ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.2.479.07, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело №_____

решение диссертационного совета от 22.09.2023 №12

О присуждении Шамсутдинову Ринату Рустемовичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем» по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 03.07.2023 г. протокол № 9 диссертационным советом 24.2.479.07, созданным на базе федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации, 450076, г. Уфа, ул. Заки Валиди, 32, созданного приказом Министерства науки и высшего образования Российской Федерации № 542/нк от 24.03.2023 г.

Соискатель – Шамсутдинов Ринат Рустемович, 29 октября 1993 года рождения. В 2016 году окончил ФГБОУ ВО «Башкирский государственный университет» по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

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

В 2022 году окончил аспирантуру ФГБОУ ВО «Уфимский государственный авиационный технический университет» по направлению подготовки 09.06.01 Информатика и вычислительная техника.

Работает в должности младшего сервис-инженера Дирекции 1С в ООО «Газпромнефть – Цифровые решения».

Диссертация выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования Российской Федерации. В период обучения в аспирантуре ФГБОУ ВО «Уфимский государственный авиационный технический университет» Шамсутдинов Р.Р. проводил исследования в рамках индивидуального гранта РФФИ № 20-37-90024 «Гибридная интеллектуальная система мониторинга информационной безопасности на основе алгоритмов искусственных иммунных систем и нечетких нейронных сетей», а также в рамках гранта РФФИ № 20-08-00668 «Разработка и исследование методологии, моделей и методов комплексного анализа и управления рисками кибербезопасности АСУ ТП промышленных объектов с использованием технологии когнитивного моделирования и интеллектуального анализа данных».

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

Официальные оппоненты:

1. Доктор технических наук, доцент Сычугов Алексей Алексеевич, директор Института прикладной математики и компьютерных наук, заведующий кафедрой информационной безопасности ФГБОУ ВО «Тульский

государственный университет» Министерства науки и высшего образования Российской Федерации;

2. Кандидат технических наук, доцент Бурлаков Михаил Евгеньевич, доцент кафедры безопасности информационных систем ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева» Министерства науки и высшего образования Российской Федерации

дали положительные отзывы на диссертацию.

Ведущая организация – федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, г. Самара в своем положительном отзыве, подписанном заведующим кафедрой информационной безопасности, доктором технических наук, профессором Карташевским Вячеславом Григорьевичем, утверждённом проректором по научной работе, доктором технических наук, профессором Горячкиным Олегом Валерьевичем, указала, что диссертация Шамсутдинова Рината Рустемовича на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны концепция построения, алгоритмы функционирования, архитектура, программные модули и методика применения интеллектуальной системы мониторинга информационной безопасности (ИБ) промышленного Интернета вещей, применение которой позволяет повысить эффективность обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей.

Диссертация соответствует требованиям пунктов 9-11, 13-14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими

изменениями), а ее автор, Шамсутдинов Ринат Рустемович, заслуживает присуждения ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 17 опубликованных работ по теме диссертации, в том числе 6 статей в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 3 – в изданиях, индексируемых в Web of Science (одна из них индексируется в Scopus), 8 – в прочих изданиях. 5 публикаций выполнены соискателем единолично, остальные – при непосредственном участии соискателя.

Общий объем публикаций – 7,6 п.л., авторский вклад – 4,4 п.л.

Наиболее значимые работы по теме диссертации:

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. (ВАК).

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. – Т. 7, № 1 (24). – С. 536-547. – DOI: 10.26102/2310-6018/2019.24.1.011. (ВАК).

3. Васильев В.И., Вульфин А.М., Гвоздев В.Е., Шамсутдинов Р.Р. Гибридная интеллектуальная система обнаружения атак на основе комбинации методов машинного обучения [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9, № 3 (34). – URL: https://moitvivt.ru/ru/journal/pdf?id=1032. – DOI: 10.26102/2310-6018/2021.34.3.019. (ВАК).

4. Васильев В.И., Гвоздев В.Е., Шамсутдинов Р.Р. Обнаружение аномалий в системах промышленного Интернета вещей на основе искусственной иммунной системы // Доклады ТУСУР. – 2021. – Т. 24, № 4. – С. 40-45. – DOI: 10.21293/1818-0442-2021-24-4-40-45. (ВАК).

5. Vasilyev V.I., Vulfin A.M., Gvozdev V.E., Shamsutdinov R.R. Hybrid intrusion detection system with the use of a classifiers committee [Электронный ресурс] // Modeling, optimization and information technology. – 2022. – Vol. 10, №4 (39). – URL: https://moitvivt.ru/ru/journal/pdf?id=1267. – DOI: 10.26102/2310-6018/2022.39.4.020. (ВАК).

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 [Электронный ресурс] // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10, №4 (39). – URL: https://moitvivt.ru/ru/journal/pdf?id=1240. – DOI: 10.26102/2310-6018/2022.39.4.001. (ВАК).

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), May 28-29, 2019, Ufa, Russia //Advances in intelligent system research. – 2019. – 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), October 06-09, 2020, Ufa, Russia //Advances in intelligent systems research. – 2020. – Vol. 174. – P. 212-217. – DOI: 10.2991/aisr.k.201029.041. – 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), November 17-19, 2020, Chelyabinsk, Russia. – 2020. – P. 291-296. – URL: https://ieeexplore.ieee.org/document/9267830. – DOI: 10.1109/GloSIC50886.2020.9267830. – WOS:000646231600048. – Scopus:2-s2.0-85098633831 (Web of Science, Scopus).

В диссертации отсутствуют недостоверные сведения об опубликованных соискателем ученой степени работах.

На диссертацию и автореферат поступили положительные отзывы:

– **ведущей организации**, ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики». *Замечания*: **1.** В первой главе можно было подробнее рассмотреть классификацию существующих сетевых атак. **2.** Не указано, в каком формате хранятся данные перехваченного сетевого трафика. **3.** Недостаточно подробно освещены механизмы естественной иммунной системы человека, которые имитирует искусственная иммунная система. **4.** Из текста диссертации не вполне ясно, должна ли предлагаемая система мониторинга ИБ использоваться в качестве основной системы обнаружения атак и аномалий IIoT, или же в качестве дополнения к существующим системам. **5.** Не указан язык программирования, на котором реализованы разработанные программные модули ИИС (искусственной иммунной системы). **6.** Не указано, существует ли возможность добавления в систему информации об известных атаках не на этапе ее первичного обучения, а непосредственно в процессе ее эксплуатации. **7.** В тексте диссертации не сказано, существует ли возможность у администратора предлагаемой системы в случае ошибочной классификации ею легитимного сетевого взаимодействия в качестве атаки или аномалии, скорректировать последующее поведение системы во избежание ее самообучения на примере данного ошибочного решения;

– **официального оппонента**, доктора технических наук, доцента Сычугова Алексея Алексеевича, директора Института прикладной математики и компьютерных наук, заведующего кафедрой информационной безопасности ФГБОУ ВО «Тульский государственный университет». *Замечания*: **1.** В тексте диссертации указано, что в качестве входных данных системы мониторинга ИБ используется информация с большого числа распределенных датчиков, собирающих сведения о сетевом трафике IIoT, но не описано, каким образом осуществляется сбор этих данных. **2.** Явным образом не определены используемые в тексте диссертации понятия опасного состояния и уровня опасности. **3.** Не представлена структура нейронной сети, используемой в составе комитета интеллектуальных классификаторов. **4.** В работе описано, что распределенные агенты ИИС обмениваются друг с другом обучающими данными, но не разъяснены конкретные механизм и порядок такого обмена. **5.** В диссертации говорится об интеграции разработанной системы мониторинга ИБ с внешней SIEM-системой, но недостаточно раскрыты механизмы взаимодействия этих систем. **6.** Не представлены конкретные требования к программно-аппаратному обеспечению, на котором может быть развернута предлагаемая интеллектуальная система мониторинга ИБ IIoT. **7.** Не указан язык программирования, на котором разработано ПО искусственной иммунной системы, является ли он кросс-платформенным;

– **официального оппонента**, кандидата технических наук, доцента Бурлакова Михаила Евгеньевича, доцента кафедры безопасности информационных систем ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С. П. Королева». *Замечания*: **1.** В первой главе можно было более подробно остановиться на существующих международных нормативных документах в области обеспечения ИБ промышленного Интернета вещей. **2.** Из текста работы не вполне ясно, какие существуют ограничения на реализацию и применение предложенных алгоритмов и программных средств распределенной интеллектуальной системы

мониторинга (РИСМ) ИБ IIoT (аппаратная и программная платформа, требуемые вычислительные ресурсы и др.). **3.** Не указано, должны ли агенты РИСМ проходить взаимную аутентификацию перед обменом данными. **4.** В работе рассмотрены интерфейсы агентов трёх уровней РИСМ, однако осталось неясным, возможно ли централизованное управление агентами, или агенты управляются в процессе своей работы всегда автономно. **5.** Из текста работы неясно, каким образом должно осуществляться оповещение и реагирование на выявленные атаки и аномалии сетевого трафика. **6.** При представлении результатов вычислительных экспериментов для оценки эффективности ансамбля методов машинного обучения (случайный лес, искусственная нейронная сеть) в работе приведены матрицы ошибок (несоответствий), а для искусственной иммунной системы этот инструмент не использовался, что также было бы наглядным и полезным.

Получено 8 положительных отзывов на автореферат:

– ФГБОУ ВО «Челябинский государственный университет», заведующий научно-исследовательской лабораторией «Интеллектуальные информационные технологии и системы», **д.т.н., доцент Вохминцев Александр Владиславович.** *Замечания*: **1.** В автореферате предоставлена в достаточно общем виде архитектура предлагаемой распределенной интеллектуальной системы мониторинга ИБ промышленного Интернета вещей, однако не представлена детально архитектура искусственной иммунной системы. **2.** В тексте отсутствует информация о структуре применяемой искусственной нейронной сети;

– ФГАОУ ВО «Омский государственный технический университет», заведующий кафедрой «Комплексная защита информации», **д.т.н., профессор Ложников Павел Сергеевич.** *Замечания*: **1.** В автореферате недостаточно подробно раскрыты детали реализации взаимодействия агентов искусственной иммунной системы;

– ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С. П. Королева», заведующий кафедрой программных систем, **д.т.н., доцент Востокин Сергей Владимирович.** *Замечания*: **1.** В работе аргументирован выбор искусственной иммунной системы в качестве одного из интеллектуальных классификаторов при решении задачи обнаружения сетевых атак и аномалий, но не представлено обоснования, почему в качестве двух других классификаторов выбраны искусственная нейронная сеть и алгоритм случайного леса. **2.** В одной из серий вычислительных экспериментов исследовалось поведение беспроводной сенсорной сети, но в автореферате не представлена архитектура данной сети, что обеспечило бы наглядное представление о ней;

– ФГАОУ ВО «Южный федеральный университет», доцент кафедры безопасности информационных технологий, **к.т.н., с.н.с., доцент Брюхомицкий Юрий Анатольевич.** *Замечания*: **1.** Не указано, каким образом в подсистеме дендритных клеток осуществляется анализ уровня опасности. **2.** Неясно, что из себя представляют агенты первого и второго уровней искусственной иммунной системы, реализуются ли они в составе программного обеспечения, устанавливаемого на уже существующие на объекте защиты устройства Интернета вещей или же они требуют отдельного аппаратного обеспечения;

– ФГБОУ ВО «Поволжский государственный технологический университет», заведующий кафедрой информационной безопасности, **д.т.н., профессор Сидоркина Ирина Геннадьевна.** *Замечания*: **1.** В автореферате описаны механизмы обнаружения сетевых атак и аномалий с помощью агентов искусственной иммунной системы, но не приведена блок-схема соответствующего алгоритма, что позволило бы получить более наглядное представление о его работе;

– ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники», президент, **д.т.н., профессор Шелупанов Александр**

Александрович; доцент кафедры комплексной информационной безопасности электронно-вычислительных систем, **к.т.н., доцент Новохрестов Алексей Константинович.** *Замечания*: **1.** Что вкладывается автором в понятие «эффективность систем мониторинга ИБ»? В чем она измеряется и где граница между высокой, средней и низкой эффективностью таких систем? **2.** В тексте сказано, что в основе обнаружения атак, проводимого агентами нижнего уровня искусственной иммунной системы, используется определение расстояния между анализируемой вектор-строкой и некоторыми эталонными векторами-строками, но осталось неясным, какие меры расстояния между векторами использовались автором. **3.** Неясно, какой конкретный перечень параметров сетевого трафика использовался для выявления сетевых атак и аномалий;

– ФГБОУ ВО «Казанский национальных исследовательский технический университет им. А.Н. Туполева-КАИ», профессор кафедры систем информационной безопасности, **д.т.н., профессор Катасёв Алексей Сергеевич**. *Замечания*: **1.** Представленную в автореферате схему функционирования разработанной искусственной иммунной системы следовало бы сделать более подробной. **2.** Неясно, каких образом осуществляется реагирование системы в случае выявления тех или иных видов атак и сетевых аномалий;

– ФГБОУ ВО «Воронежский государственный технический университет», заведующий кафедрой систем информационной безопасности, **д.т.н., профессор Остапенко Александр Григорьевич**; профессор кафедры систем информационной безопасности, **д.т.н., доцент Разинкин Константин Александрович.** *Замечания*: **1.** Несмотря на высокую точность и устойчивость к шуму, комитет (ансамбль) классификаторов (КК) всё же имеет ряд недостатков, которые, впрочем, в ряде случаев удаётся нивелировать за счет настроек КК. В этой связи хотелось бы видеть в тексте автореферата сведения о вычислительной сложности, затратах на обучение и чувствительности к переобучению при использовании КК. **2.** В целях лучшей интерпретации

результатов, желательно в тексте автореферата было бы привести не только количественные данные по метрикам качества обучения, но и графическую интерпретацию, например, матрицы ошибок.

Выбор официальных оппонентов и ведущей организации обосновывается их достижениями в данной отрасли наук, наличием публикаций в соответствующей сфере исследования и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– **предложена** концепция построения распределенной интеллектуальной системы мониторинга информационной безопасности (ИБ) промышленного Интернета вещей (Industrial Internet of Things, IIoT) на основе многоагентной платформы гибридной интеллектуальной системы обнаружения компьютерных атак и аномалий сетевого трафика IIoT, отличающаяся интеграцией механизмов искусственных иммунных систем, методов машинного обучения и подсистемы корреляции событий ИБ (SIEM-системы), что позволяет повысить оперативность, полноту и точность выявления угроз безопасности информации;

– **разработаны:**

- алгоритмы обнаружения атак и аномалий сетевого трафика IIoT на основе адаптивных механизмов искусственных иммунных систем (ИИС), отличающиеся объединением различных методов в рамках теории ИИС, и модификации известных алгоритмов клонального отбора, дендритных клеток и обновления детекторов, что позволяет значительно снизить уровень принятия ошибочных решений, выявлять в том числе новые, ранее неизвестные системе угрозы безопасности информации;

- алгоритмы обнаружения атак и аномалий сетевого трафика IIoT на основе использования комитета классификаторов, включающего в себя ИИС, методы машинного обучения и подсистему корреляции событий ИБ, отличающиеся формированием специфического иммунного ответа ИИС

совместно с другими алгоритмами искусственного интеллекта (нейронная сеть, 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;

- архитектура и программные модули исследовательского прототипа распределенной интеллектуальной системы мониторинга (РИСМ) ИБ IIoT на основе многоагентной платформы реализации многоуровневой гибридной интеллектуальной системы, что позволяет более полно учесть особенности структурно-функциональной организации объекта мониторинга, многообразие потенциальных угроз безопасности информации и уязвимостей программного обеспечения, дополняя полученную информацию текущими данными о событиях ИБ от SIEM-системы;

– **доказана** эффективность и целесообразность применения предложенной концепции, алгоритмов функционирования и архитектуры распределенной интеллектуальной системы мониторинга ИБ промышленного Интернета вещей для решения практических задач обнаружения атак и аномалий сетевого трафика сетей IIoT, что позволяет достичь более высоких значений показателей эффективности (точность, полнота и др.) обнаружения атак и аномалий по сравнению с существующими системами в среднем на 1,5% на тестовых наборах данных.

Теоретическая значимость исследования обоснована тем, что:

– применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) **использованы** методы системного анализа, защиты информации, машинного обучения, искусственных иммунных систем, нейронных сетей, многоагентных систем, SIEM-систем, компьютерного моделирования;

– **изложены** факты и аргументы, подтверждающие актуальность разработки концепции, алгоритмов и архитектуры распределенной

интеллектуальной системы мониторинга ИБ IIoT, отличающихся применением комитета классификаторов, включающего в себя двухуровневую ИИС, методы машинного обучения и подсистему корреляции событий ИБ, использованием многоагентного подхода к построению многоуровневых гибридных интеллектуальных систем, что в целом позволяет достигать высоких показателей точности обнаружения атак и аномалий на тестовых наборах данных;

– **изучены** особенности структурно-функциональной организации систем и сетей IIoT, используемые протоколы и методы мониторинга ИБ сетей промышленного Интернета вещей, на основании чего сделан вывод о том, что существующие решения не в полной мере учитывают специфику IIoT и не обеспечивают достаточно высокой точности обнаружения сетевых атак и аномалий, поэтому необходима разработка новых эффективных алгоритмов обнаружения атак и аномалий сетевого трафика IIoT с применением методов искусственного интеллекта;

– **проведена модернизация** известных алгоритмов теории ИИС: алгоритма дендритных клеток, клонального отбора, обновления детекторов, их интеграции и взаимодействия с внешними системами (SIEM), негативной селекции в составе распределенной двухуровневой ИИС, интеграция ИИС с методами машинного обучения (нейронная сеть и алгоритм случайного леса) в составе комитета классификаторов, решающего задачу выявления и классификации возможных атак и аномалий сетевого трафика IIoT.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– **разработаны и внедрены** в ЗАО «Республиканский центр защиты информации» и ФГБОУ ВО «Уфимский университет науки и технологий» результаты диссертационной работы, в том числе:

- алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием адаптивных механизмов искусственных иммунных систем;

- алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием комитета классификаторов, включающего в себя ИИС, методы машинного обучения и подсистему корреляции событий ИБ;

- архитектура, программные модули и методика применения исследовательского прототипа распределенной интеллектуальной системы мониторинга ИБ IIoT;

– **определены** границы применимости разработанных алгоритмов и программных модулей распределенной интеллектуальной системы мониторинга ИБ IIoT, даны оценки требуемых вычислительных ресурсов и временных затрат;

– **разработаны** алгоритмы и программные модули исследовательского прототипа распределенной интеллектуальной системы мониторинга ИБ IIoT, применение которых 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 IIoT;

– **представлена** методика применения разработанного исследовательского прототипа распределенной интеллектуальной системы мониторинга ИБ IIoT.

Оценка достоверности результатов исследования выявила:

– **теоретическая часть работы** построена на основе известных, проверяемых и апробированных данных, согласуется с опубликованными

работами других авторов, в том числе с располагаемыми экспериментальными данными по теме диссертации;

– **идея базируется** на результатах анализа публикаций других авторов по теме диссертации и смежным темам, обобщении опыта применения ИИС и гибридных интеллектуальных систем для обнаружения компьютерных атак и аномалий;

– **в экспериментальной части** работы продемонстрирована воспроизводимость результатов вычислительных экспериментов по обнаружению атак и аномалий сетевого трафика IIoT на основе анализа тестовых наборов данных о сетевом взаимодействии;

– **использованы** современные тестовые наборы данных о сетевых соединениях в системах IIoT, сравнение значений показателей эффективности обнаружения компьютерных атак и аномалий сетевого трафика IIoT, полученных в результате выполнения диссертационной работы, с показателями эффективности существующих систем;

– **установлено** совпадение авторских результатов с результатами, представленными в независимых источниках по решению задач обнаружения компьютерных атак и аномалий сетевого трафика IIoT, при улучшении количественных показателей эффективности результатов.

Личный вклад соискателя состоит в его участии на всех этапах процесса выполнения работы, соискатель самостоятельно проводил анализ и нормализацию наборов данных о сетевых соединениях, разрабатывал архитектуру, алгоритмы и программные модули предложенной системы, разрабатывал экспериментальный стенд для отладки и тестирования ИИС, лично участвовал в апробации результатов работы, подготовке основных публикаций по выполненной работе.

Диссертационный совет пришел к выводу о том, что в диссертации:

– соблюдены установленные Положением о присуждении ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени кандидата технических наук;

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

– соискатель ссылается на авторов и источники заимствования;

– оригинальность диссертационной работы составляет 96,6%.

Диссертационная работа Шамсутдинова Рината Рустемовича «Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем» соответствует требованиям пунктов 9-11, 13-14 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность по пунктам: 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.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. Особенностью информационно-управляющих систем является необходимость формирования управляющих воздействий на технологический процесс в реальном масштабе времени, поэтому скорость обработки информации в сети должна быть сравнимой и даже выше скорости реально протекающих физических процессов. Наличие и нейронной сети, и иммунной системы, и в целом ансамбля методов искусственного, приведет к задержкам. В банке данных ФСТЭК зафиксирована угроза УБИ.176, которая заключается в нарушении технологического процесса из-за возможных задержек, которые вносятся средствами защиты, а то, что предлагается – это средство защиты.

2. В докладе всё время говорилось об ошибках второго рода, но не говорилось об ошибках первого рода, а, как известно, они взаимосвязаны. Если увеличиваются ошибки первого рода, то уменьшаются ошибки второго рода, неясно, как это учитывается.

Соискатель Шамсутдинов Р.Р. согласился с высказанными замечаниями, но уточнил, что первичный анализ и выявление атак и аномалий осуществляется средствами распределенной искусственной иммунной системы (ИИС), особенностью которой является невысокая сложность (с вычислительной точки зрения) предложенного алгоритма обнаружения атак и аномалий, выполнение которого не требует больших временных и вычислительных затрат. Поэтому первичные данные об обнаруженных угрозах поступают в систему управления своевременно. Нейронная сеть и алгоритм

случайного леса функционируют на серверной компоненте в промышленной сети и служат средством дополнительного повышения точности классификации выявленных атак и аномалий. Эти данные уже предоставляются с некоторой задержкой, но это вторичная информация, которая тоже является полезной. Более того, ИИС реализована в качестве программного обеспечения и требует отдельного оборудования для реализации, но ни в коем случае не предполагается ее установка на уже имеющиеся устройства промышленного Интернета вещей, используемые для управления технологическим процессом. А получение данных о сетевом трафике реализуется в случае беспроводной сети – прослушиванием этой сети, в случае применения проводных технологий – подключением к зеркалирующему порту маршрутизатора. Поэтому применение данного средства защиты информации не нагружает инфраструктуру промышленной системы и не создает угрозы УБИ.176, а также предоставляет первичную информацию об атаках и аномалиях своевременно. Касательно вопроса об ошибках первого и второго рода, на слайде представлена таблица, где есть такие показатели, как False Positive Rate и False Negative Rate и это и есть ошибки первого рода и второго рода соответственно. ИИС, благодаря алгоритму негативной селекции, который является одним из ключевых в обеспечении высокой эффективности бинарной классификации, обеспечивает низкий уровень ошибок первого рода. То есть на начальном этапе система может не обнаруживать каких-либо атак, но она почти не допускает ошибок первого рода. По мере обучения, она начинает лучше обнаруживать атаки, и снижается уровень ошибок второго рода до какого-то предела, но уровень ошибок первого рода сохраняется стабильно низким.

Диссертация Шамсутдинова Р.Р. является законченной научно-квалификационной работой, в которой содержатся научно обоснованные результаты решения задач мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем, имеющих важное практическое значение.

На заседании 22.09.2023 г. диссертационный совет принял решение:

- за разработку концепции, алгоритмов функционирования, архитектуры исследовательского прототипа и программных модулей предложенной интеллектуальной системы мониторинга информационной безопасности промышленного Интернета вещей присудить Шамсутдинову Р.Р. ученую степень кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 14 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 14, против – 0.

Председатель
диссертационного совета
д-р. техн. наук, профессор Султанов Альберт Ханович

Ученый секретарь
диссертационного совета
д-р техн. наук, доцент Виноградова Ирина Леонидовна

22 сентября 2023 года