DOI 10.36622/VSTU.2023.26.2.001
УДК 004.056

БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ: ОСНОВНЫЕ РЕШЕНИЯ

В.А. Минаев, Б.А. Швырев, Т.Р. Ромашкин

Одной из основных проблем при обеспечении безопасности Интернета вещей (IoT) является, с одной стороны, огромное количество устройств, масштабирующее угрозы и риски безопасности их использования, а с другой – слабая разработанность или даже отсутствие стандартизированных протоколов безопасности. Нередко устройства IoT имеют ограниченную вычислительную мощность и память в угоду цене и коммерческой выгоде, что затрудняет реализацию надежных мер безопасности. Расширение IoT достигло критической инфраструктуры - системы здравоохранения, транспорта и других особо важных отраслей. Поскольку современные устройства IoT имеют доступ к персональной и конфиденциальной информации, нарушения их информационной безопасности могут иметь весьма серьезные последствия, поэтому крайне важно обосновать и реализовать надежные меры безопасности для их защиты от компьютерных атак. Проводится сравнительный анализ основных сетевых протоколов IoT. Выделяются наиболее вероятные компьютерные атаки на устройства IoT: нарушение безопасности сети, нарушение безопасности устройства, физический доступ к устройству, сбои в работе устройства, технологии социальной инженерии. Рассматриваются следующие меры для обеспечения безопасности устройств IoT: совершенствование нормативно-правовой базы; обучение и повышение квалификации сотрудников; развитие взаимодействия с производителями IoT; улучшение мониторинга IoT-устройств; улучшение методов анализа данных, связанных с функционированием IoT. Для реализации предложенных мер приводятся программные и аппаратные решения задач безопасности IoT-устройств.

Ключевые слова: Интернет вещей, угрозы информационной безопасности, протокол безопасности.

Введение

Интернет вещей (Internet of Things, IoT) – это сеть физических объектов, оборудованных датчиками, программным обеспечением и другими технологиями, которые позволяют им взаимодействовать и обмениваться данными между собой и с внешним миром [1].

Однако с распространением устройств IoT возникает и растет риск нарушений безопасности, которые могут иметь самые серьезные последствия [2]. Так, развитие IoT привело к возникновению ряда проблем, связанных с безопасностью данных и защитой личной информации.

Поскольку устройства IoT предназначены для подключения к Интернету, они уязвимы для тех же угроз безопасности, что и традиционные вычислительные устройства, таких как вредоносное ПО, фишинговые атаки и атаки DDoS. Однако существуют и дополнительные проблемы, характерные для устройств IoT, которые делают их особенно уязвимыми для нарушений безопасности [3].

Одной из основных проблем, связанных с безопасностью IoT, является уязвимость самих устройств: умные дома, медицинские приборы и автомобили и др., которые, будучи подключенными к Интернету, подвержены кибератакам и взлому [4].

Еще одной проблемой является защита личных данных. Многие устройства IoT собирают, хранят и передают личную информацию – адреса электронной почты, пароли и номера кредитных карт и др. При этом далеко не все устройства обеспечивают достаточную защиту данных, приводя к утечке информации и нарушению конфиденциальности.

Третьей проблемой является отсутствие стандартов безопасности. Каждый производитель может использовать свои собственные протоколы и стандарты, что затрудняет совместимость устройств и защиту от угроз безопасности. Более того, целый ряд производителей не выпускают обновления для своих устройств, что делает их уязвимыми для новых угроз [5].

Четвертой проблемой является

недостаточная обученность пользователей [6]. Многие пользователи не понимают риски, связанные с использованием устройств IoT, и не принимают меры для защиты своих данных, не изменяют стандартные пароли, не обновляют устройства, что со временем делает их все более уязвимыми.

Нельзя не сказать о том, что безопасность IoT снижается с ростом количества используемых устройств [7]. По мере увеличения их числа расширяется поле для атак, облегчая хакерам поиск уязвимых устройств. При этом многие устройства IoT имеют ограниченную вычислительную мощность и память, что затрудняет реализацию надежных мер безопасности.

Возвращаясь к проблеме отсутствия стандартизированных протоколов безопасности для устройств IoT, напомним, что производители часто отдают предпочтение цене и удобству, а не безопасности, что приводит к тому, что устройства имеют слабые или отсутствующие меры безопасности. Отсутствие стандартизации также затрудняет пользователям понимание того, как эффективно защитить свои устройства [8].

Устройства IoT активно используются в критической инфраструктуре, такой как системы здравоохранения или транспорта [9, 10]. Очевидно, что нарушение безопасности в одной из такого рода систем может иметь катастрофические последствия, поэтому крайне важно реализовать надежные меры безопасности для их защиты от атак.

Протоколы Интернета вещей

Рассмотрим основные сетевые протоколы IoT:

• Wi-Fi – протокол, который используется на промышленных предприятиях, в жилых домах, коммерческих зданиях и даже в ресторанах по соседству. Эта широко распространенная технология способна передавать большие объемы данных на разумные расстояния. Однако многие устройства IoT с низким энергопотреблением или питанием от батареи вряд ли будут использовать Wi-Fi из-за его высоких энергетических затрат.

• LTE CAT 1 – это стандарт связи, специально разработанный для обслуживания приложений IoT. По сравнению с другими стандартами он сокращает пропускную способность и требования к связи для снижения затрат крупномасштабными системами IoT с большим радиусом действия [4].

• LTE CAT M1 – также называемый представляет собой недорогую, маломощную глобальную сеть, которая специализируется на передаче средних объемов данных. Он разработан в рамках 3-го поколения стандарта LTE и является основной технологией сотового Интернета вещей. Поскольку он совместим с преобладающей сетью LTE, крупным операторам, переходящим на него, не придется вкладывать средства в новые антенны [11].

• NB-IoT – это новая, быстроразвивающаяся технология с низким энергопотреблением, предназначенная для удовлетворения потребностей устройств IoT с батарейным питанием [12].

• Bluetooth – фокусируется на двухточечной передаче на короткие расстояния относительно небольшого объема данных. Обычно используется для подключения небольших датчиков с батарейным питанием, облегчения связи со смартфонами, eBike и другими интеллектуальными устройствами.

• ZigBee – недорогая, маломощная и надежная технология беспроводной сети. Стандарт поддерживает несколько сетевых топологий, включая многоточечные ячеистые сети. Чаще всего используется в настройках систем автоматизации зданий.

• LoRaWAN – глобальная сеть дальнего действия представляет собой сетевой протокол с низким энергопотреблением. Обеспечивает беспроводное подключение нескольких устройств с батарейным питанием к Интернету в рамках региональных, национальных или глобальных сетей. В области Интернета вещей играет важную роль в комплексной безопасности и мобильных услугах [3].

Протоколы данных IoT:

• AMQP – открытый стандарт обмена сообщениями. Использует очереди данных,

позволяя подключенным системам взаимодействовать асинхронно и решать задачи, связанные со скачками трафика и плохим состоянием сети.

• MQTT – упрощенный протокол обмена сообщениями pub/sub, подходящий для подключения небольших устройств с низким энергопотреблением. Требует минимальной памяти и вычислительной мощности. Двунаправленная архитектура публикации/подписки делает протокол гибким и масштабируемым для самых разных вариантов использования и системных архитектур IoT. Безопасность обеспечивается на транспортном уровне, позволяя адаптироваться к плохим сетевым условиям и сокращать время соединения [4].

• HTTP – протокол передачи гипертекста устанавливает синхронное соединение между двумя устройствами для передачи данных, что создает ряд проблем для развертывания IoT, поскольку устройства и конечные точки могут быть не подключены к сети одновременно, а соединения могут быть ненадежными из-за сетевых условий. HTTP полагается на передачу данных в ASCII, что неэффективно для передачи небольших объемов данных, которыми часто обмениваются системы IoT, требуя большей вычислительной мощности для кодирования и декодирования сообщений на обоих концах [13].

• CoAP – протокол подходит для приложений IoT, уменьшая размер сетевых пакетов и, тем самым – перегрузку полосы пропускания сети. Другие преимущества включают улучшение экономию, а также уменьшение объема данных, необходимых для работы [14].

• DDS – промежуточная архитектура для систем реального времени, ориентированная на передачу данных между узлами на основе публикации или подписки. В основном используется в автономных транспортных средствах, производстве электроэнергии и робототехнике.

• LwM2M – предназначен для удаленного управления устройствами M2M. Снижает затраты, связанные с развертыванием модулей с низким энергопотреблением и оснащением устройств более быстрыми решениями IoT [15].

Обсуждение результатов

Один из подходов к решению проблем, связанных с обеспечением безопасности IoT, заключается во внедрении более надежных протоколов шифрования для защиты от несанкционированного доступа к устройствам IoT. Кроме того, производители могут использовать более строгие меры аутентификации, такие как биометрическая аутентификация, чтобы обеспечить доступ к устройствам только авторизованным пользователям.

Другое решение – стандартизировать протоколы безопасности для устройств IoT. Этого можно достичь за счет разработки отраслевых стандартов безопасности и программ сертификации, чтобы гарантировать соответствие устройств этим стандартам. Такие стандарты должны включать меры по защите от известных уязвимостей безопасности и требовать обновления устройств после ее усиления с помощью корректировок.

Кроме того, повышение осведомленности о рисках, связанных с устройствами IoT, может способствовать внедрению более эффективных методов обеспечения безопасности как среди производителей, так и среди пользователей. Этого можно достичь с помощью кампаний по информированию и обучению сотрудников кибербезопасности и правил, требующих от производителей раскрывать функции безопасности своих устройств.

Информация может быть похищена с устройств IoT, подключенных к сети Интернет через следующие наиболее вероятные компьютерные атаки:

1. *Нарушение безопасности сети.* Хакеры могут использовать уязвимости в сетевых протоколах, чтобы получить несанкционированный доступ к устройствам IoT и перехватить данные, передаваемые по сети.

2. *Нарушение безопасности устройства.* Устройства IoT могут быть скомпрометированы через уязвимости в операционных системах и прикладном программном обеспечении. Хакеры могут использовать такие уязвимости, чтобы взломать устройство и получить доступ к

хранимым данным.

3. *Физический доступ к устройству.* Если устройство IoT не защищено физически, злоумышленники могут получить доступ к нему и перехватить данные, хранимые на нем.

4. *Сбои в работе устройства.* Некоторые устройства IoT могут быть скомпрометированы с использованием программных ошибок или аппаратных сбоев. Хакеры могут использовать такие ошибки и сбои, чтобы получить несанкционированный доступ к устройству и перехватить данные [16].

5. *Социальная инженерия.* Хакеры могут использовать технологию социальной инженерии, чтобы убедить пользователя устройства IoT раскрыть информацию, которая может быть применена для взлома устройства. Например, можно отправить фишинговое сообщение, которое выглядит как официальное от производителя устройства, и попросить пользователя ввести свои учетные данные.

В целом, безопасность Интернета вещей характеризуется своими уникальными вызовами, и необходима разработка специальных меры для ее обеспечения. Эти меры включают: усиление методов шифрования и аутентификации, использование надежных протоколов безопасности, разработку более безопасного программного обеспечения, а также обучение пользователей тому, как защитить устройства IoT от взлома и кражи данных [17].

Для обеспечения безопасности Интернета вещей (IoT) могут использоваться современные программные и аппаратные средства, которые позволяют защитить IoT-устройства и данные от угроз.

Программные средства обеспечения безопасности IoT:

1. *Антивирусные программы* используются для обнаружения и удаления вредоносных программ, установленных на IoT-устройствах.

2. *Файерволы* применяются для контроля и ограничения трафика на IoT-устройствах, что позволяет защитить их от атак.

3. *Системы обнаружения вторжений* используются для выявления аномальной активности на IoT-устройствах и предотвращения возможных атак.

4. *Шифрование данных* позволяет защитить информацию, передаваемую между IoT-устройствами, от несанкционированного доступа.

5. *Системы управления доступом* контролируют доступ к IoT-устройствам и ограничивают не регламентируемые возможности пользователей.

6. *Обновление программного обеспечения* может использоваться для устранения уязвимостей и улучшения безопасности IoT-устройств.

Аппаратные средства обеспечения безопасности IoT:

1. *Чипы безопасности* используются для защиты хранимых на IoT-устройствах данных от несанкционированного доступа.

2. *Модули шифрования* применяются для защиты данных, передаваемых между IoT-устройствами, от несанкционированного доступа.

3. *Физические замки* необходимы для защиты IoT-устройств от физического доступа.

4. *Контроллеры доступа* ограничивают доступ к IoT-устройствам и контролируют права пользователей.

5. *Датчики* используются для обнаружения взлома и различных типов атак на IoT-устройства [12].

6. *Устройства удаленного управления* позволяет защитить IoT-устройства от несанкционированного доступа на расстоянии [11].

Заключение

Интернет вещей характеризуется множеством преимуществ, но также создает и значительные риски для своей безопасности. Задачи обеспечения безопасности IoT требуют многоаспектного подхода для их эффективного решения. Среди таких решений – более надежные меры шифрования и аутентификации, стандартизация протоколов безопасности и повышение осведомленности пользователей IoT о рисках. Внедряя указанные решения, можно гарантировать, что устройства IoT не только усилят свои преимущества, но и

позволят свести к минимуму возможные риски.

Список литературы

1. 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). URL: https://icecce.com/. (Дата обращения: 2.04.2023).

2. Серия Y: глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений – структура и функциональные модели архитектуры. URL: https://www.itu.int. (Дата обращения: 02.04.2023).

3. Верещагина Е.А., Капецкий И.О., Ярмонов А.С. Проблемы безопасности Интернета вещей: Учебное пособие. Сетевое издание. М.: Мир науки, 2021. URL: https://izd-mn.com/PDF/20MNNPU21.pdf. (Дата обращения: 02.04.2023).

4. ITU-T Recommendations. URL: https https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11830&lang=en. (Дата обращения: 02.04.2023).

5. Marques G., Ferreira C.R., Pitarma R. Indoor air quality assessment using a CO2 monitoring system based on internet of things // Journal of medical systems. 2019. 43(3). – Pp.1-10.

6. Mosenia A., Jha N. K. A Comprehensive Study of Security of Internet of Things // IEEE Transactions on Emerging Topics in Computing. 2017. 5(4). – Pp. 586-602.

7. Yang Y., Wu L., Yin G., Li L., Zhao H. A Survey on Security and Privacy Issues in Internet of Things // IEEE Internet of Things Journal. 2017. 4(5). – Pp. 1250–1258.

8. Industrial Internet of Things – IIoT: Промышленный интернет вещей. URL: https://www.tadviser.ru/a/ 342500. (Дата обращения: 02.04.2023).

9. Скрипин В. FDA впервые признало, что некоторые кардиостимуляторы уязвимы для взлома. URL: https://itc.ua/news/fda-vpervyie-priznalo-chto-nekotoryie-kardiostimulyatoryi-uyazvimyi-dlya-vzloma/. (Дата обращения: 02.04.2023).

10. Безопасность медицинских IoT-устройств. URL: http://zdrav.expert/a/367948. (Дата обращения: 02.04.2023).

11. Ли П. Архитектура интернета вещей / Перевод с английского М. А. Райтман. М.: ДМК Пресс, 2019. – 454 с.

12. Муромцев Д. И., Шматков В. Н. Интернет вещей: введение в программирование на arduino: Учебно-методическое пособие. СПб.: ИТМО, 2018. – 36 с.

13. Интернет вещей. URL: http://blogs.gartner.com/richard-gordon/2014/02/24/in-the-modern-world-of-it-all-things-are-connected/ (Дата обращения: 02.04.2023).

14. Интернет вещей. MIT Technology View URL: https://www.technologyreview.com/s /601013/the-internet-of-things-roadmap-to-a-connected-world/ (Дата обращения: 02.04.2023).

15. Интернет вещей. TM forum inform. URL: https://inform.tmforum.org/internet-of-everything/2017/03/internet-things-revolution-society-not-just-industry/ (Дата обращения: 02.04.2023).

16. Bauer H., Patel M., Veira J. The Internet of Things: Sizing up the Opportunity. NY: McKinsey & Company. URL: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity. (Дата обращения: 2.04.2023).

17. Попов Е. В., Семячков К. А. Умные города. М.: Изд-во Юрайт, 2020. – 346 с.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia

Поступила в редакцию 10.03.23

Информация об авторах

Минаев Владимир Александрович – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

Швырев Борис Анатольевич – канд. физ.-мат. наук, доцент, доцент кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: bor2275@yandex.ru

Ромашкин Тимур Рафаэльевич – курсант факультета подготовки специалистов в области информационной безопасности Московского университета МВД России имени В.Я. Кикотя, e-mail: alexanderostapenkoias@gmail.com

INTERNET OF THINGS SECURITY: KEY SOLUTIONS

Minaev V.A., Shvyrev B.A., Romashkin T.R.

One of the main problems in ensuring the security of the Internet of Things (IoT) is, on the one hand, a huge number of devices that scale the threats and security risks of their use, and on the other hand, weak development or even lack of standardized security protocols. Often, IoT devices have limited computing power and memory for the sake of price and commercial benefits, which makes it difficult to implement reliable security measures. The expansion of IoT has reached critical infrastructure - healthcare, transport and other particularly important areas. Since modern IoT devices have access to personal and confidential information, violations of their information security can have very serious consequences, therefore it is extremely important to justify and implement reliable security measures to protect them from computer attacks. A comparative analysis of the main IoT network protocols is carried out. The most likely computer attacks on IoT devices are highlighted: network security violation, device security violation, physical access to the device, device malfunctions, social engineering technologies. The following measures to ensure the security of IoT devices are considered: improvement of the regulatory and legal framework; training and professional development of employees; development of interaction with IoT manufacturers; improvement of monitoring of IoT devices; improvement of data analysis methods related to the functioning of IoT. To implement the proposed measures, software and hardware solutions to the security problems of IoT devices are provided.

Keywords: Internet of Things, information security threats, security protocol.

Submitted 10.03.23

Information about the authors

Vladimir A. Minaev – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, Moscow University of the Internal Affairs Ministry of Russia, Moscow, Russian Federation, e-mail: m1va@yandex.ru

Boris A. Shvyrev – Cand. Sc. (Physical and Mathematical), Associate Professor, Associate Professor of the Special Information Technologies Department, V.Ya. Kikot Moscow University of the Internal Affairs Ministry of Russia, Moscow, Russian Federation, e-mail: bor2275@yandex.ru

Timur R. Romashkin – cadet of the Faculty of training specialists in the field of information security, V.Ya. Kikot Moscow University of the Internal Affairs Ministry of Russia, Moscow, Russian Federation, e-mail: alexanderostapenkoias@gmail.com