УТВЕРЖДАЮ
Проректор по науке ФГБОУ ВО
«Уфимский университет науки и технологий»
д-р физ.-мат. наук, профессор
_____ С.А. Мустафина
«11» 12 2023 г.

ЗАКЛЮЧЕНИЕ

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

Диссертация Кирилловой А.Д. «Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования» 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 Кириллова Анастасия Дмитриевна работала в должности ассистента кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации.

В 2017 г. окончила магистратуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 09.04.01 «Информатика и вычислительная техника», профиль «Безопасность и защита информации».

В 2022 г. окончила аспирантуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 10.06.01 «Информационная безопасность», профиль 2.3.6. Методы и системы защиты информации, информационная безопасность.

Справка об обучении 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 Кирилловой Анастасии Дмитриевны 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 количественной оценки рисков ИБ АСУ ТП промышленных объектов и обеспечения интеллектуальной поддержки принятия решений на этапе выбора эффективных контрмер по защите информации, имеющих важное практическое значение.

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

– нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП и алгоритм ее построения;

– метод количественной оценки рисков ИБ АСУ ТП на основе нечеткого когнитивного моделирования сценариев атак;

– алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе иерархии вложенных нечетких когнитивных моделей и сценарного моделирования атак;

– архитектура и программная реализация разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов в составе исследовательского прототипа ИСППР;

– методика и практические рекомендации применения разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов при решении прикладных задач.

В перечисленных в автореферате работах соискателем лично получены следующие результаты:

– в работах [2-4, 10, 11, 17, 22, 26] разработана и исследована нечеткая когнитивная модель количественной оценки рисков ИБ АСУ ТП промышленных объектов в условиях воздействия факторов неопределенности и разброса экспертных оценок и алгоритм ее построения;

– в работах [10-12, 19-21, 24-26, 28] предложен метод сценарного моделирования атак, реализующий заключительные этапы Методики ФСТЭК России, основанный на построении и анализе комплекса моделей объекта и действий нарушителя, позволяющих формализовать и декомпозировать возможные сценарии проведения атак в выделенной зоне безопасности АСУ ТП промышленного объекта с количественной оценкой соответствующих рисков ИБ;

– в работах [5-7, 12, 16, 19, 20, 23, 27, 28] разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе иерархии вложенных нечетких когнитивных моделей и сценарного моделирования атак;

– в работах [1, 9, 14, 15, 29-31] разработана архитектура и программная реализация разработанного метода, моделей, алгоритмов и инструментальных

средств оценки рисков ИБ АСУ ТП промышленных объектов в составе исследовательского прототипа ИСППР.

– в работах [7, 8, 13, 23, 27] представлены практические рекомендации применения разработанного метода, моделей, алгоритмов и инструментальных средств оценки рисков ИБ АСУ ТП промышленных объектов при решении прикладных задач.

Опубликованные работы полностью отражают основное содержание диссертационной работы. Все основные положения и результаты, выносимые на защиту, отражены в публикациях автора: по главе 1 – [2-4, 12, 13-15, 17, 24]; по главе 2 – [2-4, 10, 11, 17, 22, 26]; по главе 3 – [5-7, 10-12, 16, 19-21, 23-28]; по главе 4 – [1, 8, 10, 11, 16, 18, 21, 23, 27, 29-31]. Пять работ 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:

1) корректной постановкой задач и выбором методов исследования;

2) результатами практического применения разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП при решении ряда прикладных задач;

3) результатами сравнительного анализа количественных оценок рисков ИБ, полученных по итогам когнитивного моделирования, и экспертных оценок рисков ИБ АСУ ТП промышленного объекта;

4) апробацией на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях.

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

4. Научная новизна работы заключается в следующем:

– Предложена нечеткая когнитивная модель оценки рисков ИБ АСУ ТП промышленных объектов и алгоритм ее построения на основе иерархии вложенных серых нечетких когнитивных карт для зональных моделей АСУ ТП, которые, в отличие от существующих, отражают особенности многоуровневой организации АСУ ТП промышленных объектов (многообразие применяемых протоколов, программного и аппаратного обеспечения, продолжительный жизненный цикл, иерархическую структуру объекта с различными уровнями логической и физической изоляции, специфику применения используемых средств защиты), позволяя формализовать сценарии компьютерных атак с требуемым уровнем их детализации в пределах выделенных зон, что позволяет повысить достоверность и обоснованность количественной оценки рисков ИБ и, как следствие, обеспечить выбор эффективных контрмер.

– Разработан метод количественной оценки рисков ИБ АСУ ТП на основе моделирования сценариев атак с использованием технологий когнитивного моделирования и методов машинного обучения, отличающийся

применением шаблонов открытых баз знаний для формализации описания объекта атаки, перечня актуальных угроз и уязвимостей в виде иерархии графовых моделей и баз данных, что позволяет автоматизировать и унифицировать их представление в виде последовательности действий, совокупности методов и средств (тактик и техник), позволяющих потенциальному нарушителю реализовать атаку на АСУ ТП промышленного объекта.

– Разработаны алгоритмы и методика количественной оценки рисков ИБ АСУ ТП на основе построения сценариев атак, отличающиеся применением нечеткого когнитивного моделирования и методов машинного обучения для оценки уровня защищенности выделенных зон АСУ ТП промышленного объекта, что позволяет определить оптимальное (рациональное) распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений.

– Разработана архитектура исследовательского прототипа интеллектуальной системы поддержки принятия решений и программная реализация инструментальных средств автоматизации моделирования сценариев атак и оценки рисков ИБ АСУ ТП промышленных объектов, применение которых позволяет повысить оперативность и достоверность оценки рисков ИБ и, в конечном итоге, повысить эффективность выбора контрмер на этапах проектирования и внедрения комплексных систем защиты информации АСУ ТП промышленного объекта.

5. Практическая значимость полученных результатов заключается в следующем:

Применение программной реализации разработанного метода, моделей и алгоритмов оценки рисков ИБ АСУ ТП позволило после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшить на 70-80 % разброс экспертных оценок, а также повысить уровень защищенности АСУ ТП конкретного промышленного объекта, снизить предварительную оценку стоимости эксплуатации предлагаемых защитных мер. Временные затраты на моделирование сценариев атак и оценку рисков ИБ при этом сократились в 2,5 раза.

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

– разработана методика и инструментальные средства автоматизации моделирования сценариев атак и оценки рисков ИБ в составе ИСППР;

– решены прикладные задачи оценки рисков ИБ АСУ ТП промышленных объектов;

– повышена обоснованность и достоверность количественных оценок рисков ИБ с учетом воздействия факторов неопределенности.

7. Обоснование выбранной специальности и отрасли науки диссертации

Диссертация «Оценка рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования» соответствует 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».

Отрасль науки – технические науки, поскольку приведенные результаты исследований в области количественной оценки рисков ИБ АСУ ТП промышленных объектов дают существенный технический эффект при их использовании и внедрении.

8. Полнота изложения материалов диссертации

Основные результаты диссертации опубликованы в 31 работе, в том числе 8 статьях в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, либо в научных изданиях, индексируемых базой данных RSCI, 4 научных работах в изданиях, включенных в базу Scopus, 16 статьях в других изданиях. Получено 3 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. Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами / В.И. Васильев, В.Е. Гвоздев, М.Б. Гузаиров, А.Д. Кириллова // Информация и безопасность. – 2017. – Т. 20, № 4. – С. 618–623.

2. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова // Информационные технологии. – 2018. – Т. 24, № 10. – С. 657–664. – DOI: 10.17587/it.24.657-664.

3. Васильев В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4(30). – С. 66–74. – DOI: 10.14529/secur180410.

4. Об интерпретируемости нечетких когнитивных моделей на этапе оценки рисков инновационных проектов / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, Л.Р. Черняховская // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 4(34). – С. 45–57. – DOI: 10.14529/secur190406.

5. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В.И. Васильев, А.М. Вульфин, А.Д. Кириллова, Н.В. Кучкарова // Системы управления, связи и безопасности. – 2021. – № 3. – С. 110–134. – DOI: 10.24412/2410-9916-2021-3-110-134.

6. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. – 2021. – № 2(42). – С. 2–16. – DOI: 10.21681/2311-3456-2021-2-2-16.

7. Васильев В.И., Вульфин А.М., Кириллова А.Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2(37). – С. 1–18. – DOI 10.26102/2310-6018/2022.37.2.022.

8. Комплексная оценка выполнения требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами / В.И. Васильев, А.М. Вульфин, М.Б. Гузаиров, А.Д. Кириллова // Инфокоммуникационные технологии. – 2017. – Т. 15, № 4. – С. 319–325. – DOI: 10.18469/ikt.2017.15.4.02.

Публикации в изданиях, включенных в международную базу Scopus

9. Decision support system in the task of ensuring information security of automated process control systems / A.D. Kirillova, V.I. Vasilyev, A.V. Nikonov, V.V. Berkholts // CEUR Workshop Proceedings DS-ITNT 2019 – Proceedings of the Data Science Session at the 5th International Conference on Information Technlogy and Nanotechnology. – 2019. – P. 477–486. – DOI: 10.18287/1613-0073-2019-2416-477-486.

10. Secure Data Exchange in the Industrial Internet of Things Network of the Fuel and Energy Complex / E.R. Hajrullin, A.M. Vulfin, K.V. Mironov, A.I. Frid, M.B. Guzairov, A.D. Kirillova // Proceedings ICOECS 2020 International Conference on Electrotechnical Complexes and Systems. USATU, Ufa, Russia 27-30 October 2020. – IEEE. – 2020. – P. 353–358. – DOI: 10.1109/ICOECS50468.2020.9278491.

11. Algorithms for detecting network attacks in an enterprise industrial network based on data mining algorithms / A.M. Vulfin, V.I. Vasilyev, S.N. Kuharev, E.V. Homutov, A.D. Kirillova // International Scientific and Practical Conference “Information Technologies and Intelligent Decision Making Systems” (ITIDMS-II 2021). – Journal of Physics: Conference Series. – 2021. –Vol. 2001. – 012004. – DOI: 10.1088/1742-6596/2001/1/012004.

12. Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS Score / Vasilyev V.I., Kirillova A.D., Vulfin A.M., Nikonov A.V. // 2021 International Conference on Information Technology and Nanotechnology (ITNT). – IEEE. – 2021. – P. 1–6. – DOI: 10.1109/ITNT52450.2021.9649191.

Другие публикации по теме диссертации

13. Кириллова А.Д. О реализации системы требований ФСТЭК к защите информации в инфокоммуникационных системах специального назначения // Материалы Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: УГАТУ. – 2016. – Т. 5. – С. 213–215.

14. Кириллова А.Д. Применение экспертной системы поддержки принятия решений в аудите информационной безопасности АСУ ТП // Труды Шестой Международной научной конференции «Информационные технологии и системы». – 2017. – С. 129–131.

15. Кириллова А.Д. Экспертная система аудита информационной безопасности АСУ ТП // Материалы V Всероссийской конференции «Информационные технологии интеллектуальной поддержки принятия решений». – 2017. – Т. 2. – С. 172–175.

16. Кириллова А.Д., Васильев В.И. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП // Материалы VII Всероссийской заочной Интернет-конференции «Проблемы информационной безопасности». – Ростов-на-Дону: Издательство ООО «АзовПринт». – 2018. – С. 138–142.

17. Analysis of confidential data protection in critical information infrastructure and the use of biometric, neural network and cryptographic algorithms (standards review and perspectives) / V.I. Vasilyev, A.D. Kirillova, A.E. Sulavko, S.S. Zhumazhanova // Труды Седьмой Всероссийской научной конференции с международным участием «Информационные технологии и системы». – 2019. – С. 193–197.

18. Decision support system for ensuring information security of an automated process control system / A.D. Kirillova, V.I. Vasilyev, A.V. Nikonov, V.V. Berkholts // V международная конференция и молодежная школа «Информационные технологии и нанотехнологии». – 2019. – Т. 4. Науки о данных. – С. 391–398.

19. Анализ защищенности системы сбора, хранения и обработки телеметрической информации о состоянии бортовых систем летательного аппарата / М.Б. Гузаиров, А.И. Фрид, А.М. Вульфин, В.В. Берхольц, А.Д. Кириллова // Вестник УГАТУ. – 2019. – Т. 23, № 4(86). – С. 132–146.

20. Анализ рисков обеспечения целостности телеметрической информации с использованием технологии когнитивного моделирования / В.И. Васильев, А.М. Вульфин, В.В. Берхольц, А.Д. Кириллова, С.М. Бельский // Вестник УГАТУ. – 2019. – Т. 23, № 4(86). – С. 122–131.

21. Система обнаружения атак в беспроводных сенсорных сетях промышленного интернета вещей / В.И. Васильев, А.М. Вульфин,

В.М. Картак, А.Д. Кириллова, К.В. Миронов // Труды ИСА РАН. – 2019. – Т. 69, № 4. – С. 70–78. – DOI: 10.14357/20790279190409.

22. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности / М.Б. Гузаиров, А.М. Вульфин, В.М. Картак, А.Д. Кириллова, К.В. Миронов // Труды ИСА РАН. – 2019. – Т. 69, № 4. – С. 62–69. – DOI: 10.14357/20790279190408.

23. Васильев В.И., Кириллова А.Д., Вульфин А.М. Методы управления рисками кибербезопасности АСУ ТП промышленных объектов // Труды Восьмой Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений». – 2020. – Т. 1. – С. 185–191.

24. Кириллова А.Д. Анализ проекта методики моделирования угроз безопасности информации ФСТЭК России // Материалы XIV Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: РИК УГАТУ. – 2020. – С. 20.

25. Васильев В.И., Кириллова А.Д., Вульфин А.М. Моделирование кибератак на объекты АСУ ТП с помощью нечетких когнитивных карт // Приоритетные направления развития науки и технологий: доклады XXVIII международной науч.-практич. конф.; под общ. ред. В.М. Панарина. – Тула: Инновационные технологии. – 2021. – С. 132–136.

26. Modeling the cyber attacks vector based on fuzzy cognitive maps / V.I. Vasilyev, A.D. Kirillova, A.M. Vulfin, A.V. Nikonov // Сборник трудов VII Международной конференции и молодежной школы «Информационные технологии и нанотехнологии» (ИТНТ-2021). – 2021. – Т. 3. – С. 031372

27. Система проактивной защиты промышленного объекта на основе алгоритмов машинного обучения / В.И. Васильев, А.Д. Кириллова, А.М. Вульфин, А.И. Фрид // Сборник докладов III Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (FISP-2021), Ставрополь, 30 ноября 2021 года. – С. 24-30.

28. Кириллова А.Д. Моделирование вектора атаки в базисе нечетких когнитивных карт с учетом оценок CVSS // Материалы XV Всероссийской молодежной научной конференции «Мавлютовские чтения». – Уфа: УГАТУ. – 2021. – С. 229–235.

Свидетельства о государственной регистрации программы для ЭВМ

29. Программа моделирования нечетких когнитивных карт: Свидетельство о государственной регистрации программы для ЭВМ 2021615069 Российская Федерация / А.М. Вульфин, Р.Р. Ягафаров, А.Д. Кириллова, В.И. Васильев. – № 2021614134; заявл. 26.03.2021; опубл. 02.04.2021.

30. Программа анализа уязвимостей программного обеспечения на основе технологий интеллектуального анализа и обработки естественного языка: Свидетельство о государственной регистрации программы для ЭВМ 2021615080 Российская Федерация / А.М. Вульфин, А.В. Никонов,

Д.Н. Габбасова, Н.В. Кучкарова, В.И. Васильев, А.Д. Кириллова. – № 2021614120; заявл. 26.03.2021; опубл. 02.04.2021.

31. Программа анализа и моделирования кибератак на основе металшаблонов в нечетком когнитивном базисе: Свидетельство о государственной регистрации программы для ЭВМ 2021619894 Российская Федерация / А.Д. Кириллова, А.М. Вульфин, Р.Р. Ягафаров, Л.Ю. Зиязетдинова. – № 2021618903; заявл. 07.06.2021; опубл. 18.06.2021.

Диссертация Кирилловой Анастасии Дмитриевны 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 рисков информационной безопасности АСУ ТП промышленных объектов с использованием методов когнитивного моделирования» Кирилловой Анастасии Дмитриевны 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 20 человек, в том числе 7 докторов наук.

Результаты голосования: «за» – 20 человек, «против» – нет, «воздержалось» – нет.

Протокол № 10 от «27» марта 2023 г.

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

Подпись Картаков В.М.
Удостоверяю «11» 04 2023 г.
Начальник общего отдела УУНиТ