УТВЕРЖДАЮ
Проректор по инновационной деятельности ФГБОУ ВО «Уфимский университет науки и технологий»
канд. тех. наук, доцент
_____ Г.К. Агеев
«__1__» ____июня____ 2023 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий»

Диссертация Кучкаровой Н.В. на тему «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов» выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

В период подготовки диссертации соискатель Кучкарова Наиля Вакилевна работала в должности ассистента, затем старшего преподавателя кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

В 2020 г. окончила магистратуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 09.04.01 «Информатика и вычислительная техника».

Приказом № 0034-А от 14.06.2022 г. зачислена в качестве экстерна для прохождения промежуточной аттестации.

Справка со сведениями о сданных кандидатских экзаменах выдана в 2023 г. ФГБОУ ВО «Уфимский университет науки и технологий».

Научный руководитель – доктор технических наук, профессор Васильев Владимир Иванович, профессор кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий».

По итогам обсуждения принято следующее заключение:

1. Диссертация Кучкаровой Наили Вакилевны является законченной научно-квалификационной работой, соответствующей п. 9 Положения о порядке присуждения ученых степеней, утвержденного Постановлением

Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), в которой содержатся научно обоснованные результаты решения задач оценки актуальных угроз и уязвимостей объектов критической информационной инфраструктуры (КИИ) и обеспечения интеллектуальной поддержки принятия решений на этапе построения сценариев реализации угроз, имеющих важное практическое значение.

2. Соискателем лично получены все основные результаты, выносимые на защиту:

– алгоритмы автоматической классификации и суммаризации специализированных текстов в области ИБ на основе технологий автоматизированной обработки слабоструктурированных текстовых данных;

– метод и алгоритм оценки и приоритизации множества релевантных угроз БИ для выявленных уязвимостей ПО объектов КИИ с использованием технологии семантического анализа текстов;

– алгоритм построения графовой модели сценария реализации угроз БИ с использованием алгоритмов векторного вложения и технологии трансформеров;

– архитектура и программная реализация модулей исследовательского прототипа интеллектуальной системы поддержки принятия решений (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.

В перечисленных в автореферате работах соискателем лично получены следующие результаты:

– в работах [4, 11] разработаны и исследованы алгоритмы автоматической классификации и суммаризации специализированных текстов в области ИБ на основе технологий автоматизированной обработки слабоструктурированных текстовых данных, позволяющих 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;

– в работах [1, 3, 14] разработаны метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз безопасности информации (БИ) для выявленных уязвимостей ПО на основе технологии семантического анализа текстов, применение которых позволяет улучшить качество работы эксперта, сократив время на поиск актуальных угроз БИ, обеспечивая при этом более высокую наглядность, полноту и достоверность результатов такого поиска;

– в работах [3,9,10] 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;

– в работах [1, 8, 13, 14] разработаны 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.

Опубликованные работы полностью отражают основное содержание диссертационной работы. Все основные положения и результаты, выносимые на защиту, отражены в публикациях автора: по главе 1 – [5-7, 10]; по главе 2 – [4, 11]; по главе 3 – [1, 3, 9, 10, 12, 13]; по главе 4 – [1-3, 8, 10, 14]. Две работы написаны автором единолично, другие совместно с научным руководителем или другими членами научного коллектива.

3. Достоверность полученных результатов и выводов основана на том, что предложенные в диссертационной работе решения подтверждаются:

– корректной постановкой задач и выбором методов исследования;

– анализом выполненных научно-исследовательских работ в данной предметной области;

– результатами сравнительного анализа количественных оценок обнаруженных актуальных угроз по итогам интеллектуального анализа текстовых описаний и экспертных оценок актуальных угроз объекта КИИ;

– результатами практического применения разработанного метода и алгоритмов оценки актуальных угроз и уязвимостей при решении прикладных задач.

Результаты исследований, выводы и предлагаемые технические решения прошли производственную апробацию.

4. Научная новизна работы заключается в следующем:

– Разработаны алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ, основанные на совместном применении алгоритмов кластеризации и извлечения признаков для построения композиции векторов вложений, отличающиеся от известных алгоритмов автоматизированной предобработкой больших корпусов слабоструктурированных русскоязычных текстов с помощью технологий трансформеров с их последующим семантическим анализом, выделением тематических направлений и автоматическим реферированием.

– 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 разработанных алгоритмов кластеризации и оценки семантической близости текстовых описаний угроз

БИ и уязвимостей ПО в многомерном векторном пространстве, применение которых позволяет сократить затрачиваемое экспертом время на поиск актуальных угроз БИ, обеспечивая более высокую наглядность, полноту и достоверность результатов такого поиска

– Разработан алгоритм построения графовой модели сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, отличающийся использованием технологии трансформеров и алгоритмов векторного вложения, что позволяет автоматизировать процесс построения графовой модели, снизив трудоемкость и когнитивную нагрузку на специалистов по ИБ, предоставляя им дополнительную информацию для формирования перечня актуальных угроз и уязвимостей объектов КИИ.

– Предложены архитектура и состав программных модулей ИСППР, реализующих предложенные в работе метод и алгоритмы, применение которых позволяет сократить временные затраты в 3-4 раза (с более 4 часов до 1 часа), повысить достоверность (на 20-40%) принимаемых специалистом по ИБ решений при оценке и анализе актуальных угроз БИ и уязвимостей ПО объектов КИИ.

5. Практическая значимость полученных результатов заключается в следующем:

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 временные затраты в 3-4 раза (с более 4 часов до 1 часа), повысить достоверность (на 20-40%, согласованность экспертной оценки и ИСППР F1 составила 0,59) 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.

6. Ценность научных работ заключается в том, что в результате выполненных исследований:

– разработан метод и алгоритмы оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО, архитектуры и программные модулей исследовательского прототипа ИСППР;

– решены прикладные задачи оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ;

– применение предложенных решений позволяет повысить оперативность, полноту и достоверность оценки актуальных угроз БИ и уязвимостей ПО.

7. Обоснование выбранной специальности и отрасли науки диссертации

Диссертация «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов» 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» – проведена оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов;

п.3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса» – разработан метод и алгоритм оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО АСУ ТП с использованием технологии семантического анализа текстов;

п.8 «Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения» – разработан алгоритм построения графовой модели сценария реализации угроз БИ для определения риска ИБ и защищенности объектов КИИ;

п.15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» – разработаны архитектура и состав программных модулей ИСППР в процессе оценки угроз БИ и уязвимостей ПО объектов КИИ.

Отрасль науки – технические науки, поскольку приведенные результаты исследований в области оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ дают существенный технический эффект при их использовании и внедрении.

8. Полнота изложения материалов диссертации

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.

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. и др. 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. Тематическое моделирование и суммаризация текстов в области кибербезопасности // Вопросы кибербезопасности. – 2023. – № 2(54). – С. 2-22.

Другие публикации по теме диссертации

5. Васильев В. И., Кучкарова Н. В., Муслимова К. И. Методика определения актуальных угроз кибербезопасности АСУ ТП на основе стандарта ГОСТ Р 62443 //Сборник избранных статей по материалам научных конференций ГНИИ" Нацразвитие". – 2018. – С. 122-126.

6. Кучкарова Н. В., Васильев В. И., Вульфин А. М. Сравнительный анализ систем классификаций АСУ ТП объектов критической информационной инфраструктуры //Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2019). – 2019. – С. 214-219.

7. Кучкарова Н. В., Васильев В. И. 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

8. 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. – 2020. – С. 55-64.

9. 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. – 2021. – С. 144.

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

11. Васильев В.И., Вульфин А.М., Кучкарова Н.В. 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.

12. Кучкарова Н. В. Применение моделей интеллектуального анализа текстов при оценке угроз информационной безопасности //Современные проблемы цивилизации и устойчивого развития в информационном обществе. – 2021. – С. 178-184.

Свидетельства о государственной регистрации программы для ЭВМ

13. 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.

14. 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.

Диссертация Кучкаровой Наили Вакилевны соответствует п. 14 Положения о порядке присуждения ученых степеней:

– отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации;

– соискатель ссылается на авторов и источники заимствования.

Диссертация «Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов» Кучкаровой Наили Вакилевны рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заключение принято на заседании кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

Присутствовало на заседании 31 человек, в том числе 15 докторов наук.

Результаты голосования: «за» – 31 человек, «против» – нет, «воздержалось» – нет.

Протокол № 13 от «31» мая 2023 г.

Заведующий кафедрой
вычислительной техники и защиты информации,
д-р физ.-мат. наук, проф. В.М. Картак

Ученый секретарь
Ученого совета университета Н.В Ефименко