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

ЗАКЛЮЧЕНИЕ

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

Диссертация «Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем» 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 Шамсутдинов Ринат Рустемович проходил обучение в аспирантуре ФГБОУ ВО «Уфимский государственный авиационный технический университет» Министерства науки и высшего образования Российской Федерации, работал по совместительству в рамках гранта РФФИ № 20-37-90024 «Гибридная интеллектуальная система мониторинга информационной безопасности на основе алгоритмов искусственных иммунных систем и нечетких нейронных сетей» в должности оператора электронно-вычислительных и вычислительных машин кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет» Министерства науки и высшего образования Российской Федерации.

В 2018 г. окончил магистратуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 10.04.01 Информационная безопасность, профиль: Информационная безопасность.

В 2022 г. окончил аспирантуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 09.06.01 Информатика и вычислительная техника, профиль: Системный анализ, управление и обработка информации.

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 Шамсутдинова Рината Рустемовича является законченной научно-квалификационной работой по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, соответствующей п. 9 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), в которой содержатся научно обоснованные результаты решения задачи мониторинга информационной безопасности сети промышленного Интернета вещей с использованием механизмов искусственных иммунных систем, имеющие важное практическое значение.

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

1. Результаты анализа современного состояния исследований в области мониторинга сетей промышленного Интернета вещей с использованием технологий искусственного интеллекта, концепция построения интеллектуальной системы мониторинга информационной безопасности (далее – ИБ) промышленного Интернета вещей.

2. Алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием адаптивных механизмов искусственных иммунных систем.

3. Алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием ансамбля методов машинного обучения и подсистемы корреляции событий ИБ.

4. Архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей, результаты ее применения при решении прикладных задач.

В перечисленных в автореферате работах соискателем лично получены следующие результаты:

– в работах [3, 6, 8-9, 17] проведён анализ современного состояния исследований в области мониторинга сетей промышленного Интернета вещей с использованием технологий искусственного интеллекта;

– в работах [1-3, 6-9, 13-14] разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета

вещей с использованием адаптивных механизмов искусственных иммунных систем;

– в работах [2, 4, 5, 9] разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием ансамбля методов машинного обучения и подсистемы корреляции событий ИБ;

– в работе [5] представлена архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей, результаты ее применения при решении прикладных задач.

Опубликованные работы полностью отражают основное содержание диссертационной работы. Основные положения и результаты, выносимые на защиту, отражены в публикациях автора: по главе 1 – [3, 6, 8-9, 17]; по главе 2 – [1-3, 6-9, 13-14]; по главе 3 – [2, 4, 5, 9]; по главе 4 – [5]. 5 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:

– корректным использованием основных теоретических положений, методов проведения вычислительных экспериментов;

– непротиворечивостью полученных результатов, а также их экспертной оценкой и степенью повторяемости;

– апробацией на научных конференциях;

– публикацией результатов в ведущих рецензируемых научных изданиях из Перечня ВАК, а также в научных изданиях, индексируемых в Scopus и Web of Science.

4. Научная новизна работы заключается в следующем:

1. Предложена концепция построения интеллектуальной системы мониторинга информационной безопасности (ИБ) промышленного Интернета вещей на основе многоагентной платформы гибридной многоуровневой интеллектуальной системы обнаружения атак и аномалий сетевого трафика IIoT, отличающаяся интеграцией механизмов искусственных иммунных систем, методов машинного обучения, подсистемы корреляции событий информационной безопасности (SIEM-системы), что позволяет повысить полноту и точность выявления внешних и внутренних угроз безопасности информации.

2. Разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе адаптивных механизмов искусственных иммунных систем (ИИС), отличающиеся интеграцией различных подходов в рамках теории ИИС (негативная селекция, клональный отбор, теория опасности, теория иммунной сети) и модификации известных алгоритмов клональной селекции, дендритных клеток и обновления детекторов, что позволяет в совокупности

существенно снизить уровень принятия ошибочных решений, выявлять в том числе новые, ранее неизвестные системе угрозы безопасности информации.

3. Разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе использования ансамбля методов машинного обучения и подсистемы корреляции событий ИБ, отличающиеся использованием специфического иммунного ответа ИИС совместно с другими алгоритмами искусственного интеллекта (нейронные сети, алгоритм случайного леса), что обеспечивает дифференцированный подход к обнаружению различных типов атак и аномалий (включая ранее неизвестные) и позволяет повысить эффективность функционирования системы мониторинга ИБ в целом.

4. Разработана архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей на основе комитета классификаторов, отличающаяся использованием многоагентного подхода к построению многоуровневых распределенных гибридных интеллектуальных систем, что позволяет более полно использовать преимущества применения различных технологий интеллектуального анализа данных, учесть особенности структурно-функциональной организации (состава подсистем) объекта мониторинга, многообразие угроз безопасности информации и уязвимостей программного обеспечения, дополняя полученную информацию текущими данными от взаимодействующей SIEM-системы.

5. Практическая значимость полученных результатов заключается в следующем:

– разработаны программные модули исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей;

– разработана методика ее применения для обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей;

– применение предложенных модулей позволяет обеспечить точность обнаружения компьютерных атак и аномалий сетевого трафика на уровне 98-99% на тестовых наборах данных, выявлять в том числе новые, ранее неизвестные системе угрозы безопасности информации;

– взаимодействие предложенных решений с существующими SIEM-системами позволяет при этом дополнительно повысить уровень достоверности принимаемых решений в процессе мониторинга ИБ сетей промышленного Интернета вещей.

6. Ценность научной работы заключается в том, что в результате выполненных исследований:

– предложена концепция построения интеллектуальной системы мониторинга ИБ промышленного Интернета вещей,

– предложены алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием адаптивных механизмов ИИС;

– предложены алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием ансамбля методов машинного обучения и подсистемы корреляции событий ИБ;

– предложена архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей.

7. Обоснование выбранной специальности и отрасли науки диссертации

Диссертация «Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем» 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» – разработаны методика и алгоритмы обнаружения и классификации компьютерных атак, представляющих угрозы безопасности информации сетей промышленного Интернета вещей;

п. 6 «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях» – разработана архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ сетей промышленного Интернета вещей;

п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» – разработаны алгоритмы обнаружения компьютерных атак и сетевых аномалий, архитектура исследовательского прототипа интеллектуальной системы мониторинга для усовершенствования существующих систем обнаружения вторжений, систем мониторинга и применения в качестве новых, отдельных решений.

Отрасль науки – технические науки, поскольку приведенные результаты исследований в области мониторинга информационной безопасности сетей промышленного Интернета вещей дают существенный технический эффект при их использовании и внедрении.

8. Полнота изложения материалов диссертации

Основные результаты диссертации опубликованы в 17 работах, в том числе в 6 статьях в научных изданиях из Перечня рецензируемых

научных изданий, рекомендованных ВАК, 3 статьях в изданиях, индексируемых в Web of Science, одна из которых индексируется в Scopus; 8 статьях в других изданиях.

Статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК

1. Васильев В.И., Шамсутдинов Р.Р. Интеллектуальная система обнаружения сетевых атак на основе механизмов искусственной иммунной системы // Моделирование, оптимизация и информационные технологии. – 2019. – Т. 7. – № 1 (24). – С. 521-535. DOI: 10.26102/2310-6018/2019.24.1.010.
2. Васильев В.И., Шамсутдинов Р.Р. Интеллектуальная система анализа инцидентов информационной безопасности (на основе методологии SIEM-систем с применением механизмов иммунокомпьютинга) // Моделирование, оптимизация и информационные технологии. – 2019. – № 1 (24). – Т. 7. – С. 536-547. DOI: 10.26102/2310-6018/2019.24.1.011.
3. Васильев В.И., Гвоздев В.Е., Шамсутдинов Р.Р. Обнаружение аномалий в системах промышленного Интернета вещей на основе искусственной иммунной системы // Доклады ТУСУР. – 2021. – №4 (24). – С. 40-45.
4. Васильев В.И., Вульфин А.М., Гвоздев В.Е., Шамсутдинов Р.Р. Гибридная интеллектуальная система обнаружения атак на основе комбинации методов машинного обучения // Моделирование, оптимизация и информационные технологии. – 2021. – № 9 (3). – С. 1-11.
5. Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Shamsutdinov R.R. Hybrid intrusion detection system with the use of a classifiers committee // Modeling, Optimization and Information Technology. – 2022. – № 10 (4). – С. 1-11.
6. Васильев В.И. Вульфин А.М. Гвоздев В.Е. Шамсутдинов Р.Р. Комплексирование механизмов искусственных иммунных систем в составе интегрированной системы обнаружения атак на промышленный Интернет вещей // Моделирование, оптимизация и информационные технологии. – 2022. – № 10 (4). – С. 1-12.

Публикации в изданиях, индексируемых в Web of Science и Scopus

7. Vasilyev V., Shamsutdinov R. Distributed Intelligent System of Network Traffic Anomaly Detection Based on Artificial Immune System // Proceedings of the 7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019), 28-30 may 2019., Ufa. Advances in Intelligent System Research. – Vol. 166. – P. 40-45. DOI:10.2991/itids-19.2019.7. – WOS:000573715000007 (Web of Science)
8. Vasilyev V., Shamsutdinov R. Providing information security on the base of artificial immune system for industrial Internet of things: Proceedings of the 8th scientific conference on Information technologies for intelligent decision making support (ITIDS'2020) // Advances in Intelligent Systems Research. – 2020. – vol. 174. – P. 212-217 (ITIDS 2020). – WOS:000678794200041 (Web of Science).

9. Vasilyev V., Shamsutdinov R. Security Analysis of Wireless Sensor Networks Using SIEM and Multi-agent Approach // Proceedings of the Global Smart Industry Conference (GloSIC'2020), 17-19 November 2020, available at: https://ieeexplore.ieee.org/document/9267830. – WOS:000646231600048. – Scopus:2-s2.0-85098633831 (Web of Science, Scopus)

Другие публикации по теме диссертации

10. Шамсутдинов Р.Р. Аттестация объектов информатизации по требованиям безопасности информации в Российской Федерации // Инновационное развитие. – 2017. – № 1 (6). – С. 36-37.

11. Шамсутдинов Р.Р. Обеспечение безопасности систем облачных вычислений // Инновационное развитие. – 2017. – № 1 (6). – С. 39-40.

12. Анянов В.М., Гилязев И.Н., Шамсутдинов Р.Р. Интеллектуальные системы обнаружения вторжений на основе искусственной нейронной сети // Аллея науки. – 2018. – № 2 (18). – С. 219-227.

13. Шамсутдинов Р.Р. Разработка подсистемы анализа данных и выявления аномалий на основе концепции искусственной иммунной системы // Проблемы информационной безопасности: материалы VII Всероссийской заочной Интернет-конференции 20-21 февраля 2018 г. – Ростов-на-Дону: АзовПринт, 2018. – 192 с.

14. Васильев В.И., Шамсутдинов Р.Р. Распределенная система обнаружения атак на основе механизмов искусственной иммунной системы // Информационные технологии интеллектуальной поддержки принятия решений: Труды VI Всероссийской научной конференции (с приглашением зарубежных ученых) 28-31 мая 2018 г., Т. 1. – Уфа: РИК УГАТУ, 2018. – 301 с.

15. Шамсутдинов Р.Р. Обеспечение безопасности информационных систем: современное состояние // European Research: сборник статей XIX Международной научно-практической конференции (7 февраля 2019 г.). – Пенза: Наука и Просвещение. – 2019. – С. 31-33.

16. Шамсутдинов Р.Р. Развертывание и тестирование системы мониторинга сетевого трафика Cisco Lancope StealthWatch в корпоративной информационной системе // Сборник статей международной заочной научной специализированной конференции International scientific review of the problems of the technical sciences, Mathematics and Computer Science (Бостон, США, Февраль 12-13, 2019). – Бостон, 2019. – С. 50-52.

17. Васильев В.И., Шамсутдинов Р.Р. Вопросы обеспечения безопасности интеллектуальной среды окружения промышленного Интернета вещей [Электронный ресурс] // Сборник статей XIV Всероссийской молодежной научной конференции Мавлютовские чтения. – Уфа: УГАТУ, 2020. – Т. 5. – Ч. 2. – С. – URL: https://www.elibrary.ru/item.asp?id=44619516 (дата обращения: 26.05.2023).

Диссертация Шамсутдинова Рината Рустемовича 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 «Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем» Шамсутдинова Рината Рустемовича рекомендуется к защите на соискание ученой степени кандидата технических наук по научной 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 14 докторов наук.

Результаты голосования: «за» – 30 человек, «против» – нет, «воздержалось» – 1 человек.

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