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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2023

Работа выполнена в ФГБОУ ВО «Уфимский университет науки и технологий» на кафедре вычислительной техники и защиты информации

Научный руководитель: доктор технических наук, профессор
Васильев Владимир Иванович

Официальные оппоненты:

Болодурина Ирина Павловна, доктор технических наук, профессор, ФГБОУ ВО «Оренбургский государственный университет», заведующий кафедрой прикладной математики
Макарян Александр Самвелович, кандидат технических наук, доцент, ФГБОУ ВО "Кубанский государственный технологический университет", заведующий кафедрой кибербезопасности и защиты информации

Ведущая организация: ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь.

Защита диссертации состоится 22.09.2023 года в $10^{\underline{00}}$ часов на заседании диссертационного совета 24.2.479.07 на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу: 450008, г. Уфа, ул. К. Маркса, д. 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский университет науки и технологий» и на сайте https://uust.ru/.

Автореферат разослан «____»_____ 2023 года.

Ученый секретарь
диссертационного совета
д-р техн. наук, доцент Виноградова Ирина Леонидовна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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 государственные и медицинские учреждения, промышленные предприятия. Предприятия упомянутых отраслей, как правило, относятся к субъектам критической информационной инфраструктуры (КИИ), являющихся собственниками различных классов объектов КИИ, большую группу которых составляют промышленные автоматизированные системы управления технологическими процессами (АСУ ТП). Обеспечение безопасности объектов КИИ является, в соответствии с Доктриной информационной безопасности Российской Федерации, одним из приоритетных направлений в области информационной безопасности (ИБ). Требования к обеспечению ИБ объектов КИИ закреплены в ряде нормативно-правовых документов, принятых в России в последние годы, таких как: Федеральный закон «О безопасности критической информационной инфраструктуры» №187-ФЗ (2017г.), Приказы ФСТЭК России №№ 31, 235 и 239 (2017г.), «Методика оценки угроз безопасности информации» ФСТЭК России от 5 февраля 2021 г. Согласно данной Методике, одним из ключевых этапов оценки угроз безопасности информации (БИ) для объектов КИИ является оценка возможности реализации угроз БИ и определение их актуальности. Реализация данного этапа связана с необходимостью определения источника угроз, т.е. актуальных нарушителей, а также построения сценариев атак. Определение сценариев атак предусматривает, в свою очередь, установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей посредством эксплуатации уязвимостей программного обеспечения (ПО).

Вместе с тем, на практике при решении данной задачи специалисты по ИБ сталкиваются с необходимостью обращения к большим массивам текстовых описаний компонентов (угроз БИ, уязвимостей ПО, 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 БИ, свыше 36 500 уязвимостей ПО, 10 тактик и от 7 до 29 соответствующих им техник. Работа с указанными БД предполагает поиск и анализ угроз БИ и уязвимостей ПО 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 БИ, уязвимостей ПО, тактик и техник их эксплуатации. Однако, существующие на данный момент отдельные разработки в области автоматизации процесса оценки угроз БИ не учитывают в полной мере требований Методики относительно определения сценариев атак. В связи с этим, тема диссертационной работы, посвященная вопросам автоматизации оценки и приоритизации актуальных угроз БИ, уязвимостей ПО, 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., Жука Р.В, Зегжды П.Д., Катасёва А.С., Котенко И.В., Лаврентьева А.М., Макаряна А.С., Машкиной И.В., Остапенко А.Г., Петренко В.И., Рагозина А.И., Рябова Д.М., Селифанова В.В., Сычугова А.А., Тебуевой 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, оценке степени опасности этих уязвимостей, необходимости 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 и анализа актуальных угроз безопасности информации и уязвимостей ПО объектов КИИ.

Целью диссертационной 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.); Мавлютовские чтения/ Всероссийская молодежная научная конференция (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.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность исследуемой темы, определены объект и предмет исследования, цель и задачи исследования, научная новизна, теоретическая и практическая значимость полученных результатов, сформулированы основные положения, выносимые на защиту.

В первой главе диссертационной работы проводится анализ современного состояния в области обеспечения ИБ объектов КИИ, дается краткий обзор открытых баз данных (NVD, CVE, CAPEC, БДУ ФСТЭК России и др.), содержащих текстовые описания угроз ИБ, уязвимостей ПО, тактик (техник) их реализации.

Проведен анализ основных требований и этапов Методики оценки угроз БИ ФСТЭК России. Показано, что в связи с возрастающим объемом слабоструктурированных текстовых описаний угроз БИ и уязвимостей ПО, содержащихся в различных БД, для их обработки и анализа целесообразно использование современных технологий интеллектуального анализа текстов (Text Mining).

Проводится сравнительный анализ известных методов и алгоритмов обработки текстов на естественном языке (ЕЯ). В качестве базовых алгоритмов для решения этой задачи выделены: Word2Vec и Doc2Vec – алгоритмы векторного вложения (Word Embedding), позволяющие получить векторное представление слов и предложений (абзацев, документов); TF-IDF – статистическая мера, используемая для оценки важности слова в контексте документа, используется при расчёте меры близости документов при их классификации (кластеризации); BERT – нейросетевая языковая модель, основанная на архитектуре трансформера, предназначенная для предобучения и обработки больших корпусов текстов на ЕЯ. Рассматривается практика использования данных технологий и алгоритмов в различных прикладных областях, в том числе в области ИБ.

Проведенный анализ показал перспективность использования технологий интеллектуального анализа текстов (Text Mining) для решения сформулированных в работе задач исследования.

Во второй главе исследуется возможность применения технологий Text Mining при решении задач автоматической классификации (тематического моделирования) и суммаризации текстов из открытых источников в области ИБ. Описываются общие подходы к решению задач автоматической классификации и суммаризации текстов. Приведены результаты экспериментов по автоматической классификации слабоструктурированой информации на примере корпуса текстов, сформированного из 438 полнотекстовых научных статей, опубликованных в журнале «Вопросы кибербезопасности» за 2013- 2022 гг. В процессе этих экспериментов исследовались различные подходы к классификации (кластеризации) указанных документов: с предварительным понижением размерности признакового пространства и использованием метода ближайших соседей (K-Means); с помощью скрытого распределения Дирихле (LDA) и неотрицательной матричной факторизации (NMF); на основе моделей векторных вложений (Text Rank, SBert). Были выполнены также эксперименты по автоматической суммаризации текстов для формирования кратких рефератов, раскрывающих смысловое содержание документа.

Использование данных технологий позволяет повысить качество анализа текстовых документов в области ИБ и одновременно снизить когнитивную нагрузку на эксперта.

В третьей главе приведена функциональная модель процесса оценки и анализа актуальных угроз БИ в соответствии с Методикой ФСТЭК. Показано, что основные сложности при работе с данной Методикой связаны с определением сценариев реализации угроз БИ, в силу необходимости использования при этом разнородной слабоструктурированной информации, включающей перечни актуальных уязвимостей ПО, типы доступа к информационным активам, типы нарушителей и т.п., а также ввиду отсутствия эффективных средств автоматизации, позволяющих формализовать и упростить процесс сопоставления имеющихся исходных данных (актуальных уязвимостей ПО, тактик (техник) их реализации, возможных угроз БИ).

Разработан метод и алгоритм решения задачи автоматизации оценки и приоритизации актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием технологий интеллектуального анализа текстов (Text Mining). Проанализированы ключевые этапы обработки текстовых описаний с применением указанных технологий, рассмотрены особенности использования алгоритмов Word2Vec, Doc2Vec, BERT в задачах обработки текстовых описаний угроз БИ и уязвимостей ПО.

Посредством агрегации данных, содержащихся в БДУ ФСТЭК России, сформирован корпус русскоязычных текстов - описаний угроз БИ, уязвимостей ПО, тактик и техник их реализации. Для анализа данного корпуса разработан алгоритм векторного представления текстовых описаний угроз БИ, уязвимостей ПО, тактик (техник) и оценки семантической близости (сходства) этих описаний. В ходе выполнения предложенного алгоритма загружаются данные из БДУ ФСТЭК, затем они нормализуются, производится экспертная разметка для выделения семантических особенностей текста, строится модель TF-IDF, позволяющая оценить важность каждого слова в корпусе, далее происходит векторизация текстовых документов с использованием моделей Word2Vec, Doc2Vec, BERT с учетом частоты встречаемости (TF-IDF) слов в корпусе. Для выявления устойчивой структуры текстовых описаний в пространстве признаков векторных вложений на основе оценки их семантической близости разработан алгоритм кластеризации текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник. Приведены результаты кластеризации текстовых описаний с предварительно заданными центрами кластеров, полученных из векторного представления описаний информационных ресурсов и компонентов промышленных систем и сетей объектов КИИ (22 объекта воздействия согласно Методике ФСТЭК) методом K-Means в признаковом пространстве. Визуализация результатов кластеризации с использованием алгоритма снижения размерности признакового пространства t-SNE (t-distributed stochastic neighbor embedding) свидетельствует о наличии структуры компактных групп текстовых описаний (рисунок 1).

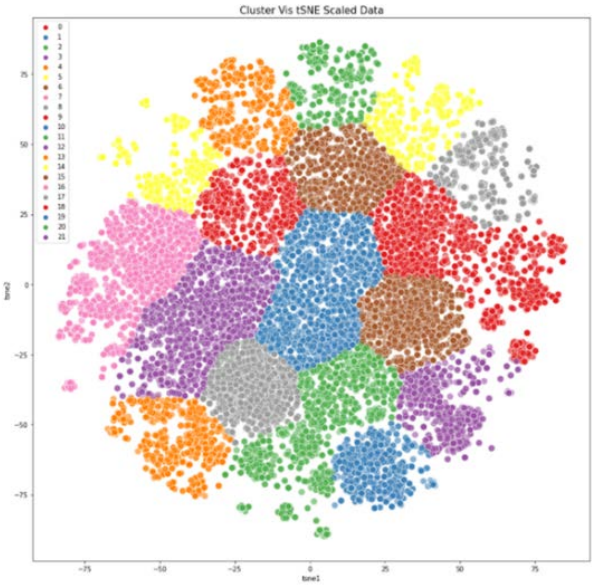

Рисунок 1 – t-SNE визуализация кластерной структуры с предварительно заданными центрами

Разработан алгоритм оценки и приоритизации актуальных угроз БИ и уязвимостей ПО (рисунок 2) с использованием технологий Text Mining. Для апробации предложенного метода и алгоритма анализировались текстовые данные из БДУ ФСТЭК. Из общего объема текстовых описаний в 740634 слова был сформирован словарь, содержащий 12884 слов. После процедуры предобработки и нормализации данных была построена модель векторных вложений Doc2Vec с помощью фреймворка Gensim.

В процессе тестирования работы предложенного алгоритма были рассмотрены несколько уязвимостей ПО, выявленных хостовым сканером уязвимостей, в частности уязвимость BDU:2015-00285 «Уязвимость программного обеспечения Flash Player, позволяющая удаленному злоумышленнику нарушить конфиденциальность, целостность и доступность защищаемой информации». Данной уязвимости эксперт в ручном режиме сопоставил угрозу УБИ.192. Используя текстовое описание выбранной уязвимости, с помощью разработанного алгоритма был проведен выбор семантически близких по описанию угроз БИ из БДУ ФСТЭК.

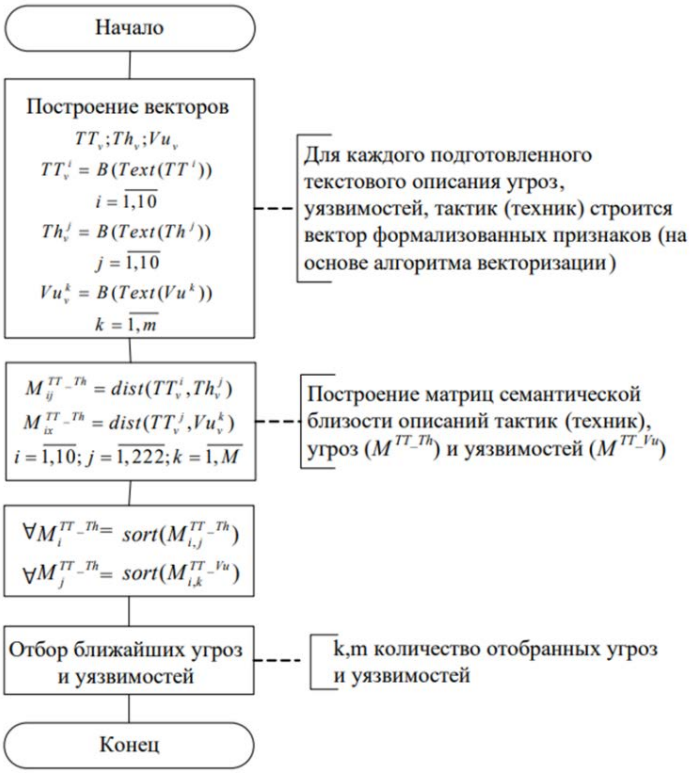

Рисунок 2 –Блок-схема алгоритма приоритизации множества угроз БИ для выявленных уязвимостей ПО, на основе сопоставления текстовых описаний угроз БИ (Th), уязвимостей (Vu), техник (тактик) (TT)

На рисунке 3 показаны результаты подбора 10 релевантных угроз БИ, ранжированных в

порядке убывания метрики семантической близости. Как видно из рисунка 3, угроза УБИ.192 попадает в данный перечень, что совпадает с результатом предварительного экспертного оценивания, но разработанный алгоритм предлагает расширенный перечень релевантных угроз БИ, которые также должны быть приняты во внимание.

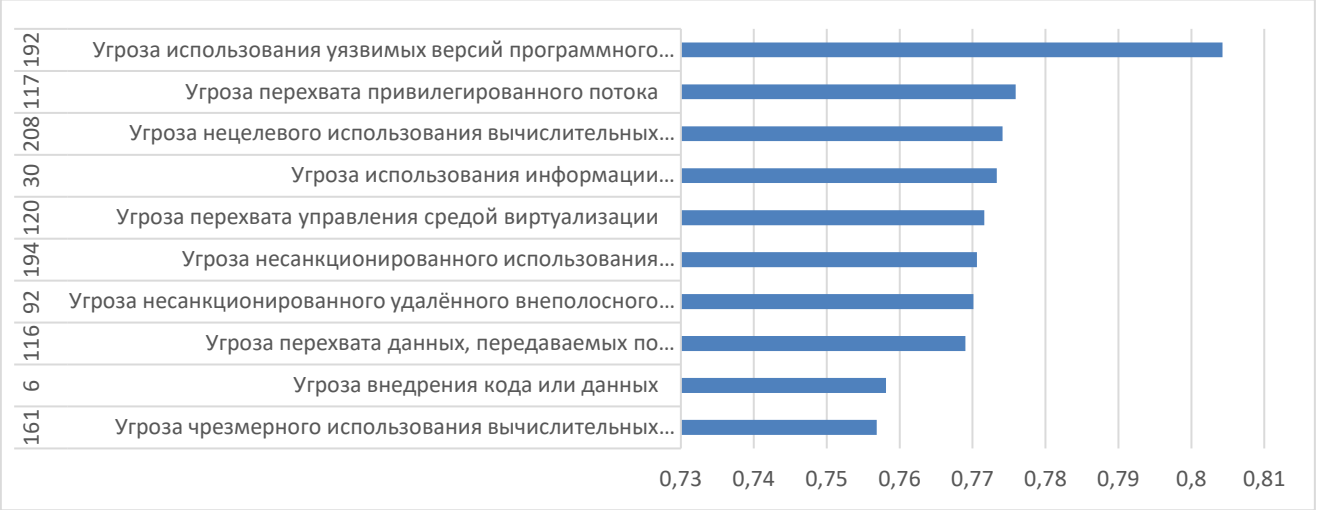

Рисунок 3 – Релевантные угрозы БИ, отсортированные в порядке убывания метрики семантической близости (score) к выявленной уязвимости BDU:2015-00285

Как показывают экспертные оценки, финальная стадия анализа позволяет значительно упростить сопоставление актуальных угроз БИ и уязвимостей ПО для конкретных версий ПО и сократить количество просматриваемых экспертом угроз БИ для каждой отдельной уязвимости ПО более чем в 10-15 раз.

Результаты проведенных исследований показывают возможность построения семантической графовой модели сценария реализации угроз БИ. Общая схема графа соответствия множеств угроз БИ, уязвимостей ПО, тактики техник их эксплуатации показана на рисунке 4.

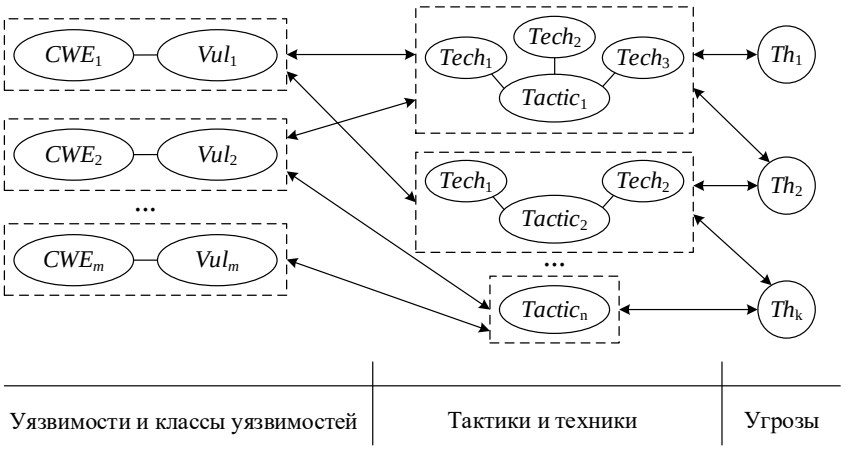

Рисунок 4 – Граф соответствия множеств угроз БИ, уязвимостей ПО, тактик и техник

Блок-схема алгоритма построения графовой модели построения фрагмента сценария реализации угроз БИ (графа соответствия) представлена на рисунке 5. На вход алгоритма подаются текстовые данные из подготовленного корпуса текстов, далее происходит выбор модели векторного представления текстов, их предобработка и векторизация. Затем, в несколько этапов, строится указанный граф соответствия, т.е. происходит соотнесение

множеств выявленных уязвимостей и слабостей ПО, затем уязвимостей – слабостей ПО с тактиками и техниками и, в заключение, тактики и техники соотносятся с угрозами БИ на основе оценки семантической близости их описаний. На выходе алгоритма эксперты проводят оценку качества полученной графовой модели.

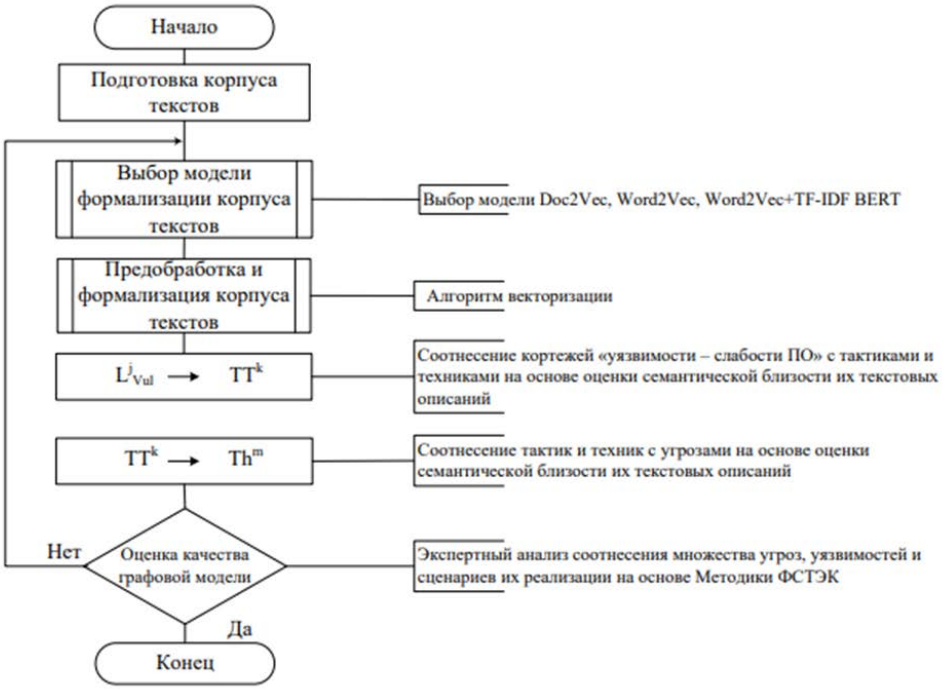

Рисунок 5 – Блок-схема алгоритма построения графа соответствия множеств угроз БИ, уязвимостей ПО, тактик и техник их эксплуатации

В основе алгоритма оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО лежит построение матриц оценок попарной семантической близости элементов двух множеств: M^{TT_Vu} тактик (техник) (TT) и уязвимостей (Vul), M^{TT_Th} тактик (техник) (TT) и угроз (Th). Далее матрицы сортируются построчно в порядке убывания метрики семантической близости текстовых описаний элементов множеств, с обрезкой по количеству элементов в строке: для угроз БИ остается $p = 10$ наиболее схожих, для уязвимостей ПО $q = 25$ наиболее схожих с текстовым описанием тактик (техник). В качестве меры оценки семантической близости используется косинусная мера, позволяющая вычислить расстояние между двумя векторами в семантическом пространстве признаков

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

где, A *и* B – векторные представления текстовых описаний сопоставляемых пар элементов: уязвимостей ПО, тактик, техник и угроз БИ.

Общий порядок моделирования и оценки актуальности угроз БИ на основе перечня актуальных уязвимостей ПО определен в Методике ФСТЭК. В соответствии с данной Методикой, предполагаются стратегический и тактический уровни построения модели угроз БИ. Стратегический уровень включает в себя определение типа нарушителя, цели воздействия, негативные последствия, а тактический – применяемые тактики и техники эксплуатации уязвимостей ПО (т.е. возможные сценарии реализации угроз БИ). Семантическая модель сценария реализации угроз БИ (рисунок 6) представляет собой граф

$$G=\{V, E, D\}, \quad (2)$$

где V – множество вершин графа – текстовые описания угроз БИ, уязвимостей ПО, тактик и техник;

$$V = V_1 \cup V_2 \cup V_3 \cup V_4 \quad (3)$$

V_1 – множество вершин, соответствующих идентификаторам выявленных уязвимостей ПО;
V_2 – множество вершин, соответствующих техникам реализации атаки, которые описывают инструменты, технологии, утилиты и т.д., используемые нарушителем;
V_3 – множество вершин, соответствующих тактикам, т.е. действиям на разных этапах реализации атаки;
V_4 – множество вершин, соответствующих актуальным угрозам БИ;
E – множество взвешенных ориентированных ребер, устанавливающих отношения между текстовыми описаниями:

$$E \subseteq V \times V, \ \ e(v_i, v_j), \ \ v_i, v_j \in V \quad (4)$$

$D(e)$ – функция, определяющая степень семантической близости для концептов v_i , v_j ∈ ;
w= dist (v_i, v_j) – весовой коэффициент, характеризующий метрику семантической близости текстовых описаний смежных вершин.

Семантическая модель фрагмента сценариев реализации угроз G объектов АСУ ТП строится на основе перекрестных ссылок в гипертекстовых документах (текстовых описаний угроз БИ, уязвимостей ПО и тактик (техник) их реализации – V графа). Ребра модели нагружаются весовыми коэффициентами $w^{i,j}$, характеризующими значения метрики семантической близости текстовых описаний смежных вершин, полученные с помощью методов машинного обучения для векторного представления текстов документов (Word2Vec, Doc2Vec и технологии трансформера).

Алгоритм построения графовой модели фрагмента сценария реализации угроз с использованием Word2Vec, Doc2Vec и технологии трансформера представлен на рисунке 7. Построение графовой модели начинается с подготовки текстовых описаний угроз, уязвимостей, тактик и техник. Затем на основе ссылочных описаний устанавливаются связи между вершинами V_1, V_2, V_3 , V_4 . Далее строится матрица семантической близости описаний угроз БИ, уязвимостей ПО, тактик и техник, несуществующие связи прореживаются на основе порогового значения. В заключение производится оценка и приоритизация рассмотренных множеств угроз БИ и уязвимостей ПО.

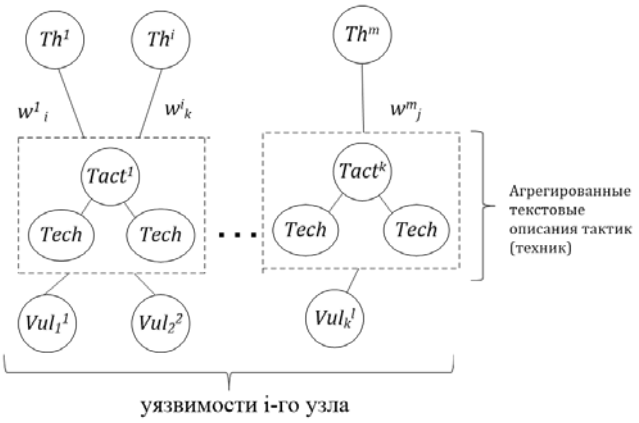

Рисунок 6 – Графовая модель фрагмента сценария реализации угроз

Далее, при построении графовой модели, описывающей отношения множеств угроз БИ, уязвимостей ПО, тактик и техник их эксплуатации, используется технология трансформеров, в частности нейросетевая языковая модель BERT (Bidirectional Encoder Representations from Transformers), основанная на объединении 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.

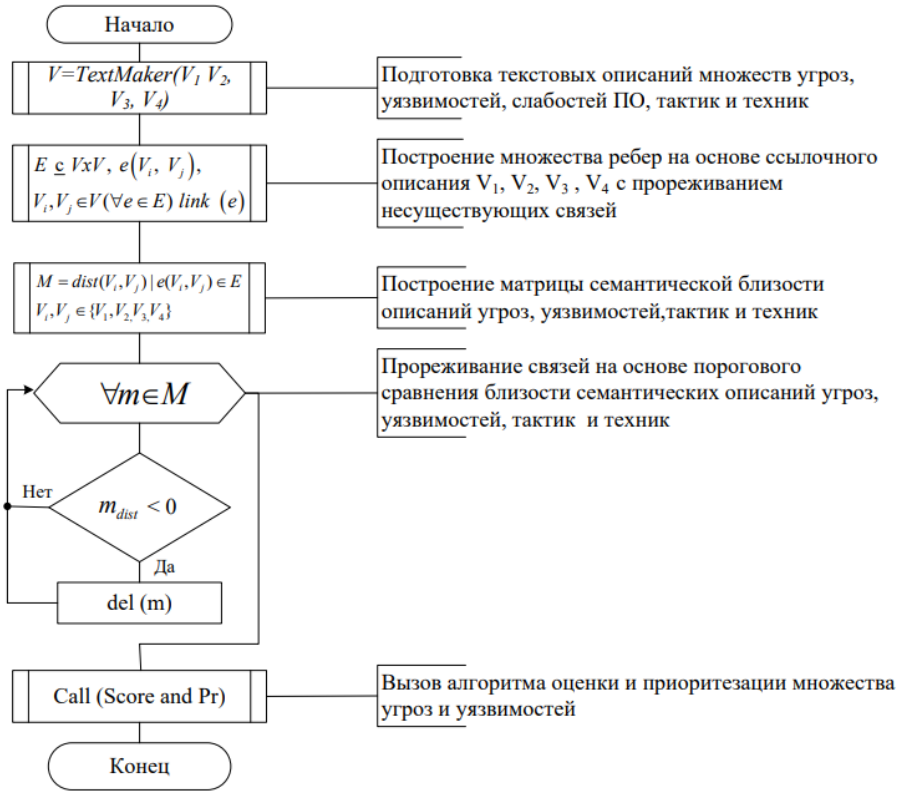

Рисунок 7 – Блок-схема алгоритма построения графовой модели фрагмента сценария реализации угроз БИ

Дальнейший анализ (сопоставление) формализованных представлений текстовых описаний угроз БИ, уязвимостей ПО, техник (тактик) основан на применении методов кластеризации многомерных данных. Визуализация полученной графовой модели показывает, что наилучший результат демонстрирует предобученная модель-трансформер BERT – Large Model. Модель ruBERT-tiny (дистиллированная модель-трансформер многозадачного обучения) также демонстрирует заметное распределение на компактные группы объектов в семантическом векторном пространстве в соответствии с семантической близостью их описаний. Результаты проведения эксперимента с применением модели BERT- Large Model для заданной уязвимости BDU:2021-02033 показывают высокую степень совпадения экспертных оценок и предложенных сценариев реализации угроз БИ.

В четвертой главе представлено описание исследовательского прототипа ИСППР, предназначенной для автоматизации процесса оценки и анализа актуальных угроз БИ объектов КИИ.

Система включает в себя следующие основные компоненты (программные модули):

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

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

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

Схема структурно-функциональной организации подсистемы анализа актуальных угроз БИ и уязвимостей ПО представлена на рисунке 8.

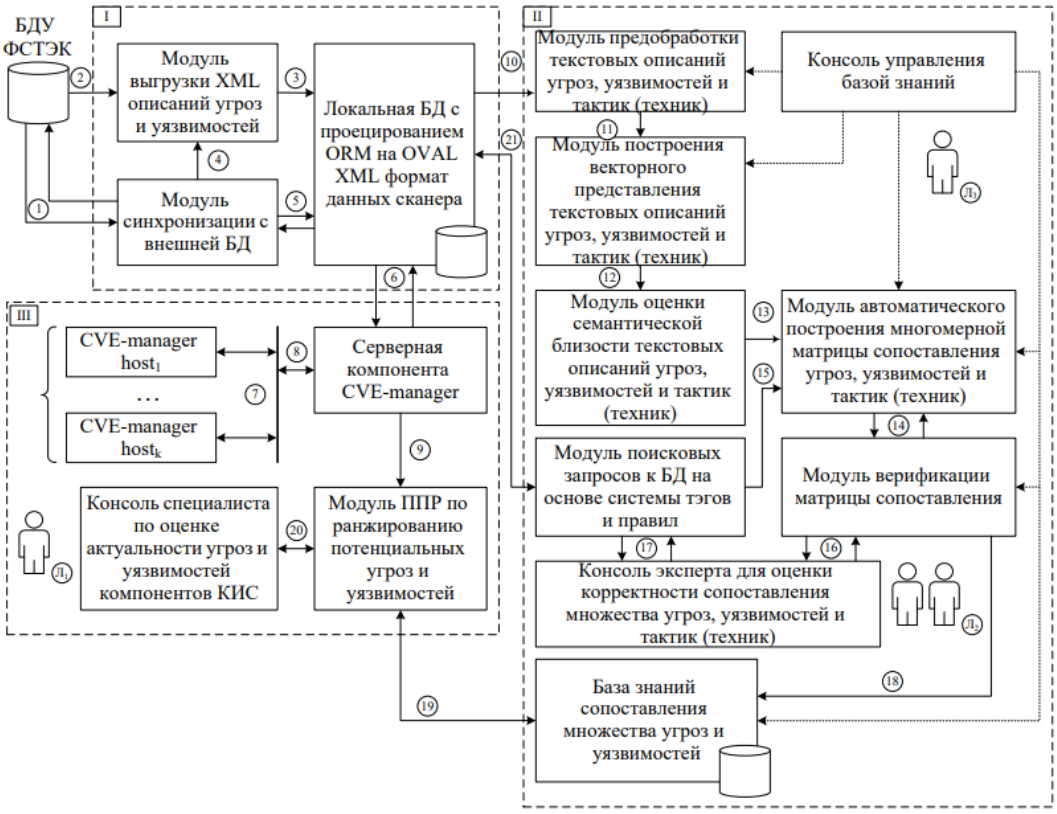

Рисунок 8 – Структурно-функциональная организация подсистемы анализа актуальных угроз БИ и уязвимостей ПО

На рисунке 9 представлена архитектура программного обеспечения ИСППР, построенная в нотации диаграммы компонент UML.

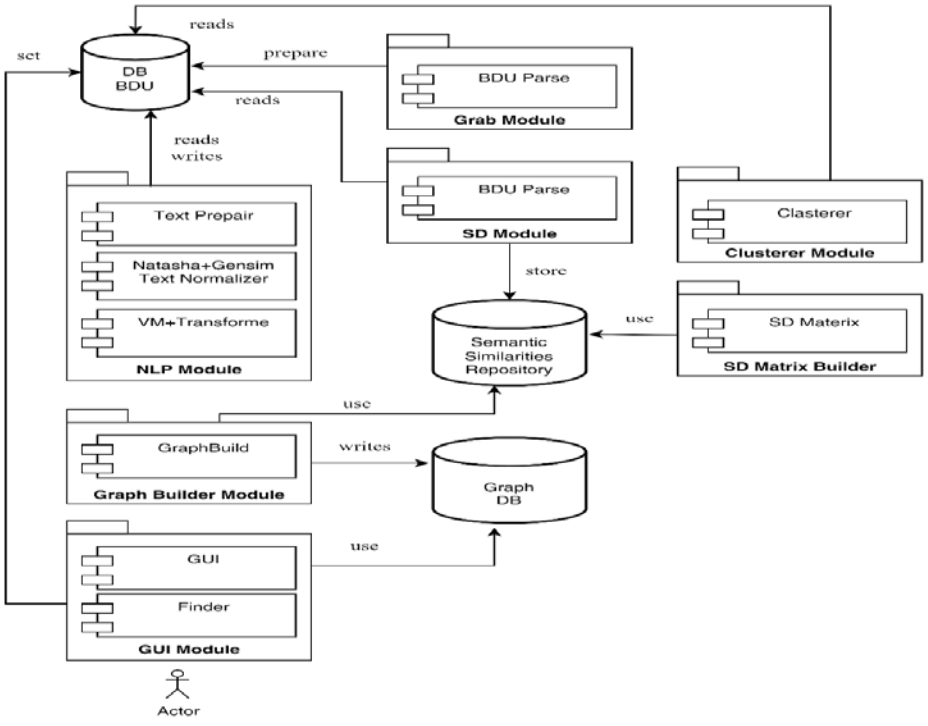

Рисунок 9 – Архитектура программного обеспечения ИСППР в нотации UML

С целью оценки эффективности применения разработанной ИСППР в работе рассматривалась задача оценки и анализа конкретного промышленного объекта КИИ - АСУ ТП приема, хранения и отпуска товарной нефти. В соответствии с ГОСТ Р 62443, были построены базовая и референсные модели архитектуры данного объекта, а также зональные модели безопасности, выделенные с учетом предъявляемых требований к ИБ.

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 1 часа. Семантический анализ с использованием разработанных технологий интеллектуального анализа текстов позволил автоматизировать процедуру префильтрации множества релевантных угроз БИ и способов их реализации, тем самым существенно сократив затраты времени эксперта.

Результаты экспериментов, проведенных для рассматриваемой АСУ ТП, представлены в виде таблицы сопоставления тактик (техник), наиболее близких угроз БИ и уязвимостей ПО, выявленных с помощью сканеров уязвимостей или определенных экспертом (таблица 3).

Таблица 3 – Фрагмент таблицы сопоставления тактик (техник), угроз БИ и уязвимостей ПО

№тактики	**Текстовое описание тактики и техник**	**Индексы семантически близких угроз**	**Текстовое описание семантически близких угроз**	**Индексы семантически 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...

Сравнение показателей процедуры анализа уязвимостей ПО, угроз БИ и сценариев их реализации, проведенного экспертом и проведенного с использованием разработанных средств автоматизации, приведено в табл. 4.

Таблица 4 – Сравнение показателей процедуры анализа уязвимостей ПО, угроз БИ и сценариев их реализации

<table>
<tr><td rowspan="2">Параметр</td><td rowspan="2">Экспертное сопоставление по тегам в БДУ ФСТЭК</td><td colspan="4">Автоматизированная система на основе технологий Text Mining</td></tr>
<tr><td colspan="2">Сопоставление уязвимостей и угроз</td><td colspan="2">Сопоставление уязвимостей, угроз и тактик (техник)</td></tr>
<tr><td>Ввод информации</td><td>Вручную, WEB-интерфейс БДУ</td><td colspan="4">Автоматизированная обработка результатов работы сканеров уязвимостей</td></tr>
<tr><td>Тип сопоставления угроз</td><td>Ручное</td><td colspan="4">Задается пороговыми метриками, определяющими чувствительность фильтра</td></tr>
<tr><td>Количество сопоставленных угроз</td><td>4</td><td colspan="2">10</td><td colspan="2">8</td></tr>
<tr><td rowspan="4">Экспертная оценка корректности сопоставления угроз (техник и тактик)</td><td rowspan="4">-</td><td>Модель</td><td>оценка</td><td>Модель</td><td>оценка</td></tr>
<tr><td>Word2Vec + TF-IDF</td><td>6 из 10</td><td>Word2Vec + TF-IDF</td><td>6 из 8</td></tr>
<tr><td>Doc2Vec</td><td>5 и 10</td><td>Doc2Vec</td><td>5 из 8</td></tr>
<tr><td></td><td></td><td>BERT 3</td><td>7 из 8</td></tr>
</table>

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)

В рамках второй серии экспериментов был использован полный список из 66 выявленных уязвимостей ПО (по группам устройств). Был проведен подбор пороговых значений для оценки семантической близости троек «угроза- уязвимость -тактика(техника)». Результаты экспериментов, проведенных для оценки уязвимостей ПО и угроз БИ рассматриваемой АСУ ТП, приведены в таблице 5 (фрагмент таблицы).

Таблица 5 – Результаты сопоставления уязвимостей ПО, угроз БИ, тактик (техник) (фрагмент)

	Идентификатор уязвимости	**Идентификатор угрозы БИ (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]

Для оценки эффективности работы ИСППР был проведен анализ результатов, полученных от ИСППР, на несоответствие мнению эксперта. Данные приведены в таблице 6.

Таблица 6 – 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.

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

В Приложениях приведены: Список сокращений и условных обозначений; Методика оценки актуальных угроз БИ объектов КИИ; Фрагмент модели угроз БИ объектов КИИ; Листинги скриптов реализации разработанной методики. Также приведены копии 2-х свидетельств о государственной регистрации программ для ЭВМ и актов внедрения результатов исследования.

Перспективы дальнейшего использования результатов. Направление дальнейших исследований связано с автоматизацией процесса выбора технических мер и средств обеспечения ИБ объектов КИИ.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

В рамках диссертационной работы получены следующие научные и практические результаты:

1.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.

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 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.

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.

Результаты представленных разработок внедрены в производственные и бизнес-процессы предприятий г. Уфы: ЗАО «Республиканский центр защиты информации», ООО «УРАЛТЕХСИСТЕМЫ», ФГБОУ ВО «Уфимский университет науки и технологий».

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, либо в научных изданиях, индексируемых базой данных RSCI

1. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining // Вопросы кибербезопасности. – 2020. – № 4(38). – С.22–31.

2. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining //Системы

управления, связи и безопасности. – 2021. – №. 3. – С. 110-134.

3. Васильев, В.И., Вульфин А.М., Кучкарова Н.В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров// Вопросы кибербезопасности. – 2022. – № 2(48). – С. 27–38.

4. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Моделирование и суммаризация текстов в области кибербезопасности // Вопросы кибербезопасности. 2023. № 2(54). С. 2-22.

Другие публикации по теме диссертации:

1. Исследование возможности использования кластерного анализа данных при оценке сценариев реализации угроз безопасности // Сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 21-22 мая 2021 года) / Уфа: РИЦ БГУ, 2021. – С.108-112.

2. Васильев В.И., Вульфин А.М, Кучкарова Н.В. Использование технологии Text Mining при оценке актуальных угроз и уязвимостей программного обеспечения // Приоритетные направления развития науки и технологий: доклады XXVIII международной научно-практической конференции. – Тула: Инновационные технологии, 2021. – С. 144-149.

3. Васильев В.И., Вульфин А.М, Кучкарова Н.В. Система поддержки принятия решений при оценке актуальных угроз и уязвимостей на основе семантического анализа // Мавлютовские чтения: материалы XIV Всероссийской молодежной научной конференции. – Уфа: РИК УГАТУ, 2020. – Т. 5, Ч. 2.

4. Васильев В.И., Кучкарова Н.В. Подход к определению актуальных уязвимостей при оценке уровня защищенности значимых объектов критической информационной инфраструктуры // Безопасность информационного пространства: труды XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. –Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – С. 356-361

5. Васильев В.И., Кучкарова Н.В. Сравнительный анализ систем классификаций АСУ ТП объектов критической информационной инфраструктуры // Информационные технологии интеллектуальной поддержки принятия решений: труды VII Всероссийской научной конференции (ITIDS). – Уфа: УГАТУ, 2019. – Т.2. – С. 214-219.

6. Васильев В.И., Кучкарова Н.В., Муслимова К.И. Методика определения актуальных угроз кибербезопасности АСУ ТП на основе стандарта ГОСТ Р 62443 // Безопасность: информация, техника, управление: материалы Международной научной конференции. – Санкт-Петербург: Национальное развитие, 2018. – С. 122-126.

7. Кучкарова Н. В. Исследование возможности использования кластерного анализа данных при оценке сценариев реализации угроз безопасности // Мавлютовские чтения. Уфа.– 2021. – С. 436-440.

8. Кучкарова Н.В. Применение моделей интеллектуального анализа текстов при оценке угроз информационной безопасности // сборник статей по материалам VI Международной научно-практической конференции «Современные проблемы цивилизации и устойчивого развития в информационном обществе». – М: ИРОК, 2021. – С.178-184.

Свидетельства о государственной регистрации программы для ЭВМ:

1. Свидетельство о государственной регистрации программы для ЭВМ № 2021615015. Программа оценки метрики опасности уязвимостей на основе технологий интеллектуального анализа и обработки естественного языка / Вульфин А.М., Никонов А.В., Карасева Е.М., Кучкарова Н.В., Васильев В.И., Кириллова А.Д. – заявл. 26.03.2021; зарег. 02.04.2021.

2. Свидетельство о государственной регистрации программы для ЭВМ № 2021615080. Программа анализа уязвимостей программного обеспечения на основе технологий интеллектуального анализа и обработки естественного языка / Вульфин А.М., Никонов А.В., Габбасова Д.Н., Кучкарова Н.В., Васильев В.И., Кириллова А.Д. заявл. 26.03.2021; зарег. 02.04.2021.

Диссертант  Н.В. Кучкарова