DOI 10.37882/2223-2966.2024.12.31

АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ АВТОМАТИЗАЦИИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ANALYSIS OF THE CURRENT STATE OF RESEARCH IN THE FIELD OF AUTOMATION OF INFORMATION SECURITY MONITORING OF INDUSTRIAL INTERNET OF THINGS NETWORKS USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

A. Rusakov
E. Bolgar
E. Ivanov

Summary. The modern development of industry, designated by the term Industry 4.0, is inextricably linked with the introduction and development of the industrial Internet of Things (IIoT). This approach to automation and optimization of production processes opens up new horizons for improving the efficiency and competitiveness of enterprises. However, with the growing popularity of IIoT, a number of serious challenges arise, among which information security plays a key role. At a time when IIoT devices are becoming increasingly vulnerable to cyber attacks, the need to develop reliable protection methods becomes critically important. This article discusses the main problems associated with ensuring the information security of IIoT networks, as well as modern approaches and technologies aimed at solving them.

Keywords: information security, Internet of things, Internet of Things security, artificial intelligence technologies.

Русаков Алексей Михайлович
старший преподаватель,
МИРЭА — Российский технологический университет
rusal@bk.ru
Болгар Евгений Петрович
МИРЭА — Российский технологический университет
sorry20iq@vk.com
Иванов Егор Сергеевич
МИРЭА — Российский технологический университет
ivanov.e.s@bk.ru

Аннотация. Современное развитие промышленности, обозначаемое термином Industry 4.0, неразрывно связано с внедрением и развитием промышленного Интернета вещей (IIoT). Этот подход к автоматизации и оптимизации производственных процессов открывает новые горизонты для повышения эффективности и конкурентоспособности предприятий. Однако с ростом популярности IIoT возникает и ряд серьезных вызовов, среди которых ключевую роль играет обеспечение информационной безопасности. В условиях, когда устройства IIoT становятся все более уязвимыми к кибератакам, необходимость в разработке надежных методов защиты становится критически важной. В данной статье рассматриваются основные проблемы, связанные с обеспечением информационной безопасности сетей IIoT, а также современные подходы и технологии, направленные на их решение.

Ключевые слова: информационная безопасность, интернет вещей, безопасность интернета вещей, технологии искусственного интеллекта.

Введение

Из-за значительного прорыва в области промышленного Интернета вещей (IIoT) произошло развитие промышленности, известное как Industry 4.0. По данным аналитической компании Research and Markets, с 2021 года мировой рынок IIoT демонстрирует среднегодовой рост на уровне 21 %, и к 2026 году его объем может достичь 344,7 миллиарда долларов. Промышленный Интернет вещей представляет собой расширение концепции Интернета вещей (IoT), ориентированное на решение промышленных задач. IoT подразумевает создание вычислительной сети, состоящей из физических устройств, или «вещей», которые оснащены встроенными технологиями для взаимодействия как между собой, так и с окружающей средой [1]. С технологической точки зрения, IoT можно рассматривать как четырехуровневую систему, включающую подключаемые устройства (сенсоры, датчики, терминалы), сети для их взаимодействия, IoT-платформы и приложения для конечных пользователей. Согласно стандарту ПНСТ 643-2022 «Информационные технологии», IIoT является важным элементом технологического прогресса. Интернет вещей промышленный. Термины и определения», IIoT представляет собой сеть, объединяющую машины, компьютеры и людей для обеспечения интеллектуальных производственных процессов с использованием расширенной аналитики данных, что приводит к качественно

новым бизнес-результатам. В области IIoT необходимыми вещами для интеграции в сеть являются различные приборы. Отметим, что коммуникационные интерфейсы, как проводные, так и беспроводные, играют центральную роль в этой системе. Однако вне зависимости от используемой технологии на канальном и физическом уровнях, устройства должны поддерживать протокол IP для интеграции в инфраструктуру IIoT. IIoT тесно связано с киберфизическими системами и автоматизированными системами управления технологическими процессами. Киберфизическая система — это умная структура, состоящая из взаимодействующих физических и вычислительных элементов. АСУ ТП традиционно рассматриваются как комплексные решения для автоматизации основных операций на производстве, однако в последние годы их функции и цели все больше смещаются в сторону идеологии IIoT. Важно отметить, что многие промышленные объекты в России, использующие или внедряющие технологии IIoT, подпадают под действие федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который охватывает информационные системы, телекоммуникационные сети и автоматизированные системы управления, В 2020 году в России был разработан стандарт ПНСТ 420-2020 «Информационные технологии, который описывает архитектуру IIoT, включая различные интересы и модели. Стандарт предлагает трехуровневую архитектуру IIoT, которая включает [2, 3]:

- Уровень предприятия: здесь реализуются приложения, системы поддержки принятия решений и интерфейсы для конечных пользователей, осуществляющие получение информации с других уровней и выдачу управляющих команд.
- Уровень платформы: на этом уровне происходит сбор и обработка данных с граничного уровня, а также передача управляющих команд от уровня предприятия к граничному уровню.

Граничный уровень: здесь осуществляется сбор данных от граничных узлов через сеть ближнего действия и реализация управляющих команд. Одной из основных проблем при создании и эксплуатации IIoT является обеспечение информационной безопасности его устройств и систем. Наиболее распространенные причины уязвимости IIoT включают:

- Устаревшее системное и прикладное программное обеспечение устройств IIoT и недостаточное внимание к обновлениям.
- Передача данных без шифрования.
- Стандартные заводские настройки безопасности устройств.
- Незащищенные интерфейсы.
- Уязвимости в операционных системах общего назначения.
- Невозможность оснастить многие устройства встроенными средствами безопасности.

Специфика IIoT заключается в подключении промышленных систем к Интернету, возможности удаленного управления ими, использовании облачных систем и ограниченности вычислительных и энергетических ресурсов автономных IIoT-устройств. Благодаря отчету «Threat Intelligence Report 2020» которая предоставила Nokia, доля атак на устройства IIoT возросла до 32,7 %. По данным Check Point, 67 % организаций столкнулись с инцидентами безопасности, связанными с IIoT. По информации Касперского, наблюдается большой всплеск новых образцов вредоносного ПО для IIoT-устройств. В 2015 году их было всего 483, а к 2020 году это число возросло до 401. 55 % респондентов опроса, проведенного данной лабораторией, считают IIoT одним из главных факторов, влияющих на кибербезопасность АСУ ТП, однако только 14 % организаций используют средства обнаружения сетевых аномалий, а 19 % — системы мониторинга сети и трафика. Также подчеркивается уязвимость устройств IIoT, где слабые места включают переход на IPv6, недостаточную аутентификацию и использование стандартных учетных записей, сложности с обновлением программного обеспечения и отсутствие поддержки со стороны производителей, открытые неиспользуемые порты, применение текстовых протоколов и уязвимых мобильных технологий. Производители активно работают над улучшением безопасности IIoT. Однако злоумышленники могут скомпрометировать сенсорные узлы, нарушая целостность данных и увеличивая расход ресурсов. «отказ в обслуживании» является одним из популярных видов атак. Например, в облачной системе Microsoft Azure для обеспечения информационной безопасности IoT используется методика моделирования угроз STRIDE, которая рассматривает все уровни и компоненты IoT с точки зрения возможных угроз и предлагает меры защиты. В других исследованиях проводится сравнение возможностей обеспечения безопасности различных IoT-фреймворков, таких как AWS IoT от Amazon, Azure IoT от Microsoft и других. Важно отметить, что в рамках IIoT часто применяются беспроводные сенсорные сети (WSN), состоящие из множества автономных сенсорных узлов, которые собирают данные и обмениваются ими через беспроводное соединение с более мощным узлом — базовой станцией. Из-за распределенной открытой архитектуры и ограниченных ресурсов сенсорных узлов такие сети подвержены атакам.

Ведутся работы по повышению защищенности беспроводных сенсорных сетей [4]. Основанное на анализе поведения соседних углов предлагается в качестве меры защиты предлагается адаптивное взаимодействие компонентов системы. Защищенность (кибербезопасность) сети и системы». Эти стандарты предлагают методику оценки защищенности промышленных коммуникационных сетей, которая включает выделение независимых зон безопасности, построение модели физической ар-

хитектуры и оценку угроз и рисков информационной безопасности. Среди международных документов в области обеспечения информационной безопасности IoT и IIoT можно выделить отчеты NISTIR, рекомендации Министерства внутренней безопасности США, а также международные стандарты, разработанные ИСО и МЭК. Принятие международного стандарта ISO/IEC 30162:2022 «Интернет вещей. Требования к совместимости устройств, сетей и систем промышленного Интернета вещей» способствует решению проблемы интеграции различных устройств IIoT, что, в свою очередь, помогает обеспечить безопасность сетевого взаимодействия этих устройств.

Методы обеспечения информационной безопасности сетей IIoT

Требования к безопасности сетей IIoT охватывают как защиту систем, так и безопасность обрабатываемой информации [1,3]. Основные нормативные акты включают Приказы ФСТЭК № 31, № 235 и № 239. Как уже упоминалось, системы IIoT имеют много общего с промышленными системами автоматизации (АСУ ТП) и объектами критической информационной инфраструктуры (КИИ). Поэтому большинство методов обеспечения их информационной безопасности будут зависеть от требований, предъявляемых к системам и объектам данного типа.

- Приказ ФСТЭК № 31 от 14.03.2014 г. устанавливает требования к защите информации в автоматизированных системах управления на критически важных объектах. Он определяет правила для систем защиты АСУ ТП и меры, необходимые для обеспечения их безопасности.
- Приказ ФСТЭК № 235 от 21.12.2017 г. касается создания систем безопасности значимых объектов критической информационной инфраструктуры и их функционирования.

Конкретные требования и состав необходимых мер по обеспечению информационной безопасности значимых объектов КИИ определяются Приказом ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Этот документ устанавливает цели и задачи обеспечения безопасности, объекты защиты, состав мер по организационно-технической защите информации, а также требования к обеспечению безопасности на всех этапах жизненного цикла значимых объектов КИИ и их программно-аппаратных комплексов. В данный момент на этапе разработки находится программа стандартизации в области IIoT, а также обсуждаются предварительные национальные стандарты (ПНСТ), некоторые из которых были упомянуты ранее. Международные стандарты уже сегодня охватывают широкий спектр вопросов, связанных с обеспечением безопасности IIoT-систем. К тематике IIoT непосредственно относится ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения». Этот стандарт описывает задачи, объекты и уровни мониторинга, а также устанавливает требования к источникам данных, сбору, хранению, агрегированию и обработке данных, а также к представлению результатов мониторинга и их защите. В контексте информационной безопасности риск определяется как количественная мера потенциального ущерба, связанного с реализацией угрозы, с учетом вероятности ее возникновения. Прогнозирование и оценка рисков информационной безопасности обсуждаются в ряде исследований, включая работы, посвященные корпоративным сетям и критическим инфраструктурам. С целью повышения уровня автоматизации процессов управления инцидентами информационной безопасности и повышения эффективности реагирования на киберугрозы создаются ситуационные центры управления информационной безопасностью (Security Operation Center, SOC). Операторы центров управления безопасностью (SOC) в основном работают с системами управления безопасностью и событиями (SIEM). Эти системы собирают данные о событиях из различных источников по всей сети, сопоставляют их и выявляют инциденты информационной безопасности. Подсистемы корреляционного анализа являются важной частью SIEM-систем, которые используются для управления информацией о событиях и инцидентах информационной безопасности. Методы SIEM эффективно применяются для обнаружения сетевых атак на IIoT.

Источники информации для SIEM-систем включают [5]:

- Системы аутентификации и контроля доступа, предоставляющие данные о попытках доступа.
- DLP-системы, информирующие о попытках инсайдерских утечек.
- IDS/IPS-системы, предоставляющие данные о сетевых атаках и изменениях конфигурации.
- Межсетевые экраны, фиксирующие атаки и вредоносное ПО.
- Антивирусные приложения, генерирующие события о работоспособности ПО и изменениях конфигураций.
- Журналы событий серверов и рабочих станций используются для контроля доступа.
- Контроль информационной безопасности (ИБ) в сетях IIoT осуществляется через анализ сетевого трафика. Сбор этих данных усложняется разнообразием протоколов и типов подключений, используемых устройствами IIoT. В системах Интернета вещей применяются:
- Беспроводные локальные сети (WLAN) и персональные беспроводные сети (WPAN), включая технологии с малым радиусом действия, такие как

Wi-Fi, 6LoWPAN, ZigBee IP, Thread, Z-Wave, ZigBee, WirelessHart, BLE 4.2 (Bluetooth Mesh) и MiWi.
- Энергоэффективные глобальные сети (LPWAN), которые предназначены для передачи небольших объемов данных на большие расстояния, такие как LoRaWAN, SIGFOX, CIoT, 4G LTE, 5G, NB-IoT и другие.

Необходимо учитывать распределенный характер объекта мониторинга ИБ. Важно учитывать распределенный характер объектов мониторинга ИБ. В качестве источников входных данных должны использоваться не только устройства IIoT, но и сетевое оборудование, включая маршрутизаторы и межсетевые экраны (МЭ). Также имеется возможность взаимодействия с SIEM-системами. Важно реализовать пространственно-временную модель сбора входных данных для систем мониторинга, где данные должны иметь привязку к конкретным узлам сети IIoT и времени их регистрации, то есть быть темпоральными. Это требует учета разнородности данных на этапе их нормализации. На этапе обучения и тестирования сервис-ориентированной архитектуры (СОА) для сети IIoT мы будем опираться на параметры, используемые в различных наборах данных о сетевых соединениях, которые содержат характеристики трафика как для нормальных соединений, так и для атак. После сбора и нормализации данные о сетевом трафике подвергаются анализу с использованием различных методов и технологий интеллектуального анализа данных. Интеллектуальные системы сегодня в первую очередь ассоциируются с искусственными нейронными сетями (ИНС), которые зарекомендовали себя как эффективный метод классификации, применяемый для решения множества задач, включая обнаружение атак и сетевых аномалий.

Методы машинного обучения охватывают различные алгоритмы, такие как деревья решений, алгоритмы муравьиной колонии, случайные леса, k-ближайшие соседи, нечеткая логика, машины опорных векторов, наивный байесовский классификатор и генетические алгоритмы. Эти методы активно применяются для решения задач интеллектуального анализа данных, включая выявление и классификацию атак на основе анализа сетевого трафика. Искусственные иммунные системы (ИИС) также находят применение для обнаружения неизвестных атак и обладают способностью к постоянному самообучению. По данным исследований, ИИС могут значительно превосходить ИНС и генетические алгоритмы по быстродействию и количеству ошибок. Повышение эффективности выявления сетевых атак и аномалий может быть достигнуто за счет интеграции различных методов искусственного интеллекта в рамках гибридной интеллектуальной системы (ГИС) [6]. ГИС объединяет технологии ИИ для получения синергетического эффекта, компенсируя недостатки одного метода преимуществами другого. Например, методы статистического анализа позволяют выявлять известные типы аномалий, но не способны обнаруживать новые, ранее неизвестные виды атак. В свою очередь, алгоритмы машинного обучения могут адаптироваться к изменяющимся угрозам, но их работа часто воспринимается как «черный ящик». Интеграция этих подходов в рамках гибридной системы дает возможность сочетать преимущества статистического анализа и машинного обучения, создавая более эффективное и прозрачное решение для обнаружения сетевых атак [7,8].

- Применительно к промышленным сетям и сетям Интернета вещей используются следующие подходы:
- Нейронные сети глубокого обучения для обнаружения сетевых атак и аномалий в IoT/IIoT.
- Методы машинного обучения для обнаружения атак на IoT и IIoT, включая сравнение различных алгоритмов с ИНС, где лучшую точность демонстрируют ИНС и случайный лес.
- Искусственные иммунные системы для идентификации вторжений в сети IoT и IIoT.
- Гибридные интеллектуальные системы обнаружения атак на IoT, IoMT, АСУ ТП и IIoT, включая алгоритмы ИИС.

В задаче обнаружения сетевых атак и аномалий функционирование искусственных иммунных систем (ИИС) аналогично работе человеческого организма по выявлению и противодействию вредным воздействиям. Алгоритм клональной селекции (CSA) моделирует процесс размножения активированных B-лимфоцитов, при этом существуют различные методы его реализации Один из подходов предполагает случайную генерацию детекторов и определение их «аффинности» — меры близости к вектору данных нормального состояния системы. Детекторы с наибольшей аффинностью клонируются в большем количестве. На этапе анализа, если ни один детектор не соответствует исследуемым данным, они считаются аномальными. Существуют различные подходы к его реализации [9]. Например, в одном из исследований описывается создание детекторов, которые обнаруживают нормальное состояние системы. В результате формируются детекторы, срабатывание которых указывает на нештатное состояние контролируемой системы или процесса. Количество детекторов для каждого класса аномалий определяется пропорционально количеству примеров этого класса в обучающих данных. Детекторы с наибольшим значением аффинности клонируются в количестве, пропорциональном этому значению. Каждый клон подвергается мутации, степень которой обратно пропорциональна аффинности. В другом подходе детекторам предоставляются обучающие данные, соответствующие аномалиям. Избыточное увеличение числа детекторов из-за клонирования может adversely

affect the system's performance, поэтому часто устанавливаются ограничения как на их количество, так и на срок их существования. Если детектор выявляет аномалию, его срок жизни существенно продлевается. В целом, алгоритм клональной селекции является адаптивным, что позволяет дообучать систему в процессе её эксплуатации. Количество необходимых детекторов определяется как отношение количества детекторов в множестве детекторов, соответствующих классу данных, к количеству строк обучающих данных об аномалиях этого класса. Увеличение числа детекторов из-за клонирования может отрицательно влиять на производительность системы, поэтому часто устанавливаются ограничения как на количество детекторов, так и на срок их существования. Если срок жизни детектора истекает, он удаляется, и на его место создается новый. В случае, если детектор выявляет аномалию, его срок существования значительно продлевается. В целом, алгоритм клональной селекции обладает адаптивностью, что позволяет дообучать систему в процессе её эксплуатации. Однако его применение не всегда обеспечивает толерантность системы к «своим» данным. Согласно теории опасности, иммунная система при определении необходимости реагирования учитывает не только обнаружение чужеродных патогенов, но и степень опасности ситуации. Это означает, что иммунитет должен более агрессивно реагировать на «свое, но опасное», а не только на «чужое, но безопасное» Это означает, что иммунитет должен более агрессивно реагировать не на «чужое, но безопасное», а на «свое, но опасное». Различные подходы к построению ИИС имеют свои преимущества и недостатки. Например, методы на основе правил экспертных систем отличаются высокой точностью в выявлении известных типов атак, но требуют ручной настройки и не способны адаптироваться к новым, ранее неизвестным угрозам. В свою очередь, алгоритмы аномального поведения, использующие обучение без учителя, могут автоматически обнаруживать нетипичные паттерны сетевого трафика, однако могут давать больше ложных срабатываний. Сочетание этих подходов в рамках гибридной системы позволяет сбалансировать точность выявления известных атак и гибкость обнаружения новых, неизвестных вторжений, повышая общую эффективность защиты.

Заключение

Таким образом, обеспечение информационной безопасности сетей промышленного Интернета вещей представляет собой сложную и многогранную задачу, требующую комплексного подхода и применения современных технологий. Учитывая растущие угрозы и уязвимости, связанные с использованием IIoT, необходимо активно развивать и внедрять методы защиты, включая использование искусственного интеллекта и машинного обучения для мониторинга и анализа сетевого трафика. Важно также учитывать требования законодательства и стандартизации в области информационной безопасности, что позволит создать надежную инфраструктуру для функционирования IIoT. В конечном итоге, успешное решение проблем безопасности в этой области будет способствовать не только защите данных и систем, но и обеспечению устойчивого развития промышленности в эпоху цифровизации.

ЛИТЕРАТУРА

1. Оценка и регулирование рисков нарушения информационной безопасности телекоммуникационных сетей связи и управления промышленного интернета вещей / С.А. Ермаков, Я.М. Каценко, А.А. Болгов [и др.] // Информация и безопасность. — 2020. — Т. 23, № 1. — С. 107–114. — EDN LDZKCF.
2. Ларионов, А.Ю. Промышленный интернет вещей: проблемы безопасности и их решения в сетях WSN / А.Ю. Ларионов, Е.Е. Каранова // Наука и образование в наши дни: фундаментальные и прикладные исследования: Материалы XLIII Всероссийской научно-практической конференции. В 2-х частях, Ростов-на-Дону, 23 декабря 2021 года. Том Часть 1. — Ростов-на-Дону: ООО «Издательство ВВМ», 2021. — С. 105–108. — EDN ZJSMRY.
3. Рылов, С.А. Промышленный интернет. Современный подход и концепции: учебник / С.А. Рылов. — Москва: РТУ МИРЭА, 2023. — 124 с. — ISBN 978-5-7339-1969-0. — EDN TVXBQA.
4. Добрынин, С.Л. Мониторинг и предиктивная аналитика технологического оборудования на базе промышленного Интернета вещей / С.Л. Добрынин, В.Л. Бурковский // Вестник Воронежского государственного технического университета. — 2020. — Т. 16, № 5. — С. 7–12. — DOI 10.36622/VSTU.2020.16.5.001. — EDN DTASGG.
5. Лазарева, Н.Б. Анализ программных продуктов SIEM-СИСТЕМ с целью выбора решения для защиты иб предприятия / Н.Б. Лазарева, М.С. Кармадонов // Far East Math — 2022 : Материалы национальной научной конференции, Хабаровск, 22–26 ноября 2022 года / Редколлегия: Е.Г. Агапова (отв. редактор) [и др.]. — Хабаровск: Тихоокеанский государственный университет, 2022. — С. 127-136. — EDN TGFQUC.
6. Александренко, Н.Д. Искусственный интеллект в информационной безопасности / Н.Д. Александренко, А.С. Зуфарова // ТОГУ-Старт: фундаментальные и прикладные исследования молодых: Материалы региональной научно-практической конференции, Хабаровск, 12–16 апреля 2022 года / Редколлегия: Е.Г. Агапова (отв. редактор) [и др.]. — Хабаровск: Тихоокеанский государственный университет, 2022. — С. 218–225. — EDN WHQTXN.
7. Антонов, И.А. Методы машинного обучения для обнаружения вторжений в сетях интернета вещей / И.А. Антонов, М.К. Исаченко // Искусственный интеллект в промышленных, коммерческих, медицинских и финансовых приложениях: СБОРНИК СТАТЕЙ НАУЧНО-ТЕХНИЧЕСКОГО СЕМИНАРА СТУДЕНТОВ КАФЕДРЫ «ИНЖЕНЕРНОЙ КИБЕРНЕТИКИ», Москва, 30 декабря 2023 года. — Москва: Национальный исследовательский технологический университет «МИСИС», 2023. — С. 9–15. — EDN THRHTS.
8. X. Liang and Y. Kim, «A survey on security attacks and solutions in the iot network», in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2021, pp. 0853–0859.
9. P.R. Maidamwar, M.M. Bartere, and P.P. Lokulwar, «Implementation of network intrusion detection system using artificial intelligence: Survey», in Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Springer, 2022, pp. 185–198.