Овсянников Р.Я. Анализ уязвимостей и методы защиты в интернете вещей (IOT) с учетом растущей сложности сетей и устройств // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 147–153

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.738.5

АНАЛИЗ УЯЗВИМОСТЕЙ И МЕТОДЫ ЗАЩИТЫ В ИНТЕРНЕТЕ ВЕЩЕЙ (IOT) С УЧЕТОМ РАСТУЩЕЙ СЛОЖНОСТИ СЕТЕЙ И УСТРОЙСТВ

Овсянников Р.Я.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: rovsyannikov23@gmail.com

В статье рассматриваются современные уязвимости, связанные с интернетом вещей (IoT), а также методы и инструменты для их обнаружения и предотвращения. Особое внимание уделяется растущей сложности сетей и устройств IoT и ее влиянию на безопасность. Анализируются основные угрозы, с которыми сталкиваются устройства IoT, и обсуждаются современные подходы к защите, включая шифрование, аутентификацию и мониторинг сетевого трафика.

Ключевые слова: Интернет вещей, уязвимости, безопасность, сети IoT, защита, шифрование.

VULNERABILITY ANALYSIS AND PROTECTION METHODS IN THE INTERNET OF THINGS (IOT) GIVEN THE INCREASING COMPLEXITY OF NETWORKS AND DEVICES

Ovsyannikov R.Ya.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: rovsyannikov23@gmail.com

This article explores contemporary vulnerabilities associated with the Internet of Things (IoT) as well as methods and tools for their detection and prevention. Special attention is paid to the growing complexity of IoT networks and devices and its impact on security. The paper analyzes the primary threats faced by IoT devices and discusses modern approaches to protection, including encryption, authentication, and network traffic monitoring.

Keywords: Internet of Things, vulnerabilities, security, IoT networks, protection, encryption.

Введение

С развитием технологий и стремительным ростом количества устройств, подключенных к интернету вещей (IoT), вопросы безопасности приобретают особую актуальность. IoT-экосистема охватывает широкий спектр устройств – от умных бытовых приборов и носимых гаджетов до промышленных систем управления и критически важных инфраструктур. Однако, несмотря на удобство и технологические преимущества, расширение IoT-среды сопровождается увеличением числа уязвимостей, которые могут использовать злоумышленники для кибератак, компрометации данных и нарушения работы сетей.

Одной из ключевых проблем безопасности IoT является ограниченность вычислительных ресурсов устройств, что не позволяет внедрять сложные алгоритмы защиты. Многие IoT-устройства разрабатываются с акцентом на функциональность и

энергоэффективность, а вопросы безопасности часто остаются второстепенными. В результате устройства могут использовать слабые механизмы аутентификации, передавать данные в незашифрованном виде и обладать уязвимым встроенным программным обеспечением. Кроме того, высокая степень взаимосвязанности IoT-устройств в сетях приводит к тому, что компрометация одного узла может повлечь за собой массовое заражение всей системы, что делает атаки особенно опасными.

Еще одной серьезной угрозой является недостаточная сегментация сетей, когда IoT-устройства подключены к той же инфраструктуре, что и критически важные системы. Это позволяет злоумышленникам проникать в корпоративные или промышленные сети, используя IoT-устройства в качестве точки входа. Помимо этого, распространенными угрозами остаются атаки типа «человек посередине» (MITM), перехват данных, взлом слабых паролей и эксплуатация уязвимостей в прошивках.

Учитывая возрастающую сложность IoT-сетей и устройств, а также расширяющийся спектр атак, необходимо разрабатывать и внедрять надежные методы защиты. Данная статья рассматривает основные уязвимости, характерные для интернета вещей, анализирует современные методы обеспечения безопасности и перспективы дальнейшего развития технологий защиты. В работе уделяется внимание таким аспектам, как шифрование данных, аутентификация устройств, сегментация сетей, мониторинг аномальной активности и внедрение современных стандартов безопасности. Кроме того, рассматриваются перспективные решения, включая применение искусственного интеллекта и блокчейн-технологий, позволяющих повысить устойчивость IoT-систем к угрозам [1].

Уязвимости в сетях IoT

Интернет вещей (IoT) сочетает в себе огромное количество устройств, взаимодействующих друг с другом в сложных сетях, что создает множество потенциальных точек уязвимости. Из-за ограниченных вычислительных возможностей, недостаточных мер безопасности и слабой стандартизации IoT-системы часто становятся мишенями для кибератак. Одной из ключевых проблем является недостаточная аутентификация и авторизация. Многие устройства используют слабые, предустановленные или статические пароли, что делает их уязвимыми для атак методом перебора или захвата учетных данных. Отсутствие многофакторной аутентификации и надежных механизмов контроля доступа увеличивает вероятность компрометации.

Еще одной серьезной уязвимостью является отсутствие шифрования данных. Передача информации между устройствами и серверами часто осуществляется по устаревшим или незащищенным протоколам, таким как HTTP вместо HTTPS, что делает возможным перехват и анализ сетевого трафика злоумышленниками в рамках атак «человек посередине» (MITM). В результате хакеры могут не только получить доступ к передаваемой информации, но и изменять ее или подделывать команды управления устройствами. Уязвимости встроенного программного обеспечения (ПО) также представляют серьезную угрозу. Многие IoT-устройства работают на прошивках, которые редко обновляются производителями, а иногда и вовсе остаются без поддержки. В случае обнаружения уязвимостей злоумышленники могут использовать их для выполнения атак, таких как удаленное исполнение кода или повышение привилегий, что дает им полный контроль над устройством [2-3].

Отдельной проблемой является недостаточная сегментация сетей. IoT-устройства часто подключаются к тем же сетям, что и критически важные сервисы, такие как корпоративные базы данных, промышленные системы управления и облачные инфраструктуры. Это позволяет злоумышленникам, взломав одно устройство, проникнуть глубже в сеть и атаковать другие узлы, включая серверы и рабочие станции. Отсутствие изоляции IoT-устройств способствует быстрому распространению атак внутри инфраструктуры. Кроме того, уязвимые IoT-устройства часто используются в составе ботнетов, как показали атаки, подобные Mirai. Массовая инфицированность устройств и их слабая защищенность делают их удобной мишенью для создания зомби-сетей, применяемых для DDoS-атак, распространения вредоносного ПО и других преступных действий.

Физическая безопасность IoT-устройств также остается актуальной проблемой. Они часто располагаются в открытых или слабо защищенных местах, например, камеры видеонаблюдения, датчики в «умных» городах и промышленные контроллеры, что делает их уязвимыми для физического взлома. Злоумышленники могут получить прямой доступ к аппаратной части, модифицировать прошивку, извлечь учетные данные или внедрить вредоносный код. Еще одна важная угроза связана с атаками на радиоинтерфейсы и беспроводные сети. Многие IoT-устройства взаимодействуют через беспроводные технологии, такие как Wi-Fi, Bluetooth, Zigbee и LoRaWAN, которые подвержены атакам, включая перехват трафика, подделку команд управления и создание помех. Отсутствие надежной аутентификации в беспроводных сетях может привести к утечке конфиденциальных данных и перехвату управления устройствами [4-5].

Таким образом, IoT-среда остается крайне уязвимой из-за множества слабых мест, включая недостаточную защиту аутентификации, слабое шифрование данных, устаревшие прошивки, отсутствие сетевой сегментации и возможность использования устройств в ботнетах. Это делает вопросы безопасности критически важными для дальнейшего развития IoT-инфраструктуры. В следующих разделах статьи будут рассмотрены методы защиты и современные подходы к обеспечению безопасности IoT-устройств и сетей.

Методы защиты и обнаружения

Для обеспечения безопасности интернет вещей (IoT) необходимо применять комплексный подход, включающий защиту на уровне устройств, сетей и облачной инфраструктуры. Одним из ключевых аспектов является безопасная аутентификация и авторизация, которые позволяют ограничить несанкционированный доступ к устройствам. Для этого следует применять многофакторную аутентификацию (MFA), цифровые сертификаты и уникальные токены доступа, что снижает вероятность атак методом подбора паролей или компрометации учетных данных. Важно также отказаться от использования статических и предустановленных паролей, внедрив механизмы их регулярного обновления.

Шифрование данных играет центральную роль в защите IoT-сетей. Все передаваемые данные должны шифроваться с использованием современных протоколов, таких как TLS и DTLS. Для устройств с ограниченными вычислительными ресурсами можно применять легковесные алгоритмы, такие как AES-CCM или ECC, которые обеспечивают баланс между безопасностью и производительностью. Кроме того, необходимо защищать не только передаваемый, но и хранимый на устройствах контент, используя встроенные механизмы шифрования.

Обновление встроенного программного обеспечения (ПО) также является важной частью стратегии безопасности. Производители должны предоставлять регулярные патчи безопасности и реализовывать механизмы автоматического обновления прошивок. Кроме того, следует внедрять технологии защищенной загрузки (Secure Boot) и контроля целостности кода, которые позволяют проверять подлинность программного обеспечения перед его запуском. Это значительно усложняет внедрение вредоносного кода в систему.

Сегментация сетей — еще один эффективный метод защиты IoT-инфраструктуры. Разделение сети на изолированные сегменты с использованием VLAN и программно-определяемых сетей (SDN) помогает ограничить распространение атак. IoT-устройства должны подключаться к отдельным подсетям с минимальными привилегиями и ограниченным доступом к критически важным сервисам. Также рекомендуется применять брандмауэры и системы обнаружения вторжений (IDS/IPS), которые анализируют трафик и выявляют подозрительную активность.

Выявление аномалий и угроз с помощью машинного обучения и поведенческого анализа позволяет оперативно обнаруживать и блокировать потенциальные атаки. Такие системы анализируют поведение устройств и пользователей, выявляют нетипичные отклонения в активности и автоматически принимают меры для предотвращения угроз. Например, если устройство внезапно начинает отправлять большой объем данных на неизвестные серверы, система безопасности может заблокировать его соединение и уведомить администратора.

Дополнительно важным элементом защиты является контроль физического доступа к устройствам. IoT-устройства, расположенные в общественных местах, таких как «умные» камеры видеонаблюдения или датчики в городской инфраструктуре, должны быть защищены от несанкционированного физического вмешательства. Для этого применяются антивандальные корпуса, системы контроля доступа и механизмы обнаружения попыток несанкционированного вскрытия или модификации оборудования.

Таким образом, эффективная защита IoT-сетей требует многослойного подхода, включающего надежную аутентификацию, шифрование данных, регулярное обновление ПО, сегментацию сетей и мониторинг активности. Внедрение этих методов позволяет существенно снизить риски атак и обеспечить безопасность устройств, пользователей и инфраструктуры.

Современные тенденции и вызовы

Правовое регулирование и стандарты безопасности играют важную роль в обеспечении защиты экосистемы интернет вещей (IoT), создавая нормативную базу для производителей, разработчиков и пользователей. Различные страны разрабатывают и внедряют законы, направленные на повышение уровня безопасности IoT-устройств и минимизацию рисков, связанных с их эксплуатацией. В Европейском Союзе действует Закон о кибербезопасности, который устанавливает требования к сертификации IoT-продуктов и обязывает производителей соблюдать стандарты безопасности на всех этапах жизненного цикла устройства. В США Национальный институт стандартов и технологий (NIST) разработал рекомендации по безопасности IoT, включая требования к управлению уязвимостями, аутентификации, шифрованию и обновлению прошивок.

Международные организации также активно разрабатывают стандарты безопасности для IoT. Международный союз электросвязи (ITU) выпускает рекомендации по обеспечению защищенных IoT-экосистем, включая требования к конфиденциальности данных,

устойчивости к атакам и надежности связи. ISO/IEC 27001 и ISO/IEC 29147 содержат ключевые принципы управления рисками и раскрытия уязвимостей, что позволяет компаниям минимизировать угрозы. Кроме того, стандарт ETSI EN 303 645, разработанный Европейским институтом телекоммуникационных стандартов (ETSI), определяет базовые требования к безопасности IoT-устройств, включая запрет на использование предустановленных паролей, обязательное шифрование данных и механизмы безопасного обновления прошивок.

Важным аспектом регулирования является защита персональных данных пользователей. Законодательные акты, такие как Общий регламент по защите данных (GDPR) в Европе и Закон о конфиденциальности потребителей Калифорнии (CCPA) в США, устанавливают строгие правила обработки, хранения и передачи пользовательской информации. IoT-устройства, которые собирают и передают персональные данные, должны соответствовать этим требованиям, обеспечивая анонимизацию, шифрование и возможность контроля со стороны пользователя.

Несмотря на наличие стандартов и законодательных норм, их соблюдение остается серьезным вызовом. Многие производители игнорируют требования безопасности из-за высокой стоимости их внедрения или нехватки компетенций в области киберзащиты. В результате на рынке продолжают появляться устройства с низким уровнем защиты, что делает их уязвимыми для атак. Для эффективного соблюдения стандартов необходимо внедрение механизмов обязательной сертификации IoT-устройств, а также разработка единых международных норм, которые позволят создать универсальные правила для всех производителей.

В перспективе развитие нормативной базы IoT будет направлено на усиление требований к безопасности, внедрение автоматизированных механизмов мониторинга и контроля устройств, а также разработку новых технологий защиты, соответствующих растущей сложности сетей и угроз. Совместная работа государств, международных организаций и частного сектора позволит создать более безопасную и устойчивую экосистему интернет вещей, способную противостоять киберугрозам и обеспечивать защиту данных пользователей.

Итоги и перспективы

Безопасность интернет вещей (IoT) остается одной из ключевых проблем цифровой эпохи, поскольку увеличение количества подключенных устройств приводит к росту потенциальных угроз и уязвимостей. В ходе анализа были рассмотрены основные риски, присущие IoT-инфраструктуре, включая недостаточную аутентификацию, слабую защиту передаваемых данных, уязвимости встроенного программного обеспечения, отсутствие сетевой сегментации и угрозы, связанные с ботнетами и DDoS-атаками. Эти факторы делают IoT привлекательной целью для киберпреступников, способных использовать скомпрометированные устройства для атак на критически важные системы.

В качестве мер защиты предлагается комплексный подход, включающий надежные механизмы аутентификации, шифрование данных, регулярное обновление прошивок, сегментацию сетей и использование средств мониторинга активности. Внедрение многофакторной аутентификации (MFA), использование цифровых сертификатов и уникальных токенов позволит предотвратить несанкционированный доступ. Шифрование трафика с применением современных алгоритмов обеспечит защиту передаваемых данных от

перехвата. Регулярные обновления прошивок и использование механизмов защищенной загрузки (Secure Boot) снизят вероятность эксплуатации уязвимостей в программном обеспечении устройств. Дополнительно сегментация сетей с помощью VLAN и SDN, а также применение систем обнаружения вторжений (IDS/IPS) помогут минимизировать риск распространения атак внутри инфраструктуры.

Особое внимание следует уделить нормативно-правовому регулированию безопасности IoT. Введение обязательных стандартов и сертификации IoT-устройств повысит общий уровень защиты экосистемы. Международные инициативы, такие как стандарты ETSI EN 303 645, рекомендации NIST и требования GDPR, уже закладывают основу для более безопасного развертывания IoT, но их соблюдение остается проблемой из-за отсутствия единых глобальных норм и механизмов контроля.

В перспективе развитие технологий искусственного интеллекта (ИИ) и машинного обучения (ML) позволит более эффективно выявлять угрозы и аномалии в поведении IoT-устройств, что обеспечит автоматизированную защиту от кибератак. Кроме того, использование технологии блокчейна может улучшить управление идентификацией устройств и повысить уровень доверия в распределенных IoT-сетях. Концепция Zero Trust, которая предполагает проверку каждого устройства и запрет на свободный доступ к сети без строгой верификации, также будет играть важную роль в будущем развитии безопасности IoT.

Таким образом, несмотря на значительные вызовы, связанные с безопасностью интернета вещей, применение современных технологий, совершенствование нормативной базы и повышение осведомленности пользователей позволят создать более защищенную и устойчивую экосистему. Важно продолжать исследования в этой области, разрабатывать новые методы противодействия угрозам и внедрять эффективные механизмы защиты, чтобы минимизировать риски и обеспечить безопасное развитие IoT-инфраструктуры.

Список литературы

1. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
2. Гельфанд А. М. и др. ОЦЕНКА РИСКОВ И УГРОЗ БЕЗОПАСНОСТИ В СРЕДЕ «УМНЫЙ ДОМ» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 316-321.
3. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.

References

1. Volkogonov V. N. et al. Application of Physically Unclonable Functions for Authentication in the Internet of Things Environment // Actual Problems of Infocommunications in Science and Education. – 2021. – pp. 409-414.
2. Gelfand A. M. et al. Risk Assessment and Security Threats in the Smart Home Environment // Actual Problems of Infocommunications in Science and Education (APINO 2020). – 2020. – pp. 316-321.
3. Katasonov A. I., Tsvetkov A. Y. Analysis of Access Control Mechanisms in Special-Purpose Systems // Actual Problems of Infocommunications in Science and Education (APINO 2020). – 2020. – pp. 563-568.
4. Petrova T. V. et al. Approaches to Detecting Rogue Wireless Access Points in a Local Area Network // Regional Informatics (RI-2022). – 2022. – pp. 572-573.
5. Shterenberg, S. I. Computer Viruses / S. I. Shterenberg, A. V. Krasov, A. Yu. Tsvetkov. Volume Part 1. – Saint Petersburg : Saint Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2015. – p. 63 – EDN CMMEML.