Социологические науки

УДК 004

Е.И. Шокола

Р.Х. Багдасарян

Шокола Елена Игоревна, студентка 3 курса группы БИД/бак-17 Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: shokola.1998@mail.ru

Багдасарян Рафаэль Хачикович, доцент кафедры библиотечно-библиографической деятельности и информационных технологий Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: rafael_555@mail.ru

О ПРОБЛЕМЕ УЯЗВИМОСТИ ИНФОРМАЦИИ В УСЛОВИЯХ ИНТЕРНЕТА ВЕЩЕЙ

В статье проанализировано современное состояние безопасности информации в условиях повсеместного внедрения интернета вещей. Рассмотрены потенциальные уязвимости в системах умных гаджетов.

Ключевые слова: кибербезопасность, интернет вещей, персональные данные, умный дом, информационная безопасность.

E.I. Shokola

R.Kh. Bagdasaryan

Shokola Elena Igorevna, student of 3rd course of BID/bak-17 group of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy St., Krasnodar), e-mail: shokola.1998@mail.ru

Bagdasaryan Rafael Khachikovich, associate professor of department of library and bibliography and information technologies of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy St., Krasnodar), e-mail: rafael_555@mail.ru

ABOUT THE PROBLEM OF INFORMATION VULNERABILITY IN THE INTERNET OF THINGS

The article analyzes the current condition of information security in the context of the widespread introduction of the Internet of things. Potential vulnerabilities in smart gadget systems are considered.

Key words: cybersecurity, Internet of things, personal data, smart home, information security.

Термин «интернет вещей» (англ. – Internet of things) означает сеть физических предметов, подключенных к глобальной сети Интернет и взаимодействующих как между собой, так и с окружающей средой. Идея интернета вещей состоит в беспроводной передаче данных и использовании самообучающегося искусственного интеллекта.

На современном этапе развития интернет вещей внедряется не только в производства и инфраструктуру, но и в повседневную жизнь человека, что вместе с удобствами подразумевает и крайнюю уязвимость персональных данных владельца устройств, использующих данную технологию.

В большинстве случаев пользователь даже не подозревает, что его окружает интернет вещей. Самым простым примером может послужить система умного дома. Датчики и электроника, установленные в доме, служат для создания комфортной повседневной жизни человека. Поддержание определенной температуры, влажности воздуха, слежение за аварийными

ситуациями и самостоятельный вызов службы безопасности – все это происходит в автоматическом режиме.

Разработкой таких технологий занимаются крупнейшие компании мира – Apple, Google, Xiaomi. К разработке подобных систем приступили и российские разработчики компании «Яндекс», выпустив в 2018 году мультимедийное устройство «Станция» с голосовым помощником «Алиса» [2].

Сейчас интернет вещей внедряется в города, создавая систему «умный город». Например, устанавливаются датчики, следящие за транспортным потоком и погодными условиями и, анализируя полученные данные, регулируют работу светофоров, тем самым минимизируя образование пробок.

Однако вместе с удобствами и автоматизацией приходит и крайняя уязвимость. Халатность производителей, экономящих на защитном ПО, и неграмотность пользователей привели к крайней уязвимости владельцев умных устройств перед хакерами. Причем как перед теми, кто действует из хулиганских побуждений, так и перед преступниками-вымогателями.

Интернет, облачные серверы, радиоэфир – с помощью этих технологий работают автономно от человека умные дома, заводы, города. Соблюдение элементарных правил цифровой гигиены помогло бы значительно сократить количество взломов устройств, однако по данным Avast, охватившей 11 млн роутеров по всему миру, 60% из них имеют уязвимые пароли или ПО (в России – 97%), что говорит о цифровой неграмотности пользователей устройств, подключенных к интернету вещей [3].

Так чем же опасен взлом умных гаджетов? Помимо заражения вредоносным ПО и шифровкой личных данных пользователя с целью вымогания денежных средств, девайс могут захватить для майнинга криптовалюты, либо, проникнув в облачный сервер через незащищенное устройство, получить личные данные множества людей. Умный робот-пылесос поделится данными о планировке квартиры, а умные электронные

няни, оснащенные камерой и микрофоном, сообщат о наличии людей в доме. С помощью камер, использующих облачное хранилище, можно получить информацию о тех или иных помещениях.

По данным Positive Technologies, камеры, видеорегистраторы, устройства беспроводного управления, датчики и роутеры – наиболее популярные устройства небезопасного интернета вещей [3].

Не так давно пассажир «Сапсана» получил доступ к паспортным данным всех пассажиров поезда. Для подключения к сети Wi-Fi поезда требовалось ввести последние четыре цифры номера паспорта, что насторожило пользователя. После некоторых манипуляций в течение 20 минут пассажир получил доступ к базе данных, хранящей в себе информацию о пассажирах текущего и прошлых рейсов. Оказалось, что у «Сапсана» везде установлены одни и те же пароли, а данные хранятся в текстовом формате. Также выяснилось, что РЖД не закупила сертификат шифрования для HTTPS, а воспользовалась бесплатным Let's Encrypt.

Пользователь опубликовал результаты своих исследований на популярном интернет-ресурсе «Хабр», а также сообщил об уязвимости в безопасности напрямую в РЖД. На данный момент компания не предприняла никаких действий в улучшении защиты персональных данных своих пассажиров [4].

Рассмотрим, что еще может сделать уязвимым умные устройства. Первая и самая распространенная проблема – недостаточно строгая аутентификация. Большинство пользователей не меняют заводские логины и пароли на своих устройствах, не зная, к чему это может привести. Подбор таких паролей и получение доступа к контролю над устройством становится легкой задачей для злоумышленника.

Вторая не менее важная проблема – обмен данными внутри сети. Зачастую они передаются в незашифрованном виде либо используя устаревшие протоколы. Так, получив доступ к одному устройству,

злоумышленник получает доступ также к любому гаджету, подключенному к сети.

Окружение себя интернетом вещей, популярность оснащения дома умными устройствами с каждым годом все растет. Но нежелание пользователей разбираться в купленном устройстве, несвоевременное обновление программного обеспечения, а также пренебрежение двухфакторной аутентификацией создают простор действиям злоумышленников.

В масштабах города при внедрении систем интернета вещей подобная уязвимость может привести к катастрофическим последствиям, так как зачастую даже специалисты в области информационной безопасности, как показывает опыт РЖД, не осознают всей опасности незащищенного доступа к данным.

Список используемой литературы:

1. *Багдасарян Р.Х.* Анализ безопасности новых приложений для умного дома / Р.Х. Багдасарян, Е.В. Вольвич, Т.Р. Хасаметдинова // IX международная научно-практическая конференция молодых ученых, посвященная 58-й годовщине полета Ю.А. Гагарина в космос: сборник научных статей. – 2019. – С. 276-278.

2. *Буторина Е.* Связанные одной сетью / Е. Буторина, И. Дмитриенко // Профиль. – № 29-30. – 2019. – С. 26-33.

3. *Дворак М.* Умные вещи века: к чему приводит экспансия интернета устройств, методично захватывающих нашу цивилизацию / М. Дворак // Профиль. – № 29-30. – 2019. – С. 16-22.

4. keklick1337 Самый беззащитный – это Сапсан / keklick1337 // Режим доступа: https://habr.com/ru/post/476034/