УТВЕРЖДАЮ

Проректор по научной работе

ФГБОУ ВО «ПГУТИ»,

д.т.н., профессор

_____ О.В.Горячкин

«21» 09 2023 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию Шамсутдинова Рината Рустемовича

на тему **«Интеллектуальная система мониторинга информационной безопасности промышленного Интернета вещей с использованием механизмов искусственных иммунных систем»**,

представленную на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

Современный этап развития промышленности характеризуется переходом к новому технологическому укладу (Промышленность 4.0), связанному с цифровой трансформацией процессов управления и принятия решений на всех уровнях производства. Этот переход сопровождается внедрением новых цифровых технологий, основанных на использовании методов искусственного интеллекта и машинного обучения, обработки и анализа больших данных, технологий расширенной реальности, виртуализации, облачных вычислений, беспроводных компьютерных сетей и др. Указанные методы и технологии играют важную роль, выступая в качестве основы организации и функционирования промышленных систем нового поколения, и в частности промышленного Интернета вещей (Industrial Internet of Things, IIoT), особенностями которых являются: распределенная

многоуровневая архитектура, наличие большого числа гетерогенных промышленных устройств (интеллектуальные датчики и исполнительные механизмы, программируемые логические контроллеры, модули сбора и аналитики данных, сетевые телекоммуникационные устройства и др.), активное взаимодействие с внешней средой посредством Интернет. Вместе с тем, несмотря на неоспоримые преимущества, которые дает применение промышленного Интернета вещей, статистика последних лет фиксирует существенные слабости (уязвимости) в его работе, заключающиеся в возможности внешних злоумышленников осуществлять несанкционированный доступ к системам и сетям IIoT с целью нарушения их нормального функционирования. Сегодня одной из ключевых проблем при развертывании и внедрении промышленного Интернета вещей является обеспечение его информационной безопасности (ИБ), что предполагает в первую очередь решение задачи своевременного обнаружения и идентификации компьютерных атак и аномалий сетевого трафика IIoT с целью предотвращения или минимизации последствий (ущерба) от их возникновения. В то же время, существующие системы обнаружения атак и аномалий не в полной мере учитывают специфику промышленного Интернета вещей и не обеспечивают достаточно высокого уровня обнаружения угроз безопасности информации (БИ).

С учетом вышеизложенного, тема диссертационной работы Шамсутдинова Р.Р., посвященная разработке методов, алгоритмов и программных средств мониторинга ИБ систем и сетей промышленного Интернета вещей с использованием современных технологий искусственного интеллекта и машинного обучения (включая механизмы искусственных иммунных систем), несомненно, является актуальной.

Оценка структуры и содержания работы

Диссертационная работа состоит из введения, четырех глав, заключения, списка сокращений, списка использованной литературы и

приложений. Диссертация изложена на 187 страницах, включает 38 рисунков, 38 таблиц и 3 приложения.

Первая глава посвящена анализу современного состояния исследований и нормативно-правовой базы в области обеспечения ИБ и мониторинга ИБ систем и сетей промышленного Интернета вещей. Рассмотрены различные подходы к организации мониторинга ИБ IIoT, в том числе подходы, основанные на использовании технологий искусственного интеллекта и машинного обучения. На основе результатов проведенного анализа сделан вывод о перспективности применения для этих целей гибридных интеллектуальных систем, основанных на объединении механизмов искусственных иммунных систем (ИИС) с другими методами машинного обучения, что позволяет существенно повысить значения показателей эффективности обнаружения сетевых атак и аномалий в сетях IIoT.

Во второй главе рассмотрена функциональная модель процесса организации мониторинга ИБ сетей IIoT на основе гибридной интеллектуальной системы, реализующей механизмы ИИС в сочетании с другими методами машинного обучения. Разработаны адаптивные алгоритмы обнаружения атак и аномалий сетевого трафика IIoT на основе интеграции модифицированных механизмов ИИС (негативной селекции, клонального отбора, дендритных клеток, обновления детекторов, теории опасности и иммунной сети). Предложена функционально-структурная схема построения интеллектуальной системы обнаружения сетевых атак и аномалий IIoT на основе двухуровневой распределенной ИИС. Приведены результаты вычислительных экспериментов по оценке эффективности применения предложенных алгоритмов обнаружения атак и аномалий с использованием стандартных обучающих наборов (датасетов).

В третьей главе рассмотрена концепция построения распределенной интеллектуальной системы мониторинга (РИСМ) сетевых атак на системы IIoT, основу которой составляют комитет интеллектуальных

классификаторов, включающий ИИС, искусственную нейронную сеть (ИНС), алгоритм случайного леса (СЛ), и подсистема корреляции событий ИБ в составе внешней взаимодействующей SIEM-системы. Представлены результаты сравнительных вычислительных экспериментов для различных вариантов построения комитета классификаторов, на основе которых предложена рациональная схема построения многоагентной РИСМ ИБ IIoT.

В четвертой главе представлена разработанная архитектура исследовательского прототипа РИСМ и методика ее применения для решения задачи обнаружения компьютерных атак и аномалий сетевого трафика IIoT. Рассмотрены прикладные практические задачи, связанные с применением предложенных решений для обнаружения атак и аномалий сетевого трафика промышленной системы перекачки воды и беспроводной мультисенсорной сети. Результаты проведенных вычислительных экспериментов продемонстрировали высокие значения показателей эффективности обнаружения атак, в среднем на (1,5-2)% превышающие показатели эффективности известных систем, а также способность предложенной системы обнаруживать новые, неизвестные ранее атаки и аномалии в сетях IIoT и самостоятельно обучаться на их основе выявлению в дальнейшем подобных атак и аномалий.

В Заключении сформулированы основные результаты и выводы, полученные в диссертационной работе.

Область исследования диссертации соответствует пунктам паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»:

п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»;

п. 6 «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях»;

п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Оформление диссертации соответствует ГОСТ Р 7.0.11-2011. Автореферат выполнен с соблюдением установленных требований, достаточно полно отражает содержание диссертационной работы, полученные в ней теоретические и практические результаты и выводы.

Новизна полученных результатов

1. Новизна предложенной концепция построения интеллектуальной системы мониторинга ИБ IIoT заключается в использовании многоагентной платформы реализации многоуровневой гибридной интеллектуальной системы обнаружения компьютерных атак и аномалий сетевого трафика IIoT, применение которой позволяет повысить полноту и точность выявления внешних и внутренних угроз безопасности информации.

2. Новизна базовых алгоритмов обнаружения компьютерных атак и аномалий сетевого трафика IIoT состоит в построении адаптивных механизмов ИИС на основе интеграции и модификации различных подходов в рамках общей теории ИИС, позволяющих в совокупности существенно снизить уровень ошибок в выявлении атак и аномалий в сетях IIoT, а также выявлять новые, ранее неизвестные системе сетевые атаки и аномалии.

3. Новизна расширенной группы алгоритмов обнаружения компьютерных атак и аномалий сетевого трафика IIoT заключается в использовании ансамбля методов машинного обучения (ИИС, ИНС, СЛ в сочетании с подсистемой корреляции событий ИБ), что позволяет получить более высокие показатели эффективности обнаружения сетевых атак и аномалий (включая ранее неизвестные) в сетях IIoT и повысить тем самым эффективность функционирования системы мониторинга ИБ в целом.

4. Новизна предложенной архитектуры исследовательского прототипа распределенной интеллектуальной системы мониторинга (РИСМ) ИБ

промышленного Интернета вещей заключается в применении многоагентного подхода к построению многоуровневых распределенных гибридных интеллектуальных систем мониторинга ИБ с использованием комитета классификаторов, что обеспечивает высокую эффективность мониторинга ИБ систем и сетей IIoT с учетом их распределенной многоуровневой организации, специфики состава угроз БИ и уязвимостей IIoT, использования в процессе мониторинга дополнительной информации об инцидентах ИБ от подсистемы корреляции событий ИБ.

Степень обоснованности и достоверности результатов исследования

Обоснованность и достоверность основных научных положений, результатов и выводов диссертации подтверждаются корректной постановкой цели и задач исследования, выбором методов исследования, повторяемостью полученных результатов вычислительных экспериментов, проведенных с использованием стандартных наборов данных (датасетов), практическим применением результатов работы, подтвержденным актами внедрения, обсуждением основных положений и выводов диссертации на научных конференциях, публикацией полученных результатов в рецензируемых научных изданиях.

Публикации. Основные результаты диссертации опубликованы в 17 работах, в том числе: в 6 статьях в научных журналах, включенных в перечень научных изданий ВАК по научной специальности 2.3.6.; в 3 статьях в изданиях, индексируемых в международной базе данных цитирования Web of Science (одна из них одновременно индексируется в базе данных Scopus); а также в 8 статьях в других изданиях.

Теоретическая и практическая значимость результатов полученных автором диссертации

Теоретическая значимость полученных результатов работы заключается в том, что они вносят существенный вклад в решение задачи мониторинга ИБ сетей промышленного Интернета вещей. В диссертации

разработаны: адаптивные алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика IIoT на основе механизмов ИИС и методов машинного обучения, реализованные в составе гибридной многоагентной распределенной системы мониторинга ИБ IIoT; механизмы взаимодействия комитета интеллектуальных классификаторов с подсистемой корреляции событий ИБ; концепция построения и архитектура исследовательского прототипа распределенной интеллектуальной системы мониторинга ИБ сетей промышленного Интернета вещей.

Практическая значимость результатов диссертации заключается в разработке алгоритмического и программного обеспечения интеллектуальной системы мониторинга ИБ сетей IIoT, методики ее применения. Практическое применение предложенных решений позволяет обеспечить точность обнаружения компьютерных атак и аномалий сетевого трафика IIoT на уровне (98-99)% на тестовых наборах данных, выявлять ранее неизвестные системе угрозы безопасности информации, учитывая при этом дополнительную информацию об инцидентах ИБ от подсистемы корреляции событий ИБ, что позволяет в совокупности существенно снизить количество принимаемых системой ошибочных решений.

Рекомендации по использованию результатов и выводов диссертации

Результаты диссертационной работы рекомендуются к расширенному использованию в промышленных организациях, реализующих современные технологии промышленного Интернета вещей, для которых проблема обеспечения ИБ устройств и систем, подключенных к сетям общего доступа, является актуальной.

Замечания по диссертационной работе

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.

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.

Вместе с тем, указанные замечания не являются принципиальными и не снижают общей положительной оценки работы, ее научной и практической ценности.

Заключение

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 ИБ промышленного Интернета вещей, применение которой позволяет повысить эффективность обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей.

Диссертация соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, 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.

Диссертационная работа Шамсутдинова Р.Р. и отзыв обсуждены на заседании кафедры Информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» (протокол заседания № 1 от 29 августа 2023 года).

Отзыв составил:
доктор технических наук, профессор,
заведующий кафедрой
Информационной безопасности,
Федеральное государственное
бюджетное образовательное учреждение
высшего образования
«Поволжский государственный университет
телекоммуникаций и информатики»

29.08.2023 Карташевский Вячеслав Григорьевич

Докторская диссертация защищена 27.11.1995г. по специальности 05.12.02 – Системы и устройства передачи информации по каналам связи

Даю согласие на обработку персональных данных.

Адрес организации: 443010, г. Самара, ул. Льва Толстого, 23
Рабочий телефон: +7(846) 333-53-50
Адрес эл. почты: v.kartashevskiy@psuti.ru

Собственноручную (ые) подпись (и)
Карташевского В.Г.
заверяю: начальник ОДО ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» И.В. Плеханова
29.08 2023

Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики»
Отдел документационного обеспечения