УТВЕРЖДАЮ
Проректор по научной
и исследовательской работе
ФГАОУ ВО «Северо-Кавказский
федеральный университет»,
к.ф.-м.н., доцент

_____ А.А. Алиханов

«31» 08 2023 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

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

Четвертая промышленная революция (Industry 4.0) предполагает переход на полностью автоматизированное цифровое производство, массовое использование интеллектуальных технологий управления промышленными объектами при интенсивном информационном взаимодействии этих объектов с внешней средой (смежники, поставщики, провайдеры и т.п.). Данное обстоятельство неизбежно усложняет задачу обеспечения информационной безопасности (ИБ) автоматизированных систем промышленных объектов, и в том числе объектов критической информационной инфраструктуры (КИИ), функционирование которых жизненно важно для развития экономики нашей страны. Одним из важнейших этапов обеспечения ИБ объектов КИИ является анализ и оценка актуальных угроз безопасности информации (БИ) и уязвимостей их программного обеспечения (ПО), что используется в основе риск-ориентированного подхода к оценке защищенности данных объектов и

ВХОД. № 2320-13
«06» 09 2023г.

выработке эффективных контрмер по защите информации в соответствии с требованиями регуляторов.

Несмотря на наличие достаточно большого числа нормативно-законодательных документов в области обеспечения ИБ объектов КИИ (федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Приказы ФСТЭК России №№ 31, 235, 239 и др.), на практике возникают определенные трудности в их реализации. В частности, для выполнения этапов «Методики оценки угроз безопасности информации» ФСТЭК России от 05.02.2021 г. эксперту (специалисту по ИБ) необходимо провести большой объем работы, связанной с анализом представленных в различных форматах в Банке данных угроз безопасности информации (БДУ) ФСТЭК России или в других открытых базах данных (БД) текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализации угроз БИ с целью последующего построения возможных сценариев реализации угроз и определения перечня актуальных для данного объекта КИИ угроз БИ. В настоящий момент данные процедуры выполняются, как правило, экспертом в «ручном» режиме и нередко сопровождаются субъективными ошибками, связанными с человеческим фактором, что приводит к необходимости разработки и применения средств автоматизированной обработки текстовых данных, позволяющих упростить и ускорить работу специалистов по ИБ, занимающихся решением указанных задач.

Таким образом, тема представленной диссертационной работы, посвященной оценке актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием технологий автоматизации интеллектуального анализа текстов, является актуальной.

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. В приложениях содержатся копии актов внедрения и дополнительные материалы результатов исследований.

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

В первой главе проведен анализ существующей нормативно-правовой базы, а также стандартов в области обеспечения ИБ объектов КИИ. Отмечена необходимость автоматизации процесса анализа и оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ, включая этап построения сценариев реализации угроз БИ с использованием определенных техник и тактик. Показана перспективность применения технологий интеллектуального анализа текстов для решения поставленных задач.

Во второй главе описаны основные методы и алгоритмы, применяемые для решения задач автоматической классификации (тематического моделирования) и суммаризации (реферирования) текстовых данных с использованием технологий обработки естественного языка. Приведены результаты экспериментов, показывающих достоинства и недостатки этих методов и алгоритмов. Показаны особенности применения технологий классификации и суммаризации текстов на примере автоматизированной обработки корпуса текстов научных статей, опубликованных в журнале «Вопросы кибербезопасности» за 2013- 2022 гг.

В третьей главе приведена функциональная модель IDEF0 процесса оценки угроз БИ, отражающая основные этапы этого процесса в соответствии с Методикой ФСТЭК России. Предложены метод и алгоритмы решения базовых задач оценки угроз БИ с использованием средств автоматизации интеллектуального анализа текстов, включая задачи: кластеризации текстовых описаний угроз БИ, уязвимостей ПО, тактик и

техник реализации угроз БИ; определения перечня релевантных угроз БИ и их приоритизации для выявленных уязвимостей ПО объекта КИИ; построения графовой модели сценария реализации угроз БИ. Вычислительные эксперименты с применением разработанного метода и алгоритмов обработки текстов, показали сокращение затрат времени в 2-3 раза на построение сценариев реализации угроз БИ по сравнению с «ручным» способом (без использования средств автоматизации).

В четвертой главе представлены архитектура исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) при оценке и анализе актуальных угроз БИ объектов КИИ, состав программных модулей этой системы и методика ее применения. Приведены результаты решения конкретной прикладной задачи, связанной с применением предложенных решений для оценки актуальных угроз БИ АСУ ТП пункта приема, хранения и отпуска товарной нефти нефтедобывающего предприятия.

В Заключении приведены основные выводы и результаты проведенных исследований.

Область исследования диссертации соответствует 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».

Согласованность автореферата и диссертации. Текст автореферата полностью отражает содержание диссертации и полученные в ней основные результаты.

Оформление диссертации соответствует ГОСТ Р 7.0.11-2011.

Достоверность полученных результатов подтверждается корректной постановкой задач и выбором методов исследования; обсуждением полученных результатов на научных конференциях; результатами практического применения разработанного метода и алгоритмов оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ при решении прикладных задач.

Научная новизна работы

К основным результатам диссертационного исследования, обладающим научной новизной, можно отнести следующие:

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 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.

2. Разработаны 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 векторном пространстве вложения.

3. Разработан 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 по ИБ.

4. Представлены 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.

Публикации. Основные результаты научного исследования опубликованы в 14 работах, в том числе в 4 статьях в изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 8 статьях в других изданиях; получено 2 свидетельства о государственной регистрации программ для ЭВМ.

Теоретическая и практическая значимость полученных автором результатов

Теоретическая значимость работы определяется, прежде всего результатами анализа исследуемой предметной области, на основании которого сделан правильный вывод об актуальности разработки комплекса методов, алгоритмов и инструментальных средств автоматизации на основе технологий интеллектуального анализа текстов для решения задач оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ в соответствии с базовой концепцией, рекомендуемой в Методике ФСТЭК России. Автором предложен метод и алгоритмы решения этих задач, ориентированные на

автоматизированную обработку текстовых описаний угроз БИ, уязвимостей ПО, тактик и техник реализацию угроз БИ, используя в качестве исходной информации открытые текстовые данные из БДУ ФСТЭК России.

Практическая значимость полученных результатов заключается в разработке и программной реализации инструментальных средств оценки актуальных угроз БИ и уязвимостей ПО, их интеграции в составе исследовательского прототипа ИСППР, разработке методики практического применения этой системы для решения прикладных задач.

Результаты проведенных исследований внедрены в производственные и бизнес-процессы предприятий г. Уфы. В ЗАО «Республиканский центр защиты информации» проведены систематизация и структурирование текстовых описаний технологических процессов, производственных цепочек и совокупности организационно-распорядительной документации с целью оценки степени опасности уязвимостей используемого прикладного ПО с использованием предложенных алгоритмов автоматической классификации и суммаризации текстов. В ООО «УРАЛТЕХСИСТЕМЫ» внедрена методика автоматизированной оценки актуальных угроз безопасности информации и построения графовой модели сценария реализации угроз БИ с использованием разработанного прототипа ИСППР. В ФГБОУ ВО «Уфимский университет науки и технологий» введен в учебный процесс подготовки бакалавров и магистрантов по направлениям 10.04.01 «Информационная безопасность» и 09.04.01 «Информатика и вычислительная техника» (профиль «Безопасность и защита информации») лабораторный практикум, в котором реализованы разработанные автором метод и алгоритм автоматизированной оценки и ранжирования множества релевантных угроз БИ для выявленных уязвимостей ПО объектов КИИ с использованием технологии семантического анализа текстов.

Применение предложенных решений позволяет автоматизировать решение задач, связанных с определением перечня актуальных угроз БИ и уязвимостей ПО объектов КИИ на основе построения наиболее вероятных

сценариев реализации угроз БИ, что позволяет существенно снизить когнитивную нагрузку на эксперта при сокращении необходимых временных затрат. Данные выводы подтверждаются представленными актами внедрения.

Рекомендации по расширенному использованию результатов диссертации. Представленные в диссертации результаты исследования рекомендуются к дальнейшему использованию как в ИТ-компаниях, занимающихся профессиональной деятельностью в области разработки и применения программных средств аудита ИБ объектов КИИ, мониторинга событий и инцидентов ИБ, предупреждения и ликвидации последствий компьютерных атак на объекты КИИ, так и непосредственно в процессе оперативного управления ИБ на объектах КИИ силами квалифицированных специалистов по ИБ.

Замечания по диссертационной работе

1. Во второй главе рассмотрены различные методы и алгоритмы кластеризации текстов применительно к задачам классификации (тематического моделирования) профильных научных статей в области ИБ. Несомненно, результаты проведенных при этом экспериментов позволили автору выделить ряд наиболее эффективных методов обработки естественного языка. Но хотелось бы видеть более четкие выводы, каким конкретно методам и почему будет предпочтение в последующих главах работы.

2. Было бы интересно рассмотреть особенности решения задачи суммаризации (реферирования) текстов на примере текстовых описаний угроз БИ и уязвимостей, заимствованных из БДУ ФСТЭК России.

3. В представленных в 3-й главе функциональных моделях IDEF0 процесса оценки и анализа актуальных УБИ в соответствии с Методикой ФСТЭК России (рисунки 3.1-3.3) не указаны точки зрения, относительно которых рассматривались представленные модели; на рисунке 3.3 не показаны все стрелки, обозначающие «механизмы».

4. Не указаны ограничения на область применения предложенного в 3-й главе метода и алгоритмов определения релевантных угроз БИ для выявленных уязвимостей ПО объекта КИИ (для каких классов объектов КИИ это относится прежде всего).

5. В явном виде не указаны требуемые вычислительные ресурсы, необходимые для реализации предложенного в работе исследовательского прототипа ИСППР.

6. Хотелось бы видеть больше примеров построения сценариев реализации угроз БИ для конкретного объекта КИИ, с комментариями степени успешности (опасности) их реализации и выбором контрмер по парированию их последствий.

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают научной и практической 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 на основании выполненных исследований решена задача разработки средств автоматизации оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием технологий интеллектуального анализа текстов, результаты которой обладают научной новизной и практической ценностью.

Диссертация соответствует требованиям пунктов 9, 10, 11, 13, 14 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.

Отзыв обсужден и утвержден на заседании кафедры организации и технологии защиты информации Федерального государственного автономного образовательного учреждения высшего образования «Северо-

Кавказский федеральный университет». Протокол заседания № 1 от «28» августа 2023 г. Присутствовало на заседании 13 чел. Результаты голосования: «за» – 13 чел., «против» – 0 чел., «воздержалось» – 0 чел.

Согласны на включение персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

Отзыв составили:
кандидат технических наук, доцент,
заведующий кафедрой организации и
технологии защиты информации,
и.о. директора Института цифрового развития,
Федеральное государственное автономное
образовательное учреждение высшего
образования «Северо-Кавказский
федеральный университет» Петренко Вячеслав Иванович

«28» 08 2023 г.

кандидатская диссертация защищена по научной специальности 20.01.09 «Военные системы управления, связи и навигации»

доктор физико-математических наук, доцент,
заведующая кафедрой компьютерной безопасности
Федеральное государственное автономное
образовательное учреждение высшего
образования «Северо-Кавказский
федеральный университет» Тебуева Фариза Биляловна

«28» 08 2023 г.

докторская диссертация защищена по научной специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ»

Сведения о ведущей организации:
Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет»
(ФГАОУ ВО «Северо-Кавказский федеральный университет»)
Адрес: 355017, г. Ставрополь, ул. Пушкина, 1
Телефоны: (8652) 95-68-08
E-mail: info@ncfu.ru
Сайт организации: https://www.ncfu.ru/glavnaya/

ПОДПИСЬ УДОСТОВЕРЯЮ: