ОТЗЫВ

официального оппонента

доктора технических наук, профессора Болодуриной Ирины Павловны на диссертацию Кучкаровой Наили Вакилевны

на тему **«Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов»**,

представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Область исследования, выбранная соискателем, занимает весомое место при решении задач обеспечения информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ). Значимость данной предметной области связана прежде всего с постоянно возрастающим количеством кибератак на промышленные системы, значительная часть которых относится к объектам КИИ. Подобные атаки могут привести не только к материальным и финансовым потерям предприятий, но и к технологическим катастрофам, загрязнению окружающей среды, угрозам здоровью и жизни людей.

Актуальность выбранной предметной области подтверждается формированием в последнее десятилетие нормативно-законодательной базы, направленной на обеспечение ИБ объектов КИИ. Это такие документы, как федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г., приказы ФСТЭК России №31 от 14 марта 2014 г, № 235 от 21.12.2017 г., № 239 от 25.12.2017 г., национальные стандарты серии ГОСТ Р 62443/56205, Методика оценки угроз безопасности информации ФСТЭК России от 05.02.2021 г. и другие.

Исследования в данной области направлены на разработку методов и инструментальных средств автоматизации анализа и оценки актуальных угроз безопасности информации и уязвимостей программного обеспечения (ПО) объектов КИИ, важным классом которых являются автоматизированные системы управления технологическими процессами (АСУ ТП). Сложность решения данной задачи связана, прежде всего, с необходимостью обработки больших массивов слабоструктурированных данных, представленных, как правило, в виде текстовых описаний угроз безопасности информации, уязвимостей ПО, тактик и техник реализации угроз (шаблонов атак) в открытых международных базах данных, а также в Банке данных угроз безопасности информации (БДУ) ФСТЭК России. Анализ публикаций отечественных и зарубежных ученых показывает перспективность использования для решения указанных задач методов обработки текстов на естественном языке (Natural Language Processing, NLP), или интеллектуального анализа текстов (Text Mining).

В связи с вышеизложенным, тема диссертационной работы Кучкаровой Н.В., посвященная разработке метода и алгоритмов автоматизированной оценки актуальных угроз и уязвимостей объектов КИИ с использованием методов интеллектуального анализа текстов, является актуальной, решение этой задачи, несомненно, имеет научную и практическую ценность.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка сокращений, библиографического списка и приложений. Основной текст работы изложен на 170 страницах, содержит 58 рисунков, 32 таблицы, 3 приложения. В список используемой литературы включено 159 наименований источников. В приложениях содержатся копии актов внедрения и дополнительные материалы по результатам исследований.

Во введении обоснована актуальность работы, степень разработанности темы исследования, представлены объект и предмет исследования,

сформулированы цель и задачи диссертационной работы, научная новизна и практическая значимость результатов диссертации.

В первой главе проведен анализ существующей нормативно-законодательной базы и стандартов в области обеспечения ИБ объектов КИИ. Рассмотрены достоинства и недостатки открытых баз данных об угрозах безопасности информации (БИ) и уязвимостях ПО объектов КИИ. На основании проведенного анализа существующих методик оценки угроз БИ и уязвимостей ПО сделан вывод о необходимости автоматизации этапов: классификации и кластеризации угроз БИ и уязвимостей ПО, сопоставления выявленных уязвимостей ПО множеству релевантных угроз БИ, построения сценариев реализации актуальных угроз БИ для конкретных объектов КИИ. Отмечена целесообразность использования для решения указанных задач технологий интеллектуального анализа текстов.

Во второй главе представлены результаты решения задачи классификации (кластеризации) и суммаризации (автоматического реферирования) русскоязычных специализированных текстов в области ИБ на примере корпуса научных статей, опубликованных в выпусках журнала «Вопросы кибербезопасности» за 2013- 2022 гг. Приведены полученные автором результаты сравнительных экспериментов, связанных с предварительной обработкой указанных документов, понижением размерности числового признакового пространства, использованием метода ближайших соседей, скрытого распределения Дирихле и матричной неотрицательной функции на основе различных моделей векторного представления слов. Разработаны основные шаги, модели и инструменты реализации алгоритмов автоматической кластеризации и суммаризации специализированных текстов. По результатам экспериментов выявлены наиболее перспективные направления современных исследований в области ИБ, подтвердившие актуальность развиваемого в диссертации подхода, основанного на анализе ключевых факторов рисков ИБ объектов КИИ с применением технологий искусственного интеллекта.

В третьей главе проведен анализ процесса оценки актуальных угроз БИ в соответствии с Методикой ФСТЭК России с использованием IDF0-модели данного процесса, на основании которого сделан вывод о наличии определенных сложностей при построении сценариев реализации угроз БИ для объектов КИИ ввиду большого объема и слабой структурированности исходных данных, представленных в БДУ ФСТЭК в текстовом формате, и отсутствия автоматизированных средств анализа этих данных. Рассмотрены алгоритмы векторного представления и кластеризации текстовых описаний угроз БИ и уязвимостей ПО объектов КИИ. Предложены метод и алгоритм автоматизированной оценки и приоритизации множества релевантных угроз ИБ для выявленных уязвимостей ПО объектов КИИ, а также семантическая (графовая) модель построения фрагмента сценария реализации угроз БИ. Данные решения представляют несомненный интерес для специалистов в сфере ИБ, поскольку их использование позволяет значительно снизить трудоемкость и когнитивную нагрузку на эксперта при формировании перечня актуальных угроз БИ в соответствии с Методикой ФСТЭК России.

В четвертой главе разработан исследовательский прототип интеллектуальной системы поддержки принятия решений (ИСППР), реализующей предложенные автором метод и алгоритмы обработки текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализации угроз, применение которой позволяет автоматизировать процессы сопоставления множества релевантных угроз БИ для выявленных уязвимостей ПО, построения графовой модели сценариев реализации угроз БИ и, как результат, – выявления перечня актуальных угроз БИ объекта КИИ.

Рассмотрен пример использования предложенных решений для оценки актуальных угроз БИ и уязвимостей ПО АСУ ТП пункта приема, хранения и отпуска товарной нефти нефтедобывающего предприятия.

В Заключении приведены основные выводы и результаты проведенных исследований.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации.

Обоснованность научных положений, выводов и рекомендаций, представленных в диссертации, подтверждается опубликованными по материалам исследований работами, включающими в себя 4 статьи в профильных научных журналах категории К1 по специальности 2.3.6, входящих в Перечень рецензируемых научных изданий, рекомендованных ВАК, 8 статьях в других изданиях, а также 2 свидетельствах о государственной регистрации программ для ЭВМ.

Диссертация содержит достаточное для понимания результатов проведенных исследований количество иллюстративного материала и таблиц.

Автореферат отражает содержание диссертации и представленные в работе основные выводы и результаты. Полученные результаты соответствуют заявленным автором пунктам паспорта специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Достоверность и новизна полученных результатов подтверждаются корректной постановкой задач и выбором методов исследования; анализом выполненных научно-исследовательских работ в данной предметной области; результатами сравнительного анализа перечня обнаруженных актуальных угроз БИ с использованием предложенных в работе инструментальных средств автоматизации и экспертных оценок актуальных угроз БИ объекта КИИ; результатами практического применения разработанного метода и алгоритмов оценки актуальных угроз БИ и уязвимостей ПО при решении прикладных задач; апробацией полученных результатов на научно-практических конференциях.

Научная новизна работы

В качестве основных результатов диссертационного исследования, обладающих научной новизной, можно отметить следующие:

1. Алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ, основанные на совместном применении алгоритмов кластеризации и извлечения признаков в семантическом векторном пространстве, отличающиеся от известных алгоритмов возможностью осуществлять автоматизированную предобработку больших корпусов слабоструктурированных русскоязычных научных текстов и их последующий семантический анализ с целью выявления семантически однородных групп документов (тематических направлений, трендов исследований, рефераты статей) .

2. Метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО объектов КИИ на основе технологии семантического анализа текстов, отличающиеся использованием предложенного алгоритма кластеризации и оценки семантической близости текстовых описаний угроз БИ и уязвимостей ПО в семантическом векторном пространстве.

3. Алгоритм построения графовой модели сценариев реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ, отличающийся использованием технологии нейросетевых языковых моделей – трансформеров, что позволяет автоматизировать процесс построения графовой модели, визуализировать результаты этого процесса, снизить трудоемкость и когнитивную нагрузку на специалистов в сфере ИБ.

4. Архитектура и совокупность программных модулей исследовательского прототипа ИСППР, позволяющей реализовать предложенные метод, алгоритмы и инструментальные средства автоматизации оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, применение которых позволяет снизить временные затраты и повысить достоверность решений, принимаемых экспертом – специалистом в сфере ИБ

при оценке уровня защищенности объекта КИИ и выработке рекомендаций по реализации необходимых контрмер по защите информации.

Теоретическая и практическая значимость полученных автором результатов

В диссертации обоснован выбор совокупности моделей и инструментов для исследования поставленных задач, Разработан ансамбль алгоритмов, позволяющих автоматизировать процедуру оценки и ранжирования релевантных угроз БИ для выявленных уязвимостей ПО объектов КИИ с использованием технологий семантического анализа текстов, а также построить графовую модель сценария реализации угроз БИ, что, в свою очередь, является обоснованием для формирования перечня актуальных угроз БИ для конкретного объекта КИИ. Применение предложенных решений позволяет значительно снизить когнитивную нагрузку на эксперта в процессе выявления актуальных угроз БИ.

Практическая значимость полученных результатов заключается в разработке архитектуры и программного обеспечения исследовательского прототипа ИСППР, применение которой позволяет автоматизировать процесс сопоставления угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ при построении сценариев их реализации, что позволяет сократить временные затраты и повысить достоверность оценки актуальных угроз БИ для объектов КИИ. Данные выводы подтверждаются применением результатов диссертационной работы для конкретного промышленного объекта КИИ – АСУ ТП пункта приема, хранения и отпуска товарной нефти, что подтверждается соответствующим актом внедрения.

Замечания по диссертационной работе

1. В работе приводятся результаты экспериментов по классификации и суммаризации текстовых данных, где для формирования корпуса текстов

используются полнотекстовые научные статьи, опубликованные в журнале «Вопросы кибербезопасности». Для более полного раскрытия темы исследований, а также с целью выявления новых типов угроз БИ и уязвимостей ПО, не представленных в рассмотренных источниках информации, рекомендуется использовать дополнительную информацию, размещаемую в открытых реестрах и классификациях уязвимостей ИБ.

2. В работе не представлено описание способа определения меры семантической близости текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ на английском (для данных из CVE, CAPEC) и русском (для данных из БДУ ФСТЭК России) языках.

3. Не получил должного освещения вопрос о выборе метода векторизации текстов (Word2Vec, Doc2Vec, GloVe, Fast Text, USE, BERT), хотя от выбора этого метода во многом зависит решение задачи кластеризации и других поставленных в работе задач.

4. Не вполне ясно, как должна оцениваться достоверность решений по оценке актуальных угроз БИ объектов КИИ, принимаемых с помощью разработанной ИСППР.

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают значимости и общей положительной оценки представленной работы.

Заключение

Диссертация Кучкаровой Н.В., представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, в которой решена задача оценки актуальных угроз безопасности информации и уязвимостей ПО объектов КИИ с использованием технологий интеллектуального анализа текстов, результаты которой обладают научной новизной и практической ценностью.

Считаю, что диссертация соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, а ее автор, Кучкарова Наиля Вакилевна, заслуживает присуждения ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
Доктор технических наук, профессор,
заведующий кафедрой прикладной математики,
Федеральное государственное бюджетное
образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Болодурина Ирина Павловна

28.08.2023

Докторская диссертация защищена
по специальности 05.13.10 – «Управление
в социальных и экономических системах»

Даю согласие на обработку персональных данных

Адрес места основной работы:
460018, г. Оренбург, просп. Победы, д. 13, каб. 20-608
Рабочий телефон: +7 (35-32) 37-25-36
Адрес эл. почты: ipbolodurina@yandex.ru

Подпись Болодуриной И.П. заверяю:
Главный ученый секретарь – начальник отдела диссертационных советов,
Доктор технических наук, профессор

Фот Андрей Петрович