ОТЗЫВ

официального оппонента

кандидата технических наук, доцента Бурлакова Михаила Евгеньевича 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 специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы исследования

По оценкам специалистов, производители устройств и систем промышленного Интернета вещей (Industrial Internet of Things, IIoT) в настоящее время сконцентрированы главным образом на обеспечении их высокой производительности и функциональности. Вопросы обеспечения их информационной безопасности (ИБ) не получают должного внимания, вследствие чего устройства и системы IIoT оказываются недостаточно защищенными от внешних и внутренних угроз. Организации, использующие такие устройства, зачастую игнорируют данную сторону вопроса, не применяя даже минимально доступных мер обеспечения защищенности, к примеру, не изменяют стандартные пароли в системах, установленные их производителями. Несмотря на то, что количество новых угроз безопасности информации (БИ) и выявленных уязвимостей программного обеспечения этих систем постоянно растет, существующие средства обеспечения их ИБ не удовлетворяют в полной мере современным предъявляемым требованиям. Достаточно узким местом в обеспечении защищенности промышленного Интернета вещей является отсутствие эффективных методов и технических средств мониторинга ИБ его систем и сетей, связанное с их

многоуровневой структурно-функциональной организацией, гетерогенностью состава входящих в них устройств, подверженностью атакам со стороны внешней среды. С учетом вышеизложенного, тема диссертационной работы Шамсутдинова Р. Р., посвященная разработке и исследованию новых методов и алгоритмов обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей с использованием технологий искусственного интеллекта, несомненно, является актуальной.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка сокращений, словаря терминов, списка литературы и приложений, выполнена на 187 страницах, содержит 38 рисунков, 38 таблиц и 3 приложения. Список использованной литературы содержит 201 наименование. Приложения включают копии актов внедрения, а также дополнительный материал.

Во введении обоснована актуальность темы исследования, степень её разработанности, указаны объект и предмет исследования, использованные методы, цель и задачи диссертации, положения, выносимые на защиту, научная новизна и значимость полученных результатов, сведения об их апробации, связь работы с научными программами.

В первой главе приведен анализ проблемы обеспечения информационной безопасности (ИБ) систем и сетей промышленного Интернета вещей (IIoT). Рассмотрена существующая нормативная база и архитектура промышленного Интернета вещей, сетевые технологии и протоколы, используемые в системах и сетях IIoT, наиболее характерные угрозы БИ и методы мониторинга ИБ систем и сетей IIoT, включая использование технологий SIEM-систем и интеллектуального анализа данных.

Отмечены преимущества применения методов искусственного интеллекта (нейронных сетей, искусственных иммунных систем, методов машинного обучения) для решения задач обнаружения компьютерных атак и аномалий сетевого трафика,

являющихся неотъемлемой компонентой процесса мониторинга ИБ IIoT. Предложена концепция построения интеллектуальной распределенной системы мониторинга ИБ промышленного Интернета вещей в классе гибридных интеллектуальных систем с использованием механизмов искусственных систем, методов машинного обучения, взаимодействия с подсистемой корреляции событий ИБ (SIEM-системой). Дан краткий обзор методов и алгоритмов искусственных иммунных систем (ИИС) и особенностей их применения в составе системы мониторинга ИБ IIoT.

Во второй главе представлена функциональная модель процесса мониторинга ИБ сетей IIoT, описан используемый способ нормализации и выделения наиболее значимых параметров сетевого трафика IIoT, приведен общий алгоритм функционирования разработанной ИИС. В основе предложенного подхода к построению распределенной двухуровневой ИИС используется объединение различных алгоритмов ИИС, включая модифицированный алгоритм клональной селекции, модификацию алгоритма дендритных клеток, алгоритмы теории опасности, в составе распределенной двухуровневой интеллектуальной системы обнаружения атак и аномалий сетевого трафика IIoT, с учетом взаимодействия подсистемы дендритных клеток ИИС с подсистемой корреляционного анализа SIEM-системы. Приведены результаты вычислительных экспериментов, подтверждающие эффективность применения разработанной ИИС для обнаружения сетевых атак с использованием датасета NSL-KDD.

В третьей главе представлены результаты разработки алгоритмов обнаружения атак и аномалий в сетях IIoT на основе применения ансамбля методов машинного обучения и подсистемы корреляции событий ИБ. Рассмотренный ансамбль методов машинного обучения включает в себя, кроме разработанной в предыдущей главе распределенной двухуровневой ИИС, также классификаторы на основе алгоритма случайного леса (СЛ) и искусственной нейронной сети (ИНС), взаимодействующие с подсистемой корреляции событий ИБ. В данной главе описаны и протестированы используемые механизмы корреляционного анализа на

основе вычисления коэффициента Пирсона, обсуждается возможность интеграции системы с другими подсистемами существующих SIEM-систем. Рассмотрены различные варианты конфигурации ансамбля методов машинного обучения (интеллектуальных классификаторов), на основе проведенных вычислительных экспериментов выявлен наиболее рациональный вариант объединения этих классификаторов.

В четвертой главе представлена архитектура исследовательского прототипа распределенной интеллектуальной системы мониторинга (РИСМ) ИБ IIoT, включающая в себя три уровня, на нижних двух уровнях которой функционирует двухуровневая искусственная иммунная система, а на верхнем – централизованный супервизор, реализующий алгоритмы случайного леса, ИНС и корреляционного анализа событий ИБ, а также принятие согласованного решения на основе схемы голосования. В данной главе также рассмотрена методика применения РИСМ, приведены результаты вычислительных экспериментов, связанные с решением двух практических прикладных задач обнаружения атак и аномалий сетевого трафика IIoT – беспроводной мультисенсорной сети, состоящей из 100 узлов, а также системы контроля состояния воды в резервуаре, используемой в промышленной автоматизированной водораспределительной системе. Результаты вычислительных экспериментов подтверждают высокую эффективность применения предложенной РИСМ для решения задач мониторинга ИБ этих систем.

В Заключении представлены выводы и полученные результаты работы.

В приложениях приведены акты внедрения результатов диссертационной работы и дополнительные результаты проведенных исследований.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, является высокой, что обеспечивается корректной постановкой цели и задач исследования, выбором методов проведения вычислительных экспериментов и решения поставленных задач, непротиворечивостью и повторяемостью полученных результатов.

Достоверность и новизна полученных результатов подтверждается сравнением полученных результатов с результатами других авторов, апробацией предложенных решений при решении ряда прикладных задач, публикацией основных результатов исследования в ведущих рецензируемых журналах, их обсуждением на представительных всероссийских и международных научно-практических конференциях.

Полученные результаты опубликованы в 17 работах, из них 6 – в журналах, включенных в перечень изданий ВАК по научной специальности 2.3.6.; 3 – в изданиях, индексируемых в международной базе данных цитирования Web of Science (одна из них одновременно индексируется в базе данных Scopus); 8 – в прочих изданиях.

Автореферат достаточно полно отражает содержание диссертации и существо полученных в ней результатов.

Научная новизна работы заключается в следующем:

1. Новизна предложенной автором концепции построения интеллектуальной системы мониторинга ИБ IIoT базируется на применении многоагентной платформы системы обнаружения атак и аномалий сетевого трафика IIoT, использующей в процессе своего функционирования механизмы ИИС, корреляционного анализа данных, ансамбль методов машинного обучения, что позволяет повысить показатели эффективности обнаружения внешних и внутренних угроз БИ.

2. Новизна разработанных алгоритмов обнаружения атак и аномалий сетевого трафика IIoT заключается в интеграции и модификации различных механизмов и подходов в рамках общей теории ИИС в составе системы мониторинга ИБ, реализованной на основе распределенной двухуровневой ИИС, что позволяет снизить дополнительно уровень принятия ошибочных решений, выявляя в том числе новые, ранее неизвестные системе угрозы БИ.

3. Новизна разработанных алгоритмов обнаружения атак и аномалий сетевого трафика IIoT на основе ансамбля методов машинного обучения заключается во введении третьего уровня распределенной интеллектуальной системы мониторинга (РИСМ), реализующего совместно с ИИС использование нескольких интеллектуальных классификаторов – алгоритм случайного леса, искусственную нейронную сеть, а также подсистему корреляционного анализа событий ИБ, что позволяет повысить полноту и точность обнаружения различных типов компьютерных атак и аномалий, способствуя повышению эффективности системы мониторинга ИБ IIoT в целом.

4. Новизна предложенной архитектуры исследовательского прототипа РИСМ ИБ IIoT заключается в реализации данной системы в классе распределенных многоагентных гибридных интеллектуальных систем, интегрирующих различные технологии интеллектуального анализа данных (в данном случае, это методы и алгоритмы искусственных иммунных систем, методы машинного обучения, подсистема корреляционного анализа, механизм принятия согласованного решения), что позволяет повысить эффективность решения задач обнаружения атак и аномалий сетевого трафика в процессе мониторинга ИБ систем и сетей IIoT, используя в качестве дополнительной информации текущие данные о событиях ИБ от взаимодействующей SIEM-системы.

Теоретическая и практическая значимость полученных автором результатов

Теоретическая значимость работы обусловлена тем, что в ней разработаны научно обоснованные положения, составляющие основу решения задач мониторинга ИБ промышленного Интернета вещей: предложена концепция построения РИСМ ИБ промышленного Интернета вещей, разработаны модифицированные алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика в составе двухуровневой ИИС, а также алгоритмы функционирования трехуровневой РИСМ ИБ с использованием на верхнем уровне

ансамбля методов машинного обучения при его взаимодействии с подсистемой корреляции событий ИБ.

Практическая значимость результатов подтверждена разработкой программных модулей в составе исследовательского прототипа РИСМ ИБ и методики ее применения, решением с помощью предложенной РИСМ ряда прикладных задач обнаружения сетевых атак и аномалий сетевого трафика IIoT. Результаты проведенных вычислительных экспериментов показали высокую эффективность предложенных решений при обнаружении сетевых атак и аномалий IIoT. Полученные значения показателей эффективности в среднем на 1,5-2% выше, чем значения аналогичных показателей известных систем обнаружения атак и аномалий. Результаты работы внедрены в ряде организаций, что подтверждается соответствующими актами внедрения.

Соответствие паспорту специальности

Диссертация соответствует следующим пунктам паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»: п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»; п. 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».

Замечания по работе

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 непосредственно 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.

В целом, указанные замечания не снижают высокой научной ценности и практической значимости выполненного исследования.

Заключение

Диссертация Шамсутдинова Рината Рустемовича, представленная на соискание ученой степени кандидата технических наук, обладает внутренним единством, научной новизной, теоретической и практической значимостью, она является законченной научно-квалификационной работой, посвященной решению актуальных задач мониторинга информационной безопасности сетей промышленного Интернета вещей, и соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней. С учетом вышеизложенного считаю, что автор диссертации – Шамсутдинов Ринат Рустемович заслуживает присуждения

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

Официальный оппонент:
кандидат технических наук, доцент,
доцент кафедры безопасности
информационных систем,
федерального государственного автономного
образовательного учреждения высшего
образования «Самарский национальный
исследовательский университет
имени академика С. П. Королева»

Бурлаков Михаил Евгеньевич

Кандидатская диссертация защищена
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Даю согласие на обработку персональных данных.

Адрес места основной работы: 443086, г. Самара, Московское шоссе, д.34
Рабочий телефон: 8 (846) 337-99-41
Адрес эл. почты: burlakov@ssau.ru

Подпись Бурлакова М.Е. удостоверяю.
Начальник отдела сопровождения деятельности
ученых советов Самарского университета
Бояркина Бояркина У.В.
«2» августа 2023 г.