ОТЗЫВ

официального оппонента

доктора технических наук, доцента Сычугова Алексея Алексеевича

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

Подключение автоматизированных промышленных объектов к сетям общего доступа, внедрение систем промышленного Интернета вещей (Industrial Internet of Things, IIoT) обуславливает возникновение новых, более сложных проблем обеспечения информационной безопасности (ИБ) по сравнению с теми, которые существовали ранее. Это вызвано, прежде всего, такими факторами, как сложность и гетерогенный характер структуры IIoT (многоуровневая архитектура IIoT, многообразие «вещей» – промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами, интеграции программно-аппаратных средств с использованием различных сетевых технологий), доступность для атак через Интернет со стороны внешних злоумышленников.

Статистика последних лет показывает значительный рост числа сетевых атак на промышленные объекты, успешная реализация которых может привести не только к значительному финансовому и материальному ущербу, но и к экологическим катастрофам, травмам и гибели людей. В то же время, нормативно-правовая база обеспечения информационной безопасности (ИБ) промышленного Интернета вещей находится еще в начальной стадии развития: подготовленные в этой области проекты стандартов большей частью пока только обсуждаются, нет единого подхода к обеспечению ИБ систем и сетей IIoT, отсутствует общая модель безопасности этих систем.

Анализ источников литературы показывает, что одно из ключевых мест при построении систем обеспечения ИБ промышленного Интернета вещей должны занимать системы мониторинга ИБ сетевого трафика устройств и сетей IIoT. Хорошие перспективы при решении этих задач показывают распределенные интеллектуальные системы мониторинга ИБ, основанные на интеграции различных технологий искусственного интеллекта (нечеткая логика, нейронные сети, искусственные иммунные системы, методы машинного обучения и др.). Поэтому выбранное в данной работе направление исследований, посвященное разработке и исследованию методов и алгоритмов построения гибридной распределенной интеллектуальной системы мониторинга ИБ систем и сетей промышленного Интернета вещей, позволяющей своевременно обнаруживать компьютерные атаки и аномалии сетевого трафика этих систем, следует считать актуальным и востребованным.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка сокращений, словаря терминов, списка литературы и приложений, она содержит 38 рисунков, 38 таблиц, 3 приложения, выполнена на 187 страницах. Список использованной литературы включает 201 источник. В приложениях содержатся копии актов внедрения и дополнительные материалы по результатам исследований.

Во введении приведены обоснование актуальности работы, степень разработанности темы исследования, представлены объект, предмет и методы исследования, сформулированы цель и задачи диссертационной работы, научная новизна, теоретическая и практическая значимость полученных результатов.

В первой главе проведен анализ архитектуры, функциональных областей и специфики промышленного Интернета вещей (IIoT). Приведена статистика компьютерных атак и инцидентов ИБ, связанных с применением IIoT, указаны существующие коммерческие решения для зашиты систем Интернета вещей. Рассмотрены российские и международные нормативные документы в области обеспечения ИБ промышленных автоматизированных систем, промышленного Интернета вещей.

В данной главе также проанализированы: применение беспроводных сенсорных сетей в составе IIoT, существующие методы обеспечения ИБ IIoT, виды сетевых атак и сетевые аномалии; подчеркивается актуальность проблемы выявления атак нулевого дня; рассмотрены методы построения интеллектуальных систем мониторинга ИБ систем и сетей IIoT, включая методы построения искусственных иммунных систем (ИИС) и гибридных интеллектуальных систем.

Во второй главе приведены результаты разработки и исследования алгоритмов обнаружения сетевых атак и аномалий на основе ИИС. Приведены функциональная модель процесса мониторинга ИБ сетей IIoT, диаграмма классов системы мониторинга на основе ИИС, используемые показатели оценки эффективности обнаружения сетевых атак и аномалий. Описан процесс нормализации анализируемых параметров сетевого трафика, предложенный алгоритм функционирования ИИС и схема ее реализации на двух уровнях в классе многоагентных распределенных систем.

Агенты первого (нижнего) уровня интегрируются в подсети устройств IIoT, собирают данные сетевого трафика, проводят нормализацию, выявляют атаки и аномалии с использованием известного алгоритма негативной селекции и модифицированного алгоритма клонального отбора. Указанная модификация позволяет агентам нижнего уровня передавать друг другу обучающие данные, сформированные на основе выявленных атак и аномалий.

Агенты второго уровня расположены на границах сетей IIoT, собирают данные от агентов первого уровня о выявленных атаках и аномалиях, а также от сторонних подключаемых систем, таких как SIEM-системы, межсетевые экраны и т.д., анализируют уровень опасности для конкретного участка сети на основе применения модифицированного алгоритма дендритных клеток. Результаты проведения вычислительных экспериментов показывают высокие значения показателей эффективности обнаружения атак и аномалий с помощью ИИС на тестовом наборе данных NSL-KDD.

В третьей главе приведены результаты разработки и исследования алгоритмов обнаружения сетевых атак и аномалий в сетях IIoT на основе применения ансамбля методов машинного обучения, реализованных в составе

распределенной интеллектуальной системы мониторинга (РИСМ). Приведена структура и концепция построения РИСМ, описана реализованная в ее составе подсистема корреляционного анализа событий ИБ. Основу построения РИСМ составляет ансамбль классификаторов, состоящий из распределенного комплекса агентов двухуровневой ИИС и супервизора (агента третьего уровня), реализующего в своем составе искусственную нейронную сеть, алгоритм случайного леса, подсистему корреляционного анализа данных, подсистему принятия решений.

Проведены вычислительные эксперименты для различных вариантов объединения классификаторов в составе ансамбля, результаты которых показали эффективность применения ИИС для первичного анализа и выявления атак (аномалий), а затем – использования комитета классификаторов для классификации выявленных атак (аномалий) на основе механизма голосования.

В четвертой главе представлена архитектура РИСМ, описаны границы применимости системы, разработана методика обнаружения компьютерных атак и аномалий сетевого трафика промышленного Интернета вещей на основе применения РИСМ. Приведены результаты решения конкретных прикладных задач – обнаружения атак и аномалий сетевого трафика системы контроля мутности и уровня воды в резервуаре с использованием тестового набора данных (датасета) WUSTL-IIOT-2021, а также беспроводной сенсорной сети с использованием набора данных WSN-DS. Вычислительные эксперименты, проведенные на указанных датасетах, показывают высокие значения показателей эффективности разработанной РИСМ.

В Заключении приведены основные выводы и результаты проведенных исследований.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации.

Обоснованность научных положений, выводов и рекомендаций, представленных в диссертации, подтверждается использованием общепринятых теоретических положений и методов проведения вычислительных экспериментов, опубликованными по материалам исследований работами, включающими в себя 6 статей в научных журналах, входящих в Перечень рецензируемых научных изданий,

рекомендованных ВАК; 3 статьи, индексируемые в Web of Science (одна из них индексируется в Web of Science и в Scopus), 8 статей в прочих изданиях.

Диссертация содержит достаточное для понимания результатов проведенных исследований количество иллюстративного материала и таблиц.

Автореферат достаточно полно отражает содержание диссертации. Полученные результаты соответствуют заявленным автором пунктам паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Достоверность и новизна полученных результатов подтверждается непротиворечивостью и степенью повторяемости полученных результатов, сравнением этих результатов с результатами других авторов, публикацией полученных результатов в ведущих рецензируемых журналах, обсуждением основных положений диссертационной работы на российских и международных конференциях, апробацией результатов работы в ряде организаций, подтвержденной актами внедрения.

Научная новизна работы

В качестве основных результатов диссертационного исследования, обладающих научной новизной, можно отметить следующие:

1. Концепция построения распределенной интеллектуальной системы мониторинга ИБ сетей промышленного Интернета вещей, отличающаяся интеграцией в составе этой системы механизмов искусственных иммунных систем, методов машинного обучения, подсистемы корреляции событий ИБ, что позволяет повысить полноту и точность выявления внешних и внутренних угроз безопасности информации.

2. Алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика IIoT на основе адаптивных механизмов ИИС, отличающиеся объединением различных подходов в рамках теории искусственных иммунных систем и модификации известных алгоритмов клональной селекции, дендритных клеток и обновления детекторов, что позволяет в совокупности существенно снизить уровень принятия ошибочных решений, а также выявлять как известные, так и ранее неизвестные системе угрозы безопасности информации.

3. Алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика IIoT, основанные на применении ансамбля методов машинного обучения и подсистемы корреляции событий ИБ, отличающиеся использованием специфического иммунного ответа ИИС совместно с другими классификаторами (нейронные сети, алгоритм случайного леса), что обеспечивает дифференцированный подход к обнаружению различных типов сетевых атак и аномалий и позволяет в целом повысить эффективность функционирования системы мониторинга ИБ.

4. Архитектура исследовательского прототипа распределенной интеллектуальной системы мониторинга ИБ IIoT, отличающаяся применением многоагентного подхода к построению многоуровневых распределенных гибридных интеллектуальных систем, что позволяет более полно учесть особенности структурно-функциональной организации IIoT как распределенного объекта мониторинга, используя при этом дополнительно полученную информацию об инцидентах ИБ от взаимодействующей SIEM-системы.

Теоретическая и практическая значимость полученных автором результатов

Значение полученных результатов для теории и методологии мониторинга ИБ заключается в том, что в диссертации разработаны концепция построения распределенной интеллектуальной системы мониторинга ИБ промышленного Интернета вещей; алгоритмы обнаружения компьютерных атак и аномалий сетевого трафика IIoT с использованием адаптивных механизмов ИИС, ансамбля методов машинного обучения и подсистемы корреляции событий ИБ; архитектура исследовательского прототипа распределенной интеллектуальной системы мониторинга ИБ IIoT.

Практическая значимость полученных результатов заключается в том, что разработанные программные модули исследовательского прототипа интеллектуальной системы мониторинга ИБ промышленного Интернета вещей и методика ее применения для обнаружения компьютерных атак и аномалий сетевого трафика IIoT позволяют значительно повысить полноту и точность обнаружения

сетевых атак и аномалий, выявлять в том числе новые, ранее неизвестные системе угрозы безопасности информации.

Замечания по работе

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.

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают значимости и общей положительной оценки представленной работы.

Заключение

Диссертация Шамсутдинова Р.Р., представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, выполненной на актуальную тему, в которой решена научная задача, изложены новые научно обоснованные технические решения и разработки, имеющие существенное значение для развития страны. Результаты работы обладают научной новизной и практической ценностью.

Считаю, что 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.

Официальный оппонент:
доктор технических наук, доцент,
директор Института прикладной
математики и компьютерных наук,
заведующий кафедрой
информационной безопасности,
Федеральное государственное
бюджетное образовательное учреждение
высшего образования
«Тульский государственный университет»

Сычугов Алексей Алексеевич

28.08.2023

Докторская диссертация защищена
по специальности 05.13.01 – Системный анализ,
управление и обработка информации

Даю согласие на обработку персональных данных

Адрес места основной работы: 300012, г. Тула, пр. Ленина, д.92, ауд. 425
Рабочий телефон: +7 (4872) 25-79-50
Адрес эл. почты: xru2003@list.ru