Impact Factor: 9.9 ISSN-L: 2544-980X

Возможности Искусственного Интеллекта В Обеспечении Безопасности Iot-Устройств

Турдиева Гавхар Саидовна [1]

Аннотация: Интернет вещей (IoT) - это развивающаяся технология, и распространение устройств IoT произвело революцию в различных областях за счет улучшения связи и осуществления интеллектуальных операций. Однако это быстрое расширение также привело к значительным проблемам безопасности, поскольку устройства IoT часто служат отправной точкой для кибератак из-за их разнообразия и различных уровней встроенной безопасности. Искусственный интеллект (AI) стал важной технологией в решении этих проблем безопасности, предлагая передовые решения для защиты устройств IoT. В данной статье исследуется роль искусственного интеллекта в обеспечении безопасности устройств IoT, анализируются проблемы и решения, связанные с его реализацией.

Ключевые слова: IoT (Интернет вещей), современные технологии, энергоэффективность, протоколы, Интернет, интеллектуальный объект, виртуальный мир, схема Intel IoT Platform.

ВВЕДЕНИЕ

По всему миру, на городских улицах, в домах и больницах, миллиарды подключенных к сети «умных» физических объектов постоянно собирают и обмениваются данными через Интернет, что наделяет их уровнем цифрового интеллекта и автономности. Интернет вещей со своими новшествами полностью изменил мир. Это необходимо для повседневной жизни людей. IoT широко распространен в офисах, домах и даже в промышленности. IoT является ключевым компонентом многих областей, таких как управление здравоохранением, сельское хозяйство, умные дома, умные города и даже автономные автомобили.

Термин «Интернет вещей» (IoT) был придуман Кевином Эштоном в 1999 году. Он работал в Массачусетском технологическом институте, где руководил Auto-ID Labs и первым предложил концепцию IoT. Развитие этой области связано с конвергенцией различных технологий, таких как повсеместные вычисления, датчики и мощные встроенные системы. Первоначально это было связано с идеей радиочастотной идентификации (RFID) для управления цепочками поставок. Постепенно концепция охватила множество других устройств и приложений.

Согласно отчету Всемирного экономического форума «Состояние подключенного мира», в мире больше подключенных устройств, чем людей, и прогнозируется, что к 2025 году 41,6 миллиарда устройств будут получать информацию о том, как мы живем, работаем, передвигаемся по городам, управляем машинами, от которых мы зависим, и обслуживаем их [3].

Мир легко подключился благодаря Интернету вещей. Теперь людям легче работать и эффективнее общаться. Способ связи устройств, систем и сервисов похож на сетевую экосистему.

Важно понимать, как работают устройства IoT и как они устанавливают связь, как работает эта система. Устройства IoT общаются через сеть, и их методы связи в основном WIFI, Zigbee и

[1] доцент кафедры прикладной математики и технологий программирования, Бухарский государственный университет

Bluetooth. Эти методы связи позволяют устройствам IoT передавать данные на другие устройства. Таким образом, мир становится взаимосвязанным.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ.

В процессе изучения данного исследования был использован ряд научных источников. В результате исследований был сделан вывод о том, что интернет вещей (IoT) продолжает привлекать внимание к своей концепции. Расширение и популяризация фитнес-браслетов и умных часов привели к тому, что люди узнали о термине "Интернет вещей".

Эта технология действительно революционизирует нашу жизнь, поскольку все становится умным. Умные браслеты, сельское хозяйство, дома, города, цепочки поставок, производство, логистика и т. д. Поэтому неудивительно, что некоторые энтузиасты рады вдаваться в подробности и узнавать об этом больше. Этот энтузиазм может быть вызван страхом отсутствия знаний или технических данных. К счастью, теперь каждый, кто интересуется Интернетом вещей, может найти множество книг для любого уровня технического опыта.

В этой статье рассматриваются основные проблемы интеграции ИИ с безопасностью IoT, включая вопросы конфиденциальности данных, сложности алгоритмов ИИ и потребность в масштабируемых решениях. Анализируя возможности и ограничения искусственного интеллекта в защите IoT-устройств, в статье обсуждаются идеи о том, как можно использовать ИИ для создания более адаптивных систем безопасности.

Проведенные исследования подчеркивают важность постоянных исследований и разработок в области технологий искусственного интеллекта для адаптации к растущему и динамичному характеру угроз IoT.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ.

IoT, то есть Internet of Things (Интернет вещей) - это совокупность физических объектов, имеющих возможность подключения к интернету. Эти объекты, благодаря датчикам, программному обеспечению и другим технологиям, обладают возможностью собирать данные, обмениваться ими и взаимодействовать друг с другом.

К основным характеристикам IoT относятся:

1. IoT-устройства общаются друг с другом через интернет или локальные сети и обмениваются данными.
2. IoT-системы могут обрабатывать данные в режиме реального времени и принимать решения, что позволяет автоматизировать многие процессы.
3. Данные из окружающей среды собираются с помощью устройств, датчиков, камер и других приборов.
4. Собранные данные могут быть проанализированы и преобразованы в полезные результаты, например, для повышения эффективности или предотвращения проблем.

Устройства IoT сегодня широко используются в следующих областях:

- В секторе «Умный дом»: умные устройства в домах, такие как лампы, термостаты и системы безопасности, умные двери.
- В промышленном секторе: использование решений IoT для оптимизации производственных процессов и повышения безопасности.
- В сфере транспорта: обмен информацией между транспортными средствами и транспортными системами, например, управление дорожным движением.
- В здравоохранении: медицинские приборы собирают данные о пациентах и анализируют эти данные.

Интернет вещей (IoT), который соединяет объекты и предоставляет нам ценные данные, стал неотъемлемой частью нашей повседневной жизни. Однако по мере того, как число устройств Интернета вещей продолжает расти, их защита от кибератак становится серьезной проблемой.

Согласно отчету исследования Checkpoint, среднее еженедельное количество атак на устройства IoT в расчете на одну организацию увеличилось на 41% за первые два месяца 2023 года по сравнению с 2022 годом. Каждую неделю примерно 54% организаций подвергаются попыткам кибератак на свои устройства IoT [4].

Почему устройства Интернета вещей подвержены риску кибератак?

За последние несколько лет число устройств Интернета вещей стремительно выросло. По имеющимся данным, к концу 2023 года число устройств IoT достигнет 16,6 млрд, а к концу 2024 года ожидается рост на 13%, достигнув на сегодняшний день 18,8 млрд.

Хотя устройства Интернета вещей имеют множество преимуществ, им не хватает тех же возможностей безопасности, что у ноутбуков и рабочих станций. Кроме того, легкость, с которой эти устройства распространяются в сетях, может создать расширенную поверхность атаки. Это может быть особенно опасно, если служба безопасности или ИТ-отдел не ведут точный учет всех устройств в сети. Чем больше устройств подключено к Интернету без надежного контроля безопасности, тем больше возможностей для злоумышленников использовать эти устройства для несанкционированного доступа[5].

Сегодня поверхность атак на информационную безопасность огромна и продолжает быстро расти и развиваться. В зависимости от размера данных они могут содержать до нескольких сотен миллиардов переменных сигналов, которые необходимо проанализировать для точного расчета риска. Однако теперь уже нет необходимости использовать человеческий фактор при анализе и улучшении состояния кибербезопасности. Появились инструменты кибербезопасности на основе искусственного интеллекта (ИИ), которые помогают службам информационной безопасности снизить риск нарушений и эффективно улучшить свой уровень безопасности. ИИ и машинное обучение (МО) могут стать важными технологиями обеспечения информационной безопасности, поскольку они способны быстро анализировать миллионы событий и помогать выявлять различные угрозы — от опасного поведения, которое может привести к фишингу. Он служит для обнаружения вредоносных кодов и предотвращения их загрузки. Также считается, что эти технологии способны обучаться на основе прошлых данных, чтобы со временем выявлять новые типы атак.

К сожалению, несмотря на популярность технологий искусственного интеллекта в настоящее время, использование старых методов все еще продолжается. В отличие от больших баз данных, облака, IoT и любых других технологий, правительства и крупные IT-компании ищут способы перехода на искусственный интеллект.

Методы искусственного интеллекта, такие как машинное обучение, обнаружение аномалий и прогнозная аналитика, все чаще используются для мониторинга, выявления потенциальных угроз и реагирования на них в режиме реального времени. Эти технологии помогают выявлять модели необычного поведения, прогнозировать потенциальные уязвимости и автоматизировать реагирование для снижения рисков.

Интеграция искусственного интеллекта (ИИ) и Интернета вещей (IoT) создает новую технологическую экосистему AIoT (искусственный интеллект вещей). Комбинация этих двух технологий позволяет расширить функциональность IoT-устройств, превратив их из простых сборщиков данных в автономные системы, способные анализировать, учиться и принимать решения в режиме реального времени. Создание AIoT открыло новые способы развития автоматизации с возможностью применения IoT-инфраструктур в различных областях.

Основное преимущество AIoT заключается в том, что IoT-устройства могут собирать данные, обрабатывать их с помощью искусственного интеллекта, делать на их основе прогнозы и

инициировать действия без вмешательства человека. Благодаря вычислениям на расширенной периферии сети эта интеграция также снижает задержки и повышает надежность таких систем.

Однако при всех преимуществах AIoT существуют некоторые проблемы, связанные с конфиденциальностью и безопасностью обрабатываемых данных.

Если рассмотреть основные компоненты AIoT, то можно увидеть, как они взаимосвязаны следующим образом.

Изделия работают с использованием устройств Интернета вещей (датчиков, исполнительных механизмов, камер). Он работает с сетью подключенных устройств, которые собирают и обмениваются данными. Функция: Устройство IoT собирает данные из окружающей среды, такие как температура, влажность, местоположение и другие параметры.

Искусственный интеллект (ИИ): (машинное обучение, глубокое обучение, обработка естественного языка/NLU, компьютерное зрение, машинное мышление, генеративный ИИ). Это технологии, которые позволяют системам анализировать данные, извлекать из них уроки и принимать решения без вмешательства человека. Задача: ИИ обрабатывает данные, собранные с устройств Интернета вещей, для выявления закономерностей, прогнозирования и оптимизации процессов.

Облачные технологии: облачные платформы хранения и обработки данных, которые обеспечивают доступ к данным и вычислительным ресурсам через Интернет. Миссия: Облачные решения обеспечивают масштабируемость и гибкость, позволяющие эффективно хранить большие объемы данных и выполнять сложные вычисления[6].

Аналитика данных: процесс извлечения полезной информации из больших объемов данных, собранных устройствами Интернета вещей. Миссия: предоставление аналитических отчетов и визуализаций, помогающих принимать обоснованные решения и повышать эффективность.

Системы управления: программное обеспечение для мониторинга и управления устройствами Интернета вещей. Задача: Обеспечивает контроль за работой устройств, их настройкой и безопасностью.

Безопасность: механизмы и протоколы защиты данных и систем от несанкционированного доступа и кибератак. Миссия: Обеспечивает информационную безопасность и целостность системы, обеспечивает безопасность пользователей.

Эти компоненты взаимодействуют друг с другом, создавая эффективные и интеллектуальные решения, которые улучшают качество жизни и оптимизируют процессы в различных отраслях.

Преимущества объединения ИИ и Интернета вещей заключаются в следующем: способность ИИ автоматизировать рутинные задачи, выполняемые людьми, помогает оптимизировать рабочие процессы и повысить эффективность использования ресурсов. Эта система повышает производительность, снижает затраты на рабочую силу и помогает быстрее выполнять операции.

Искусственный интеллект может применяться в различных областях безопасности Интернета вещей, в том числе:

- Обнаружение угроз: ИИ может обнаруживать известные и неизвестные угрозы в режиме реального времени, анализируя сетевой трафик, системные журналы и другие источники данных. Кроме того, он может обнаруживать вредоносное ПО и другие вредоносные действия.
- Контроль доступа: Улучшайте механизмы контроля доступа, внимательно изучая поведение пользователей на устройствах Интернета вещей и выявляя аномалии с помощью ИИ. С помощью ИИ пользователь также может обнаружить и предотвратить несанкционированный доступ к устройствам Интернета вещей.

- Аутентификация пользователей: Биометрическая идентификация и многофакторная аутентификация — два примера систем аутентификации пользователей, которые может улучшить ИИ. Он может проверять поведение пользователей и выявлять нарушения, такие как попытки входа в систему из необычных мест.
- Безопасность сети: отслеживайте сетевой трафик для выявления подозрительной активности и потенциальных угроз, а также извлекайте уроки из данных из различных источников, межсетевых экранов и систем обнаружения вторжений для обнаружения атак и реагирования на них в режиме реального времени с помощью искусственного интеллекта.
- Обнаружение уязвимостей: ИИ может быстро выявлять уязвимости в устройствах и приложениях Интернета вещей, анализируя код и файлы конфигурации. Он может моделировать атаки для выявления уязвимостей и давать рекомендации по обновлениям безопасности.
- Прогностическое обслуживание: с помощью искусственного интеллекта, позволяющего анализировать исторические данные и закономерности, можно прогнозировать потенциальные сбои устройств и уязвимости безопасности. ИИ может заблаговременно выявлять и устранять уязвимости до того, как они станут целью кибератак, обеспечивая проактивные меры безопасности[4].

Сегодня одной из проблем обеспечения безопасности устройств Интернета вещей является сложность алгоритмов искусственного интеллекта и необходимость масштабируемых решений. Сложность проблемы можно объяснить следующим образом. Как правило, для решения сложных задач требуются современные алгоритмы искусственного интеллекта, такие как глубокое обучение и мощные подходы к машинному обучению. Эти алгоритмы имеют многослойную и многопараметрическую структуру и требуют больших вычислительных ресурсов для достижения наилучших результатов. Это требует применения передовых алгоритмов и оптимизации для решения задач высокого уровня сложности. Это особенно важно в таких задачах, как классификация, прогнозирование и обработка естественного языка.

Далее, искусственному интеллекту требуются масштабируемые решения. Масштабируемые решения — это системы, которые можно быстро адаптировать или расширять по мере изменения конкретных потребностей. Для этого компаниям и организациям необходимы масштабируемые модели систем ИИ, которые помогут им развивать свою деятельность и адаптироваться к быстро меняющемуся рынку. Это делается логически, путем добавления новых функций или обновления систем в соответствии с требованиями пользователей.

Для защиты устройств Интернета вещей требуются ресурсы и технологии, а вычислительная мощность, необходимая для реализации алгоритмов ИИ, также связана с их сложностью. Масштабируемые решения часто предоставляются с помощью компьютерных сетей и облачных технологий, которые позволяют системам обеспечивать необходимую мощность. Для масштабируемых решений требуются отдельные системы управления и хранения данных, что повышает эффективность сложных алгоритмов.

Учитывая сложность алгоритмов ИИ и потребность в масштабируемых решениях, крайне важны подходы, совместимые с современными технологиями и этическими стандартами.

Существуют огромные возможности в обеспечении безопасности устройств Интернета вещей с использованием искусственного интеллекта. Искусственный интеллект (ИИ) создает множество возможностей и ограничений, когда речь идет о защите устройств Интернета вещей. К ним можно привести следующее. Возможны следующие варианты:

1. Обнаружение кибератак: алгоритмы ИИ помогают обнаруживать аномальное поведение, отслеживая поток данных, поступающий от устройств Интернета вещей, и сравнивая его с нормами. Это позволяет быстро обнаруживать и предотвращать кибератаки (например, DDoS-атаки).

2. Прогнозирование поведения: используя машинное обучение (МО), ИИ может изучать поведение устройств Интернета вещей и подготавливать программы принятия решений. Это позволяет быстро принять меры для предотвращения опасности.
3. Автоматизированное реагирование: системы ИИ обеспечивают механизмы быстрого реагирования на взломы или нарушения, такие как отключение устройств или отключение соединений.
4. Анализ данных: ИИ может помочь выявить слабые места в системах, анализируя большие объемы данных, собранных с устройств Интернета вещей. Это позволяет принять необходимые меры для повышения безопасности.
5. Оптимизация протоколов безопасности: с помощью ИИ можно разрабатывать новые протоколы безопасности и создавать системы, обновляемые для повышения эффективности существующих.

Существует также ряд ограничений использования искусственного интеллекта в системах безопасности:

1. Успех модели ИИ часто зависит от качества данных. Если данные неточны или предвзяты, алгоритмы ИИ могут принимать неверные решения.
2. Для реализации некоторых моделей ИИ требуются большие вычислительные мощности. Устройства Интернета вещей часто имеют ограниченные ресурсы, поэтому мощные алгоритмы ИИ не могут эффективно работать с ними.
3. Сложные взаимодействия между инструментами или неопределенные условия могут снизить эффективность систем ИИ. Зачастую они не готовы к условиям, транспортной нагрузке и другим меняющимся факторам.
4. Каждая часть экосистемы Интернета вещей имеет свои собственные функции безопасности. ИИ может защитить только часть системы, но уязвимости в других частях все равно могут представлять угрозу.
5. Вопросы личной безопасности и этики, связанные с данными, собранными с помощью систем ИИ, требуют определения того, как будут использоваться данные и для каких целей.

Хотя ИИ предлагает множество полезных возможностей для защиты устройств Интернета вещей, необходимо также учитывать его ограничения и неопределенности. Для решения этих проблем необходимо применять инновационные подходы и передовые технологии.

ЗАКЛЮЧЕНИЕ.

Интернет вещей (IoT) превращает повседневные предметы в подключенные устройства, которые облегчают жизнь и повышают функциональность, создавая интеллектуальную среду в городах, больницах и домах. От сельского хозяйства до носимых устройств: Интернет вещей меняет образ жизни и работы людей, одновременно вызывая опасения по поводу безопасности.

Цифровая трансформация, обусловленная новыми технологиями, включая робототехнику, Интернет вещей и искусственный интеллект, известна как Четвертая промышленная революция, а COVID-19 ускорил использование этих технологий.

Необходимо сосредоточиться на ряде подходов и стратегий для решения проблем искусственного интеллекта при обеспечении безопасности устройств Интернета вещей.

1. Необходимо сосредоточиться на поддержании высокого уровня качества при сборе данных с устройств Интернета вещей. Необходимо внедрить процессы тестирования и проверки данных. Данные необходимо очистить и преобразовать, а также привести к требуемому формату. Необходимо выявить и удалить аномальные данные.
2. Многие устройства Интернета вещей имеют ограниченные вычислительные и энергетические ресурсы. Сложные алгоритмы искусственного интеллекта не работают

эффективно на таких устройствах. Вместо сложных алгоритмов необходимо разрабатывать алгоритмы, обеспечивающие легкость и высокую производительность (например, трансферное обучение). При использовании подхода туманных вычислений данные должны обрабатываться не на устройствах, а с помощью компьютеров или серверов среднего уровня. Это позволяет совместно использовать вычислительную мощность.

3. Условия в средах Интернета вещей могут часто меняться, что может снизить эффективность систем ИИ. Это требует постоянного обновления моделей ИИ и адаптации их к меняющимся условиям. Необходимо будет использовать динамические подходы к обучению. В этом случае было бы целесообразно заранее смоделировать условия эксплуатации устройств Интернета вещей и разработать оптимальные стратегии.
4. Экосистемы Интернета вещей состоят из множества различных устройств, и обеспечение их совместимости друг с другом — сложный процесс. В этом случае необходимо упростить интеграцию путем создания стандартных протоколов между устройствами Интернета вещей и системами ИИ. Разработка эффективных протоколов и интерфейсов для обмена данными между устройствами и обеспечения взаимодействия будет иметь положительные результаты.
5. Используйте шифрование и протоколы безопасности для защиты данных. Получение согласия пользователя и разработка этических кодексов дадут эффективные результаты.

При защите устройств Интернета вещей важно применять современные подходы и стратегии решения задач искусственного интеллекта. Эти решения включают в себя ряд инноваций, необходимых для дальнейшего повышения эффективности систем и обеспечения безопасности.

Литература

1. Chowdhury, Rakibul Hasan. "Advancing fraud detection through deep learning: A comprehensive review." World Journal of Advanced Engineering Technology and Sciences 12, no. 2 (2024): 606-613.
2. Chowdhury, Rakibul Hasan. "AI-driven business analytics for operational efficiency." World Journal of Advanced Engineering Technology and Sciences 12, no. 2 (2024):
3. https://www.visionofhumanity.org/what-is-the-internet-of-things/
4. https://www.einfochips.com/blog/enhancing-iot-security-with-artificial-intelligence/
5. Турдиева Г. С. СЕТЕВЫЕ АТАКИ И ИСПОЛЬЗОВАНИЕ ЗАЩИТЫ ОТ NIX //Универсум: технические науки. – 2022. – № 2-1 (95). – С. 60-62
6. Г.Г.С.Турдиева ВОПРОСЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ПЛАТФОРМ: РИСКИ И УГРОЗЫ // Межобразование и глобальное исследование. 2024. № 4.