д.т.н., профессор кафедры ВТиЗИ Фрид А.И.; начальник Учебного управления, к.э.н., доцент, Гумерова З.Ж. составили настоящий акт о том, что следующие результаты диссертационной работы Кучкаровой Н.В.

– метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов

были использованы в образовательном процессе ФГБОУ ВО УУНиТ для проведения дисциплин «Безопасность критически важных информационных систем», «Искусственный интеллект в системах защиты информации», «Системы защищенного электронного документооборота» для обучающихся по направлениям 10.04.01 «Информационная безопасность», 09.04.01 «Информатика и вычислительная техника», профиль «Безопасность и защита информации»

Теоретические и экспериментальные результаты предложенного в диссертации метода и алгоритма автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов используются для выполнения практических, лабораторных и выпускных квалификационных работ при решении задач, связанных с оценкой и анализом уязвимостей и угроз объектов АСУ ТП критической информационной инфраструктуры

Заведующий кафедрой ВТиЗИ,
д.ф.-м.н., профессор _____ В.М. Картак

Д.т.н., профессор кафедры ВТиЗИ _____ А.И. Фрид

Начальник Учебного управления,
к.э.н., доцент _____ З.Ж. Гумерова

«УТВЕРЖДАЮ»

Директор

ЗАО "Республиканский центр защиты информации"

_____ С.Н. Зарипов

«8» июня 2023г.

АКТ

о внедрении в ЗАО "Республиканский центр защиты информации" результатов диссертационной работы Кучкаровой Наили Вакилевны на тему «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов»

Комиссия в составе:

главный инженер ЗАО "Республиканский центр защиты информации (РЦЗИ)" к.т.н. Бакиров А.А.; заместитель директора ЗАО РЦЗИ Хисамутдинов Т.З.; ведущий специалист ЗАО РЦЗИ Федотов Д.Б. составили настоящий акт о том, что следующие научно-технические результаты диссертационной работы Кучкаровой Н.В. «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов», представленной на соискание ученой степени кандидата технических наук:

– алгоритм автоматической классификации и суммаризации текстов из открытых источников в области информационной безопасности

были использованы на предприятии с целью решения задач по обеспечению информационной безопасности объектов критической информационной инфраструктуры (КИИ).

В ходе категорирования объектов КИИ предложенные решения используются для структурирования текстовых описаний бизнес-процессов, технологических

процессов, производственных цепочек и совокупности организационно-распорядительной документации для оценок количественных значений показателей критериев значимости.

Главный инженер ЗАО "РЦЗИ"
к.т.н. Бакиров А.А. _____ /Бакиров А.А./

Заместитель директора ЗАО "РЦЗИ"
Хисамутдинов Т.З. _____ /Хисамутдинов Т.З./

Ведущий специалист ЗАО "РЦЗИ"
Федотов Д.Б. _____ /Федотов Д.Б./

Приложение Б. Методика оценки актуальных угроз ИБ объектов АСУ ТП КИИ

Методика устанавливает единый подход к оценке уязвимостей и актуальных угроз ИБ объектов КИИ.

Методика разработана в соответствии со следующими нормативно-правовыми документами [1,2,6,7,11,12,14].

Для реализации этапов Методики необходимо использовать банк данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru), так же возможно использование иных открытых баз данных, содержащих информацию о векторах и шаблонах атак.

Требования к результату.

Оценка актуальных угроз ИБ объекта КИИ должна включать в себя сценарий реализации угроз, т.е. сопоставленные на основе семантического сходства описаний следующие элементы:

1) уязвимости исследуемого объекта АСУ ТП КИИ;

2) тактики и техники, при помощи которых могут быть реализованы соответствующие уязвимости;

3) актуальные угрозы.

Каждый из вышеперечисленных элементов должен содержать полное описание, содержащиеся в БДУ ФСТЭК для угроз: описание угрозы, источники угрозы, объект воздействия, последствия реализации угрозы; для уязвимостей: описание уязвимости, вендор, наименование (версия, тип) ПО, операционные системы и аппаратные платформы, тип ошибки (идентификатор CWE и других систем), базовый вектор уязвимости, уровень опасности уязвимости и др.

Оценка угроз безопасности информации предполагает выполнение следующих этапов.

1. Анализ документации систем и сетей и иных документов.

2. Определение негативных последствий, которые могут наступить от реализации угроз безопасности информации (БИ).

3. Проведение инвентаризации АСУ ТП объекта КИИ с целью определения возможных объектов воздействия угроз, несанкционированный доступ к которым может привести к негативным последствиям.

Для систематизации подхода по определению перечня компонентов (инвентаризации) исследуемого объекта КИИ целесообразно воспользоваться рекомендациями, изложенными в ГОСТ Р 62443-2-1. В целях автоматизации процесса инвентаризации возможно использование специализированного программного продукта для комплексной защиты промышленных объектов Kaspersky Industrial CyberSecurity for Networks, либо сканерами безопасности (RedCheck, XSpider, ScanOVAL и др.).

4. Определение источники угроз безопасности информации и оценить возможности нарушителей по реализации угроз БИ.

Целью данного этапа является определение актуальных нарушителей

а) типы нарушителей:

б) виды нарушителей:

г) определить уровни возможностей нарушителей (Н1, Н2, Н3, Н4)

д) определить возможные цели реализации угроз.

5. Оценка способов реализации (возникновения) угроз БИ КИИ.

На основе анализа исходных данных и возможностей нарушителей необходимо определить основные способы реализации угроз БИ объекта КИИ. Одним из способов реализации угроз БИ объекта АСУ может быть использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

6. Определение сценариев реализации угроз безопасности информации АСУ ТП объекта КИИ.

Определение сценариев реализации угроз БИ предполагает установление последовательности возможных тактик и соответствующих им техник, применение

которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации

7. Определение актуальности угроз безопасности информации АСУ ТП объекта КИИ.

На основе анализа исходных данных определяются возможные для объекта КИИ угрозы БИ, к которым относятся осуществляемые нарушителем воздействия на информационные ресурсы и компоненты АСУ ТП (объекты воздействия), в результате которых возможно нарушение БИ и (или) нарушение или прекращение функционирования объекта КИИ (останов технологического процесса, аварии и др.).

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для объекта КИИ и включается в модель угроз безопасности объекта КИИ для обоснования выбора организационных и технических мер по обеспечению безопасности, а также выбора средств защиты информации.

Для реализации п.п. 1-6 предлагаемой методики целесообразно воспользоваться алгоритмом оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объектов КИИ, алгоритмом построения графа соответствия множеств угроз, уязвимостей, тактик и техник их эксплуатации, алгоритмом построения графовой модели фрагмента сценария реализации угроз на основе алгоритма векторизации, а также ИСППР предложенными в Главах 3 и 4 диссертации. Для работы ИСППР необходимо:

1) с помощью клиент-серверного сканера (CVE-manager) обеспечить сбор данных об уязвимостях программного обеспечения рабочих станций и серверов объекта КИИ;

2) обеспечить передачу собранных данных в локальную БД ИСППР;

3) загрузить текстовые описания угроз, уязвимостей, тактик и техник из внешнего хранилища БДУ ФСТЭК в локальную СУБД ИСППР в требуемом формате.

После загрузки данных ИСППР выполняет следующие преобразования данных:

– предобработку текстовых описаний угроз БИ, уязвимостей ПО и тактик (техник) путем извлечения данных из локального хранилища и выполнения ряда преобразований текстовых описаний (фильтрацию и нормализацию и т.д.);

– векторизацию текстовых описаний угроз, уязвимостей, тактик и техник;

– оценку семантической близости текстовых описаний, используя формализованные векторы признаков каждой сущности для попарной оценки их близости на основе косинус-метрики;

– приоритизацию угроз БИ на основе меры семантической близости;

– подбор семантически близких тактик и техник к выделенным угрозам и уязвимостям;

– построение сценариев реализации актуальных угроз.

В завершении работы программы ИСППР выведет информацию в табличном виде, содержащую идентификационные номера выявленных уязвимостей, сопоставленных им угроз и тактики/техники с использованием которых угрозы могут быть реализованы. Далее эксперту необходимо:

1) с помощью консоли доступа необходимо выполнить:

– оценку корректности сопоставления множества угроз БИ и уязвимостей ПО;

– оценку корректности построенных сценариев реализации угроз;

– произвести корректировку результатов, в случае необходимости;

2) сделать выводы о наличии на исследуемом объекте КИИ актуальных угроз.

Приложение В. Фрагмент модели угроз КИИ

Этап	Определяемые параметры	Значения параметров
Определение негативных последствий	Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации	– причинение вреда жизни и здоровью граждан; – нарушение штатного режима функционирования КИИ: – предпосылка к нарушению технологического процесса, вызванная искажением (изменением) циркулируемой в КИИ защищаемой информации; – возникновение аварийных ситуаций на объекте из-за выдачи неверных команд управления или несанкционированного изменения значений параметров и границ блокировок; – нарушение технологического процесса (возникновение аварийных ситуаций на объекте) из-за блокировки работы контроллера и несанкционированного выключения (уничтожения) программных или аппаратных средств; – Отсутствие возможности контроля и управления ходом технологического процесса вследствие блокировки выполнения функций АРМ операторов, серверов, инженерной станции, коммуникационного сервера – неспособность выполнять договорные обязательства; – возникновение ущерба субъекту КИИ; – вредные воздействия на окружающую среду;
Определение объектов воздействия	Объекты воздействия	– Программируемый логический контроллер (ПЛК) для управления насосными станциями – SCADA-server; – БД сервер; – АРМ КИП и А; – АРМ системного инженера; – Север ввода/вывода

Этап		Определяемые параметры	Значения параметров
		Виды воздействия	Несанкционированная модификация (изменение) логики работы или установок ПЛК, которая приводит к включению (или не отключению) насосной станции при закрытой аварийной задвижке в нефтепроводе Несанкционированная модификация (изменение) данных SCADA-системы, которое может привести к выводу из строя (отключению) аварийной сигнализации или нарушению логики работы ПЛК; Несанкционированная модификация (изменение) данных БД сервера, которое может привести к нарушению целостности технологических данных объекта КИИ; Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК;
Оценка возможности реализации угроз и их актуальности	Определение цели реализации угроз безопасности информации нарушителями	Виды нарушителя	– Авторизованные пользователи систем и сетей; – Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем; – Системные администраторы и администраторы безопасности; – Террористические, экстремистские группировки; – Разработчики программных, программно-аппаратных средств; – Специальные службы иностранных государств.
		Категории нарушителя	Внутренний, внешний
		Возможные цели реализации угроз безопасности информации	– любопытство или желание самореализации; – непреднамеренные, неосторожные или неквалифицированные действия; – совершение террористических актов, угроза жизни граждан. – нанесение ущерба отдельным сферам деятельности или секторам экономики государства; – дестабилизация общества;
	Определение уровня возможностей наруши-	Уровень возможностей нарушителей	– Нарушитель, обладающий базовыми возможностями; – Нарушитель, обладающий базовыми повышенными возможностями; – Нарушитель, обладающий средними возможностями; – Нарушитель, обладающий высокими возможностями.

Этап		Определяемые параметры	Значения параметров
	телей по реализации угроз безопасности информации	Возможности нарушителей по реализации угроз безопасности информации	– нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов; – нарушитель, обладающий базовыми повышенными возможностями имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами, однако хорошо владеют этими средствами и инструментами, понимают, как они работают и могут вносить изменения в их функционирование для повышения эффективности реализации угроз; – нарушитель, обладающий средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей; – имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.
	Определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности	Доступные интерфейсы	– локальная вычислительная сеть ; – Веб-интерфейс системы – интерфейсы удаленного доступа; – интерфейсы для использования съемных машинных носителей информации и периферийного оборудования; – интерфейсы для установки, настройки, испытаний, пусконаладочных обеспечения функционирования компонентов систем и сетей.