ОТЗЫВ

официального оппонента

кандидата технических наук, доцента Макаряна Александра Самвеловича

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

Процессы цифровизации современной экономики сопровождаются неуклонным ростом числа и масштабов последствий целенаправленных компьютерных атак, использующих существующие уязвимости программного обеспечения (ПО) объектов критической информационной инфраструктуры (КИИ). Статистика последних лет показывает расширение ландшафта угроз безопасности информации (БИ), появление новых, ранее не встречавшихся уязвимостей ПО объектов КИИ, использование злоумышленниками для реализации своих целей разнообразных подходов и стратегий, включая применение методов искусственного интеллекта. Всё это, конечно, дает мощный импульс к развитию нормативно-законодательной базы в области обеспечения информационной безопасности (ИБ) объектов КИИ (федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Приказы ФСТЭК России №31, №235, №239, «Методика оценки угроз безопасности информации» ФСТЭК России от 05.02.2021 г. и др.). Особенности реализации угроз БИ, уязвимостей ПО, возможных сценариев реализации компьютерных атак сегодня находятся в центре внимания специалистов всего мира. По инициативе и при участии ведущих

IT-компаний созданы и непрерывно пополняются открытые базы данных, представляющие собой структурированные текстовые описания ранее зафиксированных угроз БИ и уязвимостей ПО – CVE, CVSS, NVD, CAPEC, Банк данных угроз безопасности информации (БДУ) ФСТЭК России и др. Использование этой информации оказывает своевременную оперативную помощь специалистам по ИБ при проектировании и эксплуатации систем защиты объектов КИИ с учетом предъявляемых нормативных требований со стороны регуляторов.

Вместе с тем, на практике использование указанных нормативных документов и перечисленных баз данных на этапе определения актуальных угроз БИ объектов КИИ и построения возможных сценариев их реализации (что является необходимым признаком актуальности угрозы в соответствии с Методикой ФСТЭК России) встречается с серьезными затруднениями. Выявление актуальных угроз происходит, как правило, экспертным способом и связано с необходимостью обработки больших массивов разнородных, представленных в различных форматах, текстовых данных – описаний уязвимостей ПО, угроз БИ, тактик и техник реализации этих угроз. Поэтому разработка методик и инструментальных средств автоматизации процесса анализа и оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием современных технологий обработки естественного языка - интеллектуального анализа текстов (Text Mining)- является крайне необходимой и вызывает интерес широкого круга специалистов.

Таким образом, тема представленного научного исследования, посвященного оценке актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием технологий интеллектуального анализа текстов, является актуальной и своевременной.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, 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.

Структура и содержание представленных материалов соответствует заявленной цели и задачам диссертации.

Во введении обоснована актуальность работы, исследована степень разработанности темы диссертации, описаны объект и предмет исследования, сформулированы цель и задачи диссертационной работы, а также научная новизна и практическая значимость результатов диссертации.

В первой главе диссертационной работы проведен анализ существующей нормативно-законодательной базы и стандартов в области обеспечения ИБ объектов КИИ. Рассмотрены достоинства и недостатки наиболее известных открытых баз данных, содержащих информацию об угрозах БИ и уязвимостях ПО объектов КИИ. Подчеркивается практическая значимость использования русскоязычной базы данных БДУ ФСТЭК, ориентированной на отечественный опыт эксплуатации компьютерных систем.

На основании проведенного анализа существующих методик оценки угроз БИ и уязвимостей ПО сделан вывод о необходимости автоматизации основных этапов Методики ФСТЭК России, включая классификацию и кластеризацию угроз БИ и уязвимостей ПО, сопоставление выявленных уязвимостей ПО с релевантными угрозами БИ, а также построение сценариев реализации актуальных угроз БИ для конкретных объектов КИИ. В качестве наиболее эффективных средств автоматизации для решения указанных задач предложены технологии интеллектуального анализа текстов (Text Mining).

Во второй главе рассмотрены основные методы и алгоритмы автоматической классификации (тематического моделирования) и суммаризации (реферирования текстов) с использованием технологий интеллектуального анализа текстов. Исследованы особенности решения

задач классификации и суммаризации слабоструктурированной информации на примере корпуса текстов, сформированного из выпусков полнотекстовых научных статей журнала «Вопросы кибербезопасности» за 2013 - 2022 гг. Проведенный анализ статей подтвердил, в частности, рост за последние 2-3 года интереса научной общественности к выбранному соискателем направлению исследований («Анализ, угроз, уязвимостей и рисков ИБ»). Показана возможность обработки профессиональных текстов в области ИБ с использованием широкого набора инструментов Text Mining, применение которых позволяет повысить скорость обработки больших массивов текстовых данных, сохраняя при этом высокое качество анализа документов.

В третьей главе выполнено системное моделирование процесса оценки угроз БИ в соответствии с Методикой ФСТЭК России, выявлены основные затруднения в практике ее применения, заключающиеся в необходимости совместной обработки (контентного анализа) содержащихся в БДУ ФСТЭК России текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ при построении возможных сценариев реализации атак на объекты КИИ. С использованием методов интеллектуального анализа текстов разработаны: алгоритмы векторизации и кластеризации текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ на основе оценки семантической близости их описаний; метод и алгоритм оценки и ранжирования (приоритизации) множества релевантных угроз БИ для выявленных уязвимостей ПО объекта КИИ. Результаты вычислительных экспериментов, проведенных с использованием предложенного метода и алгоритмов, демонстрируют возможность построения множества сценариев реализации актуальных угроз БИ при значительном снижении трудоемкости соответствующей процедуры.

В четвертой главе разработаны инструментальные средства автоматизации процесса анализа и оценки актуальных угроз БИ и

уязвимостей ПО объектов КИИ, интегрированные в виде прототипа интеллектуальной системы поддержки принятия решений (ИСППР). Применение этих средств позволяет в значительной степени автоматизировать процесс сопоставления (оценки семантической близости) текстовых описаний угроз БИ, уязвимостей ПО, тактик, техник и сценариев реализации угроз БИ, и определить в итоге перечень актуальных угроз объекта КИИ.

Приведены результаты применения предложенного соискателем метода и алгоритмов оценки актуальных угроз БИ и уязвимостей ПО для конкретного объекта КИИ – АСУ ТП пункта приема, хранения и отпуска товарной нефти нефтедобывающего предприятия, подтверждающие эффективность предложенных решений.

В Заключении приведены основные выводы и результаты проведенных исследований.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации – высокая, что подтверждается результатами анализа известных методов и научных подходов, применяемых в процессе анализа и оценки угроз БИ и уязвимостей ПО объектов КИИ; ссылками на результаты исследований, опубликованные в рецензируемых отечественных и зарубежных изданиях; статистическими данными авторитетных компаний в области ИБ; использованием официальными нормативно-правовыми документами в области обеспечения ИБ объектов КИИ.

Достоверность и новизна полученных результатов подтверждаются: строгостью применяемых алгоритмов; сравнительным анализом количественной оценки результатов экспериментов, полученных автоматизированным и «ручным» (экспертным) способом; использованием полученных результатов на ряде предприятий, что подтверждается соответствующими актами внедрения; обсуждением полученных результатов исследований на российских и международных конференциях,

а также публикацией основных результатов диссертации в рецензируемых научных изданиях, входящих в перечень ВАК по профилю специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Соответствие паспорту специальности.

Результаты диссертационной работы соответствуют следующим пунктам паспорта научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность:

– 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.10 «Модели и методы оценки защищенности информации и информационной безопасности объекта».

Научная новизна работы заключается в следующем:

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 с их последующим семантическим анализом.

2. Разработаны метод и алгоритм автоматизированной оценки и 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.

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, позволяющий автоматизировать процесс построения графовой модели, снизить трудоемкость и когнитивную нагрузку на специалистов по ИБ.

4. Разработана архитектура и совокупность программных модулей ИСППР, позволяющих реализовать метод и алгоритмы, применение которых снижает временные затраты и повышает достоверность решений, принимаемых экспертом.

Теоретическая и практическая значимость полученных автором результатов

Теоретическая значимость полученных автором результатов заключается в повышении эффективности процесса оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием предложенного метода и алгоритмов интеллектуального анализа текстов, значительно снижающих когнитивную нагрузку на эксперта (специалиста по ИБ) и одновременно предоставляющих ему дополнительную возможность расширения множества сценариев реализации атак и перечня актуальных угроз БИ объектов КИИ.

Практическая значимость полученных результатов заключается в разработке инструментальных средств автоматизации построения сценариев реализации атак, интегрированных в составе ИСППР, использование которых позволяет существенно сократить временные затраты и повысить качество оценки актуальных угроз БИ, что подтверждается результатами применения ИСППР при оценке актуальных

угроз БИ для промышленного объекта – АСУ ТП пункта приема, хранения и отпуска товарной нефти.

Замечания по диссертационной работе

1. В первой главе (п.1.4) можно было более подробно остановиться на вопросе о выборе косинус-меры для определения семантической близости текстовых описаний.

2. Вообще говоря, для более точного определения актуальных угроз БИ для конкретного рассмотренного в работе примера целесообразно было бы использовать не только данные БДУ ФСТЭК, но и открытые зарубежные базы данных.

3. В таблице 4.12 главы 4 следовало указать, в чем выражается оценка несоответствия выданных ИСППР результатов мнению эксперта (специалиста по ИБ).

4. Не вполне ясны ограничения на область применения предложенных решений (метод, алгоритмы, инструментальные средства).

5. Целесообразно было бы указать более четкие формулировки относительно необходимой аппаратной платформы, объема вычислительных ресурсов и трудозатрат, квалификации пользователя и т.п., требуемых для развертывания и сопровождения разработанной ИСППР,

6. Возможно, в 4-й главе следовало привести дополнительные данные, отражающие экономическую эффективность предложенных автором решений.

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают общей высокой 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 БИ и уязвимостей ПО объектов КИИ с использованием технологий

интеллектуального анализа текстов, результаты которой обладают существенной 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 специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

кандидат технических наук, доцент,
заведующий кафедрой кибербезопасности
и защиты информации,
Федеральное государственное бюджетное
образовательное учреждение высшего
образования «Кубанский государственный
технологический университет»

Макарян Александр Самвелович
21.08.2023 г.

Ученый секретарь ФГБОУ ВО «Кубанский
государственный технологический университет»,

кандидат технических наук, доцент Гонтар Виктория Викторовна
21.08.2023 г.

Кандидатская диссертация защищена
по специальности 05.13.01 – «Системный анализ,
управление и обработка информации (по отраслям)».

Даю согласие на обработку персональных данных.

Адрес места основной работы: 350000, г. Краснодар,
ул. Красная, д. 91, каб. 204.

Рабочий телефон: (861) 255-03-46
Адрес эл. почты: masnya@yandex.ru