http://vestnik.mrsu.ru

ISSN Print 0236-2910
ISSN Online 2313-0636

УДК 004.056:004.738.5

DOI: 10.15507/0236-2910.027.201701.027-040

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ИНТЕРНЕТ ВЕЩЕЙ

С. А. Шиков
ФГБОУ ВО «МГУ им. Н. П. Огарёва» (г. Саранск, Россия)
stenlav@mail.ru

Введение. В статье рассматриваются возможные угрозы в сфере информационной безопасности при переходе от технологии информационного взаимодействия типа «машина-машина» к глобальному коммуникационному взаимодействию типа «интернет вещей». Угрозы рассматриваются на примерах системы «Умный Дом», беспроводного стандарта ZigBee, электрокаров фирмы Tesla и бесконтактной системы оплаты Apple Pay. Приводится определение термина *интернет вещей*; рассматривается история развития данной области, кратко излагается структура работы интернета вещей. Описывается разработанный в 2011 г. IoT-связанный стандарт – IEEE 1888, целью внедрения которого является повышение энергоэффективности решений, построенных на базе интернета вещей. Рассматриваются базовые проблемы безопасности при создании системы «Умный дом».
Материалы и методы. В качестве объектов исследования были выбраны Apple Pay, беспроводной стандарт ZigBee, электрокары Tesla Model S. Методами анализа и сравнения, а также путем моделирования были определены угрозы безопасности для интернета вещей.
Результаты исследования. В ходе исследования была выявлено, что даже самые современные технологии не дают 100 % гарантии безопасности. Наиболее безопасной из рассмотренных примеров оказалась система Apple Pay. Главным фактором недостаточной безопасности во многом является желание производителя максимально удешевить процесс производства. И поскольку рядовые пользователи, как правило, в последнюю очередь обращают внимание на безопасность систем, то производители предпочитают сокращать затраты именно в этой сфере, соблюдая необходимые стандарты по нижней границе.
Обсуждение и заключения. Было установлено, что современный интернет вещей не соответствует всем необходимым требованиям безопасности. Устранять уязвимости рекомендуется путем разработки новых стандартов безопасности с предварительным полным анализом существующих угроз интернета вещей. Кроме этого, необходимо наладить контроль над логистикой таких устройств от производителя до этапа инсталляции оборудования на объекте.

Ключевые слова: интернет вещей, информационная безопасность, угроза безопасности, программное обеспечение, операционная система, логистика вещей, ZigBee, Apple Pay, Tesla

Для цитирования: Шиков С. А. Проблемы информационной безопасности: интернет вещей // Вестник Мордовского университета. 2017. Т. 27, № 1. С. 27–40. DOI: 10.15507/0236-2910.027.201701.027-040

PrOBleMS OF INFOrMatION SeCUrIty : INterNet OF tHINGS

S. a. Shikov
National Research Mordovia State University (Saransk, Russia)
stenlav@mail.ru

Introduction. The article deals with the threats to information security in the internetworking of physical devices, also known as Internet of Things (IoT), and the security challenge in terms of home automation systems, ZigBee protocol, Tesla electric cars and Apple Pay mobile payment. Section provides the term definition and history of the Internet of Things. The IEEE 1888 IoT-related standard developed in 2011 as integrated solution based on energy-saving technologies for the Internet of Things. The author considers security challenges for the "smart home" system. Next section reviews the experiments of the author involved in testing of the Internet of Things devices.
Materials and Methods. The subjects of study are the Apple Pay, the ZigBee wireless standard, Tesla Model S electric cars. The main methods for identification of security threats are analysis and comparison.
Results. The companies of electronic devices simplify and reduce the price of manufacturing process. The customers and users are rarely interested in levels of electronic devices security policies. This is the weakest link of electronic products in terms of security and safety. The tests demonstrated that modern electronic-based technologies do not reach the 100-percentage security level. Apple Pay mobile payment system demonstrated the highest security rating.
Discussion and Conclusions. Modern electronic devices for Internet of Things does not meet all safety requirements, from the point of view of the author. The article recommends analyzing the potential threats and developing new security standards. In addition, the logistics of electronic devices for Internet of Things need to be under control from the manufacturer to equipment installation time.

Keywords: Internet of Things, information security, safety threats, software, operating systems, logistics of things, ZigBee, Apple Pay, Tesla

For citation: Shikov SA. Problems of information security: Internet of Things. *Vestnik Mordovskogo universiteta* = Mordovia University Bulletin. 2017; 1(27):27-40. DOI: 10.15507/0236-2910.027.201701.027-040

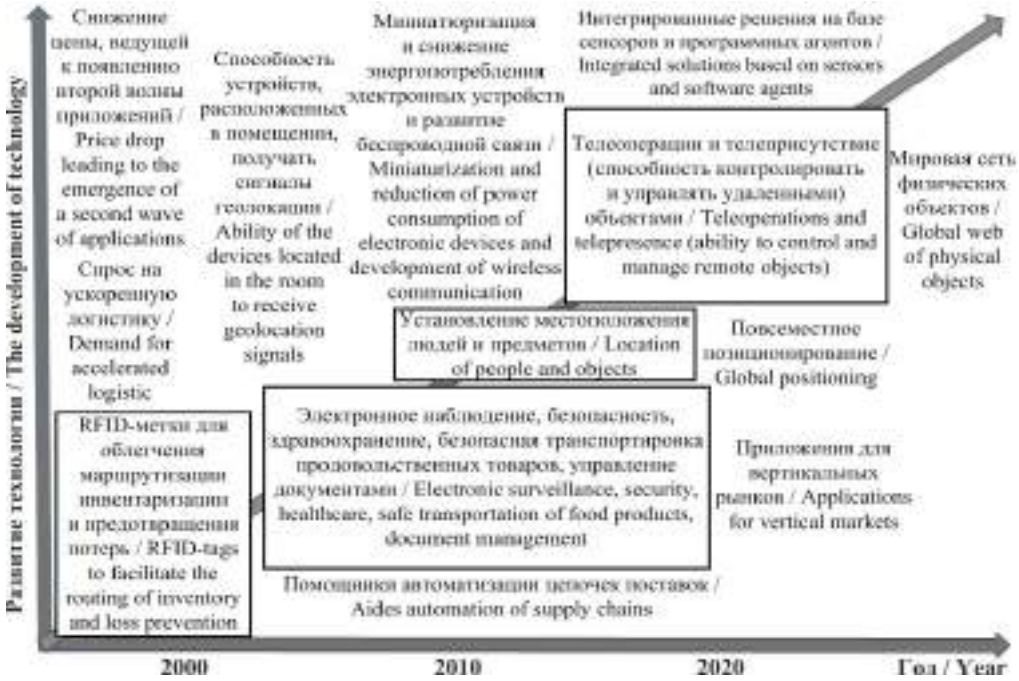
Введение

Целью исследования является изучение влияния глобального взаимодействия типа «машина-машина» на техногенную безопасность и устойчивость работы систем жизнеобеспечения современного общества. В статье рассматриваются наиболее вероятные угрозы нарушения конфиденциальности, доступности и целостности информации, циркулирующей в информационных сетях, которые предназначены для управления промышленными объектами.

Одним из современных трендов развития глобальных информационных систем является т. н. *интернет вещей* (например, бесконтактная система оплаты Apple Pay; автомобили, управляемые со смартфона, и др.). Официальное определение данного термина приводится в МСЭ-Т Y.2060, Overview of the Internet of Things: «…интернет вещей (Internet of Things, IoT) – это глобальная инфраструктура информационного общества, обеспечивающая передовые услуги за счет организации связи между вещами (физическими или виртуальными) на основе существующих и развивающихся совместимых информационных и коммуникационных технологий».

Особый интерес к данному направлению проявляет Китай. Глобальное сотрудничество в этой области привело к разработке в 2011 г. IoT-связанного стандарта – IEEE 1888, целью вне-

дрения которого является повышение энергоэффективности решений. Данный стандарт на основе универсального протокола контроля сети помогает крупным коммерческим объектам снизить энергопотребление благодаря дистанционному наблюдению, управлению и обслуживанию с использованием датчиков и мониторов наблюдения. На рис. 1 представлено развитие технологии IoT как поступательное развитие ПО и телекоммуникаций [1].



Р и с. 1. Эволюция технологии IoT

F i g. 1. Evolution of IoT technologies

Вместе с тем ряд специалистов в области информационной безопасности отмечают, что распространение взаимодействия технических систем без участия человека несет в себе достаточно серьезные угрозы безопасности [2]. С одной стороны, удаленное управление системами типа «Умный дом» позволяет с большим комфортом организовать свое жизненное пространство; а с другой, датчики и элементы управления системами жизнеобеспечения, оказавшись в руках злоумышленника, значительно увеличивают риски в области информационной безопасности.

Например, в 2008 г. национальный разведывательный совет США, осуществляющий координацию усилий разведки в определенных географических регионах и промышленных отраслях, опубликовал документ «Disruptive Civil Technologies», в котором среди шести гражданских технологий с наибольшей «взрывной силой» был назван IoT. Согласно указанному документу, к 2025 г. узлами IoT, т. е. потенциальными целями хакеров, смогут стать все окружающие нас предметы.

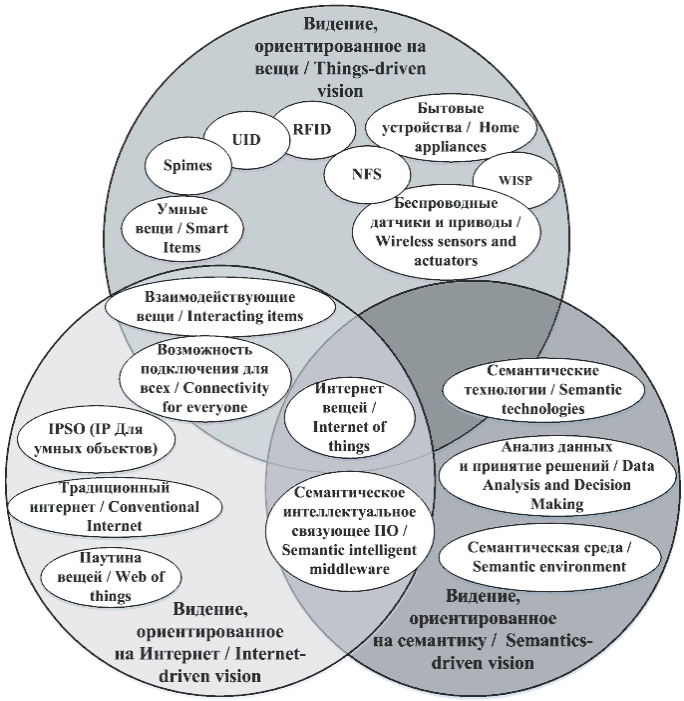
Предлагаемый аналитический материал касается некоторых проблем в области информационной безопасности интернета вещей.

1. Угроза нарушения конфиденциальности. Датчики системы «Умный дом» передают третьей стороне данные о своем состоянии и местонахождении.

Таким образом, считывание этих данных злоумышленником позволит получить информацию, касающуюся, например, перемещения или образа жизни.

2. Сложности в проведении авторизации. Надежная авторизация предусматривает обмен сообщениями между сторонами и использование криптографических ключей. Такая технология обеспечения безопасности не всегда реализуема из-за повышения энергопотребления; кроме этого, датчики часто обладают возможностями только односторонней коммуникации. По этой же причине в интернете вещей затруднительно использовать обычные средства обеспечения целостности информации.

Интернет вещей – достаточно сложная информационная среда. Эксперт в области информационной безопасности Л. Черняк предлагает рассматривать проблему внедрения интернета вещей с трех различных точек зрения (рис. 2) [3].



Р и с. 2. Три взгляда на интернет вещей

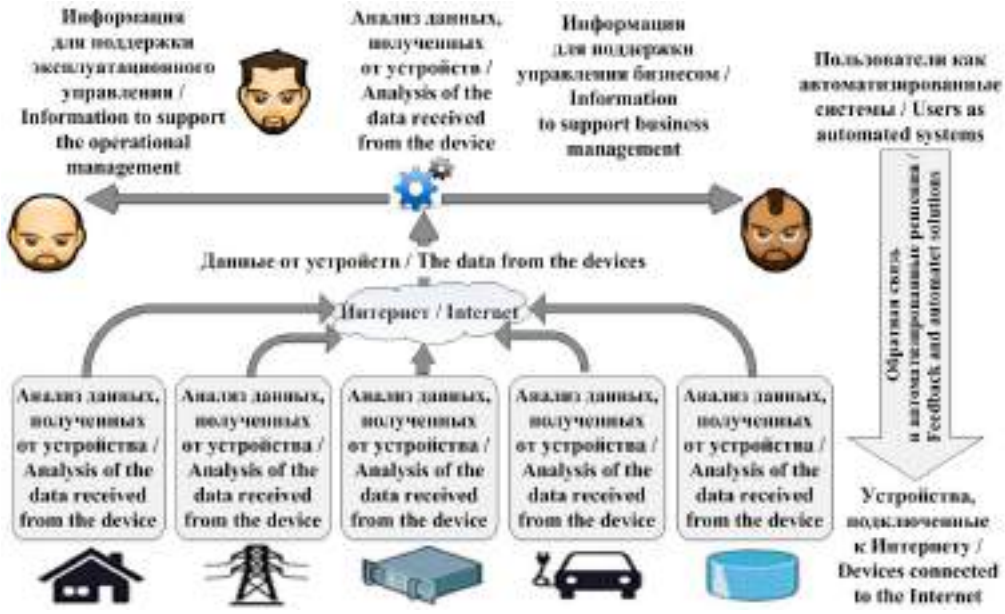
F i g. 2. Three views on Internet of Things

Как видно из рис. 2, для управления и доступа к бытовым устройствам через датчики и приводы необходимо семантическое интеллектуальное связующее программное обеспечение (ПО). Данная необходимость влечет за собой не только увеличение количества технических каналов утечки информации, но и потенциальные угрозы от уязвимостей ПО.

Интернет вещей представляет собой дальнейшее развитие взаимодействия типа M2M «машина-машина». В общем случае в IoT каждая вещь будет иметь свой идентификатор; в комплексе образуется континуум вещей, передающих друг другу информацию, создающих временные или постоянные сети. В ряде случаев процесс их функционирования может быть

полностью автоматизирован, а наличие систем искусственного интеллекта позволит изменять свои свойства и адаптироваться к окружающей среде. Более того, IoT позволяет создавать комбинацию из интеллектуальных устройств (например, различного рода средства дистанционного сбора данных и роботы), объединенных мультипротокольными сетями связи, и людей-операторов.

С точки зрения информационной безопасности, каждая вещь приобретает своего виртуального двойника. При этом количество уязвимостей системы прямо пропорционально количеству вещей. На всех этапах логистики, от производителя до магазина, данные об уникальных идентификаторах могут быть похищены, что порождает ряд проблем, связанных с защитой персональных данных. О сложности решения проблем безопасности «интернета вещей» можно судить по обобщенной архитектуре IoT-решения, представленной на рис. 3.



Р и с. 3. Типовая архитектура IoT-приложения от Microsoft
F i g. 3. Typical architecture of IoT applications from Microsoft

Изучая данную схему, нетрудно заметить, что обеспечение безопасности взаимодействия лежит в первую очередь на протоколах обмена между устройствами и, во-вторых, на операционных системах устройств, подключаемых к глобальной сети. Если технология обеспечения безопасности протоколов межсетевого обмена в настоящее время достаточно изучена, то операционные системы большинства вновь подключаемых устройств (бытовая техника, автомобили и т. д.) абсолютно не учитывают требований информационной безопасности.

По указанной проблеме компанией ISACA в 2013 г. был проведен опрос, касающийся проблем безопасности в технологии IoT, согласно которому «повышенные риски безопасности» назвали 38 % респондентов, а «угрозы конфиденциальности данных» вызвали беспокойство у 28 % опрошен-

ных. Такой результат напрямую связан с тем, что 51 % участников последнего глобального исследования планируют извлечь выгоду из внедрения интернета вещей, а 45 % полагают, что он уже повлиял на их бизнес [4]. В середине января 2014 г. компания Proofpoint объявила об обнаружении кампании по рассылке спама, источником которой стал ботнет, примерно на четверть состоявший не из компьютеров, а из скомпрометированных роутеров, мультимедийных центров, смарт-телевизоров «и как минимум одного холодильника» [5].

Большинство аналитиков в области информационной безопасности сходятся во мнении, что интернет вещей содержит слишком много неформализованных параметров [6–10]. В связи с этим наряду с такими формализованными компонентами как криптозащита протоколов и сетей передачи данных необходимо учитывать т. н. «человеческий» фактор. Другими словами, развитие информационной культуры общества и учет интересов бизнеса играет даже более значительную роль в обеспечении безопасности IoT, чем защита от технических средств разведки. Пользователь должен грамотно контролировать собственный интернет вещей и не допускать выхода данных за пределы домашней локальной сети, например, с помощью защищенного соединения.

В упомянутом выше отчете Национального разведывательного совета США «Интернет вещей» фигурирует еще одна потенциально разрушительная технология – незаметное для потребителей и повсеместное превращение в интернет-узлы распространенных вещей, к которым можно отнести мебель, товарную упаковку, различные документы, способные нанести огромный урон интересам национальной безопасности. Например, оставленная солдатом в танке обертка от конфеты может стать ценным источником информации о местонахождении и перемещениях бронированной машины, а следовательно, своеобразным маяком для нанесения ракетно-бомбовых ударов [11].

В настоящее время в бизнес-сообществе активно обсуждаются вопросы информационной безопасности интернета вещей как одного из самых активно развивающихся сегментов рынка. Данная работа посвящена анализу уязвимостей от различных хакерских атак с возможностью получения конфиденциальной информации о пользователе, последующей краже, перепродаже или другого нецелевого использования полученной информации.

Обзор литературы

Работа является продолжением исследований в области технической защищенности систем обработки конфиденциальной информации и систем обработки персональных данных, проводимых на кафедре информационной безопасности и сервиса ФГБОУ ВО «МГУ им. Н. П. Огарева» [6–11].

Методики взлома подробно рассмотрены в литературе таких авторов как Б. Бейзер [13], А. Петровский [14], Д. Михайлов и И. Жуков [15], а также М. Саттон, А. Грин, П. Амини [16].

В результате анализа научной литературы были выявлены наиболее популярные и эффективные методы атак:

1. Атака посредника, или атака «человек посередине» (англ. Man in the middle (MITM)) – вид криптографической атаки, когда злоумышленник перехватывает и подменяет сообщения, которыми обмениваются корреспонденты, причем ни один из последних не догадывается о его присутствии в канале.

2. Метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию [14].

3. Фишинг – вид интернет-мошенничества, направленный на получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Цель достигается путем массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить его ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту.

Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности; в частности, того факта, что сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и т. д. [16].

4. DoS (от англ. Denial of Service – отказ в обслуживании) – хакерская атака на вычислительную систему с целью довести ее до отказа, т. е. создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ затруднен. Отказ «вражеской» системы может быть шагом к овладению системой (если в нештатной ситуации ПО выдает какую-либо критическую информацию – например, версию или часть программного кода), однако чаще это мера экономического давления: потеря простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки наносят «цели» ощутимый финансовый урон. В настоящее время DoS и DDoS-атаки наиболее популярны, поскольку позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик [15].

Материалы и методы

Целью работы является оценка информационной безопасности объектов интернета вещей. Под безопасностью понимают уровень защищенности конфиденциальных данных, используемых объектами во время своей работы. В качестве основной характеристики защищенности рассматривается устойчивость системы к распространенным способам хакерского взлома (фишинг, MITM и DDoS-атаки).

Для оценки защищенности информационной безопасности структур интернета вещей используется анализ архитектуры входящих в него элементов и детальный разбор возможных хакерских способов взлома. На наш взгляд, наиболее предпочтительным является оценка уязвимости от популярных в настоящее время фишинговых, MITM-атак, а также методов социальной инженерии.

В качестве объектов для исследования были выбраны наиболее популярные системы:

1. Apple Pay – система мобильных платежей от корпорации Apple. Была представлена 9 сентября 2014 г. С помощью программ Apple Pay пользователи iPhone 6/6+, 6s/6s+, SE, iPhone 7/7+, Apple Watch могут оплачивать покупки по технологии NFC («ближняя бесконтактная связь») в сочетании с программой Wallet и Touch ID, а также для платежей в интернете.

2. Беспроводной стандарт ZigBee – спецификация сетевых протоколов верхнего уровня (уровня приложений APS (application support sublayer) и сетевого уровня NWK), использующих сервисы нижних уровней (уровня управления доступом к среде MAC и физического уровня PHY) и регламентированных стандартом IEEE 802.15.4. ZigBee и IEEE 802.15.4 описывают беспроводные персональные вычислительные сети (WPAN).

3. Электрокары Tesla Model S – пятидверные электромобили производства американской компании Tesla Motors. Прототип был впервые показан во Франкфуртском автосалоне в 2009 г.; поставки автомобиля в США начались в июне 2012 г. [17].

Результаты исследования

В настоящее время набирают популярность различные стандарты для управления интернет-вещами. Они предлагают готовые наборы протоколов управления и дают возможность достаточно быстро развернуть свою сеть для управления устройствами [11].

ZigBee – беспроводной стандарт, надстройка IEEE 802.15.4, при помощи которого устройства, подключенные к IoT, связываются друг с другом. Данный стандарт используют для своих устройств Samsung, Philips, Motorola и другие крупные производители. Исследователи венской компании Cognosec обнаружили в ZigBee критический недочет, который способен скомпрометировать любой умный дом.

Основная проблема заключается в том, что производители используют стандартные ключи связи (link key) для своих устройств, в погоне за совместимостью с устройствами других производителей, дешевизной и удобством пользователя. Использование стандартных link keys ставит под угрозу безопасность сети в целом. К тому же сам стандарт ZigBee недостаточно ответственно относится к вопросу безопасности и сохранности ключей, то есть безопасная инициализация и передача зашифрованных ключей внутри сети сильно уязвимы. При помощи простого сниффинга атакующий способен перехватить обмен ключами и внедриться в сеть, используя стандартный link key. В итоге устройства оказываются открыты для MITM-атак, а сеть, активный сетевой ключ и все коммуникации внутри сети – скомпрометированы [16].

После опытов с IoT-лампочками, датчиками движения, датчиками температуры и дверными замками в Cognosec был сделан вывод, что производители оснащают устройства для домашнего использования лишь необходимым минимумом функций, чтобы соответствовать минимальному стандарту. К сожалению, это обычная практика, не оставляющая пользователям выбора, даже если они хотят повысить стандарт безопасности на своем устройстве (хотя бы изменив пароли и установив дополнительное защитное ПО) [17]. По мнению исследователей, эта проблема куда серьезнее недочетов в самом стандарте ZigBee.

С подобными недостатками системы безопасности сталкиваются также обладатели новых электрокаров фирмы Tesla Motors [11].

Например, в сентябре 2016 г. исследователи компании Tencent Keen Security Lab продемонстрировали удаленный взлом Tesla Model S P85 и Model 75D. Как правило, для реализации подобных атак исследователи компрометируют бортовое ПО самого автомобиля, но специалисты норвежской компании Promon решили подойти к вопросу с другой стороны и атаковать Android-приложение.

По умолчанию во время установки официального приложения Tesla владелец автомобиля должен ввести имя пользователя и пароль, для которых приложение сгенерирует ключ OAuth. Впоследствии, когда пользователь вновь обращается к приложению, оно использует данный ключ, поэтому повторный ввод учетных данных не требуется. Приложение удаляет данный ключ после 90 дней использования и повторно запрашивает имя пользователя и пароль.

Исследователи Promon обнаружили, что приложение Tesla хранит ключ OAuth в формате обычного текста в директории sandbox. Следовательно, атакующий способен прочитать ключ, если ему удастся получить доступ к смартфону жертвы [18].

Специалисты пишут, что в настоящее время совсем не сложно создать вредоносное приложение для Android, которое содержало бы root-эксплоиты, например, Towelroot или Kingroot [Там же]. Эксплоиты помогут повысить привилегии приложения в системе,

а затем прочесть или подменить данные других приложений.

Однако просто узнать ключ недостаточно. Заполучив его, злоумышленник сможет проделать с машиной ряд действий, но не сможет ее завести, – для этого необходим пароль владельца. Исследователи придумали, как справиться и с этим: если вредоносное приложение удалит ключ OAuth с устройства жертвы, ей придется вновь ввести имя пользователя и пароль, т. е. у атакующего появится возможность перехватить учетные данные. Исследователи пришли к выводу, что атакующий может без особого труда внести изменения в код приложения Tesla. Если благодаря Malware злоумышленник уже получил root-доступ к устройству, ему будет нетрудно настроить пересылку копии учетных данных владельца автомобиля на свой сервер.

Имея ключ, а также учетные данные от официального приложения Tesla, злоумышленник может направить серверам Tesla правильно составленные HTTP-запросы, используя токен и, если понадобится, имя пользователя и пароль жертвы. В итоге у атакующего появится возможность завести двигатель без ключа, открыть двери, отследить машину и т. д. [Там же].

Бесконтактные системы оплаты с помощью смартфонов также имеют ряд уязвимостей. Рассмотрим в качестве примера самую популярную систему – Apple Pay. Суть ее работы состоит в том, что вместо использования пластиковой карты или наличных средств любую покупку можно оплатить с помощью гаджета Apple. Оплата происходит, когда пользователь подносит свой iPhone или Apple Watch к бесконтактному терминалу. Через несколько секунд на экране появляется сообщение о возможности проведения оплаты и предложение подтвердить транзакцию через сканер отпечатка или пароль.

Система Apple Pay состоит из 4 основных частей:

1. Основной механизм основан на технологии, близкой передачи данных NFC (на расстоянии до 20 см), в связке с чипом Secure Element, который представляет собой индустриальный стандарт в области финансовых операций. На этом чипе выполняется специальное Java-приложение.

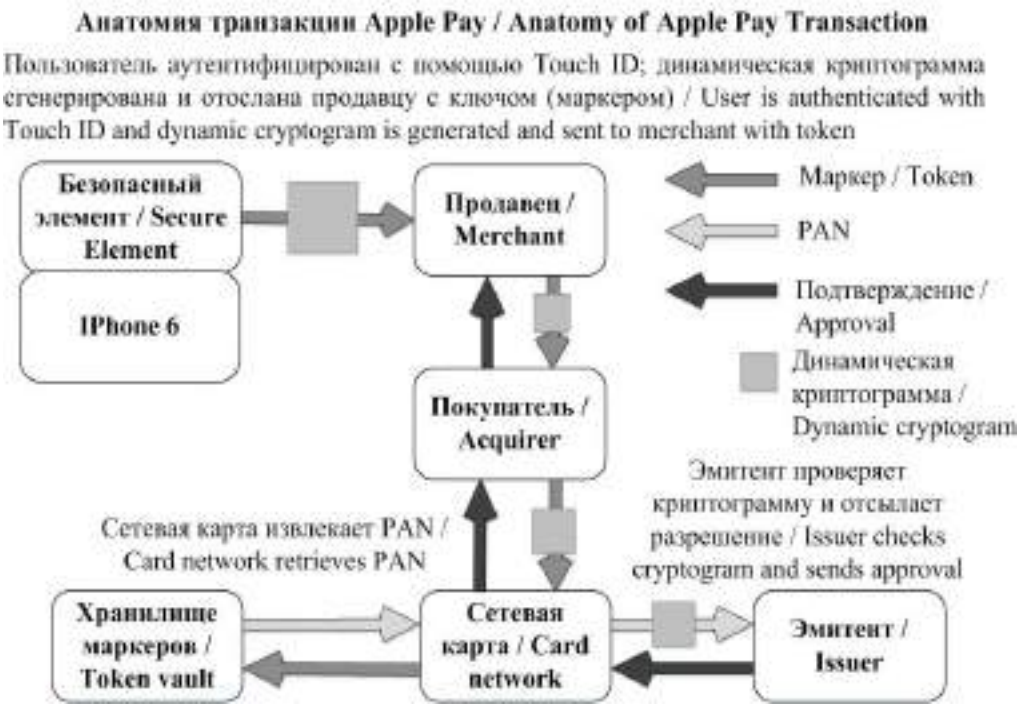
2. Secure Element – область выделенной памяти, отделенной от системной. В этой области хранятся данные банковских карт пользователя в зашифрованном виде. Ни одна программа не имеет к ней доступ, данные никуда не передаются, и даже Apple не может повлиять на эту стратегию.

3. Secure Enclave – компонент, который управляет процессом аутентификации и запускает платежные транзакции, а также хранит отпечаток пальца для Touch ID.

4. Apple Pay Servers – серверная часть, управляющая состоянием кредитных и дебетовых карт в приложении Wallet, вместе с номером устройства, хранящимся в Secure Element. Apple Pay Servers также отвечают за перекодирование платежных сведений внутри приложений.

Apple Pay обладает многоуровневой системой защиты: уникальный идентификатор устройства, динамически генерируемые коды безопасности для каждой платежной транзакции, биометрические сведения – отпечаток пальца [20].

Во время создания подключения устройства обмениваются одноразовыми ключами, которые удаляются при окончании связи. Ключ призван заменить номер карты в целях безопасности и представляет собой сгенерированный случайным образом номер. Номер банковской карты, скрываемым за ним, расшифровке не поддается.



Р и с. 4. Анатомия транзакции Apple Pay
F i g. 4. Anatomy of Apple Pay transaction

Все это заменяет CVV банковской карты для платежной транзакции. После установки связи и обмена ключами для передачи данных они подвергаются шифрованию, информацию об алгоритме которого Apple не раскрывает. Зашифрованные сообщения отражают принадлежность определенному устройству, создавшему используемый ключ.

Даже если ключ будет перехвачен, это не даст злоумышленнику ценной информации, поскольку после разрыва соединения ключ удаляется.

В совокупности эти средства обеспечивают более надежную защиту, чем магнитная полоса и даже чип в банковской карте.

Однако несмотря на усилия разработчиков, в сервисе Apple Pay есть проблемные места, которые во многом зависят не от Apple: в процессе движения средств задействованы другие структуры, в том числе банки с их значительными пробелами в безопасности.

Сканер отпечатков пальцев не всегда работает корректно. Являясь современным и, на первый взгляд, надежным средством удостоверения личности, оно одновременно представляет собой риск для безопасности. Если Touch ID выйдет из строя, можно воспользоваться Pin-кодом, что ликвидирует достижения продвинутой системы безопасности.

При оплате с помощью часов Apple Watch отпечаток не требуется, и в этом случае вопрос о безопасности приобретает особую актуальность. Но вместе с тем транзакция с помощью Apple Watch может быть совершена только в том случае, если часы находятся на запястье владельца.

В связи с этим появились дополнительные инструменты проверки: се-

кретный код, одноразовый пароль, звонок в службу поддержки клиентов или предоставление информации о предыдущих покупках.

Некоторые банки в других странах требуют от пользователя авторизации в мобильном интернет-банкинге. Эти действия уменьшают удобство использования Apple Pay из-за появления дополнительных уровней проверки [20].

В настоящее время в Российской Федерации используется самый простой формат оплаты без дополнительных авторизаций в процессе.

Обсуждения и заключения

В ходе проведенной работы по анализу уязвимостей были сделаны следующие выводы:

1. Ни одна современная система «Умного дома» не является действительно безопасной. Одна из основных причин недостаточного качества информационной безопасности заключается в желании производителей максимально удешевить свои продукты с целью привлечения максимального количества клиентов, которые, как правило, при выборе товара отдают предпочтение не безопасности, а функционалу и цене.

2. Даже такие популярные беспроводные стандарты как ZigBee не лишены уязвимостей. Причины их наличия также заключаются в желании максимально удешевить продукты, соблюдая минимальные требования информационной безопасности.

3. Набирающие популярность электрокары Tesla с возможностью дистанционного управления также имеют ряд проблем с удаленным управлением автомобилем. Риск в данном случае зависит не столько от самого производителя автомобилей, сколько от мобильных устройств, с которых ведется контроль за транспортным средством.

Для подготовки к переходу к всеобъемлющим информационным сетям, включающим технологии типа IoT, на наш взгляд, необходимо решение следующих задач в области информационной безопасности.

1. Оценка уязвимости подключаемых устройств на этапе производственного процесса. К сожалению, в настоящее время в связи с лавинообразным спросом на подобные устройства многие производители не уделяют достаточного внимания данной проблеме;

2. Разработка ПО, отвечающего требованиям безопасности с использованием стандартов разработки безопасных приложений. Кроме этого, необходимо предусмотреть возможность обновления данного ПО.

3. Управление логистикой устройств на всех этапах, от производства до инсталляции на объекте. Данный подход позволит значительно снизить уязвимость в аппаратно-зависимом коде.

На основании проведенного изучения проблем информационной безопасности взаимодействия типа «машина-машина» следует отметить, что в настоящее время не существует достаточного количества стандартов и рекомендаций в области информационной безопасности интернета вещей. Более того, многие рекомендации, касающиеся данной сферы, не могут быть использованы при подключении к глобальным сетям (например, компоненты, применяемые в системе «Умный дом», не предполагают авторизацию и аутентификацию).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. **Найдич А.** «Интернет вещей» – реальность или перспектива? [Электронный ресурс] // КомпьютерПресс, 2013. № 12. URL: http://compress.ru/article.aspx?id=24290

2. **Круз Л.** Интернет вещей и информационная безопасность: защита информации // Инсайд. 2013. № 6. С. 60–61.

3. Интернет вещей: новые вызовы и новые технологии [Электронный ресурс] // Открытые системы. 2013. № 4. URL: http://www.osp.ru/os /2013/04/13035551

4. **Мойл Э.** Пять составляющих безопасности интернета вещей [Электронный ресурс]. URL: http://www.ecommercetimes.com/story/Securing-the-Internet-of Things-5-Easy-Pieces-79438.html

5. **Suo H.** Security in the Internet of Things : A review // Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. 2012. P. 648–651.

6. **Ивлиев С. Н.** Предварительный анализ технической защищенности системы дистанционного образования (на материале Мордовского государственного университета) // Интеграция образования. 2012. № 4 (69). С. 27–31. URL: http://elibrary.ru/item.asp?id=18353911

7. **Ивлиев С. Н.** Решение вопросов технической защиты информации в системе дистанционного образования Мордовского государственного университета // Отраслевые аспекты технических наук. 2012. № 6 (18). С. 13–16. URL: http://elibrary.ru/item.asp?id=18311421

8. **Ивлиев С. Н.** Интернет вещей: новые угрозы информационной безопасности // Проблемы и перспективы развития отечественной светотехники, электротехники и энергетики : мат-лы XII Всерос. науч.-техн. конф. с междунар. участием (г. Саранск, 28–29 мая 2015 г.). Саранск, 2015. С. 435–441. URL: http://elibrary.ru/item.asp?id=24179239

9. Ивлиев С. Н. Решение проблем безопасности информационно-технологического комплекса предприятий светотехнической отрасли на основе международных стандартов // Проблемы и перспективы развития отечественной светотехники, электротехники и энергетики : мат-лы XII Всерос. науч.-техн. конф. с междунар. участием (г. Саранск, 28–29 мая 2015 г.). Саранск, 2015. С. 428–434. URL: http://elibrary.ru/item.asp?id=24179114

10. **Ивлиев С. Н.** Геоинформационные системы и новые угрозы информационной безопасности // Картография и геодезия в современном мире : мат-лы II Всерос. науч.-практ. конф. (г. Саранск, 8 апреля 2014 г.). Саранск : Изд-во Мордов. ун-та, 2014. С. 187–193. URL: http://elibrary.ru/item.asp?id=23934378

11. **Шиков С. А., Ивлиев С. Н.** Интернет вещей: новые угрозы информационной безопасности // Мат-лы XX науч.-практ. конф. молодых ученых, аспирантов и студентов Национального исследовательского Мордовского государственного университета им. Н. П. Огарева : в 3 ч. Саранск, 2016. С. 278–283. URL: http://elibrary.ru/item.asp?id=27222070

12. **Бобылев А. Е., Трофимова А. В.** Проблема защиты данных в интернете вещей [Электронный ресурс]. 2016. № 3. С. 25. URL: Nauka-Rastudent.ru

13. **Бейзер Б.** Тестирование черного ящика: технологии функционального тестирования программного обеспечения и систем. СПб. : Питер, 2004. 320 с.

14. **Петровский А.** Эффективный хакинг для начинающих и не только. 3-е изд. Москва : Майор, 2001. 164 с.

15. **Михайлов Д., Жуков И.** Защита мобильных телефонов от атак. Москва : Фойлис, 2011. 192 с. URL: http://www.samomudr.ru/d2/Mixajlov%20D.%20M.,%20Zhukov%20I.%20Ju.%20-%20Zashita%20mobilnyx%20telefonov%20ot%20atak%20-%202011.pdf

16. **Саттон М., Грин А., Амини П.** Fuzzing: исследование уязвимостей методом грубой силы. СПб. : Символ-Плюс, 2009. 560 с.

17. **Нефедова М.** Уязвимость в ZigBee ставит IoT-устройства под удар [Электронный ресурс]. URL: https://xakep.ru/2015/08/10/zigbee-devices-problems

18. **Нефедова М.** Автомобиль Tesla можно угнать, заразив смартфон его хозяина Malware [Электронный ресурс]. URL: https://xakep.ru/2016/11/25/tesla-android-hack

19. **Юферев С.** Будущее на пороге: Интернет вещей. Военное обозрение [Электронный ресурс]. URL: http://vpk-news.ru/articles/18834

20. **Язев Ю.** Что такое Apple Pay и как он работает на самом деле [Электронный ресурс]. URL: https://www.iphones.ru/iNotes/600660

Поступила 30.11.2016; принята к публикации 08.01.2017; опубликована онлайн 31.03.2017 г.

Об авторе:

Шиков Станислав Александрович, преподаватель кафедры информационной безопасности и сервиса Института электроники и светотехники ФГБОУ ВО «МГУ им. Н. П. Огарёва» (430005, Россия, г. Саранск, ул. Большевистская, д. 68), **OrCId: http://orcid.org/0000-0002-8412-5163**, stenlav@mail.ru

Автор прочитал и одобрил окончательный вариан рукописи.

REFERENCES

1. Naydich A. “Internet veshchey” – realnost ili perspektiva? [Internet of Things – reality or prospect?]. *KompyuterPress* = Computer Press. 2013; 12. Available from: http://compress.ru/article.aspx?id=24290 (In Russ.)

2. Kruz L. Internet veshchey i informatsionnaya bezopasnost: zashchita informatsii [Internet of Things and information security: information security]. *Insayd* = Inside. 2013; 6:60-61. Available from: http://www.cisco.com/c/ru_ru/about/press/press-releases/2013/03-032813c.html (In Russ.)

3. Internet veshchey: novyye vyzovy i novyye tekhnologii [Internet of Things: new challenges and new technologies]. *Otkrytyye sistemy* = Open systems. 2013; 4. Available from: http://www.osp.ru/os/2013/04/13035551(In Russ.)

4. Moyl E. Pyat sostavlyayushchikh bezopasnosti interneta veshchey [Five components of Internet Security]. Available from: http://www.ecommercetimes.com/story/Securing-the-Internet-of Things-5-Easy-Pieces-79438.html (In Russ.)

5. Suo H. Security in the Internet of Things: A review. In: Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. 2012; 648-651.

6. Ivliyev SN. Predvaritelnyy analiz tekhnicheskoy zashchishchennosti sistemy distantsionnogo obrazovaniya (na materiale Mordovskogo gosudarstvennogo universiteta) [Preliminary analysis of technical protection of the system of distant learning (based on Mordovia State University materials)]. *Integratsiya obrazovaniya* = Integration of Education. 2012; 4(69):27-31. Available from: http://elibrary.ru/item.asp?id=18353911 (In Russ.)

7. Ivliyev SN. Resheniye voprosov tekhnicheskoy zashchity informatsii v sisteme distantsionnogo obrazovaniya Mordovskogo gosudarstvennogo universiteta [Addressing the technical protection of information in the system of distance education in Mordovia State University]. *Otraslevye aspekty tekhnicheskikh nauk* = Sectoral Aspects of Technical Sciences. 2012; 6(18):13-16. Available from: http://elibrary.ru/item.asp?id=18311421 (In Russ.)

8. Ivliyev SN. Internet veshchey: novyye ugrozy informatsionnoy bezopasnosti [Internet of Things. New information security challenges]. In: Zheleznikova OYe., editor. Problemy i perspektivy razvitiya otechestvennoy svetotekhniki, elektrotekhniki i energetiki: mat-ly XII Vseros. nauch.-tekhn. konf. s mezhdunar. uchastiyem (g. Saransk, 28-29 maya 2015 g.) [Problems and prospects of development of domestic lighting, electrical engineering and energy: Proceedings of 12th Russian Scientific Engineering Conference, Saransk, May 28-29, 2015]. Saransk, 2015; 435-441. Available from: http://elibrary.ru/item.asp?id=24179239 (In Russ.)

9. Ivliyev SN. Resheniye problem bezopasnosti informatsionno-tekhnologicheskogo kompleksa predpriyatiy svetotekhnicheskoy otrasli na osnove mezhdunarodnykh standartov [Solving the security problems of information-technological complex of lighting industry enterprises based on international standards]. In: Problemy i perspektivy razvitiya otechestvennoy svetotekhniki, elektrotekhniki i energetiki: mat-ly XII Vseros. nauch.-tekhn. konf. s mezhdunar. uchastiyem (g. Saransk, 28-29 maya 2015 g.) [Problems and prospects of development of domestic lighting, electrical engineering and energy: Proceedings of 12th Russian Scientific Engineering Conference, Saransk, May 28-29, 2015]. Saransk, 2015; 428-434. Available from: http://elibrary.ru/item.asp?id=24179114 (In Russ.)

10. Ivliyev SN. Geoinformatsionnyye sistemy i novyye ugrozy informatsionnoy bezopasnosti [Geographic information systems and new information security challenges]. In: Kartografiya i geodeziya v sovremennom mire: materialy II Vseros. nauch.-prakt. konf. (g. Saransk, 8 aprelya 2014 g.) [Cartography and Geodesy in the Modern World: Proceedings of 2nd Russian Scientific-Practical Conference (Saransk,

April 8, 2014)]. Saransk: Mordovia State Univercity Publ.; 2014:187-193. Available from: http://elibrary.ru/item.asp?id=23934378 (In Russ.)

11. Shikov SA, Ivliyev SN. Internet veshchey: novyye ugrozy informatsionnoy bezopasnosti [Internet of Things: New information security threats]. In: Materialy XX nauch.-prakt. konf. molodykh uchenykh, aspirantov i studentov Natsionalnogo issledovatelskogo Mordovskogo gosudarstvennogo universiteta im. N. P. Ogareva [Proceedings of 20th Scientific-Practical Conference of Young Scientists and Students of National Research Mordovia State University]. Saransk: Mordovia State Univercity Publ.; 2014; 278-283. Available from: http://elibrary.ru/item.asp?id=27222070 (In Russ.)

12. Bobylev AYe, Trofimova AV. Problema zashchity dannykh v internete veshchey. 2016; 3:25. Available from: http://nauka-rastudent.ru/27/3279 (In Russ.)

13. Beyzer B. Testirovaniye chernogo yashchika: tekhnologii funktsionalnogo testirovaniya programmnogo obespecheniya i system [Black Box testing: Functional testing technology software and systems]. St. Petersburg: Piter; 2004. (In Russ.)

14. Petrovskiy A. Effektivnyy khaking dlya nachinayushchikh i ne tolko [Effective hacking for beginners and not only]. 3rd ed. Moskva: Mayor; 2001. (In Russ.)

15. Mikhaylov D, Zhukov I. Zashchita mobilnykh telefonov ot atak [Protecting mobile phone from attacks]. Moscow: Foylis, 2011. Available from: http://www.samomudr.ru/d2/Mixajlov%20D.%20M.,%20Zhukov%20I.%20Ju.%20-%20Zashita%20mobilnyx%20telefonov%20ot%20atak%20-%202011.pdf (In Russ.)

16. Satton M, Grin A, Amini P. Fuzzing: issledovaniye uyazvimostey metodom gruboy sily [Fuzzing: vulnerability research brute force]. St. Petersburg: Simvol-Plyus; 2009. (In Russ.)

17. Nefedova M. Uyazvimost v ZigBee stavit IoT-ustroystva pod udar [Vulnerability in the ZigBee device puts IoT-pass]. Available from: https://xakep.ru/2015/08/10/zigbee-devices-problems (In Russ.)

18. Nefedova M. Avtomobil Tesla mozhno ugnat, zaraziv smartfon ego khozyaina Malware [To steal a car Tesla is necessary to infect a smartphone of its owner]. Available from: https://xakep.ru/2016/11/25/tesla-android-hack (In Russ.)

19. Yuferev S. Budushcheye na poroge: Internet veshchey [Future on threshold: Internet of Things]. *Voennoye obozreniye* = Military review. Available from: http://vpk-news.ru/articles/18834 (In Russ.)

20. Yazev Yu. Chto takoe Apple Pay i kak on rabotaet na samom dele [What is Apple Pay and how it actually works]. Available from: https://www.iphones.ru/iNotes/600660 (In Russ.)

Submitted 30.11.2016; revised 08.01.2017; published online 31.03.2017

About the author:

Stanislav a. Shikov, Lecturer of Information Security and Service Chair, Institute of Electronics and Lighting Engineering, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russia), **OrCId: http://orcid.org/0000-0002-8412-5163** , stenlav@mail.ru

The author have read and approved the final manuscript.