На правах рукописи

ШАМСУТДИНОВ Ринат Рустемович

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМОВ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

Специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2023

Работа выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий»

Научный руководитель: доктор технических наук, профессор, **Васильев Владимир Иванович**

Официальные оппоненты:

Сычугов Алексей Алексеевич, доктор технических наук, доцент, ФГБОУ ВО «Тульский государственный университет», директор Института прикладной математики и компьютерных наук, заведующий кафедрой информационной безопасности

Бурлаков Михаил Евгеньевич, кандидат технических наук, доцент, ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», доцент кафедры безопасности информационных систем

Ведущая организация: ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», г. Самара.

Защита диссертации состоится 22 сентября 2023 года в 13^{00} часов на заседании диссертационного совета 24.2.479.07, на базе ФГБОУ ВО «Уфимский университет науки и технологий», по адресу 450008, г. Уфа, ул. К. Маркса, д. 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский университет науки и технологий» и на сайте *https://uust.ru/*.

Автореферат разослан «___»_____2023 года.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современный этап развития промышленного производства (Индустрия 4.0) связан с массовым внедрением информационных технологий и киберфизических систем, масштабной автоматизацией бизнес-процессов, распространением технологий искусственного интеллекта. Ключевые позиции в нарождающейся 4-й промышленной революции начинает занимать промышленный Интернет вещей (Industrial Internet of Things, IIoT). Промышленный Интернет вещей представляет собой систему объединенных компьютерных сетей и подключенных к ним промышленных (производственных) объектов со встроенными датчиками и программным обеспечением (ПО) для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека. По прогнозам, к 2030 г. этот сектор будет добавлять к мировому валовому продукту (ВВП) 14,2 трлн. долл., а количество подсоединенных к сети устройств составит 75.4 млрд.

Важным условием работы сетей и систем промышленного Интернета вещей является обеспечение их информационной безопасности (ИБ). Согласно данным компании Check Point, число кибератак за 2022 г. выросло на 38%. 94% производственных компаний столкнулись с инцидентами ИБ в 2022 г., при этом менее трети из них внедрили на своих объектах системы безопасности IIoT и операционных технологий (Operational technologies, OT). Наиболее распространенные причины слабой защищенности IIoT: устаревшее ПО и недостаточное внимание к программным обновлениям, передача данных без шифрования, стандартные заводские настройки безопасности устройств IIoT, незащищенные интерфейсы, уязвимости в операционных системах общего назначения, невозможность оснастить многие устройства встроенными средствами безопасности и т.п. В качестве средств мониторинга ИБ сетей используются системы обнаружения атак и аномалий, применяемые в том числе в промышленных автоматизированных системах (АСУ ТП), но существующие системы обнаружения сетевых атак и аномалий не в полной мере учитывают специфику IIoT.

Невысокая эффективность существующих систем обнаружения атак (СОА) в решении задачи мониторинга ИБ сетей IIoT обуславливается следующим. Существуют атаки, эксплуатирующие специфичные уязвимости IIoT, к примеру, атаки, нацеленные на повышение расхода электроэнергии устройствами IIoT, в том числе сенсоров беспроводных сенсорных сетей, не выявляемые штатными средствами защиты промышленных систем. Существующие СОА, основанные на анализе сигнатур, в принципе не могут выявлять новые, неизвестные ранее атаки (атаки нулевого дня), а также новые виды уже известных атак, для которых пока не существует сигнатур. СОА на основе выявления злоупотреблений (аномалий) характеризуются большим количеством допускаемых ошибок. Существующие СОА, реализующие в том числе методы и алгоритмы искусственного интеллекта, демонстрируют более высокую, но всё еще недостаточную эффективность

обнаружения сетевых атак и аномалий в сетях IIoT.

Поэтому проблема разработки и исследования новых методов и алгоритмов к обнаружению атак и аномалий в работе систем и устройств IIoT с целью повышения их уровня защищенности в условиях воздействия возможных внешних и внутренних угроз безопасности информации является актуальной.

Степень разработанности темы исследования. Исследованиям в области оценки рисков ИБ и уровня защищенности промышленных автоматизированных систем (АСУ ТП) посвящены работы таких российских и зарубежных ученых, как: Ажмухамедов И.М., Аникин И.В., Васильев В.И., Вульфин А.М., Катасёв А.С., Костогрызов А.И., Котенко И.В., Машкина И.В., Шелупанов А.А., Massacci F., Noel S. и др. Конкретные технические решения в области построения систем обнаружения сетевых атак и аномалий предложены в работах таких авторов, как: Абрамов Е.С., Аралбаев Т.З., Бурлаков М.Е., Карташевский В.Г., Поздняк И.С., Aydin M., Dilek S., Çakır H., He J., Jing C., Li Y., Powers S.T., Xu J. и др. Достаточно большое количество работ посвящено решению задач, связанных с реализацией процессов мониторинга ИБ в IIoT-системах, в том числе с применением методов и технологий искусственного интеллекта. Исследования в данном направлении отражены в публикациях таких авторов, как: Заводцев И.В., Зегжда Д.П., Глухих И.Н., Дойникова Е.В., Милославская Н.Г., Полтавцева М.А., Сычугов А.А., Тебуева Ф.Б., Alaparthy V., Gupta G.P., Joshi A., Morgera S., Raja K., Singh A., Xiao X., Zhang R., Zou Z. и др.

Вместе с тем, существующие методики обнаружения атак и аномалий сетевого трафика IIoT-систем нуждаются в развитии и совершенствовании, что может быть реализовано на основе применения технологий искусственного интеллекта, включая применение искусственных иммунных систем, чему и посвящена настоящая работа.

Объект исследования – сети и системы промышленного Интернета вещей.

Предмет исследования – защищённость сетей промышленного Интернета вещей от угроз информационной безопасности.

Методы исследования. В работе использовались методы системного анализа, защиты информации, машинного обучения, искусственных иммунных систем, нейронных сетей, многоагентных систем, SIEM-систем, компьютерного моделирования

Цель работы – повышение эффективности систем мониторинга ИБ сетей промышленного Интернета вещей на основе разработки и применения алгоритмов обнаружения компьютерных атак и аномалий сетевого трафика с использованием механизмов искусственных иммунных систем.

Задачи исследования:

1. Анализ современного состояния исследований в области мониторинга ИБ сетей промышленного Интернета вещей с использованием технологий искусственного интеллекта.
2. Разработка алгоритмов обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием адаптивных механизмов искусственных иммунных систем.

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

4. Разработка архитектуры исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей, оценка эффективности ее применения при решении прикладных задач.

Положения, выносимые на защиту:

1. Результаты анализа современного состояния исследований в области мониторинга сетей промышленного Интернета вещей с использованием технологий искусственного интеллекта, предложенная концепция построения интеллектуальной системы мониторинга 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.

Научная новизна полученных результатов.

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.

Теоретическая значимость полученных результатов заключается в том, что в работе предложены: концепция построения интеллектуальной системы мониторинга ИБ промышленного Интернета вещей; алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием адаптивных механизмов ИИС; алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием ансамбля методов машинного обучения и подсистемы корреляции событий ИБ; архитектура исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей.

Практическая значимость полученных результатов заключается в разработке: программных модулей исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей; методики 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.

Достоверность результатов работы обеспечивается 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.

Связь исследований с научными программами. Исследования выполнялись в рамках грантов РФФИ № 20-37-90024 «Гибридная интеллектуальная система мониторинга информационной безопасности на основе

алгоритмов искусственных иммунных систем и нечетких нейронных сетей», № 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».

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют 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.

Апробация результатов. Полученные результаты исследований докладывались и обсуждались на следующих научных конференциях: VII Всероссийская заочная Интернет-конференция «Проблемы информационной безопасности», г. Ростов-на-Дону, 2018 г.; VI – IX Всероссийские научные конференции (с приглашением зарубежных ученых) «Информационные технологии интеллектуальной поддержки принятия решений», гг. Уфа, Ставрополь, Ханты-Мансийск, 2018-2021 гг.; XIII Всероссийская молодёжная научная конференция «Мавлютовские чтения», г. Уфа, 2019 г.; 13-я Всероссийская зимняя школа-семинар магистрантов, аспирантов и молодых ученых «Актуальные проблемы науки и техники», г. Уфа, 2020 г.; XIV Всероссийская молодежная научная конференция «Мавлютовские чтения», г. Уфа, 2020 г.; Международная научная конференция «Цифровая индустрия: состояние и перспективы развития 2020», г. Челябинск, 2020 г.; Студенческая научно-техническая конференция «Неделя науки», г. Уфа, 2021 г.; Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO-2021», г. Томск, 2021 г.

Результаты диссертационной работы внедрены в ЗАО «Республиканский центр защиты информации» и в учебный процесс кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский университет науки и технологий» Министерства науки и высшего образования РФ.

Публикации по теме исследования. По проблеме диссертационного исследования опубликовано 17 работ, в том числе: 6 в рецензируемых научных журналах, входящих в перечень изданий, рекомендованных ВАК, 3 – в изданиях, индексируемых в Web of Science, одно из них индексируется в Scopus; 8 – в прочих изданиях.

Структура и объем работы. Работа состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, словаря терминов, списка литературы и приложений, содержит 38 рисунков, 38 таблиц, 26 формул, 3 приложения, выполнена на 187 страницах. Список использованной литературы включает 201 источник.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, определены объект и предмет диссертационного исследования, цель работы и решаемые задачи. Отмечена научная новизна полученных результатов, их теоретическая и практическая значимость, представлены положения, выносимые на защиту.

В первой главе проводится анализ современного состояния исследований в области автоматизации мониторинга информационной безопасности (ИБ) сетей промышленного Интернета вещей (IIoT) с использованием технологий искусственного интеллекта (ИИ). Проанализированы архитектура, функциональные области и домены IIoT, наиболее распространенные причины слабой защищенности IIoT, основные виды сетевых атак на промышленные сети и методы противодействия им, применение систем управления информацией о безопасности и событиями безопасности (SIEM-систем). Отмечается, что используемые в научной литературе методы ИИ для обнаружения сетевых атак на IIoT включают нейронные сети глубокого обучения, методы машинного обучения, искусственные иммунные системы (ИИС). Рассматриваются основные алгоритмы и подходы, применяемые в теории ИИС, а также гибридные интеллектуальные системы, демонстрирующие более высокую эффективность в сравнении с отдельными методами ИИ. Подчеркивается актуальность разработки гибридной распределенной интеллектуальной системы мониторинга (РИСМ) ИБ промышленного Интернета вещей с целью достижения более высоких значений показателей эффективности обнаружения атак и аномалий в сетях IIoT. Показаны преимущества применения ИИС в составе РИСМ ИБ для решения задач обнаружения атак и аномалий сетевого трафика IIoT.

Во второй главе разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика IIoT с использованием двухуровневой ИИС, построенной в классе распределённых многоагентных систем, объединяющей различные подходы и алгоритмы теории ИИС. Алгоритм функционирования разработанной ИИС представлен на рисунке 1, курсивом выделены подпроцессы, построенные на основе существующих алгоритмов, полужирным шрифтом – на основе новых и доработанных алгоритмов.

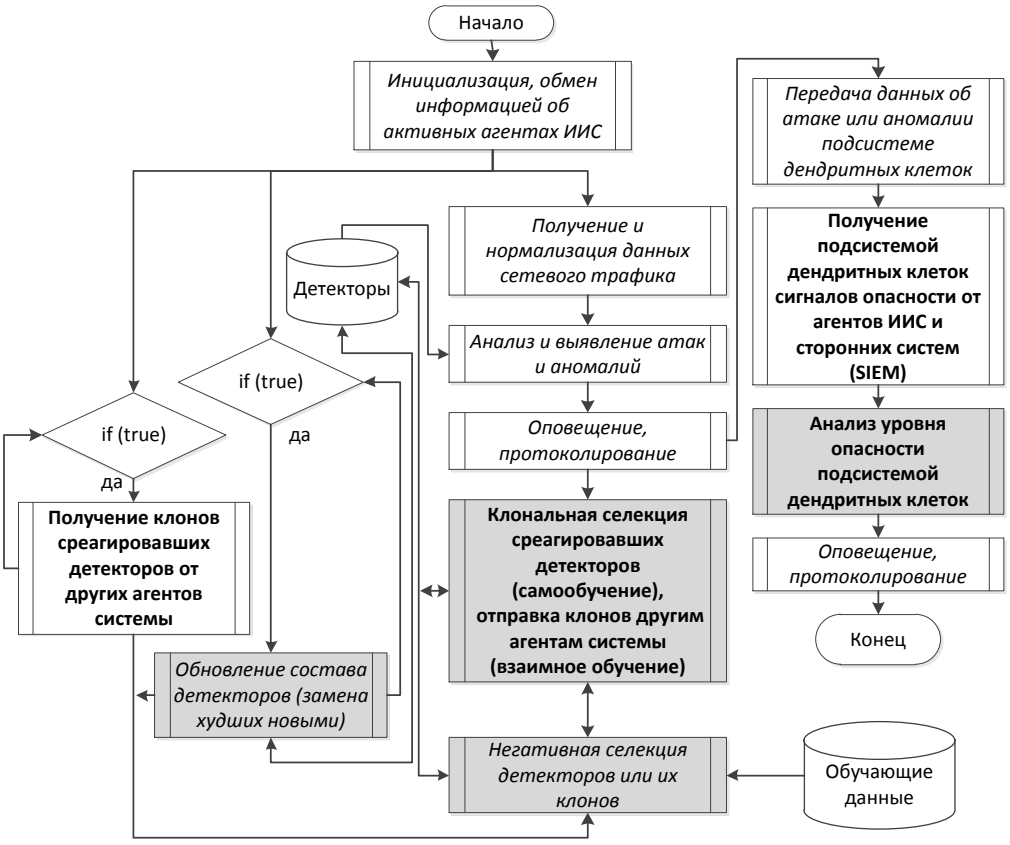

Рисунок 1 – Алгоритм функционирования разработанной ИИС

В целом, относительно построения ИИС новым является:

– объединение различных алгоритмов ИИС, выделенных на рисунке 1 серой заливкой, в единой системе;

– модификация алгоритма дендритных клеток, исключающая анализ сигналов безопасности, блокирующая уязвимость, связанную с навязыванием ложных сигналов безопасности в момент проведения атаки для обеспечения видимости легитимного сетевого взаимодействия;

– модификация алгоритма клональной селекции для функционирования в многоагентной распределенной архитектуре таким образом, что каждый агент, проводящий анализ и выявление атак и аномалий, на основе результатов анализа не только самообучается, но и передаёт обучающие данные всем другим агентам нижнего уровня, обеспечивается взаимное обучение агентами друг друга;

– разработанные механизмы взаимодействия подсистемы дендритных клеток с подсистемами корреляционного анализа – SIEM-системами.

Предложенная ИИС реализована на двух уровнях:

1) агенты нижнего уровня ИИС распределены и интегрированы в подсети устройств IIoT, производят локальные вычисления, выявляют известные и неизвестные сетевые атаки и аномалии по принципу «свой/чужой». *Атака* – целенаправленное злонамеренное воздействие на систему. *Неизвестная атака* – атака, неизвестная конкретной системе защиты, выявляется на основе анализа аномалий. *Аномалия* – статистически значимое отклонение характеристик трафика, которое может или являться признаком атаки, или нет.

2) агенты второго уровня ИИС расположены на границах сетей IIoT, получают данные от соответствующих агентов ИИС нижнего уровня, всех агентов ИИС второго уровня и от подключаемых внешних систем, таких как SIEM-системы, SCADA, межсетевые экраны и пр., реализуют граничные вычисления, производят анализ по принципу «опасно/безопасно», выделяют из потока неизвестных аномалий те, которые с большей вероятностью могут свидетельствовать о реализации неизвестной атаки.

Для обучения и тестирования ИИС использованы датасеты – наборы данных о сетевых соединениях, содержащие параметры трафика, соответствующие нормальному сетевому взаимодействию, а также определенным атакам. Проанализированы известные подходы к уменьшению размерности пространства параметров датасетов на примере NSL-KDD, отмечены их недостатки, реализован собственный алгоритм решения этой задачи.

Обучение агента нижнего уровня ИИС заключается в создании набора детекторов ($\vec{d}$), каждый из которых содержит вектор-строку параметров сетевого взаимодействия, служащую эталоном потенциальной атаки или аномалии. Эти векторы проходят процедуру негативной селекции: уничтожаются те из них, которые расположены близко к векторам примеров нормального сетевого взаимодействия и векторам других детекторов.

Анализ заключается в определении расстояния между вектором анализируемых данных и вектором каждого детектора, если хотя бы одно значение расстояния достаточно мало, то считается, что выявлена атака или аномалия, соответствующий детектор подвергается клональной селекции. Блок-схема алгоритма клональной селекции представлена на рисунке 2.

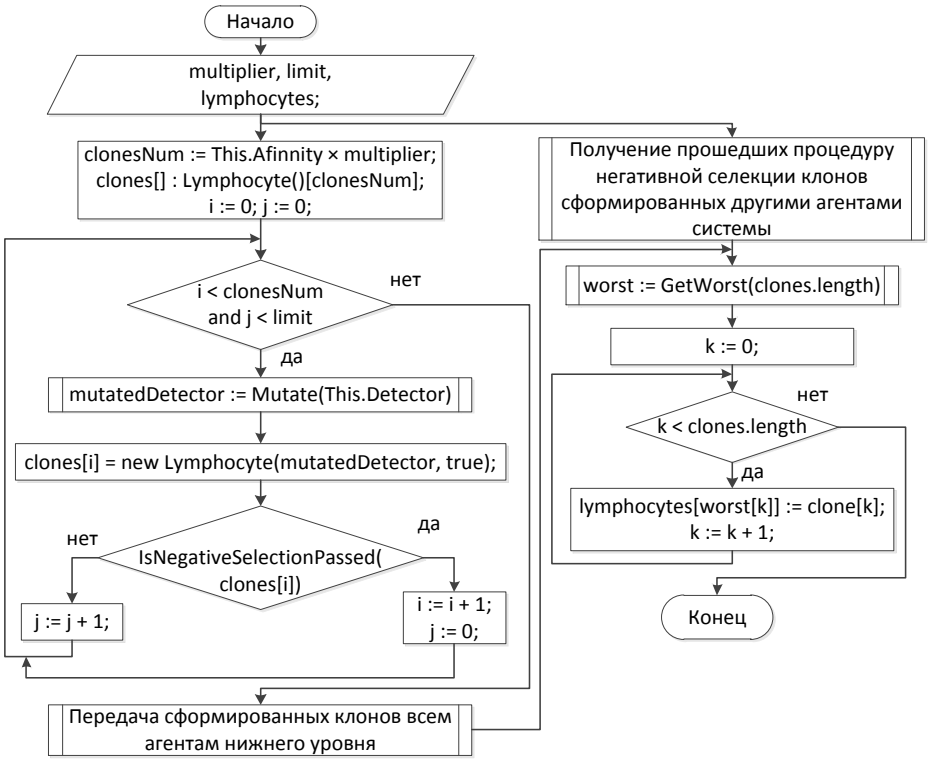

Рисунок 2 – Блок-схема алгоритма клональной селекции

Агенты второго уровня реализуют алгоритм дендритных клеток, основанный на теории опасности. Исходный алгоритм анализирует сигналы опасности, безопасности, сигналы наличия атаки, имеет существенный недостаток: атакующий во время атаки может имитировать сигналы безопасности, что приведет к игнорированию атаки. Модифицированный алгоритм дендритных клеток не анализирует никаких сигналов безопасности. На вход алгоритма подаются сигналы опасности от разных систем, включая агентов нижнего уровня, существующие сторонние системы мониторинга, такие как SIEM-системы, определяется общий уровень опасности в конкретных подсетях и всей анализируемой сети в целом. Поступление данных об одиночной аномалии увеличивает уровень опасности незначительно, повторные аналогичные сигналы увеличивают уровень опасности ощутимее, и, наконец, когда этот уровень достигает порогового значения, осуществляется оповещение об опасности. Сигналы о выявлении известной атаки мгновенно повышают уровень опасности до реализации оповещения. Всё это позволяет избежать параноидального реагирования на каждую выявленную аномалию, выделить из случайных аномалий наиболее существенные, которые могут быть вызваны неизвестными атаками.

Некоторые единичные неизвестные атаки, могут определяться как безвредные аномалии, но если оповещать администратора о каждой аномалии, это приведет к большому количеству оповещений и, как правило, их игнорированию администратором, тогда единичная неизвестная атака, скорее всего, тоже затеряется в числе проигнорированных администратором оповещений.

В третьей главе представлены результаты разработки и исследования алгоритмов мониторинга ИБ промышленного Интернета вещей с использованием гибридных технологий ИИ на базе ИИС и методов машинного обучения. Предложена концепция построения гибридной распределенной интеллектуальной системы мониторинга (РИСМ) промышленного Интернета вещей, использующей в качестве ключевых элементов многоагентную платформу и адаптивные механизмы функционирования ИИС.

Определены механизмы взаимодействия РИСМ с подсистемой корреляции событий ИБ на примере встроенной подсистемы корреляционного анализа данных (КАД) и внешней SIEM-системы – OSSIM (Open Source Security Information Management). РИСМ передаёт SIEM-системе данные о выявленных атаках и получает от SIEM-системы данные о выявленных инцидентах ИБ, статистику событий ИБ для определения уровня опасности. Блок-схема функционирования РИСМ представлена на рисунке 3, где ИНС – искусственная нейронная сеть, СЛ – случайный лес, ИИС – искусственная иммунная система. На первом уровне осуществляется сбор данных о сетевом взаимодействии IIoT-устройств посредством сниффинга, зеркалирования трафика. Затем происходит извлечение анализируемых параметров, их нормализация, анализ данных посредством двухуровневой ИИС, подробно рассмотренной во второй главе. Данные об атаках, обнаруженных двухуровневой ИИС, отправляются на верхний уровень системы (уровень серверов), где осуществляются агрегация данных, их

дополнительный анализ с помощью других методов машинного обучения – ИНС и СЛ.

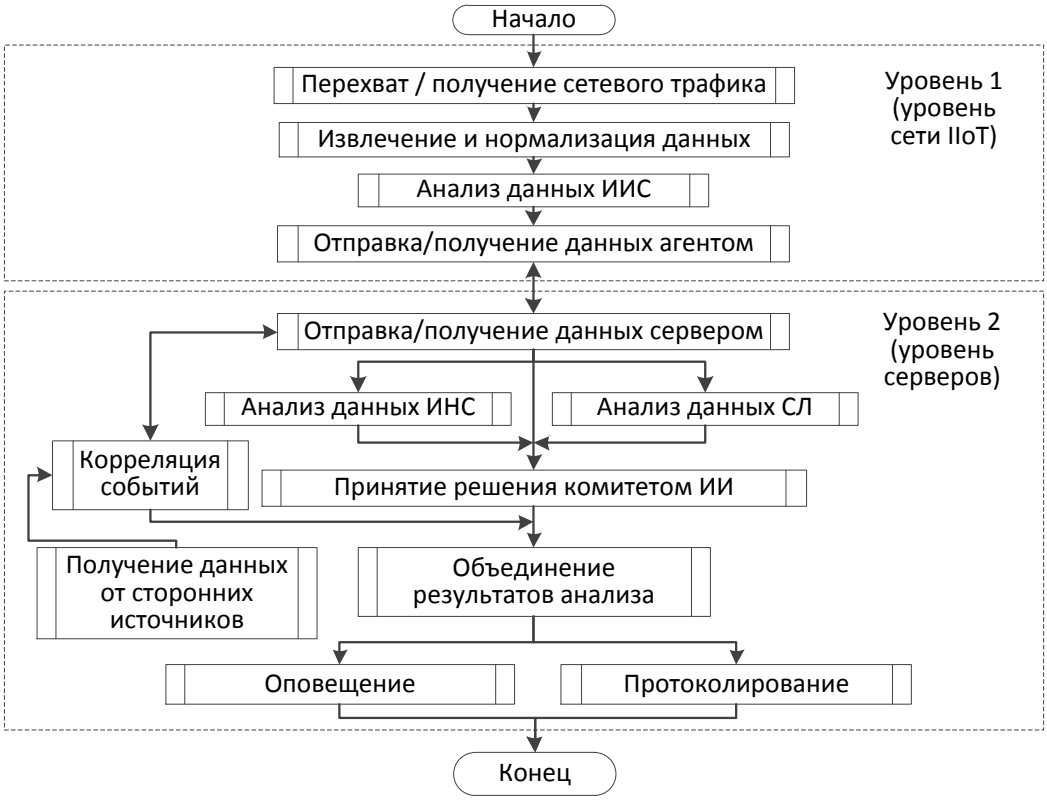

Рисунок 3 – Блок-схема алгоритма функционирования РИСМ

На основе выводов, полученных с помощью трёх классификаторов (ИИС, ИНС, СЛ) принимается решение об отсутствии или наличии и итоговом классе атаки (аномалии), параллельно выполняется КАД. Затем, с учетом выявленного класса атаки (аномалии) и результатов КАД, принимается окончательное решение о критичности атаки (аномалии). Принятие решения о классе атаки (аномалии) осуществляется с учетом известной теоремы Кондорсе о комитете экспертов (присяжных), согласно которой, если компетентность каждого эксперта выше 0,5, то увеличение числа экспертов приводит к повышению точности результата. Рассмотрены различные схемы голосования и принятия решений при использовании комитета классификаторов.

Первоначальная гипотеза относительно построения комитета классификаторов заключалась в следующем. Благодаря алгоритму негативной селекции, ИИС должна демонстрировать один из самых низких уровней ошибок первого рода (False Positives), к тому же она способна выявлять как известные, так и неизвестные атаки. Рационально построить схему последовательного принятия решений, где ИИС выявляет в совокупности известные и неизвестные атаки. Если выявлена атака, то она передается другому алгоритму ИИ для определения её класса. Вычислительные эксперименты проводились с использованием искусственной нейронной сети (ИНС) и алгоритма случайного леса (СЛ) по схеме, представленной рисунком 4.

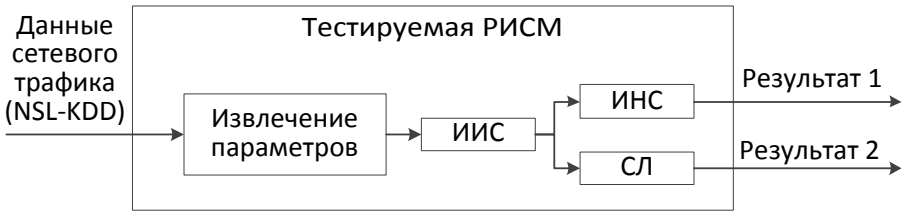

Рисунок 4 – Схема взаимодействия классификаторов (серия экспериментов №1)

Вычислительные эксперименты проводились с использованием датасета NSL-KDD. Получены следующие значения показателей эффективности:

– ИИС+ИНС: Accuracy – 0.997, F_1-score – 0.997;

– ИИС+СЛ: Accuracy – 0.999, F_1-score – 0.999.

Полученные результаты демонстрируют, что объединение ИИС с СЛ является более предпочтительным вариантом из рассмотренных. ИИС оказывает содействие в определении факта наличия (отсутствия) атаки, а СЛ отвечает за классификацию обнаруженной атаки. Уменьшаются уровни ошибок первого и второго рода, и осуществляется достаточно точная классификация атак. Но, во-первых, СЛ в одиночку классифицирует атаки, если бы решение о классе атаки принималось с учетом мнения не только СЛ, но и других классификаторов, это бы уменьшило ошибки определения класса атаки; во-вторых, если ИИС обнаружит неизвестную для СЛ атаку, то СЛ может некорректно ее классифицировать.

Один из вариантов решения – обучить ИИС классификации известных атак, но тогда могут возникать ситуации, когда ИИС сообщает об одном классе атаки, а СЛ – о другом. Возникнет конфликт и появится проблема разрешения таких ситуаций. Возможно, мнению одного из классификаторов стоит увеличить вес, но при этом допускаемые ошибки приоритетного алгоритма не будут чем-либо компенсированы. Выход – необходим третий классификатор. Тестируемая система с использованием 3-х классификаторов была построена согласно схеме на рисунке 5.

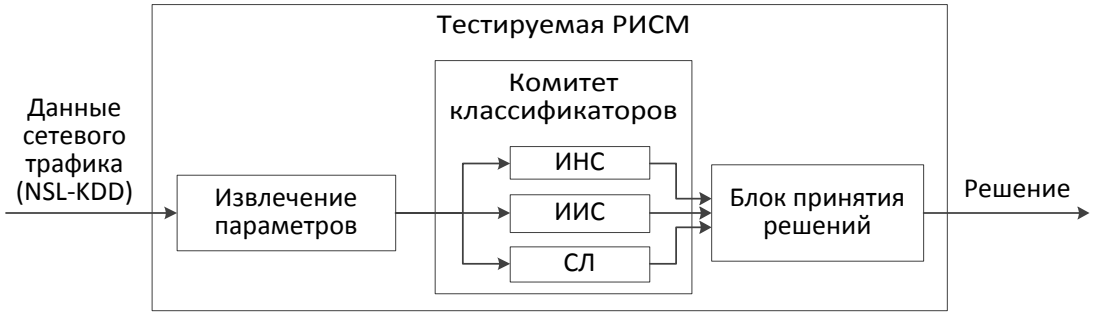

Рисунок 5 – Схема взаимодействия классификаторов (серия экспериментов №2)

При таком построении возникали ситуации, когда ИНС и СЛ одновременно ошибались в определении факта наличия (отсутствия) атаки, а ИИС определяла верно, но большинством принималось неправильное решение. Наиболее высокие показатели эффективности были получены при построении комитета классификаторов по схеме, представленной рисунком 6.

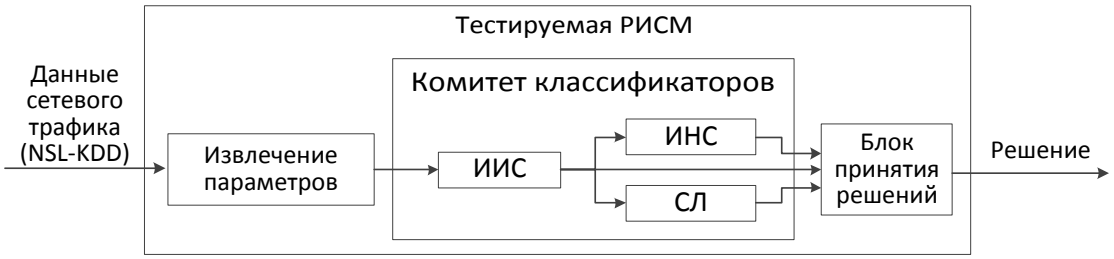

Рисунок 6 – Лучший вариант построения комитета классификаторов из рассмотренных

То есть лучшим из рассмотренных является вариант построения комитета классификаторов, при котором в решении легитимности анализируемого сетевого соединения полный приоритет отдаётся ИИС, а класс выявленной атаки при ее наличии определялся равнозначным голосованием на основе большинства (по мажоритарному принципу).

В четвертой главе разработана трехуровневая архитектура исследовательского прототипа РИСМ, представленная на рисунке 7, разработана методика обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием РИСМ.

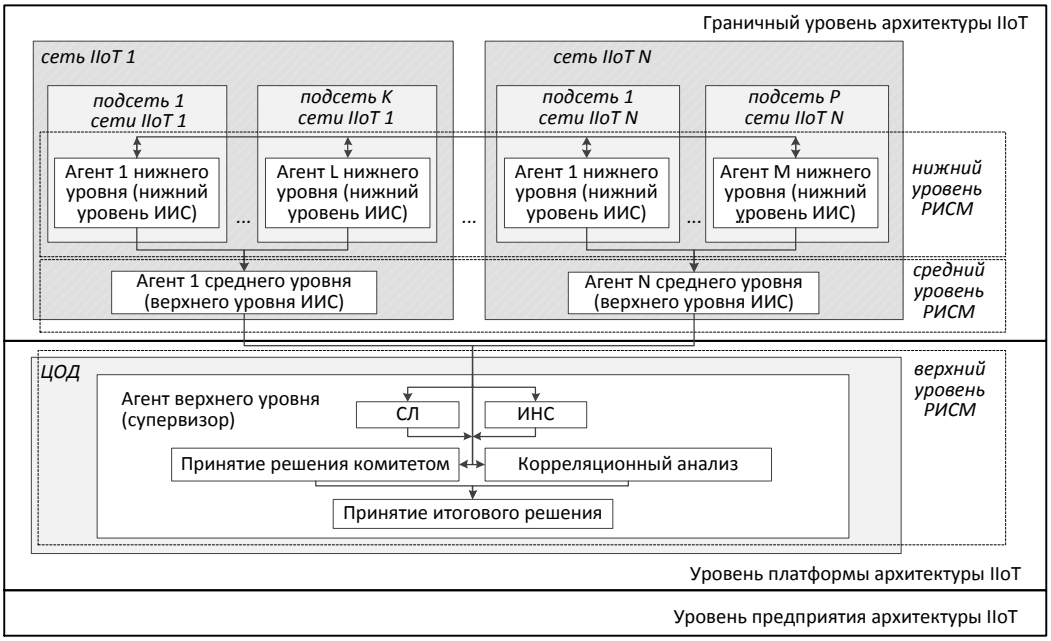

Рисунок 7 – Архитектура РИСМ ИБ IIoT

На рисунке 7 для наглядности уровни архитектуры РИСМ выделены пунктирными линиями, уровни архитектуры IIoT – непрерывными линиями. На нижнем уровне РИСМ функционирует расположенное в непосредственной близости к устройствам IIoT множество агентов, реализующих перехват или получение трафика, выявление атак и аномалий средствами ИИС, взаимодействующих друг с другом в части обмена обучающих данных, передающих информацию о выявленных атаках и аномалиях на второй уровень РИСМ. Агенты второго (среднего) уровня расположены на границах сетей IIoT,

они получают данные об атаках от агентов нижнего уровня и (по возможности) от подключаемых сторонних систем, таких как межсетевые экраны, SIEM, выполняют оценку уровня опасности средствами ИИС, отделяют одиночные аномалии от реальных и потенциальных атак, передают данные на верхний уровень.

Агент верхнего уровня (супервизор) получает информацию о выявленных атаках, осуществляет дополнительный ее анализ подсистемами ИНС и СЛ, на основе мнений трёх интеллектуальных классификаторов (ИИС, ИНС, СЛ) принимает решение о классе атаки, проводит дополнительный корреляционный анализ данных (КАД), на основе решения комитета классификаторов и результата КАД принимает решение о критичности того или иного инцидента, передает информацию в консоль администрирования, осуществляет оповещение.

Эффективность предлагаемой РИСМ оценивалась на тестовом примере IIoT-системы контроля уровня и мутности воды в резервуаре (баке) (рисунок 8), которая входит в состав автоматизированной системы очистки и распределения воды в промышленных резервуарах. Проводились вычислительные эксперименты по обнаружению сетевых атак на основе датасета WUSTL-IIOT-2021. Анализировалось несколько вариантов построения классификаторов, оценивались показатели эффективности использования отдельных алгоритмов и комитета классификаторов. Наибольшую эффективность продемонстрировал комитет классификаторов, полученные результаты представлены в Таблице 1.

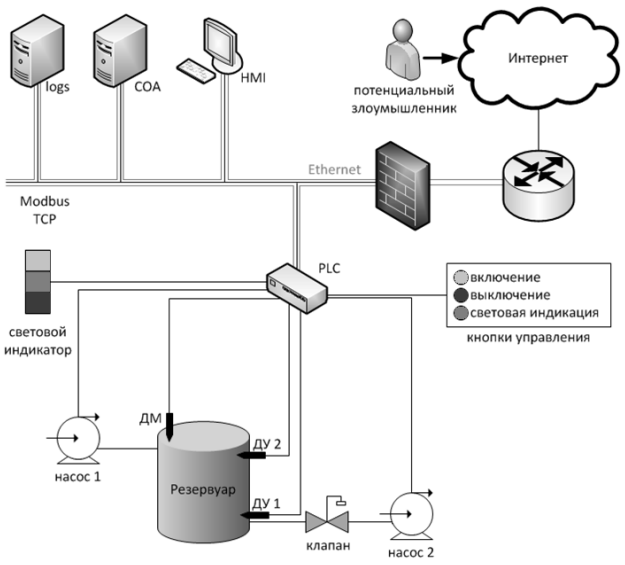

Рисунок 8 – Схема системы контроля уровня и мутности воды в резервуаре

Таблица 1 – Показатели эффективности РИСМ. Датасет WUSTL-IIOT-2021

Показатели эффективности бинарной классификации «свой/чужой»				Точность определения класса атаки после успешного выявления атаки				
Precision	Recall	Accuracy	F_1-score	DoS	Reconn	Comm	Backdoor	ИТОГО
0,99989	0,99983	0,99998	0,99986	100%	100%	98,08%	90,48%	99,97%

Эффективность РИСМ также оценивалась на основе данных испытательного стенда беспроводной мультисенсорной сети (WSN), состоящей из 100 сенсорных узлов, объединенных в 5 кластеров, на основе соответствующего датасета WSN-DS, содержащего 4 вида атак на протокол LEACH, часто используемый в WSN. Результаты экспериментов демонстрируют высокие значения показателей эффективности РИСМ, представленные в Таблице 2.

Таблица 2 – Показатели эффективности РИСМ. Датасет WSN-DS

FNR	FPR	TNR	TPR (Recall)	Precision	Accuracy	F_1-score
0,001	0,001	0,999	0,999	0,999	0,999	0,999

Дополнительно на основе WSN-DS сравнивалось применение в ИИС различных мер близости между векторами: расстояния Хэмминга, Евклидова расстояния и косинусной меры. Вычислительные эксперименты показали рациональность применения расстояния Хэмминга в ИИС.

В заключении представлены основные выводы и результаты проведенного исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. В работе проведен анализ современного состояния исследований в области мониторинга сетей промышленного Интернета вещей с использованием технологий искусственного интеллекта, предложена концепция построения интеллектуальной системы мониторинга ИБ промышленного Интернета вещей с использованием механизмов искусственных иммунных систем, методов машинного обучения, взаимодействия с подсистемой корреляции событий информационной безопасности (SIEM-системой), что позволило повысить полноту и точность выявления внешних и внутренних угроз информационной безопасности.
2. Разработаны алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе механизмов искусственных иммунных систем (ИИС), реализованные в составе двухуровневой распределенной ИИС, состоящей из множества взаимодействующих агентов, интегрирующих различные подходы 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 атак и аномалий сетевого трафика промышленного Интернета вещей с использованием ансамбля методов машинного обучения, включающего искусственную иммунную систему, искусственную нейронную сеть, алгоритм случайного леса, с интеграцией подсистемы корреляции событий ИБ, реализующего трёхуровневый интеллектуальный анализ данных сетевого трафика с целью определения наличия сетевых атак и аномалий с учетом уровня опасности, с возможностью корректировки чувствительности, что позволило достичь более высоких значений показателей эффективности в сравнении с применением данных алгоритмов по отдельности.
4. Разработана архитектура исследовательского прототипа распределенной интеллектуальной системы мониторинга (РИСМ) ИБ

промышленного Интернета вещей, состоящей в классе многоуровневых многоагентных гибридных систем, что облегчает её интеграцию в различные подсети IIoT непосредственно, позволяет использовать преимущества не только централизованной обработки данных, но и локальных, а также граничных вычислений, обеспечивает возможность интеграции с существующими системами безопасности и мониторинга, включая межсетевые экраны, SIEM, SCADA и др.

Эффективность предлагаемой РИСМ оценивалась на тестовой IIoT-системе контроля уровня и мутности воды в резервуаре, на основе датасета WUSTL-IIOT-2021, а также на основе данных сетевого взаимодействия беспроводной сенсорной сети, сведенных в датасет WSN-DS. Значения показателей эффективности РИСМ на тестовых наборах данных были на уровне 98-99%, что превышает значения показателей эффективности существующих систем в среднем на 1,5% и обеспечивает высокий уровень обнаружения сетевых атак и аномалий, демонстрирует высокую эффективность системы.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ИССЛЕДОВАНИЯ

Публикации в журналах, рекомендованных Высшей аттестационной комиссией:

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. – Т. 7, № 1 (24). – С. 536-547. – DOI: 10.26102/2310-6018/2019.24.1.011.
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.
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.
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.
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, № (39). – URL: https://moitvivt.ru/ru/journal/pdf?id=1240. – DOI: 10.26102/2310-6018/2022.39.4.001.

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), 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).

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. – Т. 1, № 2 (18). – С. 789-797.

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, Ростов-на-Дону, 20-21 февраля 2018 года. – Ростов-на-Дону: АзовПринт, 2018. – С. 181-184.

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. – С. 237-244.

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 // International scientific review of the technical sciences, mathematics and Computer science : сборник научных статей IX Международной заочной научной специализированной конференции, Бостон, США, 12–13 февраля 2019 года. – Бостон, США: PROBLEMS OF SCIENCE, 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. – URL: https://www.elibrary.ru/item.asp?id=44619516.

Диссертант Р.Р. Шамсутдинов