УДК 004.056.5

Ю.С. Корякина , jk169@list.ru
Институт машиноведения автоматики и геомеханики НАН КР
Б.О. Елизаров elizarovbakii@gmail.com
Институт информационных технологий КГТУ им. И.Раззакова

МЕТОДЫ, ТЕХНОЛОГИИ И МЕХАНИЗМЫ КИБЕРЗАЩИТЫ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ (IOT)

В статье представлен комплексный анализ угроз и методов обеспечения безопасности устройств Интернета вещей (IoT). Рассмотрены ключевые категории угроз: сетевые атаки, физические воздействия, уязвимости на уровне приложений и риски нарушения конфиденциальности данных. Проведен обзор современных методов защиты IoT-устройств, включая меры на сетевом, аппаратном и программном уровнях, криптографические технологии, а также передовые подходы, такие как архитектура Zero Trust, интеграция с SIEM/XDR/SOAR-системами и применение искусственного интеллекта для обнаружения аномалий. Особое внимание уделено построению безопасных архитектур IoT и механизмам киберзащиты, учитывающим ограниченные вычислительные ресурсы устройств и специфику их эксплуатации. На основе анализа угроз и существующих технологий сформулированы рекомендации по выбору и комбинированию методов защиты для различных типов IoT-систем. Представленные материалы могут быть использованы исследователями и практиками при разработке стратегий обеспечения безопасности IoT-инфраструктур и проектировании устойчивых к кибератакам систем.

Ключевые слова: Интернет вещей (IoT), кибербезопасность, угрозы IoT, архитектуры защиты, криптография, Zero Trust, SIEM, XDR, SOAR, безопасные IoT-системы

Введение. В последнее десятилетие Интернет вещей (Internet of Things, IoT) стал одной из наиболее быстро развивающихся областей информационных технологий. IoT представляет собой экосистему взаимосвязанных устройств, способных обмениваться информацией через сеть без активного участия человека. Такие устройства охватывают самые разные области повседневной жизни и промышленности: от умных домов и систем безопасности до сложных решений в сфере здравоохранения и промышленной автоматизации.

Устройства IoT собирают, передают и обрабатывают огромные объёмы данных, зачастую имеющих конфиденциальный характер, что делает вопросы их информационной безопасности чрезвычайно актуальными. Согласно исследованиям, число подключённых IoT-устройств к 2030 году превысит 50 миллиардов единиц, что значительно увеличивает площадь потенциальных атак.

Несмотря на очевидные преимущества Интернета вещей, такие как автоматизация процессов, повышение комфорта и эффективности, данная технология сопряжена с серьёзными рисками информационной безопасности. Из-за специфики устройств IoT (ограниченные вычислительные ресурсы, отсутствие стандартизированных решений в области безопасности, постоянная подключенность к сети), они становятся уязвимыми для различных атак и угроз. В последнее время возросло количество инцидентов, связанных с кражей данных, атаками типа «отказ в обслуживании» (DoS/DDoS), взломами камер видеонаблюдения, компрометацией медицинских приборов и систем управления «умными домами».

В этой связи критически важной задачей становится проведение всестороннего анализа существующих угроз и методов защиты устройств IoT, позволяющего не только минимизировать риски, но и определить оптимальные стратегии и подходы к обеспечению их безопасности. Целью данной статьи является обзор и систематизация существующих угроз и подходов к защите устройств Интернета вещей, а также формирование рекомендаций по обеспечению безопасности IoT-систем.

Существуют **основные угрозы для устройств IoT**. С ростом количества устройств Интернета вещей и их повсеместного распространения увеличивается и спектр угроз, с которыми сталкиваются пользователи и компании, использующие IoT-решения. Уязвимости IoT обусловлены как техническими особенностями устройств, так и специфическими

условиями их эксплуатации. Ниже приведен обзор основных типов угроз, разделённых на несколько категорий [1]:

1. Сетевые угрозы. Сетевые угрозы представляют собой одну из наиболее критичных категорий рисков для инфраструктуры Интернета вещей (IoT), поскольку большинство IoT-устройств функционируют за счёт постоянной сетевой связанности. Из-за ограниченной вычислительной мощности и слабых механизмов защиты устройства IoT становятся лёгкой мишенью для атак через сеть. Ниже рассмотрены также ключевые векторы атак:

• **DDoS-атаки (Distributed Denial of Service).** IoT-устройства зачастую эксплуатируются для организации распределённых атак отказа в обслуживании. Такие устройства могут быть захвачены вредоносным ПО и объединены в ботнеты, как это произошло в случае с ботнетом *Mirai* в 2016 году, когда миллионы IoT-устройств были использованы для масштабной DDoS-атаки на DNS-провайдера Dyn. Устройства, слабо защищённые паролями по умолчанию и без механизмов обнаружения аномалий, представляют собой идеальную цель для подобных атак. Помимо участия в ботнете, сами IoT-устройства и шлюзы могут стать жертвами DDoS, что приводит к потере связи, нарушению работы системы и в случае критической инфраструктуры к сбоям в управлении технологическими процессами.

• **Атаки «человек посередине» (Man-in-the-Middle, MitM).** MitM-атаки особенно опасны в случае IoT-систем, которые часто используют незащищённые каналы передачи данных. При отсутствии TLS или других механизмов шифрования злоумышленник, получивший доступ к маршрутизатору или точке между устройством и облачной инфраструктурой, может перехватывать аутентификационные данные, модифицировать команды управления, внедрять вредоносные обновления прошивки.

Особенно уязвимы решения, не реализующие проверки подлинности конечных точек связи и использующие устаревшие протоколы без криптографической защиты.

• **Эксплуатация уязвимостей протоколов связи.** IoT-устройства опираются на специализированные протоколы связи (например, MQTT, CoAP, Zigbee, Z-Wave, LoRaWAN), разработанные с упором на минимизацию трафика и энергопотребления, но зачастую не имеющие встроенной защиты. Примеры угроз: MQTT (Message Queuing Telemetry Transport) — уязвим к подмене сообщений, отказам в обслуживании и неавторизованному доступу при отсутствии TLS и контроля подписки; CoAP (Constrained Application Protocol) — может быть использован для UDP-флуда, отражённых DDoS-атак и атак replay-типа; Zigbee/Z-Wave — подвержены перехвату команд и обратному инжинирингу, особенно при использовании устаревших схем шифрования.

• **Сканирование и перебор конфигураций (IoT Reconnaissance).** IoT-устройства часто регистрируются в интернете с предсказуемыми именами и открытыми портами (например, порт **554** для **RTSP-камер, 23** для Telnet, **80/443** для веб-интерфейсов). Это делает их уязвимыми к автоматизированному сканированию с помощью специализированных поисковиков, таких как **Shodan** или **Censys**, которые позволяют злоумышленникам находить подключённые к сети устройства по определённым признакам (заголовки, баннеры, протоколы). После идентификации открытого и доступного устройства (например, IP-камеры) атакующий может: использовать учётные данные по умолчанию или перебор для получения доступа; получить доступ к видеопотоку или панелям управления; **превратить скомпрометированную камеру в прокси-сервер**, через который можно выполнять дальнейшее сканирование или проникновение **во внутреннюю сеть организации,** если устройство расположено на границе NAT или имеет прямой маршрут во внутренний сегмент. Таким образом, даже единичная уязвимая IoT-камера может служить точкой входа в изолированные части сети, что нарушает традиционные модели периметровой безопасности.

• **DNS и ARP спуфинг.** IoT-системы, не реализующие защиту на сетевом уровне, могут быть подвержены спуфингу: DNS Spoofing позволяет направить устройства на ложный сервер, откуда они могут загрузить вредоносную конфигурацию или отправить

конфиденциальные данные. ARP Spoofing может быть использован для захвата всего трафика внутри локальной сети, что особенно опасно в «умных домах» и офисах, где IoT-устройства используют общий сегмент.

2. Физические угрозы. Физические угрозы касаются атак, в которых злоумышленник получает прямой доступ к устройству IoT, его корпусу, интерфейсам или окружающей инфраструктуре. Такие атаки особенно опасны в условиях слабой физической защиты устройств, что характерно для промышленных объектов, городских систем (умные камеры, датчики) и удалённых сенсоров. Ниже приведены основные векторы физического воздействия:

• **Кража устройств и физическое вскрытие.** Физическое изъятие IoT-устройства предоставляет злоумышленнику доступ ко всем его аппаратным и программным компонентам:

можно извлечь конфигурационные файлы, учётные данные и ключи шифрования из памяти (например, из SPI Flash или EEPROM); возможно клонирование устройства или эмуляция его поведения в тестовой среде для последующего анализа; устройства, не использующие аппаратное шифрование хранения, особенно подвержены утечке данных после кражи. Такой вектор атаки критичен для IoT в медицинских, военных и производственных системах, где конфиденциальные данные (например, логи или параметры управления) могут быть использованы для подготовки последующих кибератак.

• **Несанкционированный физический доступ и замещение.** Даже кратковременный физический контакт с устройством может быть достаточным для его компрометации. Наиболее распространённые сценарии включают: подключение через отладочные интерфейсы (UART, JTAG), которые часто оставлены активными в финальных версиях устройств; инъекция вредоносного ПО через USB или microSD-интерфейсы; замена оригинального устройства модифицированным клоном, сохраняющим внешние признаки, но реализующим скрытую функциональность (например, перехват или ретрансляцию данных, встроенный радиомодуль). В условиях массового развёртывания IoT в публичных или открытых пространствах (например, парковках, остановках, умных мусорных контейнерах) физическая защита редко обеспечивается должным образом, что делает такие атаки реалистичными.

• **Атаки через боковые каналы (Side-channel attacks).** Боковые каналы позволяют извлекать чувствительную информацию, не нарушая логической целостности системы. Эти атаки используют: анализ энергопотребления (Power Analysis) — для извлечения криптографических ключей (например, в устройствах, реализующих AES, RSA, ECC); измерение электромагнитного излучения (EM Analysis) — для восстановления операций процессора; анализ теплового профиля — для выявления работающих компонентов, особенно в многочиповых сборках. Несмотря на то, что такие атаки требуют специальных навыков и оборудования, они успешно применялись против реальных IoT-устройств — от плат Arduino до смарт-карт и медицинских приборов. Особо уязвимы устройства, не использующие схемы аппаратной защиты, такие как Tamper Detection, Shielded Enclosures или Secure Boot. Однако, как показывает практика, даже наличие таких механизмов не гарантирует абсолютной защиты. В 2025 году исследователь в области информационной безопасности смог обойти механизм **Secure Boot**, воспользовавшись возможностями языковой модели ChatGPT для генерации эксплойта на базе анализа прошивки и реверс инжиниринга, что демонстрирует растущую угрозу со стороны инструментов ИИ при проведении целевых атак на прошивку и загрузочные цепочки доверия.

3. Угрозы на уровне приложений. Программная составляющая IoT-экосистемы, включая встроенные прошивки, веб-интерфейсы, мобильные приложения и облачные API, представляет собой ключевую поверхность атаки. Учитывая, что большинство устройств работают в тесной связке с удалёнными сервисами, ошибки на уровне приложений могут привести к масштабным компрометациям. Ниже представлены наиболее критичные векторы атак:

• **Уязвимости в прошивках и встроенном ПО.** Прошивки IoT-устройств зачастую создаются с акцентом на функциональность и энергоэффективность, в ущерб безопасности. Это приводит к появлению следующих проблем: отсутствие механизмов верификации обновлений (или реализация OTA Update без подписи и проверки контрольной суммы); небезопасная реализация стеков сетевых протоколов, приводящая к переполнению буфера (buffer overflow) и возможности удалённого выполнения кода (RCE); наличие встроенных учётных записей с жёстко заданными паролями (hardcoded credentials) или отладочных бэкдоров. В реальной практике известны случаи массовых атак на IoT-устройства с использованием публично доступных эксплойтов для прошивок, в частности, многочисленные CVE, связанные с маршрутизаторами и видеокамерами (например, CVE-2021-36260 — удалённое выполнение команд на устройствах Hikvision).

• **Атаки на API и облачные интерфейсы.** Большинство современных IoT-систем используют REST API или MQTT over WebSockets для связи с облачными платформами или мобильными приложениями. Ошибки в их реализации или настройке могут включать: отсутствие аутентификации или слабые механизмы авторизации (например, токены, не привязанные к IP или сессии); уязвимости типа Insecure Direct Object References (IDOR), когда злоумышленник может получить доступ к чужим данным путём подбора идентификаторов;

отсутствие ограничения скорости (rate limiting) и механизма защиты от перебора (brute-force protection). Атаки на API позволяют не только получить доступ к управлению устройствами, но и массово извлекать конфиденциальные данные о пользователях, включая координаты, аудио- и видеозаписи, логи активности.

• **Ошибки конфигурации и администрирования.** Ошибки в конфигурации системного и прикладного уровня являются одной из самых распространённых причин компрометаций: устройства, оставленные с настройками по умолчанию, включая пароли «admin/admin»; включённые отладочные интерфейсы, доступные по сети; широкие политики доступа в облачных системах (например, открытые S3-бакеты, в которых хранятся резервные копии настроек или токены). Зачастую администраторы недостаточно внимательно подходят к изоляции устройств внутри сети или не реализуют Zero Trust-модель, что создаёт дополнительные риски при компрометации одного из узлов.

4. Угрозы конфиденциальности и утечки данных. IoT-экосистемы по своей природе ориентированы на непрерывный сбор, обработку и передачу данных о пользователях, окружающей среде и объектах управления. В условиях отсутствия должных мер защиты это делает IoT одним из наиболее уязвимых компонентов с точки зрения конфиденциальности. Ниже приведены ключевые категории угроз, связанных с утечкой или неправомерным доступом к данным:

• **Нарушение конфиденциальности персональных данных.** Множество IoT-устройств, от фитнес-браслетов и «умных» колонок до медицинских имплантов, собирают чувствительную информацию: биометрические параметры, историю активности, геопозицию, поведенческие шаблоны и пр. Часто эти данные: передаются на внешние серверы без надлежащего шифрования (например, по HTTP); сохраняются в локальных логах без контроля доступа; используются третьими сторонами без согласия пользователя (в нарушение принципов GDPR, HIPAA и других стандартов). Примером может служить утечка через трекеры активности, при которой стало возможно идентифицировать расположение военных объектов, как это произошло с **Strava** в 2018 году, когда данные пользователей были визуализированы на публичной карте тепловой активности.

• **Неавторизованное слежение и слом приватности.** Многие IoT-устройства, изначально предназначенные для обеспечения комфорта или безопасности (например, камеры видеонаблюдения, умные дверные звонки, голосовые помощники), могут быть перепрофилированы злоумышленником в инструменты скрытого наблюдения. Основные риски: доступ к видеопотоку или микрофону в реальном времени через удалённые уязвимости (веб-интерфейс, API); сохранение записей в облаке без уведомления

пользователя и без возможности их удалить; геолокационные трекеры без шифрования, передающие местоположение в открытом виде или слабо защищённым API. Фактически скомпрометированное IoT-устройство может стать цифровым эквивалентом подслушивающего или наблюдающего жучка, особенно в домашней или офисной среде.

• **Перехват и утечка данных через облачные платформы.** IoT-данные редко остаются локальными, большинство решений используют облачные хранилища и платформы для агрегации, визуализации и аналитики. При этом: данные хранятся на сторонних сервисах, не всегда соответствующих требованиям локального законодательства о защите данных; плохо защищённые API, отсутствие шифрования at-rest и in-transit, или открытые публичные бакеты (например, Amazon S3) приводят к массовым утечкам; один скомпрометированный аккаунт администратора может открыть доступ к информации всех пользователей платформы (модель «одной точки отказа»). Учитывая, что многие IoT-платформы обрабатывают видео, аудио, телеметрию, биометрию и поведенческие паттерны, их компрометация может иметь последствия, сопоставимые с крупными утечками в финансовом или медицинском секторах.

Примеры реальных атак на устройства IoT. Практика последних лет ясно показывает, что угрозы для IoT-среды не являются теоретическими, а напротив, они уже привели к ряду масштабных инцидентов с серьёзными последствиями для бизнеса, частных лиц и даже человеческой жизни. Ниже приведены наиболее показательные случаи, отражающие широкий спектр возможных атак на IoT-инфраструктуру:

Ботнет Mirai (2016). Один из наиболее известных и разрушительных примеров злоупотребления IoT — ботнет Mirai, впервые зафиксированный в 2016 году. Он сканировал сеть в поисках устройств с заводскими паролями (видеокамеры, маршрутизаторы, DVR) и автоматически подключал их к ботнету. Среди наиболее пострадавших — провайдер DNS Dyn, атака на которого привела к масштабному отключению сервисов, включая Twitter, Netflix, Reddit и GitHub. Mirai стал поворотной точкой в осознании угроз от IoT-устройств. Он показал, что даже простые уязвимости, такие как пароли по умолчанию, могут быть использованы для создания глобальных сетей вредоносных устройств.

Взлом системы умного дома Nest (2019). В 2019 году было зафиксировано несколько инцидентов, связанных со взломом IoT-устройств Google Nest, включая камеры и «умные» термостаты. В одном случае злоумышленник получил доступ к камере и передал через динамик голосовое сообщение с угрозой пользователю, симулируя захват дома. Хотя взлом был осуществлён с использованием утекших учётных данных (credential stuffing), инцидент продемонстрировал серьёзную проблему: отсутствие двухфакторной аутентификации (2FA) по умолчанию, недостаточное оповещение пользователей о входах и слабую реакцию на инциденты со стороны сервисов. Это событие вызвало широкий резонанс и стало примером того, как IoT-устройство может превратиться в инструмент психологического давления.

Уязвимости в медицинских устройствах Medtronic (2018–2020). Между 2018 и 2020 годами исследователи выявили критические уязвимости в кардиостимуляторах и инсулиновых помпах Medtronic, включая: отсутствие шифрования связи между устройствами и контроллерами; возможность перехвата и модификации управляющих команд; отсутствие механизма проверки подлинности обновлений ПО (firmware updates). В рамках демонстрации атаки было показано, что злоумышленник, находящийся на расстоянии до 6 метров, может изменить ритм стимуляции сердца или прекратить подачу инсулина, что представляет прямую угрозу жизни пациента. Несмотря на выпуск обновлений и отзыв части продукции, инцидент выявил критическую уязвимость IoT-медицинских систем, где безопасность жизненно важна, но исторически оставалась на вторичном месте [2].

Эти и многие другие инциденты демонстрируют, что угрозы безопасности IoT охватывают все уровни архитектуры — от физического устройства до облачных сервисов, включая сетевые протоколы и приложения. Более того, IoT-устройства всё чаще становятся частью киберфизических систем, где атака в цифровом пространстве может привести к реальным последствиям — от вторжения в личное пространство до угрозы жизни.

Формирование эффективной стратегии защиты IoT должно базироваться не только на теоретических моделях, но и на анализе уже произошедших атак, их сценариев и последствий [3].

Анализ методов защиты устройств IoT. Эффективная защита устройств Интернета вещей (IoT) должна быть комплексной и учитывать уязвимости на всех уровнях: аппаратном, сетевом и программном. Рассмотрим современные методы и технологии, направленные на снижение рисков и защиту устройств IoT [4].

1. Методы защиты на уровне сети. Надёжная защита сетевого взаимодействия IoT-устройств является основополагающим элементом общей архитектуры безопасности. С учётом постоянной сетевой активности и ограниченных вычислительных ресурсов большинства устройств, защита на сетевом уровне требует тщательно подобранных решений, сочетающих эффективность и лёгкость реализации.

Использование защищённых протоколов передачи данных. Безопасная передача данных критична при взаимодействии IoT-устройств с облачными платформами, шлюзами и друг с другом. Наиболее эффективные протоколы: TLS (Transport Layer Security) — стандарт для защиты соединений TCP. Используется во всех современных HTTPS-сессиях, позволяет обеспечивать аутентификацию устройств (через X.509-сертификаты) и защищённую передачу данных. В IoT применяется при передаче данных в облако или при обновлении прошивок (FOTA). DTLS (Datagram Transport Layer Security) — версия TLS, адаптированная под UDP-соединения, используемые многими IoT-протоколами (например, CoAP). Поддерживает сквозное шифрование и верификацию целостности, даже в нестабильных или низкопроизводительных сетях. IPsec (Internet Protocol Security) — протокол защиты на уровне IP-стека. Часто применяется в промышленных IoT-сетях (IIoT), где требуется строгая политика безопасности между шлюзами и управляющими центрами. Обеспечивает шифрование, аутентификацию и защиту от подмены трафика на сетевом уровне.

Важно учитывать: встраивание TLS/DTLS в устройства с ограниченными ресурсами требует оптимизированных реализаций (например, mbedTLS, WolfSSL) и грамотной работы с хранилищами ключей и сертификатов.

Межсетевые экраны и сегментация сети. Сетевые меры защиты служат барьером между IoT-устройствами и потенциальными источниками атак: межсетевые экраны (Firewall) обеспечивают фильтрацию исходящего и входящего трафика на основе IP, портов, протоколов или контекста сессии. На практике применяются: на шлюзах, соединяющих локальную IoT-сеть с Интернетом; внутри предприятия — в составе систем контроля межсегментного трафика; на уровне облака — с помощью виртуальных фаерволов (например, AWS Security Groups, Azure NSG). Сегментирование сети — логическое разделение инфраструктуры на изолированные зоны: VLAN или VRF позволяют разграничить домены доверия (например, отделить IoT-камеры от системы управления доступом или SCADA). Применение технологии microsegmentation на базе SDN (Software Defined Networking) даёт возможность управлять связями между устройствами на уровне политик, что особенно эффективно в дата-центрах и промышленных развертываниях. Сегментация существенно снижает поверхность атаки и ограничивает горизонтальное перемещение злоумышленника после компрометации одного из узлов (lateral movement)[5].

Использование VPN-соединений. Для безопасной передачи данных между устройствами, распределёнными по различным физическим локациям (например, между удалённым сенсором и центральным сервером), широко применяется: VPN (Virtual Private Network) — защищённый туннель, обеспечивающий конфиденциальность, аутентификацию и целостность данных; IPsec VPN — часто используется между промышленными контроллерами и диспетчерскими; OpenVPN и WireGuard — лёгкие реализации для встраивания в устройства с ограниченным объёмом памяти; VPN также применяется при удалённом администрировании IoT-устройств — как альтернатива небезопасному прямому подключению по SSH или Telnet. Однако следует помнить, что использование VPN без

должного управления ключами и контроля точек входа может привести к новым векторам атак, включая захват сессий и обход межсетевых экранов.

2. Методы защиты на уровне устройств. Безопасность на уровне устройств IoT — это фундаментальный слой, обеспечивающий доверие ко всей остальной инфраструктуре. Ввиду ограниченных ресурсов и длительного жизненного цикла таких устройств особое значение приобретают меры, которые могут быть встроены в саму архитектуру устройства и функционировать без постоянного вмешательства администратора [6].

Аутентификация и авторизация устройств. Разграничение прав доступа и проверка подлинности устройств и пользователей — ключ к предотвращению несанкционированного управления: Двухфакторная аутентификация (2FA) — добавление второго фактора при доступе к веб-интерфейсам, API или мобильным приложениям управления устройствами (например, Push-уведомление, OTP-код). 2FA особенно актуальна для удалённого управления или администрирования устройств в критичных зонах (например, системы контроля доступа, SCADA-панели). Управление идентичностью устройств (Device Identity Management) — внедрение инфраструктуры открытых ключей (PKI) позволяет каждому устройству иметь уникальный сертификат X.509. Использование TLS-ручного или автоматического взаимного аутентифицирования (mTLS) предотвращает атаки типа «device spoofing», а также обеспечивает доверительную связь в масштабируемых IoT-сетях. Дополнительно применяется автоматический отзыв сертификатов (OCSP/CRL), что позволяет оперативно блокировать компрометированные устройства.

Обновление и защита прошивок. Большинство атак на IoT-устройства эксплуатируют устаревшее ПО и небезопасные обновления, поэтому обновляемость и контроль целостности прошивки являются обязательными требованиями: OTA (Over-the-Air) обновления — позволяют централизованно развёртывать патчи безопасности и новые версии прошивки без физического доступа к устройству. При этом важно: реализовать криптографическую проверку подписи прошивки до её установки; использовать безопасные каналы (например, HTTPS/TLS) для доставки обновлений; предусматривать fail-safe механизм — возврат к последней рабочей версии при сбое обновления. Цифровая подпись прошивок — гарантирует, что загружаемое ПО поступает от доверенного источника и не было изменено. Подпись выполняется закрытым ключом вендора, а проверка — на стороне устройства, с использованием встроенного корневого сертификата. Некоторые производители реализуют также Secure Boot, при котором каждый компонент цепочки загрузки проверяется на подлинность и целостность, начиная от загрузчика до основного ПО.

Аппаратная защита и устойчивость к физическим атакам. Учитывая распространённость IoT в публичных и уязвимых локациях, особенно важны механизмы аппаратной безопасности, которые защищают устройства даже при физическом доступе: Secure Elements (SE), TPM (Trusted Platform Module), HSM (Hardware Security Module) — специализированные микросхемы для хранения криптографических ключей, цифровых сертификатов и проведения криптографических операций (например, генерация подписи, шифрование/дешифрование). Ключи, хранящиеся в SE/TPM, невозможно извлечь стандартными средствами.

Физическая защита от взлома (tamper-resistant / tamper-evident / tamper-proof): экранирование чипов от электромагнитного анализа (side-channel attacks); стирание ключей при попытке вскрытия корпуса; использование клеевых или антиклейких матриц на контактах отладочных интерфейсов (UART/JTAG). Обфускация прошивки и защита от обратной инженерии также может относиться к этому уровню: например, внедрение антивандальных механизмов или самоуничтожения ключей при аномальном доступе.

3. Методы защиты на уровне приложений. Поскольку взаимодействие между пользователями, облачными платформами и IoT-устройствами осуществляется в значительной степени через прикладной уровень, надёжность и безопасность приложений, API и систем конфигурации является критически важной. Уязвимости в логике приложений,

ошибочная реализация API или неверные настройки по умолчанию нередко становятся основными векторами атак на IoT-инфраструктуру.

Безопасное программирование и кодирование. Надёжная защита IoT начинается на этапе проектирования программного обеспечения. Принципы Secure Software Development Lifecycle (SSDLC) включают:

Безопасное кодирование с учётом рекомендаций OWASP IoT Top 10 и CWE/SANS. Это включает защиту от переполнения буфера, внедрения кода, XSS/SQL-инъекций (если используется веб-интерфейс) и т.п.

Статический анализ кода (SAST) — используется для выявления уязвимостей ещё на стадии компиляции. Популярные инструменты: SonarQube, Fortify, Cppcheck.

Динамический анализ (DAST) — имитация взаимодействия с работающим приложением позволяет выявить ошибки логики, проблемы аутентификации и авторизации.

Фаззинг и тестирование на проникновение (IoT Pentesting) особенно актуальны для прошивок и нестандартных протоколов, где традиционные средства анализа бессильны. Кроме того, важно применять контейнеризацию и изоляцию компонентов, особенно в сложных IoT-приложениях с микросервисной архитектурой.

Защита API-интерфейсов. API — один из наиболее частых векторов атак на IoT-системы. Надёжная защита включает:

Аутентификацию и авторизацию на уровне API: использование OAuth 2.0 или JWT;

обязательная проверка клиента (client-side verification), в том числе Mutual TLS (mTLS); разграничение прав доступа по принципу наименьших привилегий (least privilege). Rate limiting и throttling — защита от brute-force атак и перегрузки сервисов.

Журналирование и аудит активности: сохранение логов всех запросов и отклонённых попыток; интеграция с SIEM-системами и платформами аналитики безопасности (например, ELK, Graylog, QRadar) для выявления аномалий. Фильтрация ввода и валидация параметров — предотвращает внедрение вредоносных данных, особенно важно для открытых API, используемых внешними приложениями. Пример: уязвимость IDOR (Insecure Direct Object Reference) может позволить злоумышленнику получить доступ к чужим данным, просто изменив идентификатор устройства в URL. Это должно предотвращаться строгой проверкой полномочий на уровне API.

Управление конфигурацией устройств. Ошибки конфигурации — одна из главных причин компрометаций IoT-систем. Эффективное управление включает:

Отказ от настроек и паролей по умолчанию: обязательное изменение паролей при первичной настройке; отключение неиспользуемых сервисов (SSH, Telnet, WebUI).

Централизованное управление конфигурацией: внедрение IoT Device Management Platform (например, AWS IoT Core, Azure IoT Hub, Eclipse Kura); возможность массового применения политик безопасности, настройки параметров TLS, периодической смены ключей.

Слежение за состоянием устройств в реальном времени: оповещения о попытках входа, отклонениях от заданных параметров, устаревших прошивках; аудит активности на уровне устройств (например, syslog, auditd). Централизованный контроль критичен для масштабируемых развертываний: он снижает риск ручных ошибок, ускоряет реагирование и делает возможным автоматизированную реакцию на инциденты[7].

4. Использование криптографических методов защиты данных IoT. Криптографическая защита — один из краеугольных камней обеспечения безопасности в IoT-среде. Она обеспечивает базовые свойства информационной безопасности: конфиденциальность, целостность, аутентичность и непротиворечивость. Учитывая постоянную передачу данных по сетям, взаимодействие с облачными сервисами и ограниченность ресурсов большинства устройств, выбор и реализация криптографических механизмов должны быть адаптированы к особенностям IoT.

Шифрование данных (конфиденциальность). Для защиты данных в процессе передачи (in transit) и хранения (at rest) используются: симметричное шифрование (например,

AES-128/256): применяется на уровне каналов связи (например, в DTLS, IPsec); эффективно при защите данных внутри локальных IoT-сетей; требует безопасного управления ключами (key provisioning, rotation, revocation). Асимметричное шифрование (например, RSA, ECC):

используется для обмена ключами, аутентификации устройств и подписей; **ECC** (Elliptic Curve Cryptography) предпочтительнее для IoT благодаря меньшему размеру ключей при равной криптостойкости; поддерживается во многих современных микроконтроллерах и модулях TPM/SE. Очень важным считается, что криптографическая реализация должна учитывать особенности устройства, то есть должно применяться аппаратное ускорение (AES-NI, ARM Crypto Extensions) или лёгкие криптобиблиотеки (mbedTLS, WolfSSL, TinyCrypt).

Хеш-функции и цифровые подписи (целостность и подлинность). Криптографические хеш-функции (например, **SHA-256, SHA-3**): используются для контроля целостности данных (например, при проверке обновлений прошивки, подписанных конфигураций); играют ключевую роль в построении схем аутентификации и цифровых подписей. Цифровые подписи: реализуются на базе асимметричной криптографии; позволяют удостовериться, что данные или прошивка поступили от доверенного источника и не были изменены; применяются в Secure Boot, OTA-обновлениях, подписанных сообщениях API и конфигурационных файлах. Пример: устройство получает обновление прошивки, подписанное вендором. Сначала выполняется верификация подписи по хешу содержимого и открытому ключу из доверенного хранилища. Только в случае успешной проверки устройство применяет обновление.

Управление криптографическими ключами Криптография эффективна только при надёжном управлении ключами: защита от утечек через secure storage (TPM, HSM, Secure Element); автоматизированная ротация ключей; централизованная PKI-инфраструктура для выпуска, отзыва и обновления сертификатов. Особое внимание следует уделять **zero-touch provisioning** — безопасному внедрению ключей и сертификатов при первом подключении устройства к сети, без ручного участия[8].

5. Современные технологии и подходы. С ростом масштабов и сложности IoT-инфраструктур традиционные методы защиты (шифрование, фаерволы, контроль доступа) становятся необходимыми, но недостаточными. Современные угрозы требуют проактивных и интеллектуальных подходов, обеспечивающих безопасность на всём жизненном цикле устройства — от производства и развёртывания до эксплуатации и утилизации. Ниже представлены ключевые направления технологического развития в области кибербезопасности IoT.

Zero Trust Architecture (ZTA) для IoT. Классическая модель периметровой защиты становится неэффективной в условиях распределённых IoT-систем. Модель Zero Trust предполагает: отсутствие автоматического доверия даже к устройствам внутри корпоративной сети; обязательную проверку идентичности и целостности для каждого запроса (device attestation, continuous authentication); микросегментацию и контроль привилегий на уровне отдельных устройств, API и микросервисов. Интеграция IoT в Zero Trust требует поддержки механизмов PKI, политики least privilege, а также мониторинга поведения (behavioral analytics).

Интеграция с SIEM, XDR и SOAR-системами. Современные IoT-решения генерируют значительные объёмы телеметрии, логов и метрик. Их использование возможно только при интеграции с системами класса: **SIEM** (Security Information and Event Management) — централизованный сбор и корреляция событий безопасности (например, через Graylog, Splunk, QRadar); **XDR** (Extended Detection and Response) — анализ событий на всех уровнях (сеть, устройства, облако) с использованием машинного обучения; **SOAR** (Security Orchestration, Automation and Response) — автоматизация реагирования на инциденты: изоляция устройства, блокировка IP, генерация оповещений в реальном времени. Особенно важна поддержка протоколов syslog, MQTT, RESTful API для экспортирования логов и состояния устройств.

Аппаратная корневая доверия (Hardware Root of Trust). Системы, построенные на принципе аппаратного корня доверия, используют защищённые аппаратные модули для старта загрузки и хранения ключей: TPM, SE, HSM; Secure Boot + Measured Boot (например, на базе Arm TrustZone, Intel Boot Guard); встроенные механизмы защиты от клонирования и side-channel атак. Такие платформы позволяют реализовать безопасное начальное состояние устройства и восстанавливать доверие даже после компрометации уровня ОС.

ИИ и машинное обучение для анализа аномалий. IoT-устройства, особенно в промышленных сетях (IIoT), создают повторяющиеся шаблоны поведения, что делает их удобными объектами для поведенческого анализа (Behavioral Analytics). Современные подходы включают: обнаружение отклонений от нормы (например, резкое изменение частоты передачи данных, появление новых узлов); классификацию атак по паттернам (например, DoS, lateral movement, spoofing); обучение моделей в рамках платформ XDR/EDR или на границе сети (edge AI). Решения на базе ИИ позволяют выявлять угрозы в режиме реального времени и усиливают возможности классических систем мониторинга.

Secure-by-Design и стандарт ISO/IEC 27402. Переход от реактивной безопасности к встроенной (secure-by-design) становится стандартом. Это включает: закладывание требований безопасности на уровне архитектуры; формализацию процессов разработки согласно DevSecOps; соответствие новым стандартам — в частности, ISO/IEC 27402 (IoT Security Baseline Requirements**)**, который определяет минимальные требования к производителям устройств: наличие механизма обновлений, управление доступом, защита данных и т.д. Современные подходы демонстрируют смещение парадигмы: от защиты по периметру — к динамическому, контекстному и адаптивному управлению безопасностью, при котором IoT-системы становятся активными участниками своей собственной защиты. Внедрение этих технологий требует как технической зрелости инфраструктуры, так и организационного подхода к безопасности на всех уровнях — от инженеров до топ-менеджмента[9].

Сравнение и рекомендации по использованию методов защиты. Для эффективной защиты IoT-устройств необходимо учитывать специфику конкретной ситуации, тип устройства, условия эксплуатации и уровень критичности данных. Рассмотрим краткое сравнение описанных выше методов защиты и рекомендации по их применению на практике в таблице 1[10].

Таблица 1 – Сравнительный анализ методов защиты

Уровень защиты	Методы защиты	Преимущества	Недостатки	Рекомендуемая область применения
Сетевой уровень	TLS, DTLS, IPsec, VPN	Высокий уровень защиты от перехвата трафика, конфиденциальность данных	Требуют дополнительных ресурсов, усложняют инфраструктуру	Применимы везде, особенно в передаче критически важных и конфиденциальных данных
	Межсетевые экраны, сегментирование сети	Простота реализации, эффективная защита от сетевых атак	Ограничены в защите от атак на программном уровне	Все типы IoT-сетей, от домашних до промышленных
Аппаратный уровень	Secure Elements, TPM, аппаратная защита	Высокая устойчивость к физическим атакам и взлому устройств	Дополнительные затраты и сложности в разработке	Критически важные устройства (медицина, промышленность, критическая инфраструктура)

Программный уровень	Аутентификация, OTA-обновления, цифровая подпись прошивок	Эффективны против большинства атак на уровне приложений и прошивок	Требуют постоянного контроля и поддержки, дополнительных ресурсов для разработки	Любые устройства с подключением к сети
	Безопасное программирование, защита API	Минимизация рисков взлома и утечки данных	Требуют высококвалифицированных специалистов	Все IoT-решения, особенно облачные приложения
Криптография	AES, RSA, ECC, хеширование	Высокий уровень конфиденциальности и целостности данных	Нагрузка на аппаратные ресурсы, необходимость безопасного управления ключами	Универсальное применение
Передовые технологии	Блокчейн, ИИ и машинное обучение	Эффективность в предотвращении атак и обеспечении целостности данных	Сложность интеграции и реализации, требуются значительные вычислительные ресурсы	Средние и крупные IoT-проекты с высокими требованиями к безо

Рекомендации по выбору методов защиты. На основе проведённого анализа угроз и методов защиты устройств Интернета вещей сформулированы следующие рекомендации:

Комплексный подход. Наиболее эффективна комбинация методов защиты на сетевом, аппаратном и программном уровнях. Особое внимание стоит уделять криптографическим методам, которые обеспечивают высокий уровень защиты данных[11].

Выбор методов с учётом специфики устройства. Для устройств с ограниченными ресурсами рекомендуется использовать облегчённые протоколы и схемы шифрования (например, DTLS, ECC). А для устройств, работающих с критически важной информацией (здравоохранение, промышленность, безопасность), необходимы аппаратные решения защиты и строгая аутентификация.

Регулярное обновление и мониторинг. Обязательным условием безопасности является использование регулярных OTA-обновлений для устранения уязвимостей. А также внедрение систем мониторинга и анализа поведения устройств для оперативного реагирования на угрозы[12].

Заключение

В данной статье проведён комплексный анализ угроз, с которыми сталкиваются устройства Интернета вещей (IoT), а также рассмотрены современные методы и технологии, применяемые для обеспечения их безопасности. На фоне стремительного роста количества IoT-устройств и их интеграции в критически важные сферы, от промышленности и здравоохранения до умных домов и городов, вопросы информационной безопасности приобретают первостепенное значение. Анализ показал, что угрозы безопасности охватывают все уровни IoT-архитектуры: от сетевых атак и физического доступа до уязвимостей в прошивках, API и облачных сервисах. Особую опасность представляют нарушения конфиденциальности, компрометация устройств через незащищённые интерфейсы, а также масштабируемость угроз за счёт автоматизированного распространения атак в распределённых системах.

Для противодействия этим вызовам требуется реализация многоуровневой стратегии защиты, включающей сетевые меры (шифрование, VPN, сегментация), защиту устройств (аутентификация, Secure Boot, TPM), безопасную разработку приложений и API, применение криптографических алгоритмов, адаптированных под ограничения IoT, интеграцию с современными системами мониторинга и анализа инцидентов (SIEM, XDR, SOAR), а также внедрение архитектур Zero Trust и моделей Secure-by-Design. Отдельное внимание следует уделить применению искусственного интеллекта, поведенческого анализа, а также перспективных технологий, таких как блокчейн и аппаратный корень доверия (Hardware

Root of Trust). Эти решения позволяют не только минимизировать вероятность атаки, но и существенно сократить время её обнаружения и реагирования.

Перспективными направлениями дальнейших исследований являются формализация международных стандартов (например, ISO/IEC 27402) и их унификация, оптимизация криптографических протоколов для энергоэффективной работы, автоматизация процессов управления идентификацией и обновлениями устройств, а также развитие самообучающихся систем обнаружения аномалий в IoT-сетях. Таким образом, обеспечение безопасности IoT требует не только технических решений, но и формирования культуры ответственности на всех этапах жизненного цикла устройств, от проектирования и производства до внедрения, администрирования и утилизации. Только комплексный и системный подход может обеспечить надёжную защиту в условиях всё более усложняющейся цифровой среды.

Литература

1. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A. IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices // IEEE Internet of Things Journal. – 2019. – Vol. 6, No. 5. – P. 8182–8201. DOI: 10.1109/JIOT.2019.2935189.
2. Lee, I., Lee, K. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management // Future Internet. – 2021. – Vol. 13, No. 6. – Article 154. DOI: 10.3390/fi13060154.
3. Sharma, V., You, I., Kumar, R. IoT Security: Review, Blockchain Solutions, and Open Challenges // Future Generation Computer Systems. – 2021. – Vol. 122. – P. 42–61. DOI: 10.1016/j.future.2021.03.019.
4. Bertino, E., Islam, N. Botnets and Internet of Things Security // Computer. – 2017. – Vol. 50, No. 2. – P. 76–79. DOI: 10.1109/MC.2017.62.
5. Fernandez-Carames, T.M., Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things // IEEE Access. – 2018. – Vol. 6. – P. 32979–33001. DOI: 10.1109/ACCESS.2018.2842685.
6. Alrawais, A., Alhothaily, A., Hu, C., Cheng, X. Fog Computing for the Internet of Things: Security and Privacy Issues // IEEE Internet Computing. – 2017. – Vol. 21, No. 2. – P. 34–42. DOI: 10.1109/MIC.2017.37.
7. Mosenia, A., Jha, N.K. A Comprehensive Study of Security of Internet-of-Things // IEEE Transactions on Emerging Topics in Computing. – 2017. – Vol. 5, No. 4. – P. 586–602. DOI: 10.1109/TETC.2016.2606384.
8. Zhang, Z.-K., Cho, M.C.Y., Shieh, S., Wang, Y.-C. IoT Security: Ongoing Challenges and Research Opportunities // IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA). – 2014. – P. 230–234. DOI: 10.1109/SOCA.2014.58.
9. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey // Computer Networks. – 2019. – Vol. 148. – P. 283–294. DOI: 10.1016/j.comnet.2018.11.025.
10. Maple, C. Security and privacy in the internet of things // Journal of Cyber Policy. – 2017. – Vol. 2, No. 2. – P. 155–184. DOI: 10.1080/23738871.2017.1366536.
11. Корякин, С. В. Современные тенденции развития систем информационной безопасности / С. В. Корякин // Проблемы автоматики и управления. – 2017. – № 2(33). – С. 82-91. – EDN ZXPAXD.
12. Корякин, С. В. Аналитический обзор технологий построения аппаратно-ориентированных облачных систем защиты информации с применением нейросетевых технологий / С. В. Корякин // Проблемы автоматики и управления. – 2025. – № 2(53). – С. 41–51. – EDN RCCRHC.