УДК 330

# УЯЗВИМОСТЬ МОБИЛЬНОГО УСТРОЙСТВА

***Переспелов Анатолий Витальевич***
*кандидат технических наук, доцент*
***Гнездов Владислав Константинович,***
***Демаков Ярослав Александрович,***
***Назаров Никита Михайлович***
*Студенты*
*ФГБОУ ГУМРФ имени адмирала С. О. Макарова*

**Аннотация.** Если раньше мобильное устройство из себя представляло лишь самостоятельное электронное портативное устройство, то с появлением и развитием интернета к этому термину приписывается так же наличие выхода в интернет. Развитие интернет-сетей пятого и шестого поколения позволяет расширить функционал любого устройства, так как дает возможность пользователю управлять им из любой точки мира. Это в свою очередь раскрывает проблему безопасности каждого устройства, которое имеет выход в глобальную сеть, с каждым днем появляется все больше гаджетов, а количество их уязвимостей не уменьшается.

**Abstract.** If earlier a mobile device was just an independent electronic portable device, then with the advent and development of the Internet, this term is also attributed to the presence of an Internet connection. The development of Internet networks of the fifth and sixth generations makes it possible to expand the functionality of any electronic device, as it enables the user to control any purchased device from anywhere. This, in turn, reveals the problem of the security of each device that has access to the global network, every day more and more gadgets appear, and the number of their vulnerabilities does not decrease.

**Ключевые слова:** информационные технологии, интернет вещей, информационная безопасность, уязвимости, сеть.

**Key words:** information technology, internet of things, information security, vulnerabilities, network.

---

Современные устройства собирают массивы данных о своих пользователях. Некоторым из них для работы требуется не только пароль, но и имя пользователя, его контактная информация, сведения о биографии. Такое количество информации требует надежной и качественной защиты, однако на данный момент IoT не может похвастаться защищенностью.

Также проблема усугубляется тем, что пользователи часто не изменяют установленные по умолчанию логины и пароли. Это значительно облегчает задачу злоумышленникам и вероятность того, что устройство попадет в ботнет становится гораздо выше.

Боты позволяют злоумышленникам скрытно управлять зараженными устройствами. С появлением интернета вещей возникло больше возможностей для создания целых ботнетов, что связано с потерей автономии физическими устройствами — многие вещи перестали работать самостоятельно, они интегрируются в единую систему и не способны функционировать в отрыве от нее. А как уже упоминалось выше, процессы внутри IoT зачастую не контролируются [1].

С появление IoT устройств так же появились первые серьезные уязвимости, первым таким примером является ботнет червь под названием Mirai, еще в 2016 году, в этом же году по данным IDC, общий мировой объём капиталовложений в направления, связанные с интернетом вещей, в 2016 году составил $737 млрд.

На данный момент согласно прогнозам GSMA, к 2025 году количество подключений к IoT удвоится и достигнет почти 25 млрд во всем мире, а по мере увеличения популярности IoT возрастает риск кибератак. Кибербезопасность IoT вызывает беспокойство у 95% респондентов опроса, проведенного аналитиками IoT Analytics, причем почти 40% «очень обеспокоены» возможными уязвимостями интернета вещей. 88% указали, что поддерживают внедрение правил обеспечения безопасности IoT и принятие отраслевых стандартов для управления передовыми методами кибербезопасности. Предполагается, что рынок безопасности IoT вырастет до $36,6 млрд к 2025 году по сравнению с $12,5 млрд в 2020 году.

Специалисты признают, что причина возникновения проблем безопасности интернета вещей заключается вовсе не в недостаточной квалификации разработчиков, а в погоне за прибылью. Для компаний важно ускорить выпуск нового устройства на рынок. Некоторые производители предпочитают пожертвовать защищенностью, ради получения преимущества перед конкурентами (рис. 1).

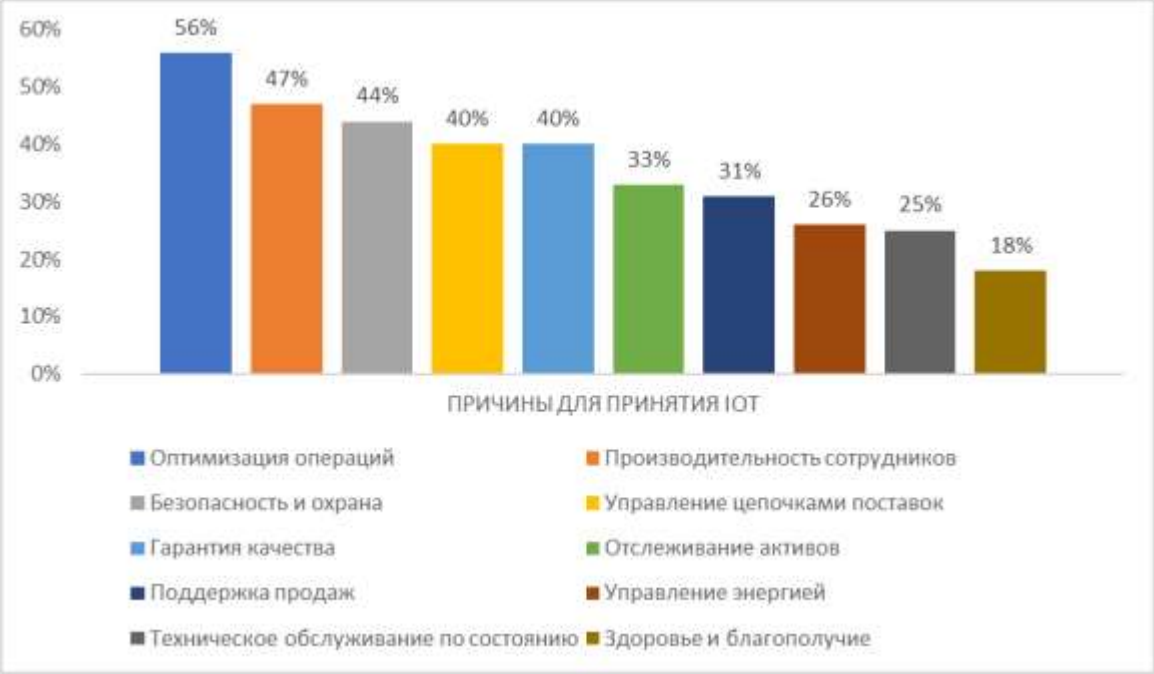


*Рис. 1. Причины принятия IoT*

Многие компании и сегодня выпускают умные гаджеты, не вкладывая большие ресурсы денег и времени в тестирование кодов, доработку систем безопасности. По этой причине рынок растет очень быстро, технологии развиваются, но страдают пользователи.

Заставить производителей пересмотреть свое отношение к безопасности изготавливаемых «умных» гаджетов может введение сертификации. Это не революционная идея, однако в перспективе она дает возможность уменьшить масштабы проблемы.

В идеале сертификация должна быть достаточно простой и быстрой для производителя, чтобы не стать преградой на пути прогресса, но в то же время она должна обеспечивать пользователям хорошую защиту от любых возможных атак.

Однако сертификация не может гарантировать защищенность на сто процентов, это лишь один из уровней защиты. И наличие такого документа все же оставляет вероятность получения злоумышленниками доступа к устройству.

То, что делает IoT-устройство удобным для использования, — возможность удаленного и централизованного управления из любой точки мира — является и самой большой угрозой безопасности.

Как отмечается в отчете за 2020 г. «Unit 42 IoT Threat Report» компании Palo Alto Networks, 98% трафика IoT-устройств не шифруется и передается в открытом виде через интернет.

Один из самых распространенных протоколов Интернета вещей — MQTT. Он поддерживает аутентификацию пользователей и шифрование, однако по умолчанию эти опции в IoT-устройствах не задействуются.

Протокол MQTT на базе TCP/IP (без опции шифрования) работает с 1883-м портом. Поисковая система Shodan находит свыше 300 тыс. устройств, которые передают данные в глобальную сеть без шифрования. Это в 10 тыс. раз больше, чем количество найденных устройств, использующих его (порт для работы с MQTT через TLS 8883.

Установка патчей безопасности на устройства Интернета вещей может вызвать много сложностей. Мало того, что обновление работающего оборудования — дело рискованное, так еще и многие производители вообще не выпускают обновления ПО [2].

Только 17% умных устройств работают на поддерживаемых операционных системах. Остальные 83% используют старые версии ОС Linux, Unix, Embedded, Windows 7 и даже Windows XP.

Исследователи Мичиганского университета и Федерального университета Пернамбуко проанализировали 37 самых популярных приложений для устройств Интернета вещей и обнаружили, что:

- у 31% приложений отсутствует шифрование;
- у 19% приложений ключи шифрования жестко закодированы и не могут быть изменены пользователем;
- 50% всех приложений потенциально уязвимы для эксплойтов;

- Многие приложения контролируют устройства через локальную сеть или широковещательные сообщения, например, по UDP.

Безопасность Интернета вещей стала одной из первых сфер использования блокчейн-технологии. Благодаря технологии распределенного реестра появилась возможность обеспечивать высокий уровень безопасности IoT-устройств в сети и устранить существующие ограничения и риски для IoT, связанные с централизацией.

Она позволяет быстро и безопасно сохранять протоколы обмена и результаты взаимодействия различных IoT-устройств в децентрализованной системе. Именно распределенная архитектура блокчейна гарантирует достаточно высокую безопасность всей IoT-системы. Но если часть из устройств сети все же будет подвержена взлому, в целом, это не скажется на общей работе системы. Упомянутое использование ботнетами «умных» устройств, работающих в IoT-системах, стало возможным вследствие их слабой защищенности. Распределенный тип доверительных отношений позволяет избавиться от взломанного устройства без ощутимого ущерба для всей модели взаимодействия между «здоровыми» объектами.

В контексте безопасности сегодня блокчейн может использоваться в ряде сфер, в которых Интернет вещей развивается наиболее интенсивно. Например, это управление аутентификацией, проверка работоспособности разных сервисов, обеспечение неделимости информации и другие. В начале года ряд ведущих компаний, среди которых Cisco, BNY Mellon, Bosch, Foxconn и ряд других образовали консорциум, который будет находить решения по использованию блокчейна для увеличения безопасности и улучшения взаимодействия IoT-продуктов. Главная задача, которую поставили перед собой его члены — разработка на основе блокчейн-технологии распределенной базы данных и протокола обмена информацией между IoT-устройствами.

**Слабые места:**

- Переход на IPv6;
- Питание датчиков;
- Стандартизация архитектуры и протоколов, сертификация устройств;
- Информационная безопасность;
- Стандартные учётные записи от производителя, слабая аутентификация;
- Отсутствие поддержки со стороны производителе для устранения уязвимостей;
- Трудно или невозможно обновить ПО и ОС;
- Использование текстовых протоколов и ненужных открытых портов;
- Используя слабость одного гаджета, хакеру легко попасть во всю сеть;
- Использование незащищённых мобильных технологий;
- Использование незащищённой облачной инфраструктуры;
- Использование небезопасного ПО.

**Интернет вещей состоит из нескольких уровней:**

- Smart-приборы – конечные IoT-устройства (датчики, сенсоры, контроллеры и пр.), которые собирают малые данные с технологического оборудования или бытовой техники и передают их в сеть;
- Каналы передачи данных – проводные и беспроводные сетевые протоколы (Serial, RS-485, MODBUS, CAN bus, OPC UA, BLE, WiFi, Bluetooth, 6LoRaWAN, Sigfox и пр.) для отправки информации с конечных IoT-устройств на промежуточные шлюзы и в облака;
- Сетевые шлюзы и хабы – роутеры, объединяющие и подключающие конечные устройства к облачной IoT-платформе;
- Облачная Big Data система (IoT-платформа) – удаленный сервер или кластер в датацентре, на котором развернуто ПО для приема, обработки, хранения и анализа информации.

Для защиты каналов передачи данных и программных приложений, в т.ч. Big Data, от утечек информации применяются современные криптографические методы:

- Симметричные (DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 и др.) и асимметричные (RSA и Elgamal) алгоритмы;
- Электронная подпись (ЭЦП);
- Хеш-функции (MD4, MD5, MD6, SHA-1, SHA-2, ГОСТ Р 34.11-2012);
- Управление ключами;

Несмотря на то, что во многие IoT-устройства встроены энергоэффективные микрочипы криптографической защиты, они не защитят от взлома или утечки данных, если пользователь smart-прибора не применяет их по назначению или злоумышленник проявляет особую настойчивость [3]. Например, закрытые ключи можно считать из памяти IoT-устройства, вычислить по динамическому изменению тока питания или даже по электромагнитному излучению.

Усилить безопасность smart-приборов поможет установка дополнительной защитной электроники – миниатюрных компонентов, которые соединяют периферийные устройства с принимающими

микроконтроллерами или микропроцессорами, и отвечают за персонализированные сертификаты, безопасное размещение закрытых ключей и управление криптографическими элементами.

Аналогичным образом можно защитить шлюз, который собирает малые данные от smart-устройств и передает их в облачную IoT-платформу. Для этого к главному процессору IoT-шлюза устанавливается дополнительный микрочип, который обеспечивает бесперебойное TLS-соединение с сервером и выполняет задачу обеспечения шлюза ресурсами по протоколам HTTPS или MQTTS.

Отметим, что эти прикладные протоколы семейства TCP/IP также широко используются в программной части IoT-систем, на стороне облачной Big Data платформы для отправки/приема запросов и управления очередями сообщений в брокерах RabbitMQ, Apache Qpid, Apache ActiveMQ и Apache Kafka.

Зачастую производители микроконтроллеров для IoT-устройств встраивают в них специализированное оборудование для реализации криптографических алгоритмов. Например, крупный производитель микрочипов Texas Instruments включает в свои микросхемы ускоритель алгоритма AES, который реализует процессы шифрования и дешифрования. Аналогичные аппаратные ускорители применяются для других распространенных криптографических функций, в частности, для MAC-алгоритма аутентификации, используемого для проверки достоверности.

Наиболее распространенным MAC-алгоритмом является функция SHA (Secure Hash Function), утвержденная Национальным институтом стандартов и технологий США. Для ее выполнения в микроконтроллерах IoT-устройств предусмотрены свои ускорители. Например, микроконтроллеры Kinetis от компании Freescale имеют сопроцессор для ускорения AES и SHA, который может работать автономно от центрального процессора и использовать выделенную память, чтобы команды и данные могли быть буферизованы для устройства криптографического ускорения.

IoT-электроника компании Atmel обеспечивает безопасность с помощью устройства защиты памяти. Оно использует симметричную аутентификацию, шифрование данных и MAC-функции, чтобы обеспечить безопасное хранение информации через стандартный последовательный интерфейс микроконтроллера. Благодаря дополнительным схемам определения несанкционированного доступа информация защищена от атак внешних устройств.

Компания Maxim Integrated производит серию микросхем с аппаратной реализацией стандарта SHA-256 для безопасной передачи данных с помощью обычного однопроводного интерфейса. Распознавание ведущего IoT-устройства ведомым защищает память от изменений, которые может внести неидентифицированный прибор. Это обеспечивает высокую надежность, что актуально в IoT-устройствах, когда аутентификация прибора определенного производителя предотвращает использование поддельной техники.

Среди основных целей внедрения респонденты выделили необходимость оптимизации рабочих процессов (56%), повышения продуктивности сотрудников (47%), а также общую безопасность компании (44%). Респонденты прогнозируют, что искусственный интеллект, современные вычислительные технологии, 5G, цифровые двойники и блокчейн ускорят распространение Интернета вещей. (2019 год). 19 мая 2020 года аналитическая компания Counterpoint Research назвала ведущие платформы для интернета вещей (IoT) по степени завершенности (возможности от начала до конца удовлетворять нуждам клиентов) и ряду других параметров (рис. 2). Наиболее завершенной платформой, по оценке аналитиков, является Microsoft Azure, следом за ней — Amazon Web Services (AWS). На третьем месте — Huawei OceanConnect, на четвертом — PTC ThingWorx. Замыкает пятерку IBM Watson.

Платформа Google Cloud заняла шестое место, а места с 7 по 10 — Cisco Kinetic, Software AG Cumulocity, Baidu AIoT и Alibaba Cloud.

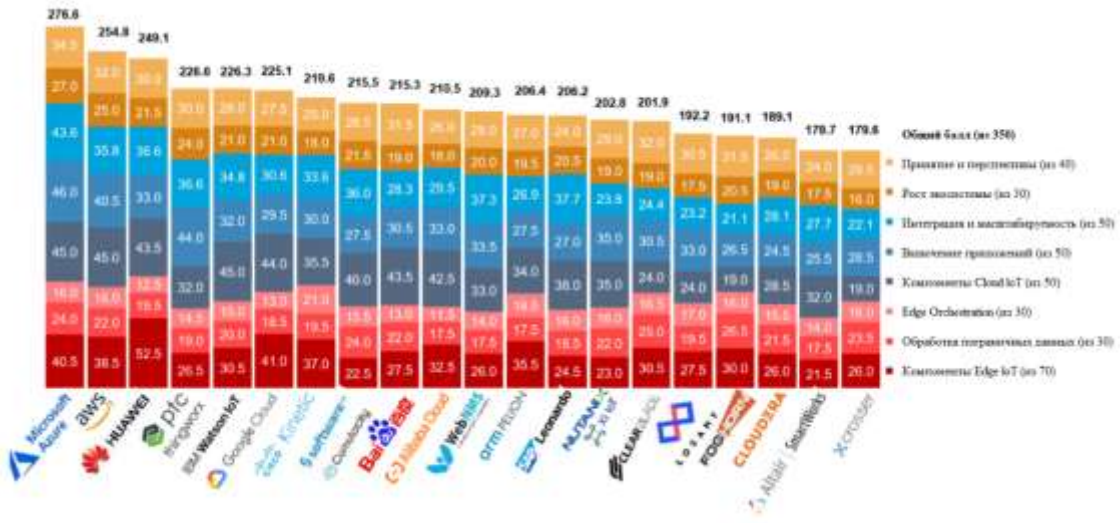


*Рис. 2. Платформы для IoT*

В своей итоговой оценке Counterpoint учитывала 8 слагаемых: распространение и перспективы, темпы роста, способности к интеграции и масштабированию, поддержка приложений, облачные компоненты, периферийная оркестрация, периферийная обработка данных и периферийные компоненты [4].

Каждое из слагаемых имело определенный вес. Например, темпы роста и периферийная оркестрация по отдельности могли прибавить не более 30 баллов к общему рейтингу, а периферийные компоненты — 70 баллов. Общий балл Microsoft Azure составил 276,6 из 350, AWS — 254,8, Huawei OceanConnect — 249,1, PTC ThingWorx — 226,6 и IBM Watson — 226,3.

В корпоративном сегменте к 2030 году 34% устройств будут приходиться на «кросс-вертикальные» варианты использования, такие как в качестве общего отслеживания, офисного оборудования и транспортных средств, 31% коммунальных предприятий, наиболее заметно умных счетчиков, 5% транспорта и логистики, 4% правительства, 4% сельского хозяйства и по 3% финансовых услуг и розничной торговли (оптовая) (рис. 3). Самым распространенным вариантом использования являются бытовые устройства Интернета и мультимедиа, на которые в 2030 году будет приходиться 1/3 всех устройств. Следующим по величине является Smart Grid, включая интеллектуальные счетчики, составляющие 14% подключений. Подключенные автомобили являются третьей по величине категорией, составляющей 7% от мировой установленной базы.

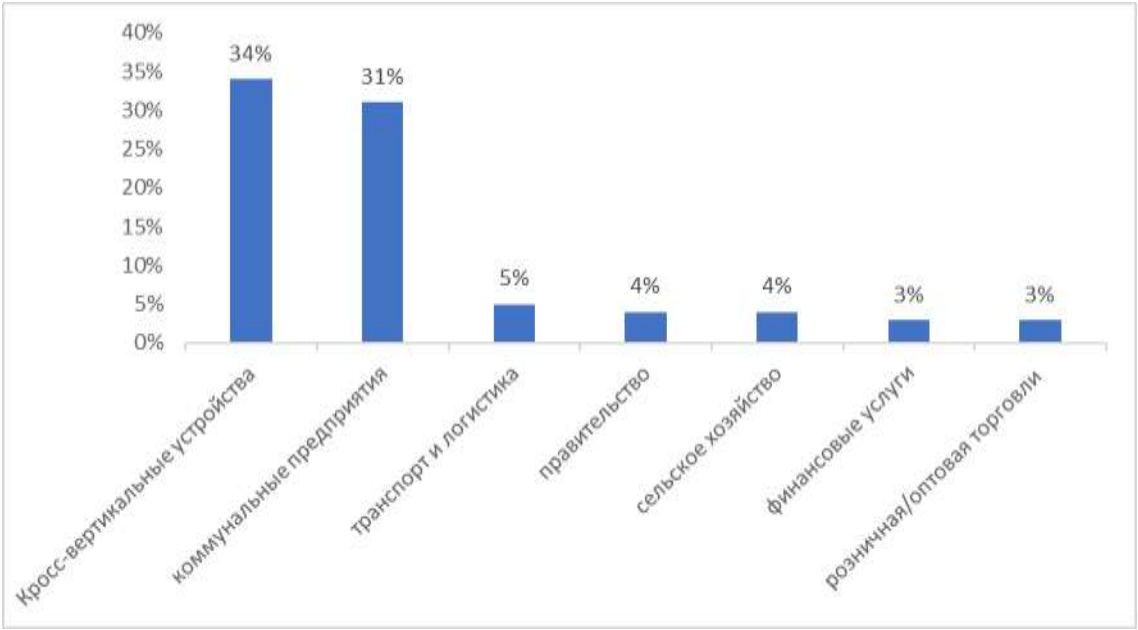


*Рис. 3. Корпоративный сегмент IoT*

Подведя итог можно сказать, что на данный момент рынок интернета вещей находится на подъеме своего развития и в будущем скорее всего произойдет еще множество изменений от модификации самих устройств до усложнения и улучшения системы их безопасности при подключении к сети интернет. На данный момент ответ на вопрос «находятся ли данные интернета вещей в безопасности?» практически однозначен – нет, так как любой более-менее разбирающийся в логике работы данных устройств человек, и понимающий принцип используемого ими программного обеспечения может получить доступ к передаваемой ими информации. Но пока люди не столкнулись с реальными проблемами незащищенного обмена данными устройств интернета вещей, создатели этих устройств не будут прилагать достаточно усилий для совершенствования безопасности своих творений.

**Список литературы**

1. Юдина М.А. Интернет вещей: проблемы социальной экспертизы // Коммуникология. Том 5.№2.С.50-67 DOI 10.21453/2311-3065-2017-5-2-50-67 [Электронный ресурс]. – Режим доступа: URL: https://cyberleninka.ru/article/n/internet-veschey-problemy-sotsialnoy-ekspertizy

2. Евдокимов И.В., Алалван А.Р.Д., Тимофеев Н.А., Нехоношин С.Р. Интернет вещей в контексте экономики программной инженерии и управления стоимостью проекта // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) [Электронный ресурс]. – Режим доступа: URL: https://naukovedenie.ru/PDF/56TVN617.pdf (25.04.2021)

3. Пушкарев М.С. Интернет вещей (IoT): понятие и значение для формирования правовой основы цифровой трансформации экономики [Электронный ресурс]. – Режим доступа: URL: http://publishing-vak.ru/file/archive-law-2018-1/2-pushkarev.pdf (18.04.2021)

4. Дежина И., Нафикова Т. Интернет вещей: концепции и государственная политика. Мировая экономика и международные отношения, 2019, т. 63, № 7, сс. 23-31. [Электронный ресурс]. – Режим доступа: URL: https://doi.org/10.20542/0131-2227-2019-63-7-23-31 (14.05.2021)