УДК 004.6 DOI 10.21685/2227-8486-2020-2-11

ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРНЕТ ВЕЩЕЙ: ПРОБЛЕМА ЗАЩИТЫ ДАННЫХ

С. В. Рындина, С. В. Куликова, К. Д. Михайлова

CUSTOM INTERNET OF THINGS: THE PROBLEM OF DATA PROTECTION

S. V. Ryndina, S. V. Kulikova, K. D. Mikhailova

Аннотация. *Предмет и цель работы.* Рассмотрены основные угрозы пользовательского Интернета вещей для компрометации и злоупотребления пользовательскими данными. *Методы.* Проведена классификация угроз информационной безопасности пользователей, связанных с распространением технологий Интернета вещей. *Результаты и выводы.* Рассмотрены основные способы обеспечения безопасной эксплуатации пользовательских решений для Интернета вещей со стороны пользователей. Развитие технологий Интернета вещей и отставание регулирования этой отрасли как законодательного, так и технологического предъявляет ко всем участникам, в том числе и к конечным пользователям, повышенные требования к осознанному использованию умных устройств, к соблюдению цифровой гигиены и самостоятельному принятию мер для обеспечения безопасной циркуляции пользовательских данных.

Ключевые слова: Интернет вещей, пользовательские данные, информационная безопасность.

Abstract. *Subject and goals.* The main threats of the user Internet of things for compromising and abusing user data are considered. *Methods*. The classification of threats to information security of users associated with the spread of Internet of things technologies is carried out. *Results*. The article describes the main ways to ensure the safe operation of user solutions for the Internet of things by users. *Results and conclusions.* The development of Internet of things technologies and the lagging regulation of this industry, both legislative and technological, places increased demands on all participants, including end users, to consciously use smart devices, to comply with digital hygiene and to take independent measures to ensure the safe circulation of user data.

Keywords: Internet of things, user data, information security.

Введение

Интернет вещей имеет большой потенциал встраивания в повседневную жизнь людей, так как его технологические решения приспособлены для разнообразных задач: упрощение бытовых процессов, управление устройствами вне дома, мониторинг и контроль над физиологическими процессами, в том числе по медицинским показаниям, оповещение о возможных неблагоприятных событиях, угрозах, авариях и т.д. Пользовательский Интернет вещей позволяет охватить самые различные области и сферы жизни. Однако использование технологий Интернета вещей связано с потенциальными угрозами для пользовательских данных: компрометацией данных пользователя, злоупотреблением данными в коммерческих целях различными компаниями,

обусловленное отставанием законодательной базы от развития технологий, мошенничествами и противоправными действиями с пользовательскими данными.

Инструменты защиты от различных видов угроз в отношении пользовательских данных совершенствуются по мере развития технологий Интернета вещей и выявления все новых вариантов использования пользовательских данных с неблагоприятными для источников этих данных последствиями. Однако есть препятствия, существенно усложняющие противостояние угрозам Интернета вещей.

Во-первых, это низкая цифровая грамотность пользователей: их беспечность в предоставлении доступа к данным, в бездумной и бесконтрольной выдаче разрешений на использование данных неопределенному кругу лиц, неосведомленность о потенциальных угрозах и инструментах их ослабления или ликвидации, например, смене заводских паролей устройств или своевременном обновлении программных оболочек и приложений. Также пользователи зачастую не подозревают о сетевой активности ряда домашних устройств, подключенных к сети. Всплеск возмущения пользователей обычно связан с платными подписками, которые внезапно обнаруживаются на устройствах, никак не предназначенных для потребления подобного контента. Но проблема бытовых устройств в сети гораздо шире, зачастую они подключены не только к провайдеру конечной услуги, но и к другим сервисам, например, обработка голосовых сообщений, получение автоматических обновлений, сбор пользовательских данных для рекламных компаний в интересах поставщика услуги и т.п.

Во-вторых, это недостаточное внимание производителей конечных устройств Интернета вещей и телекоммуникационного оборудования к потенциальным угрозам использования пользовательских данных и, как следствие, заметное отставание в развитии инструментов противодействия таким угрозам. Следование стандартам безопасности часто коммерчески невыгодно, требует дополнительных трат на тестирование, создание обновлений. Также для индустрии Интернета вещей характерно слабое развитие саморегулирования, норм и правил использования пользовательских данных, которые могли бы стать лучшей практикой.

Пользовательский Интернет вещей

Интернет вещей (IoT, Internet of Things) – это глобальная сеть компьютеров, датчиков (сенсоров) и исполнительных устройств (актуаторов), связывающихся между собой с использованием Интернет протокола IP (Internet Protocol) [1].

Согласно исследованию компании J’son &Partners Consulting, Интернет вещей от Интернета людей (традиционного Интернета, в котором за каждым подключенным устройством стоял человек, и большая часть информации создавалась для человека и при его участии) отличается [2]:

- смещением фокуса с человека на машины;
- значительным увеличением числа подключенных вещей;
- уменьшением размеров устройств и ростом скорости передачи данных;
- смещением фокуса с коммуникаций на сбор и обработку данных с различных устройств;

– возникновением новых стандартов и новой инфраструктуры.

Подключенные вещи (Connected Things) – это всевозможные сенсоры, датчики (акустические, визуальные, температурные и т.п.), а также узлы передачи и обработки информации. Среди подключенных вещей можно выделить отдельный подкласс подключенных устройств, которые кроме уникальной идентификации в пространстве, часто реализуемой с помощью RFID-меток (Radio Frequency IDentification), т.е. меток радиочастотной идентификации, обладают также способностью захватывать данные из окружающей среды [3]. Для подключенных вещей реализуется концепция M2M – возможность контактировать между собой, обмениваясь данными, без вмешательства человека, что стимулирует развитие нового класса приложений с поддержкой устройств.

Роб Ван Краненбург рассматривает четыре уровня IoT [4]:

1. BAN (Body Area Network) – отдельные устройства, например, носимые устройства: фитнес-трекеры, умные часы, умная одежда, VR-очки и т.п., а также имплантируемые датчики и устройства, например инсулиновые помпы.

2. LAN (Local Area Network) – умный интерфейс, сеть вещей, обслуживающая потребности одного человека или небольшой группы лиц, например, устройства умного дома или умный автомобиль.

3. WAN (Wide Area Network) – умные сети: сеть электроснабжения, сеть ЖКХ, транспортная сеть и т.п., т.е. технологии, реализующие концепцию умного города.

4. VWAN (Very Wide Area Network) – сенсорная планета или сеть умных городов, взаимодействие всех элементов в которых происходит через электронное управление.

И де-факто и де-юре обладатели новой власти в мире, пронизанном технологиями и сервисами Интернета вещей, те, кто создает и контролирует инфраструктуру: обеспечивает связь между устройствами, безопасность и устойчивость ее функционирования.

Угрозы пользовательским данным

С увеличением числа присоединенных к сети устройств увеличиваются также и риски, которые связаны с незаконным доступом в IoT-систему и захватом данных этой системы злоумышленниками.

Технологии пользовательского Интернета вещей основаны на сборе и обработке пользовательских данных, которые делают программную начинку обычных устройств персонифицированной, а в некоторых случаях и действительно умной: умные колонки не просто распознают специально сконструированные фразы, а подстраиваются под речевые особенности своего владельца и готовы распознавать и анализировать обычную речь.

С одной стороны, устройству Интернета вещей часто необходим определенный объем пользовательских данных для выполнения своих функций: фитнес-трекер должен регистрировать физиологические данные пользователя и его активности, чтобы давать обратную связь о нагрузках и их переносимости организмом. Чем больше данных о пользователе, тем точнее отклик и полезнее устройство. С другой стороны, по мере проникновения Интернета вещей в повседневную жизнь и в связи с легкостью эксплуатации умных вещей степень наблюдаемости отдельных устройств резко снижается, их потенци-

альная опасность перестает восприниматься: пользователи редко читают инструкции и предупреждения, меняют заводские настройки, следят за обновлениями. Однако, если злоумышленник получит доступ к данным, то ему откроется возможность не только безучастно наблюдать, но и активно вмешаться в личную жизнь, что может послужить причиной различных негативных последствий, таких как APT-атаки (advanced persistent threat – развитая устойчивая угроза или целевая кибератака), шантаж или организация настоящего ограбления.

Еще больше угроз для пользователя содержит в себе LAN: система безопасности, система освещения, система обогрева с управлением по Интернету при взломе или нарушении их работы представляют собой опасность для имущества и жизни клиента. Например, если злоумышленник сможет взять управление над системой безопасности в умном доме, то ему станут доступны такие опции, как открытие или блокировка дверей.

Причины реализации угроз:

1. Стандартные учетные записи от производителя, слабая проверка и принятие введенной информации на сервере.
2. Отсутствие поддержки со стороны производителя с целью ликвидации недостатков.
3. Сложности при обновлении программного обеспечения и операционных систем.
4. Эксплуатация текстовых протоколов и лишних открытых портов.
5. Уязвимость одного устройства, которая приводит к угрозе для всей системы.
6. Эксплуатация незащищенных устройств.
7. Эксплуатация незащищенной облачной инфраструктуры.
8. Эксплуатация небезопасного программного обеспечения.

Вирусные аналитики из компании «Доктор Веб» с помощью ханипотов – ловушек, имитирующих различные устройства Интернета вещей и регистрирующих попытки их взлома и заражения вредоносным программным обеспечением (ПО), зафиксировали рост попыток взлома и заражения на 13 497 % с четвертого квартала 2016 г. по второй квартал 2019 г. [5]. Аналогичные исследования есть и от других компаний, занимающихся разработкой инструментов защиты от вредоносного ПО. Так, например, в «Лаборатории Касперского» зафиксировали с помощью ханипотов почти десятикратный рост попыток взлома устройств Интернета вещей в 2019 г. по сравнению с 2018 г. [6]. При этом увеличилось количество повторных атак с IP-адресов злоумышленников.

Классификация угроз

Пользовательские решения для Интернета вещей содержат в себе множество потенциальных угроз для пользователей (рис. 1):

1. Непреднамеренный и несанкционированный доступ к пользовательским данным:

– утечка личных данных (в том числе биометрических): сообщения, фотографии, видео-, аудиозаписи разговоров;

– утечка платежных реквизитов: данные для совершения онлайн-платежей, данные личных кабинетов в платных приложениях;

– кража аккаунтов и кража личности.

2. Использование пользовательских данных для совершения правонарушений и преступлений:

– шантаж и вымогательство на основе полученной информации в отношении пользователя или связанных с ним лиц;

– использование украденных аккаунтов и украденной личности для совершения противоправных действий в сети.

3. Перехват управления над устройствами Интернета вещей:

– доступ к камерам и микрофонам домашних устройств с целью слежения;

– заражение устройств вредоносным ПО для получения доступа к конфиденциальной информации;

– использование устройства для получения контроля над внутренней сетью, в которое оно включено;

– включение устройств пользователя в бот-сеть.

Рис. 1. Классификация угроз

Способы защиты от угроз

Научное сообщество активно предлагает технологические и законодательные решения для обеспечения безопасности данных, собираемых с помощью технологий IoT. Не остаются в стороне и компании, активно использующие технологии Интернета вещей для разработки новых устройств, цифровых продуктов или сервисов, а также компании, эксплуатирующие эти разработки в своей деятельности.

Безопасность должна стать приоритетом развития пользовательского Интернета вещей.

Повысить уровень защищенности данных может обеспечить соблюдение пользователем следующего перечня рекомендаций:

1. Знакомство с инструкцией и политикой конфиденциальности (чтобы знать, какие данные устройство собирает, где они будут храниться, как будут использоваться).

2. Изменение стандартных настроек (прежде всего смена дефолтных паролей).

3. Регулярные обновления для всех устройств пользовательской части Интернета вещей, смена прошивки самих конечных устройств, маршрутизаторов, роутеров.

4. Соединение с сетью и связь между устройствами должны быть зашифрованы.

5. Отключение удаленного доступа.

6. Контроль центральных управляющих устройств: использование антивирусных программ.

7. Контроль над передачей информации устройствами. При необходимости переводите устройства на автономный режим.

Ресурсоемкость самого эффективного метода защиты – шифрования – становится ограничением для использования этого метода в устройствах с малой вычислительной и энергетической мощностью.

И главное препятствие на пути следования рекомендациям: все эти действия причиняют определенные неудобства пользователю, так как нужно прилагать усилия для их совершения.

Производители оборудования могут подтолкнуть пользователей к соблюдению критически важных рекомендаций для обеспечения безопасности пользовательских данных. Так, требование смены пароля при подключении устройства может уменьшить риски самого частого способа получения удаленного доступа к устройству через подбор дефолтных паролей производителя.

Профессиональное сообщество может предложить механизмы саморегулирования для обеспечения безопасности использования технологий Интернета вещей.

Есть немало примеров, когда отдельные частные компании разрабатывают требования к безопасной эксплуатации устройств Интернета вещей, внутренние стандарты сертификации, которые становятся лучшей практикой в отрасли и даже используются регулирующими госорганами при создании государственных и международных стандартов.

Неформальное объединение заинтересованных представителей индустрии, среди которых Verisign, Microsoft и DigiCert, под названием Online Trust Alliance разрабатывает критерии безопасного функционирования Интернета вещей IoT Trust Framework [7]. Этот фреймворк стал основой нескольких программ сертификации и используется при оценке рисков, связанных с безопасной эксплуатацией IoT-устройств: преимущественно бытовых, офисных и носимых.

Независимое подразделение компании Verizon предложило программу тестирования безопасности и сертификации IoT-устройств Securing the Internet of Things [8], в которой тестируются следующие компоненты: уведомление/протоколирование, криптография, аутентификация, связь, физическая безопасность и безопасность платформы.

Компания UL (Underwriters Laboratories, США), деятельность которой связана со стандартизацией и сертификациией в области техники безопасно-

сти [9], реализует программу обеспечения кибербезопасности UL CAP (Cybersecurity Assurance Program), в которой используются новые стандарты UL 2900 для проверки инновационных продуктов и систем Интернета вещей на соответствие критериям безопасной эксплуатации: оценка уязвимостей, средств контроля безопасности и т.п..

Cybersecurity National Action Plan (CNAP, национальный план действий по кибербезопасности), разработанный в правительстве США, включает положения программы CAP в качестве способа тестирования и сертификации сетевых подключаемых устройств в рамках цепочки поставок «Интернет вещей» и экосистем [10].

Выводы

Очевидно, что распространение технологий Интернета вещей кардинально меняет жизнь вокруг нас, делая ее более комфортной. «Сквозным» технологиям, к которым относится и Интернет вещей, уделяется все большее внимание на российском пространстве [11]. Однако важно осознавать, что технологический прогресс должен быть направлен не только на введение инноваций, но и на обеспечение безопасности в процессе их использования.

Новые возможности влекут за собой и новые вызовы, роль пользователей в обеспечении безопасности использования собственных данных не может быть пассивной. Как одна из заинтересованных сторон пользователь должен формировать свои требования к технологиям Интернета вещей, следовать лучшим практикам обеспечения безопасной эксплуатации устройств Интернета вещей: выполнять рекомендации, следовать инструкциям, своевременно обновлять программное обеспечение и, отказываясь от сомнительных в плане обеспечения информационной безопасности пользовательских решений, способствовать уходу таких решений с рынка или изменению политики обеспечения безопасности компаний, их предлагающих.

Библиографический список

1. Росляков, А. В. Интернет вещей : учеб. пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. – Самара : ПГУТИ, 2015. – 200 с.
2. J’son & Partners Consulting представляет исследование «Интернет вещей и межмашинные коммуникации: современные технологии, тренды, дорожные карты. Обзор ситуации в России и мире» / APPS4ALL. – URL: http://apps4all.ru/post/12-23-13-json-partners-consulting-predstavlyaet-issledovanie-quotinternet-veschej-i-mezhmashinnye-kommunikatsii-sovremennye-tehnologii-trendy-dorozhnye-karty-obzor-situatsii-v-rossii-i-mirequot (дата обращения: 21.02.2020).
3. Зараменских, Е. П. Интернет вещей. Исследования и область применения : монография / Е. П. Зараменских, И. Е. Артемьев. – Москва : ИНФРА-М, 2019. – 188 с. – URL: https://new.znanium.com/catalog/product/1020713 (дата обращения: 21.02.2020).
4. Риски и угрозы в Интернете вещей (IoT) / Доктор Веб. – URL: https://news.drweb.ru/show/?i=13353&lng=ru (дата обращения: 21.02.2020).
5. Деметер, Д. Интернет вещей (IoT): история зловредов / Д. Деметер, М. Пройсс, Я. Шмелев // Лаборатория Касперского. – URL: https://securelist.ru/iot-a-malware-story/94900/ (дата обращения: 21.02.2020).
6. Rob van Kranenburg: What is IoT? / IoT Council. – URL: https://www.theinternetofthings.eu/rob-van-kranenburg-what-iot (дата обращения: 21.02.2020).

7. Internet of Things (IoT) Trust Framework v2.5. – URL: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/ (дата обращения: 21.02.2020).
8. Securing the Internet of Things / ICSA Labs. – URL: https://www.icsalabs.com/sites/default/files/2015-11-02_FS16579%20a%20ICSA_Securing_IoT.pdf (дата обращения: 21.02.2020).
9. Underwriters Laboratories [Официальный сайт] / URL: https://www.ul.com/ (дата обращения: 21.02.2020)
10. FACT SHEET: Cybersecurity National Action Plan / Obamawhitehouse. – URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (дата обращения: 21.02.2020).
11. Суровицкая, Г. В. «Сквозные» цифровые технологии в региональной экономике / Г. В. Суровицкая // Модели, системы, сети в экономике, технике, природе и обществе. – 2019. – № 4 (32). – С. 16–23.

References

1. Roslyakov A. V., Vanyashin S. V., Grebeshkov A. Yu. *Internet veshchey: ucheb. posobie* [The Internet of things : a tutorial]. Samara: PGUTI, 2015, 200 p. [In Russian]
2. *J'son & Partners Consulting predstavlyaet issledovanie «Internet veshchey i mezhmashinnye kommunikatsii: sovremennye tekhnologii, trendy, dorozhnye karty. Obzor situatsii v Rossii i mire»* [J'son & Partners Consulting presents the study " Internet of things and machine-to-machine communications: modern technologies, trends, road maps. Overview of the situation in Russia and the world»]. APPS4ALL. Available at: http://apps4all.ru/post/12-23-13-json-partners-consulting-predstavlyaet-issledovanie-quotinternet-veschej-i-mezhmashinnye-kommunikatsii-sovremennye-tehnologii-trendy-dorozhnye-karty-obzor-situatsii-v-rossii-i-mirequot (accessed Febr. 21, 2020). [In Russian]
3. Zaramenskikh E. P., Artem'ev I. E. *Internet veshchey. Issledovaniya i oblast' primeneniya: monografiya* [Internet of things. Research and application: monograph]. Moscow: INFRA-M, 2019, 188 p. Available at: https://new.znanium.com/catalog/product/1020713 (accessed Febr. 21, 2020). [In Russian]
4. *Riski i ugrozy v Internete veshchey (IoT)* [Risks and threats in the Internet of things (IoT)]. Doctor Veb. Available at: https://news.drweb.ru/ show/?i=13353&lng=ru (accessed Febr. 21, 2020). [In Russian]
5. Demeter D., Proyss M., Shmelev Ya. *Laboratoriya Kasperskogo* [Kaspersky lab]. Available at: https://securelist.ru/iot-a-malware-story/94900/ (accessed Febr. 21, 2020). [In Russian]
6. *Rob van Kranenburg: What is IoT?* IoT Council. Available at: https://www.theinternetofthings.eu/rob-van-kranenburg-what-iot (accessed Febr. 21, 2020).
7. *Internet of Things (IoT) Trust Framework v2.5*. Available at: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/ (accessed Febr. 21, 2020).
8. *Securing the Internet of Things*. ICSA Labs. Available at: https://www.icsalabs.com/sites/default/files/2015-11-02_FS16579%20a%20ICSA_Securing_IoT.pdf (accessed Febr. 21, 2020).
9. *Underwriters Laboratories* [Official site]. Available at: https://www.ul.com/ (accessed Febr. 21, 2020)
10. *FACT SHEET: Cybersecurity National Action Plan*. Obamawhitehouse. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (accessed Febr. 21, 2020).
11. Surovitskaya G. V. *Modeli, sistemy, seti v ekonomike, tekhnike, prirode i obshchestve* [Models, systems, and networks in Economics, technology, nature, and society]. 2019, no. 4 (32), pp. 16–23. [In Russian]

Рындина Светлана Валентиновна
кандидат физико-математических наук,
доцент,
кафедра экономической кибернетики,
Пензенский государственный
университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: svetlanar2004@yandex.ru

Ryndina Svetlana Valentinovna
candidate of physical and mathematical
sciences, associate professor,
sub-department of economic cybernetics,
Penza State University
(40 Krasnaya street, Penza, Russia)

Куликова София Вячеславовна
студентка,
Пензенский государственный
университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: sofiia.kulikova.00@mail.ru

Kulikova Sofia Vyacheslavovna
student,
Penza State University
(40 Krasnaya street, Penza, Russia)

Михайлова Кристина Дмитриевна
студентка,
Пензенский государственный
университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: khristina-mikh@mail.ru

Mikhailova Kristina Dmitrievna
student,
Penza State University
(40 Krasnaya street, Penza, Russia)

Образец цитирования:

Рындина, С. В. Пользовательский Интернет вещей: проблема защиты данных / С. В. Рындина, С. В. Куликова, К. Д. Михайлова // Модели, системы, сети в экономике, технике, природе и обществе. – 2020. – № 2 (34). – С. 145–153. – DOI 10.21685/2227-8486-2020-2-11.