УДК 004.056

Накиев Р.Р.
студент магистратуры 1-го курса
Российский экономический университет имени Г. В. Плеханова
(г. Москва, Россия)

Ульянов В.В.
студент магистратуры 1-го курса
Российский экономический университет имени Г. В. Плеханова
(г. Москва, Россия)

АНАЛИЗ УЯЗВИМОСТЕЙ ИНТЕРНЕТ ВЕЩЕЙ (IOT) И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Аннотация: *Интернет вещей (IoT) изменил цифровой ландшафт, подключив различные устройства и позволив им общаться и обмениваться данными. Однако эта взаимосвязанная сеть устройств вызвала серьезные опасения по поводу безопасности и конфиденциальности. Эта статья направлена на изучение проблем безопасности, связанных с IoT, и предложения возможных решений для снижения этих рисков. Анализируя существующую литературу и исследования, в этом документе определяются общие проблемы безопасности IoT и обсуждаются различные стратегии повышения безопасности IoT. Полученные данные подчеркивают важность решения проблем безопасности IoT для обеспечения безопасного и устойчивого развития этой быстро развивающейся технологии.*

Ключевые слова: *Информационная безопасность, Интернет вещей, IoT, цифровизация, информационные технологии, автоматизация, безопасность Интернет вещей (IoT), угрозы Интернет вещей (IoT)*

ВВЕДЕНИЕ

Глобальная цифровизация ускорилась благодаря появлению новых информационных технологий и меняющимся потребительским предпочтениям.

Пандемия COVID-19 еще больше подтолкнула к цифровой трансформации, поскольку организации были вынуждены перейти на удаленную работу. Этот сдвиг превратил цифровую трансформацию из отдаленной цели в непосредственную реальность. В 2024 году компании, пренебрегающие внедрением новых цифровых решений, столкнутся со снижением своей конкурентоспособности и финансовых показателей. Среди заметных технологических тенденций, определяющих эту трансформацию — использование Интернета вещей, также известного как IoT.

В настоящее время в мире насчитывается более миллиарда подключенных устройств, и это число продолжает ежегодно расти. По прогнозам, к 2025 году будет использоваться более 75 миллиардов устройств, подключенных к Интернету вещей (IoT) [1]. Развитие IoT открыло новую эру подключения, изменяя то, как мы живем, работаем и взаимодействуем с окружающим миром.

Интернет вещей представляет собой идею связанных в сеть физических предметов, которые соединяются и взаимодействуют друг с другом и другими службами через Интернет или другую сеть, и имеют датчики, программное обеспечение и средства коммуникации для сбора и обмена данными. Эта технология нашла применение в жилых домах, промышленности, системах здравоохранения, на транспорте и даже в городах, коренным образом изменив то, как мы справляемся с повседневными задачами и оптимизируем процессы. Однако эта взаимосвязанная сеть интеллектуальных устройств также представляет собой серьезную проблему — необходимость защитить эту обширную сеть от потенциальных угроз.

В этой статье мы рассмотрим различные проблемы безопасности, связанные с распространением устройств IoT, а также приведем возможные способы защиты, которым следует руководствоваться разработчикам таких систем.

Основные уязвимости в IoT

Важной проблемой является то, что разработчики при проектировании новых IoT систем больше всего берут такие критерии как функциональность, простота использования, и самое главное низкая стоимость конечного продукта, чтобы в дальнейшем иметь больше выгоды с продажи своего устройства на ряду с большой конкуренции на рынке, где основной заказчик — это обычный пользователь. Этой проблемой пользуется злоумышленник для достижения своих целей, которые могут включать повреждение устройств или получение контроля над ними для выполнения своих вредоносных команд. Опасность есть везде от умных домов, уязвимых для несанкционированного доступа, до промышленных систем управления, подверженных манипуляциям, потенциальные последствия взлома могут быть далеко идущими.

Изучим многочисленные проблемы и их последствия для безопасности, связанные с быстрым распространением устройств IoT.

1. Уязвимости устройства и меры их безопасности.

Большое количество IoT устройств, подключенных к Интернету, которые в настоящее время представлены на рынке, по-прежнему не имеют даже самых элементарных средств кибербезопасности. Многие устройства IoT разработаны с ограниченными мерами безопасности, что делает их уязвимыми для кибератак. В этих устройствах часто отсутствуют протоколы шифрования, надлежащие механизмы аутентификации, и они получают нечастые обновления безопасности, что делает их уязвимыми для потенциальных угроз.

Примером можно привести историю со взломом взлом камер от компании Verkada [2]. Группа хакеров успешно проникла в базу данных Verkada Inc., получив несанкционированный доступ к прямой трансляции с примерно 150 000 камер наблюдения, установленных в различных местах, таких как больницы, компании, полицейские управления, тюрьмы и школы. Кроме того, злоумышленники смогли получить доступ к видеозаписям из женских консультаций, психиатрических больниц и офисов компании Verkada. Среди

компаний, которые стали жертвами утечки данных, были автопроизводитель Tesla Inc. и поставщик программного обеспечения Cloudflare Inc.

Это показывает, что в первую очередь большие компании по созданию IoT преследую идеи быстрого материального обогащения и забывают о современных методах защиты.

2. Вопрос конфиденциальности данных.

Устройства Интернета вещей собирают и отправляют большие объемы данных, которые могут включать личные и конфиденциальные данные. Хранение и обработка этих данных вызывает опасения относительно конфиденциальности и риска несанкционированного доступа. Если происходит утечка данных, это может привести к серьезным последствиям, таким как кража личных данных и ненадлежащее использование личной информации.

Часто при создании Интернет вещей производители не смотрят на основные правила защиты устройств и используют для всех устройств, которые выпускаются с конвейера, стандартный список паролей доступа. Их еще называют заводскими паролями.

Были случаи, когда производители все же обращали внимание на функции безопасности, но небрежно их использовали.

В пример можно привести уязвимость Pixie-Dust [3].

Или же есть пример, где киберпреступник выложил в открытый доступ списки учетных данных Telnet для более 515 тыс. серверов, домашних маршрутизаторов и IoT-устройств [4]. 20 января 2020 года стало известно, что списки, содержащие IP-адреса, логины и пароли для службы Telnet, были опубликованы на известном хакерском форуме, как сообщает ZDNet. Служба Telnet — это протокол удаленного доступа, позволяющий управлять устройствами через Интернет. Получив доступ к маршрутизатору пользователя, злоумышленник имеет возможность управлять трафиком и собирать интересующую его информацию. При использовании небезопасных протоколов

злоумышленник в данном случае выступает как “Человек посередине”, что может очень плохо сказаться на конфиденциальности данных.

3. Распределенные атаки типа «отказ в обслуживании» (DDoS) генерируемые Интернет вещами.

Устройства IoT можно легко скомпрометировать и использовать как часть ботнета для запуска DDoS-атак. Эти атаки перегружают целевые системы, нарушая работу служб и нанося значительный ущерб. При получении доступа через вышеперечисленную уязвимость злоумышленник может использовать данное устройство для своих целей. В основном использование вашего устройства в других деструктивных целях, часто это использование в сети ботнет для генерации DDOS трафика на цель, указанную злоумышленником.

Ботнет из IoT гораздо слабее если считать по мощности каждого устройства, но десяток устройств IoT легче захватить, чем реальный хост какой-нибудь компании [5]. Согласно многочисленным источникам, было замечено, что в первом квартале 2022 года объем мусорного трафика достиг своего пика, превысив 100 ГБ/с. Однако по сравнению с прошлогодними атаками, мощность которых превышала 1 ТБ/с, она не выглядит особенно примечательной.

4. Уязвимости цепочки поставок.

Сложная цепочка поставок, связанная с производством устройств IoT, может создавать уязвимости в системе безопасности. Так как системы разрабатывают и создают мелкие компании, у которых нет своего производства компонентов, потому что это достаточно трудоемкая задача, которые требует большого оборудования, сотрудников и определенных сертификатов безопасности, им приходится обращаться к сторонним производителям, и не всегда идеального качества.

Уязвимости возникают из-за ненадежных поставщиков или возможности вмешательства в производственный процесс, что позволяет использовать бэкдоры или другие уязвимости в системе безопасности, которые могут быть внедрены при производстве компонентов некомпетентным поставщиком.

Так же не стоит забывать и о программном обеспечении. Для разработки часто используются библиотеки, подготовленные сторонними разработчиками и энтузиастами.

В пример можно привести веб сервер Boa, который снят с производства еще в 2005 году, но до сих пор используется как ПО для доступа в камеры, коммутаторы и другие системы [6]. В данном случае это ПО использовалось так как оно включено в популярные SDK и используется как самый доступный инструмент.

Или другой пример, где компания по кибербезопасности Eclypsium обнаружила в прошивке Gigabyte бэкдор, который подвергает риску взлома 271 модель материнских плат [7,8]. Уязвимость связана с программой обновления, используемой Gigabyte для обновления прошивки материнской платы. После перезапуска системы фрагмент кода активирует программу обновления, которая подключается к Интернету для проверки и загрузки последней версии встроенного ПО. Проблема возникает из-за того, что средство обновления встроено в прошивку материнской платы, что затрудняет удаление пользователями.

Важно признать, что Gigabyte не единственный поставщик, использующий этот тип программного обеспечения для обновления прошивки, поскольку другие производители материнских плат, такие как Asus, с их программным обеспечением Armoury Crate, используют аналогичный подход.

Этот выявляет важную проблему. Большинство производителей аппаратного обеспечения не создаёт свои собственные прошивки, полагаясь вместо этого на своих партнёров в цепочке поставок

Возможные решения безопасности IoT

Перед тем как говорить о возможных решениях хотелось бы отметить, что некоторые государства участвуют в создании определенных правил и политик для защиты своих граждан. В пример можно привести Правительство

Великобритании, которое вместе с исследователями в 2018 году участвовала в выпуске правила и практики создания IoT устройств на государственном уровне [9].

Рассмотрим ряд возможных решений для решения проблем безопасности IoT. Эти решения направлены на повышение общей безопасности устройств, сетей и приложений Интернета вещей. Применяя эти меры можно снизить риски, связанные с IoT, и обеспечить более безопасную и защищенную среду для пользователей и организаций.

1. Использование безопасных компонентов при разработке устройств Интернета вещей.

Некоторые компоненты начинают устаревать и быть неактуальными. Поскольку количество устройств IoT, подключающихся к сетям, продолжает расти, становится необходимым иметь устройства, оснащенные встроенными функциями безопасности. Это влечет за собой гарантии того, что устройства имеют безопасную прошивку, надежные механизмы аутентификации и протоколы шифрования. Более того, существует необходимость реализации упреждающих и защитных механизмов безопасности в режиме реального времени. Эти механизмы предназначены для быстрого отключения или принудительного отключения любых скомпрометированных устройств IoT при обнаружении угрозы безопасности. Это гарантирует, что злоумышленники не смогут дистанционно управлять взломанными устройствами IoT или манипулировать ими.

Всем пользователям стоит иметь ввиду что можно столкнуться с такой проблемой как End Of Life (EOL) устройство. Данные устройства больше не получают никаких обновлений безопасности от разработчиков, а значит потенциально могут иметь уязвимости [10].

Разработчики при производстве продукта изначально закладывают определенное время поддержки устройства и пытаются исправлять любые проблемы, которые могут возникнуть в программном обеспечении, но бывают

случаи, когда устройство невозможно починить при помощи патчей системы. При возникновении таких случаев компании просят пользователей вернуть некачественное устройство взамен нового или полного возмещения средств, но бывают и случаи, когда компании преждевременно выводят устройство в EOL [11].

Следует внимательно относится к каждому поставщику и понимать, что старое ПО уже может быть неактуальным и искать ответственных подрядчиков для разработки безопасного ПО.

2. Защита каналов связи.

Чтобы обеспечить безопасность данных во время передачи, крайне важно установить безопасные протоколы связи и использовать методы шифрования в устройствах IoT, использующих беспроводные каналы связи. Кроме того, рекомендуется использовать безопасные и зашифрованные каналы при загрузке обновлений. Перед загрузкой обновлений в сеть IoT-устройств важно проверить их целостность. Предприятия также могут решать проблемы безопасности IoT, избегая небезопасных конфигураций операционной системы устройства.

При отсутствии проверок сертификатов или подписей новых обновлений злоумышленник может заставить устройства обновиться на вредоносную прошивку с бэкдором или полным доступ через C2C сервер. Чтобы исключить это, как не странно, требуется использовать подписи, шифрованные каналы получения обновление и другие технологии которые исключают модифицирования трафика или установку не официального ПО на устройство. Часто злоумышленник получив физический доступ до устройства на короткое время, может внедрить вредоносный код в устройство через SPIO или другие порты устройства.

Бывают случаи, когда IOT имеют на борту незащищенные протоколы чтобы пользователи без проблем могли сразу пользоваться устройством сразу доступны и для управления злоумышленником.

Для исключения этого требуется полная валидация между устройством и владельцем для создания качественного защищенного соединения. Требуется исключения возможностей “Быстрого” подключения на лету и делать ставку на лучшую безопасность [12].

3. Создание безопасных сетей IoT.

Сети IoT требуют надежных мер безопасности для защиты от несанкционированного доступа и утечки данных. Внедрение сегментации сети, контроля доступа и систем обнаружения вторжений может повысить безопасность сети.

Требуется с осторожностью относиться как к выбору беспроводных протоколов для общения между собой [13], так и к качественной сегментации в сети для исключения влияния извне.

4. Внедрение стандартов безопасности IoT.

Разработка и внедрение отраслевых стандартов безопасности для устройств IoT может помочь обеспечить согласованность функций безопасности на разных устройствах. Это может способствовать функциональной совместимости и обеспечить основу для требований безопасности. Как говорилось ранее некоторые правительства давно взялись за определенные стандарты в разработке IoT.

Некоторые исследовательские компании выпускают свои инструкции для безопасной разработки устройств, что хорошо сказывается на общей тенденции медленного перевеса взглядов из простоты использования в надежную безопасную систему [14].

Говоря про стандарты можно привлечь также использования стандартов ГОСТ в той или иной функции. Например, использование каналов связи с использованием шифрования данных по «Магма», ГОСТ Р 34. 12-2015 [15].

5. Мониторинг и обнаружение угроз.

Развертывание систем мониторинга и обнаружения угроз в режиме реального времени имеет решающее значение для обнаружения и смягчения угроз безопасности в сетях IoT. Это может включать использование алгоритмов машинного обучения для обнаружения аномалий и выявления потенциальных атак. Кроме того, важно установить надежные протоколы обслуживания для устранения выявленных уязвимостей безопасности IoT. Это включает в себя внедрение передовых систем предотвращения вторжений и межсетевых экранов нового поколения, которые обеспечивают безопасное и проверенное резервное копирование данных. Также важно иметь альтернативные устройства для удовлетворения необходимых вычислительных требований.

Постоянный мониторинг сети и мониторинг интернет ресурсов на предмет вовлеченности в исследования новых уязвимостей может помочь превентивно исправить возможные недочеты ПО или переработать связность устройств для повышения безопасности. Сбор метрик устройств тоже важная часть мониторинга. Нужно быть уверенным что ваше по имеет возможность передавать информацию о состоянии устройства по требования авторизированных лиц [16].

Если в устройство заранее внедрить средство реагирования на аномалии использования с оповещением владельца, это в разы уменьшит инциденты нарушения безопасности.

6. Обучение пользователей и разработчиков.

Содействие обучению и обучению передовым методам обеспечения безопасности IoT может сыграть важную роль в повышении осведомленности и укреплении общих мер безопасности. Это включает в себя информирование пользователей о важности использования надежных паролей, регулярном обновлении программного обеспечения и отказе от использования небезопасных устройств IoT.

Кроме того, крайне важно назначить специальную подготовку по безопасности для отдельных сотрудников или категорий сотрудников, вооружив их необходимыми знаниями и навыками для эффективного противодействия различным типам атак, с которыми они могут столкнуться в своих областях.

Так как говоря о IoT системах мы не задумываемся что это могут быть все устройства, имеющие доступ в сеть от серверов до автомобилей, стоит помнить, что для безопасности каждого устройства нужно иметь свой подход. Повышая общий уровень осведомленности персонала ответственного за создания IoT уменьшает риски ИБ. Для повышения осведомленности требуется постоянное следование за прогрессом и изучения не только новых протоколов, но и методов атак как на инфраструктуру, так и на каждое отдельное устройство. Участие в постоянных конференция по информационной безопасности достаточно хорошо справляется с этим [17, 18].

7. Сотрудничество с заинтересованными сторонами в улучшении общей безопасности использования IoT.

Установление партнерских отношений и сотрудничества между производителями устройств IoT, сетевыми поставщиками и экспертами по безопасности может помочь коллективно решать проблемы безопасности. Это может включать в себя обмен информацией об угрозах, проведение аудитов безопасности и распространение передового опыта в области безопасности.

Связи с исследовательскими компаниями, которые смогут протестировать устройство или целый программный комплекс на соответствие передовой безопасности хорошо улучшат репутацию на рынке как производителя безопасного продукта.

Эти возможности подчеркивают необходимость постоянных инноваций и сотрудничества для решения постоянно меняющихся проблем безопасности в экосистеме IoT.

Заключение

В заключение следует отметить, что Интернет вещей (IoT) создает как серьезные проблемы безопасности, так и многочисленные возможности для развития и инноваций. Поскольку все больше устройств становятся взаимосвязанными и интегрируются в нашу повседневную жизнь, крайне важно устранять уязвимости и риски, связанные с системами IoT. От защиты данных и конфиденциальности до защиты от кибератак. Потребность в надежных и комплексных мерах безопасности имеет первостепенное значение.

Однако эти проблемы также открывают возможности для отраслей, правительств и частных лиц для сотрудничества и улучшения методов обеспечения безопасности IoT. Внедряя надежные протоколы аутентификации, методы шифрования и непрерывный мониторинг, мы можем защитить сети IoT от потенциальных угроз. Кроме того, передовые технологии, такие как искусственный интеллект и блокчейн, предлагают многообещающие решения для повышения безопасности IoT.

Крайне важно, чтобы все заинтересованные стороны применяли упреждающий подход к пониманию и снижению этих рисков, обеспечивая безопасную и надежную реализацию потенциала Интернета вещей. Решая эти проблемы напрямую, мы можем создать экосистему IoT, которая способствует инновациям, повышает эффективность и уважает конфиденциальность и безопасность.

СПИСОК ЛИТЕРАТУРЫ:

1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 // Statista [Электронный ресурс]. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (дата обращения: 29.06.2023).
2. Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals // Bloomberg [Электронный ресурс]. URL:

https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams (дата обращения: 01.07.2023).

3. WPS Pixie Dust Attack (Offline WPS Attack) // KALI [Электронный ресурс]. URL: https://forums.kali.org/showthread.php?24286-WPS-Pixie-Dust-Attack-(Offline-WPS-Attack) (дата обращения: 01.07.2023).

4. Telnet // TADVISER [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Telnet (дата обращения: 02.07.2023).

5. Статистика DDoS-атак и BGP-инцидентов в 2022 году // IT World [Электронный ресурс]. URL: https://www.it-world.ru/news-company/releases/190619.html (дата обращения: 02.07.2023).

6. Vulnerable SDK components lead to supply chain risks in IoT and OT environments // Microsoft [Электронный ресурс]. URL: https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/ (дата обращения: 04.07.2023).

7. VULNERABLE FIRMWARE IN THE SUPPLY CHAIN OF ENTERPRISE SERVERS // Eclypsium [Электронный ресурс]. URL: https://eclypsium.com/wp-content/uploads/Vulnerable-Firmware-in-the-Supply-Chain.pdf. (дата обращения: 21.07.2023).

8. SUPPLY CHAIN RISK FROM GIGABYTE APP CENTER BACKDOOR // Eclypsium [Электронный ресурс]. URL: https://eclypsium.com/blog/supply-chain-risk-from-gigabyte-app-center-backdoor/ (дата обращения: 07.07.2023).

9. Code of Practice for Consumer IoT Security // GOV.UK [Электронный ресурс]. URL: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security (дата обращения: 09.07.2023).

10. End-of-Sale and End-of-Life Products // CISCO [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/products/eos-eol-listing.html (дата обращения: 10.07.2023).

11. Hyundai готовит отзыв Kona из-за ошибки в тормозной системе // Auto.Today [Электронный ресурс]. URL: https://auto.today/news/18225-hyundai-gotovit-otzyv-kona-iz-za-oshibki-v-tormoznoy-sisteme.html (дата обращения: 15.07.2023).

12. The Fresh Smell of ransomed coffee // DECODED [Электронный ресурс]. URL: https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/ (дата обращения: 19.07.2023).

13. Абраров Р.Р., Бурлаков М.Е. Уязвимости протокола маршрутизации в MESH-сети стандарта 802.11S // Вестник ПНИПУ. - 2017. - №23. - С. 66.

14. ГОСТ "ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Информационные технологии. ИНТЕРНЕТ ВЕЩЕЙ. Совместимость систем интернета вещей. Часть 2. Совместимость на транспортном уровне" от 18.08.2020 № ИСО/МЭК 21823-2:2020 // РОССТАНДАРТ. - 2020 г. - Ст. 1.

15. ГОСТ "Информационная технология КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Блочные шифры" от 19.06.2015 № ГОСТ Р 34.12─ 2015 // НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. - 2015 г. - Ст. 1.

16. Баев Д.А., Волков Р.О., Зонов А.Д. Мониторинг безопасности в IOT-сетях // StudNet. - 2021. - №6. - С. 1122.

17. Гатиятуллин Т.Р., Сухова А.Р. К вопросам обучения основам информационной безопасности сотрудников предприятия // Символ науки. - 2015. - №12. - С. 129.

18. Халявин Н.И., Иванчук М.А., Джураева Д.Х. Программа повышения осведомленности сотрудников в вопросах информационной безопасности // Сборник материалов X Международной научно-практической конференции. - 2022. - С. 247.

Nakiev R.R.
Plekhanov Russian University of Economics
(Moscow, Russia)

Ulyanov V.V.
Plekhanov Russian University of Economics
(Moscow, Russia)

INTERNET OF THINGS (IOT) VULNERABILITY ANALYSIS AND HOW TO PREVENT THEM

Abstract: *the Internet of Things (IoT) has changed the digital landscape by connecting various devices and allowing them to communicate and share data. However, this interconnected network of devices has raised serious security and privacy concerns. This article aims to explore the security issues associated with the IoT and suggest possible solutions to mitigate those risks. By reviewing existing literature and research, this paper identifies common IoT security issues and discusses various strategies for improving IoT security. The findings highlight the importance of addressing IoT security issues to ensure the safe and sustainable development of this rapidly evolving technology.*

Keywords: *information security, Internet of things, IoT, digitalization, information technology, automation, Internet of things (IoT) security, Internet of things (IoT) threats.*