ТЕХНИЧЕСКИЕ НАУКИ
И ТЕХНОЛОГИИ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК. АҚПАРАТТЫ ҚОРҒАУ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЗАЩИТА ИНФОРМАЦИИ
INFORMATION SECURITY. INFORMATION PROTECTION

DOI 10.51885/1561-4212_2021_1_82
МРНТИ 81.93.29

**А.Т. Тохметов[1], А.С. Амирова[2], А.С. Жанасбаева[3]**
Евразийский национальный университет им. Л.Н. Гумилева
[1]*E-mail: attohmetov@mail.ru*
[2]*E-mail: whitesilk@mail.ru* *
[3]*E-mail: janasbaeva@inbox.ru*

# ӨНДІРІСТІК ЗАТТАР ИНТЕРНЕТІНІҢ НЕГІЗГІ ҚАУІПСІЗДІК МӘСЕЛЕЛЕРІНЕ ШОЛУ

# ОБЗОР ОСНОВНЫХ ПРОБЛЕМ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

# OVERVIEW OF THE MAIN SECURITY ISSUES IN THE INDUSTRIAL INTERNET OF THINGS

***Аңдатпа.*** *Заттардың өндірістік Интернетінің (IIoT) қарқынды дамуымен жылдам әрекет ету, интрузияларды анықтау және алдын-алу қажеттілігі туындады. IIoT желілері арнайы функцияларға ие және кибершабуылдан қорғауда ерекше қиындықтарға тап болады. Бұл проблемалар, әсіресе IIoT пайдаланушыларының болжамды өсуімен байланысты. Бұл мақалада біз 2018 жылдан 2020 жылға дейін, өнеркәсіптік Интернет заттарында машиналық оқыту алгоритмдері мен блокчейн әдістерін қолдана отырып, қауіпсіздік мәселелерін шешуге бағытталған зерттеулерді қорытындылаймыз. Біріншіден, біз индустриалды IoT саласында соңғы бірнеше жылда айтылған әр түрлі таксономияларды талқылаймыз. Сонымен қатар біз IIoT-да қауіпсіздіктің негізгі аспектілерін зерттейміз. Содан кейін біз IIoT доменіндегі машиналық оқыту алгоритмдері мен блокчейн әдістеріне негізделген қауіпсіздік шешімдері туралы әдебиеттерді талдаймыз. Соңында, заттардың өнеркәсіптік интернетіндегі қауіпсіздік мәселелерін шешу үшін машиналық оқыту алгоритмдерін және BC техникасын қолдана отырып, бірнеше қиындықтар мен болашақ зерттеу бағыттарын анықтаймыз.*

***Түйін сөздер:*** *процестерді басқарудың автоматтандырылған жүйесі (APCS), блокчейн (BC), заттардың өндірістік интернеті (IIoT), машиналық оқыту (ML), қауіпсіздік, қауіп-қатер.*

***Аннотация.*** *В связи с развитием промышленного Интернета вещей (IIoT) возникла необходимость быстро реагировать, обнаруживать и предотвращать вторжения. Сети IIoT имеют особые функции и сталкиваются с уникальными проблемами в защите от кибератак. Эти проблемы особенно актуальны с учетом прогнозируемого роста пользователей IIoT.*

*В этом документе мы резюмируем исследования, проведенные с 2018 по 2020 год, для решения проблем безопасности с использованием алгоритмов машинного обучения и технологий блокчейна в промышленном Интернете вещей. Во-первых, мы обсуждаем различные таксономии, о которых сообщалось за последние несколько лет в области промышленного Интернета вещей. Также мы изучаем ключевые аспекты обеспечения безопасности в IIoT. Затем мы анализируем литературу о решениях безопасности, основанных на алгоритмах машинного обучения и методах блокчейна в области IIoT. Наконец, мы выявляем и выделяем несколько проблем и будущих направлений исследований с использованием алгоритмов машинного обучения и методов BC для решения проблем безопасности в промышленном Интернете вещей.*

***Ключевые слова:*** *автоматизированная система управления процессами (APCS), блокчейн (BC), промышленный Интернет вещей (IIoT), машинное обучение (ML), безопасность, угрозы.*

***Abstract.*** *With the rapid development of the industrial Internet of Things (IIoT) the need to respond quickly, detect and prevent intrusions has arisen. IIoT networks have special functions and face unique challenges in defending against cyber attacks. These problems are especially relevant as the predicted growth of IIoT users.*

*In this document, we summarize the research undertaken over the past few years, from 2018 to 2020, to address security challenges using machine learning algorithms and blockchain techniques in the Industrial Internet of Things. First, we discuss various taxonomies that have been reported over the past few years in the Industrial IoT field. Also we study key aspects of securing in IIoT. Then we analyze the literature on security solutions based on machine learning algorithms and blockchain techniques in the IIoT domain. Finally, we identify and highlight several challenges and future research directions using machine learning algorithms and BC techniques to address security challenges in the Industrial Internet of Things.*

***Keywords:*** *Automated Process Control System (APCS), blockchain (BC), Industrial Internet of things (IIoT), machine learning (ML), security; threats.*

*Введение.* Промышленный Интернет вещей – это система взаимосвязанных компьютерных сетей и подключенных к ним промышленных объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматическом режиме без вмешательства человека. IIoT позволяет создавать отрасли более экономичные, гибкие и эффективные, чем существующие. Для развития IIoT проблема обеспечения адекватного уровня кибербезопасности остается, пожалуй, единственным существенным препятствием.

Согласно Market Data Forecast, мировой рынок промышленного Интернета вещей (включая оборудование, датчики, датчики, роботизированные системы, платформы, программное обеспечение и услуги) в 2019 году достиг 264,22 миллиарда долларов. С 2021 по 2025 годы он будет расти в среднем на 18,7 процентов (рис. 1). К 2025 году его объем составит 622 миллиарда долларов. В связи с пандемией коронавируса рост рынка в 2020 году скорректирован и составил 0 процентов с 2019 года [1]. По словам Honeywell, основной тенденцией, связанной с развитием промышленных экосистем Интернета вещей, является привлечение лицензиаров и производителей промышленного оборудования к разработке приложений на основе существующей инфраструктуры IIoT, которые впоследствии могут быть размещены в магазине/торговых площадках приложений. Эти приложения повысят мобильность и продуктивность сотрудников на предприятии, а также помогут решить узкоспециализированные задачи повышения эффективности [2].

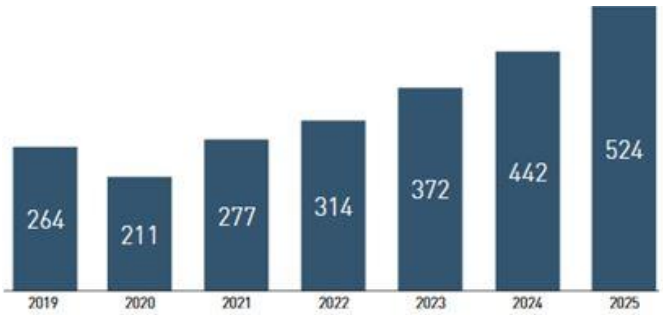


**Рисунок 1.** Динамика мирового рынка промышленного Интернета вещей (млрд долларов США) [1]

Согласно опросу компании Accenture, проведенному среди 1400 руководителей выс-

шего звена во всем мире, вклад промышленного Интернета вещей (IoT) в мировую экономику к 2030 году составит порядка 14 триллионов долларов США. Внедрение технологий IIoT за тот же период может добавить до 6 триллионов долларов в ВВП США и не менее 70 миллиардов долларов в экономику Германии. Исследование Accenture показывает, что перспективы и влияние промышленного Интернета вещей еще не ясны для крупного бизнеса. Отсутствие планов использования таких технологий во многом связано с их сложностью с потенциальной доходностью [3].

Эти прогнозы дополнительно подчеркивают сложности, связанные с обеспечением безопасности IIoT. Несмотря на то, что большое количество промышленных устройств было переведено на использование более безопасных методов связи, большинство этих устаревших систем по-прежнему полагаются на устаревшие протоколы. Эта ситуация сохраняется, несмотря на то, что общественность знает об присущих им уязвимостях из-за отсутствия каких-либо требований к идентификации или аутентификации.

Однако система IIoT имеет ряд серьезных проблем. Сложность системы является наиболее серьезной проблемой, поскольку операции IIoT различаются, а гибкая интеграция между устройствами отсутствует. Существуют разные устройства с разным дизайном, развертыванием и услугами, поэтому любые недостатки программного или аппаратного обеспечения могут вызвать серьезные проблемы. В сети IIoT есть проблемы с аутентификацией и контролем доступа, поскольку смарт-объекты представляют собой разнородные устройства, основанные на разных платформах (аппаратных средствах и сетях). Более того, все устройства должны связываться с другими устройствами по разным сетям. Таким образом, IIoT требует механизма безопасности более высокого уровня, который учитывает требования к срокам, количество устройств в сети, механизм восстановления в случае атаки и тому подобные факторы.

В первой половине 2020 года атакам подверглись многие промышленные системы по всему миру. Например, 23 апреля Национальное управление кибербезопасности Израиля (INCD) опубликовало уведомление о попытках атак на системы SCADA на очистных сооружениях, водонасосных станциях и канализационных сетях. В качестве меры по предотвращению вторжений водохозяйственным и энергетическим организациям было рекомендовано срочно изменить пароли для всех систем, подключенных к Интернету. 7 мая 2020 года швейцарский производитель поездов Stadler объявил о кибератаке на свои промышленные объекты. Некоторые компьютеры в корпоративной сети были заражены вредоносным ПО, и данные с этих устройств были похищены. Злоумышленники связались с представителями компании и потребовали выкуп, угрожая опубликовать украденную информацию в случае неуплаты. 14 мая крупная британская электроэнергетическая компания Elexon объявила о заражении своих ИТ-систем вредоносным ПО. В результате атаки пострадали только внутренние системы ИТ-сети компании, включая почтовую систему, и ноутбуки. Ключевые информационные службы и системы электроснабжения не пострадали от кибератаки [4].

*Вклад статьи:* В этой статье представлен подробный обзор алгоритмов машинного обучения и методов BC, используемых для защиты приложений IIoT от атак. Насколько нам известно, это первая статья, в которой представлен обзор уязвимостей безопасности в среде IIoT и меры борьбы с ними, основанные на алгоритмах машинного обучения и методах BC.

• Мы предоставляем таксономию угроз для Интернета вещей, о которых сообщается в недавней литературе, на основе угроз безопасности.

• Мы изучаем ключевые аспекты безопасности в IIoT.

• Мы классифицируем обзоры литературы по алгоритмам машинного обучения и методам ВС для безопасности IIoT и выделяем пробелы в исследованиях в существующих обзорах литературы.

• Мы выделяем и обсуждаем существующие проблемы для алгоритмов машинного обучения и методов ВС в безопасности IIoT с попыткой предложить некоторые направления на будущее.

Остальная часть статьи организована следующим образом. В разделе 2 представлена таксономия известных угроз IIoT, а также обсуждаются некоторые ключевые аспекты защиты в IIoT. В разделе 3 мы классифицируем обзоры литературы по безопасности IIoT с использованием алгоритмов машинного обучения и методов ВС. Наконец, в разделе 4 мы завершаем представление пробелов с некоторыми направлениями на будущее.

*Материалы и методы исследования.* Таксономия атак помогает понять и классифицировать инциденты безопасности [5]. Симмонс разработал таксономию кибератак AVOIDIT [6], которая имеет пять измерений: а именно вектор атаки, оперативное воздействие, защиту, информационное воздействие и цель. Эта таксономия могла легко классифицировать кибератаки, но не смогла классифицировать атаки в Industrial IoT, поскольку в нем отсутствовали векторы физических атак, которые открыты в промышленных атаках. Таксономия междоменных атак на киберпроизводственные системы была разработана Мингтао Ву [5] и имеет четыре аспекта, а именно атаку. Авторы в [7] предложили таксономию, которая может быть полезна при классификации атак на IIoT. Отличие от [5] заключается во включении вредоносного ПО вектора атаки, которое содержит различные типы вредоносного кода. Эта таксономия состоит из четырех измерений, которые раскрывают информацию о том, как была проведена атака, какие компоненты были затронуты и чего удалось достичь злоумышленнику.

В нашей статье мы будем рассматривать только первое измерение – вектор атаки. Это измерение - путь или средство, с помощью которого злоумышленник может получить доступ к компьютеру или сети. Векторы атак подразделяются на кибератаки и физические атаки. Векторы кибератак содержат точки входа в ИТ-сети, к которым не требуется физический доступ, тогда как векторы физических атак требуют, чтобы злоумышленник взаимодействовал с устройством или людьми в отрасли. Мы считаем, что в таксономии следует выделить еще один вектор – атаки с использованием ложных данных (FDI). Среди различных возникающих проблем безопасности FDI-атака является одной из наиболее существенных, которая может значительно увеличить стоимость процесса распределения энергии (рис. 2).


**Рисунок 2.** IIo T атаки

Выход из строя АСУ ТП может замедлить производство на несколько часов, нанести миллионы материальных убытков и даже больше. Например, перезапуск открытой печи или котла емкостью 10 000 галлонов, который обрабатывает коррозионные химикаты, может иметь разрушительные физические последствия [9].

Автоматизированная производственная среда с постоянной доступностью и надежной работой должна быть безопасной для обслуживающего персонала и остальной окружающей среды. Устройства, приложения и операционные системы, подключенные к промышленным сетям, редко обновляются, потому что для их исправления или обновления может потребоваться выключение целых систем.

Попытки снизить риски информационной безопасности промышленных сетей путем развертывания межсетевых экранов, систем IPS и т.д. Приводят к неприемлемым и даже разрушительным результатам. Такие инструменты информационной безопасности должны быть специально разработаны с учетом используемых протоколов, коммуникаций и сервисов, чтобы обеспечить их безопасность и доступность.

При проектировании доступность и безопасность промышленной сети должны быть обеспечены на высшем уровне, чтобы система безопасности не встраивалась в готовую инфраструктуру. Если в проекте не применяется интегрированная стратегия информационной безопасности, а делается попытка защитить каждый компонент инфраструктуры отдельно, система безопасности может оказаться неэффективной и даже уязвимой. Например, в системах автоматизации зданий комплексный, сегментированный и многоуровневый подход не только обеспечивает безопасность системы кондиционирования на уровне ее блокировки, но и путем предоставления аналитики и контроля в реальном времени комплексную защиту других систем, таких как система пожаротушения.

Путь к обеспечению безопасности современной промышленной среды начинается с непрерывного мониторинга – видимости любых процессов, происходящих в контролируемых системах. Решения для управления доступом к промышленной сети могут помочь в инвентаризации и мониторинге устройств IIoT, включая отслеживание каждого подключен-

ного устройства, даже когда оно перемещается из одного места в другое. Чтобы установить контроль в промышленной среде, необходимо прежде всего определить и записать, каким будет нормальный профиль трафика для данной системы и какие функции будут обеспечивать в реальном времени реакцию на любое поведение, выходящее за пределы нормального диапазона. К счастью, поведение устройств в промышленной среде по своей природе довольно статично и предсказуемо, поэтому ненормальные ситуации, вероятно, будут обнаружены быстро.

Мониторинг сетевых устройств IIoT – это первый шаг к защите промышленных сетей. Это помогает идентифицировать и документировать каждое новое устройство, подключенное к сети, и отслеживать изменения в их профилях [10].

Однако опрос устройств в промышленной сети намного сложнее, чем в ИТ-сетях, потому что активное сканирование здесь неприменимо из-за возможности нарушения нормального функционирования подключенных устройств IIoT. Поэтому сбор данных в промышленных сетях должен осуществляться максимально пассивно. Один из способов решения проблемы - предназначен для сбора информации с сетевых устройств, а не с самих устройств ICS. Даже после обнаружения зараженного устройства ситуация остается сложной. Вы не можете, например, автоматически поместить его в карантин, поскольку последствия отключения от производственных процессов непредсказуемы. Это означает, что группа информационной безопасности должна работать в тесном контакте со специалистами, обслуживающими промышленную сеть, чтобы определить варианты возможного вмешательства.

Сегментация - еще одна важная стратегия защиты промышленной среды. Как и в случае с ИТ-сетями, это подразумевает разделение север / юг и восток / запад. ISO 99 описывает подходы к сегментации для промышленных сред [11].

Сегментация Север / Юг. Даже если промышленные и ИТ-сети сближаются, они должны оставаться максимально изолированными друг от друга. Это помогает решить две основные проблемы в промышленной сети – инсайдерскую активность и распространение червей. Если эти сети соединены между собой по одному периметру, промышленные системы могут непреднамеренно столкнуться с проблемами, возникающими в результате обычной ИТ-деятельности, например, активного сканирования ИТ-трафика для определения его источника и назначения. Как уже было сказано, это совершенно неприемлемо для многих устройств IIoT. Для защиты от злонамеренного или непреднамеренного взлома важно, чтобы трафик промышленной сети был полностью отделен от трафика ИТ. Даже при обновлении или исправлении промышленных систем следует избегать прямого подключения к Интернету или ИТ-сети.

*Решения безопасности на основе блокчейн и машинного обучения в IIOT.* В этом разделе представлен обзор существующей литературы и классифицируются усилия, предпринятые на основе алгоритмов машинного обучения и методов BC, для обеспечения безопасности IIoT. Этот раздел разделен на два подраздела: алгоритмы машинного обучения и методы BC. Сборник статей. Первоначально поиск проводился по ключевым словам. Такие ключевые слова, как IIoT, промышленный Интернет вещей, безопасность, угрозы, машинное обучение и блокчейн, использовались для загрузки последних статей из ведущих журналов и конференций. Статья должна была удовлетворять следующим условиям: опубликована в период с 2018 по 2020 год (включительно); анализирует угрозы безопасности, связанные с IIoT, и охватывет ML или BC как вычислительную парадигму. Статистика отбора статей по годам (рис.3) показывает, что большая часть работы

началась совсем недавно.

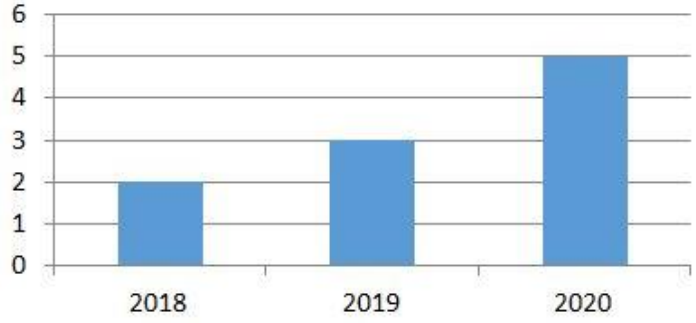


**Рисунок 3.** Годовая статистика выбранных исследовательских работ с 2018 по 2020 год включительно

Существующие обзорные статьи с использованием алгоритмов машинного обучения в качестве решения:

– Yao и др. предложили новую гибридную архитектуру IDS для периферийного IIoT, в которой новый алгоритм машинного обучения и алгоритм глубокого обучения используются в сети нижнего уровня и сети верхнего уровня соответственно [12]. Они использовали новый алгоритм машинного обучения LightGBM 1 для обнаружения вторжений в исходные данные и повысили точность обнаружения на основе отсутствия увеличения затрат времени, что можно рассматривать как быстрое, распределенное и высокопроизводительное решение древовидная структура подъема градиента.

– Aboelwafa и др. представили подход на основе машинного обучения применяется для обнаружения атак с использованием ложных данных (FDI). Этот метод основан на использовании автоэнкодеров, представляющих собой тип нейронных сетей, которые оказались очень эффективными при обнаружении аномалий. Данный метод предлагает лучшую производительность обнаружения по сравнению с методами на основе SVM [13].

– Авторы в [14] предложили новую структуру под названием PriMod-Chain, которую можно использовать для надежного машинного обучения и совместного использования в среде IIoT. PriModChain объединяет концепции смарт-контрактов, блокчейна, федеративного обучения (FedML), дифференциальной конфиденциальности и IPFS для обеспечения конфиденциальности и надежности машинного обучения в IIoT. Федеративное обучение использовалось в качестве глобального подхода к объединению и совместному использованию моделей машинного обучения, в то время как DP обеспечивает конфиденциальность моделей машинного обучения. Интеграция смарт-контрактов и EthBC обеспечивает отслеживаемость, прозрачность и неизменность структуры. IPFS обеспечивает неизменность, малую задержку и быстрое децентрализованное архивирование с безопасной доставкой контента P2P.

– Zolanvari et al. в своей работе изучали случаи, когда современные алгоритмы машинного обучения не обеспечивают требуемый уровень безопасности, в частности проблема несбалансированного набора данных в IIoT [15].

– Qiao et al. проанализировали подходы на основе машинного обучения к обнаружению аномалий в сетях промышленной автоматизации. Они представили подход, который отслеживает активность фабричного сетевого трафика на основе двух алгоритмов линейного выделения признаков, то есть линейного дискриминантного анализа (LDA) и анализа главных компонентов (PCA) [16]. Результаты экспериментов показали осуществимость

предложенного метода по точности, частоте обнаружения и частоте ложных тревог.

Существующие обзорные документы, использующие блокчейн в качестве решения:

– Puri et al. сосредоточены на Индустрии 4.0 или IIoT и на том, как к ней можно применить архитектуру блокчейн [17]. Также они отметили, что безопасность имеет решающее значение для IIoT, и есть несколько приложений, требующих более высокого уровня безопасности.

– Авторы в [18] использовали инновационную архитектуру IIoT на основе блокчейнов, чтобы помочь построить более безопасную и надежную систему IIoT. Они модернизировали существующую платформу автоматического производства, чтобы обсудить улучшения по сравнению с традиционной архитектурой IIoT. Предлагаемая архитектура может достичь большего расширения в будущем, например, за счет интеграции смарт-контрактов, достигая автоматической конфигурации ресурсов; через распределенную систему может быть реализовано дистанционное онлайн-обновление всего оборудования.

– Блокчейн Fabric предлагается использовать для безопасной передачи данных в [19]. Сертификаты транзакций используются для защиты передачи данных, а вновь добавленные блоки аутентифицируются для обеспечения безопасности. Без сертификатов транзакции остаются недействительными. Данные остаются неизменными, если один узел будет взломан из-за использования алгоритма хеширования. Безопасность транзакций данных обеспечивается за счет использования пары открытого / закрытого ключей.

– В [20] Yeasmin et al. использовал разрешенный блокчейн, позволяющий использовать IIoT для устранения уязвимостей безопасности IIoT с точки зрения защищенной связи устройств, сервера, совместного использования данных и механизма контроля доступа. Использование компонента CA, смарт-контракта и узлов консенсуса, а также выполнение ограниченных транзакций в разрешенной цепочке блоков обеспечивает конфиденциальность и безопасность во всей сети. Он также изучает важность IIoT с разрешенной блокчейном по сравнению с общедоступным, который обеспечивает и гарантирует безопасность сети.

– Sani предложили Xyreum - новый высокопроизводительный и масштабируемый блокчейн для повышения безопасности и конфиденциальности IIoT. Xyreum использует основанное на времени доказательство знаний с нулевым разглашением (T-ZKPK) с аутентифицированным шифрованием для выполнения взаимной многофакторной аутентификации (MMFA). Свойства T-ZKPK также используются для поддержки установления ключа (KE) для защиты транзакций [21].

*Заключение.* В этой статье мы рассмотрели последние угрозы для IIoT и проанализировали различные атаки IIoT. Кратко описаны их эффекты, типы, слой воздействия. Затем мы всесторонне представили последний существующий обзор литературы по безопасности IIoT с использованием алгоритмов машинного обучения, а также методов блокчейна. В этом документе представлены текущие решения для безопасности IIoT с использованием алгоритмов машинного обучения и технологий BC. Генерация, хранение, анализ и передача данных имеют фундаментальное значение для экосистемы IIoT. Требуется целостный подход, при котором необходимо создать систему, свободную от уязвимостей, с помощью таких мер, как соблюдение передовых практик и постоянное тестирование. Система должна быть способна учиться и адаптироваться к последним тенденциям в области угроз (атаки нулевого дня), поскольку вредоносные действия являются динамическими. В этом отношении ML / DL может быть чрезвычайно полезным при анализе трафика. В тоже время BC может служить основой для ведения реестра журналов и обмена данными в среде IoT. Эта

работа выявляет множество исследовательских возможностей в области безопасности IIoT и показывает, что машинное обучение и блокчейн могут стать мощными инструментами в обеспечении безопасности различных связанных промышленных сред, если будут преодолены его ограничения и проблемы. В настоящее время интеграция алгоритмов машинного обучения с методами ВС для обеспечения безопасности IIoT является относительно новой областью, требующей дальнейшего изучения.

Список литературы


1. Industrial IoT Market Research Report. Market Data Forecast, 2020.
2. Промышленный Интернет вещей. Департамент инвестиционной и промышленной политики города Москвы, 2020.
3. The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity. M.Purdy, L.Davarzani // Accenture. 2015. – P. 21-26.
4. Ландшафт угроз для систем промышленной автоматизации. Kaspersky ICS CERT, 2020.
5. Taxonomy of Cross-Domain Attacks on Cyber Manufacturing System. M.Wu, Y. B. Moon // Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems. 2015. – С. 367-374.
6. Security Attacks on Cloud Computing With Possible Solution. P. Chouhan, R. Singh // International Journal of Advanced Research in Computer Science and Software Engineering. – 2016. – С. 92-96.
7. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. C.Abhijeet, M. Vijay, Khadse, N.Parikshit // IEEE Global Conference on Wireless Computing Networking. – 2018. – С. 124-130.
8. A cyber attack taxonomy. C.Simmons, S.Ellis, D.Shiva // Annu. Symp. Inf. Assur. – 2014. – С.12-22.
9. A Taxonomy of Cyber Attacks on SCADA Systems. A.Zhu, S. Sastry // International Conference on Internet of Things. – 2011. – С. 380-388.
10. Taxonomy for description of cross-domain attacks on CPS. M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue, J. Sztipanovits // ACM International Conference on High Confidence Networked Systems. – 2013. – С. 135-142.
11. An effective method for preventing SQL injection attack and session hijacking. K. D'silva, J. Vanajakshi, K. N. Manjunath, S. Prabhu // IEEE International Conference on Recent Trends in Electronics, Information Communication Technology. – 2017. – С. 697-701.
12. Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection. H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, L. Lu // IEEE Network. 2019. – № 5. – С. 75-81.
13. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. M.N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallahб M. Gidlund // IEEE Internet of Things Journal. 2020. – № 9. – С. 8462-8471.
14. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systemsю C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepeб M. Atiquzzaman // IEEE Transactions on Industrial Informatics. – 2020. – № 9. – С. 6092-6102.
15. Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learningю M. Zolanvari, M.A. Teixeira, R. Jain // IEEE International Conference on Intelligence and Security Informatics. – 2018. – С. 112-117.
16. A Machine learning based intrusion detection approach for industrial networks. H. Qiao, J.O. Blech, H. Chen // IEEE International Conference on Industrial Technology. – 2020. – С. 265-270.
17. Blockchain meets IIoT: An architecture for privacy preservation and security in IIoT. I. Puri, R. Priyadarshini, L. Kumar, C. Kim // International Conference on Computer Science, Engineering and Applications. – 2020. – С. 1-7.
18. A Blockchain-Based Solution for Enhancing Security and Privacy. J. Wan, J. Li, M. Imran, D. Li // IEEE Transactions on Industrial Informatics. – 2019. – № 6. – С. 3652-3660.
19. A Secure FaBric Blockchain-Based Data Transmission Technique for Industrial Internet-of-Things. W. Liang, M. Tang, J. Long, X. Peng, J. Xu, K. Li // IEEE Transactions on Industrial Informatics. – 2019. – № 6. – С. 3582-3592.
20. Permissioned Blockchain-based Security for IIoT. S. Yeasmin, A. Baig // IEEE International IOT,

Electronics and Mechatronics Conference. – 2020. – С. 1-7.
21. Xyreum: A High-Performance and Scalable Blockchain for IIoT Security and Privacy. S. Sani // IEEE 39th International Conference on Distributed Computing Systems. – 2019. – С. 1920-1930.