ИНФОРМАТИКА
ИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 004.056:004.384

Уязвимости системы "Умный дом"

А. В. Вольвач, Н. С. Поддубная
Московский государственный технический университет гражданской авиации
Россия, 125493, г. Москва, Кронштадтский б-р, 20
poddubnaya1999@bk.ru; +79852120431

Рассмотрены существующие уязвимости системы "Умный дом". Определены характерные уязвимости информационной безопасности некоторых устройств, входящих в систему "Умный дом". Предложены методы повышения информационной безопасности систем "Умный дом".

Ключевые слова: *аутентификация; защита информации; информационная безопасность; несанкционированный доступ; уязвимость.*

DOI: 10.17072/1993-0550-2021-1-49-52

Введение

Концепция "Интернет вещей" базируется на повсеместном внедрении следующих технологий: беспроводные сети, облачные вычисления, межмашинное взаимодействие. Данная концепция набирает популярность, потому что направлена, в первую очередь, на повышение комфорта каждого человека начиная от смартфона, который может проверять почту и сигнализировать о новых сообщениях в социальных сетях и заканчивая беспилотным автомобилем [1].

По мере того, как IoT все больше проникает в повседневную жизнь людей, возрастают и риски информационной безопасности. В реалиях современного информационного пространства риски, связанные с использованием технологий IoT, актуальны для всех пользователей.

1. Информационная безопасность IoT

С точки зрения информационной безопасности "Интернет вещей" несет в себе риски, связанные, в первую очередь, с личными данными человека. Например, сенсоры в системе "Умный дом" отслеживают передвижения человека по дому и корректируют освещение, служба такси при вызове получает данные о местоположении от смартфона, с которого осуществляется вызов, "умные часы контролируют пульс и могут вызвать "скорую", если человеку будет плохо, браузер собирает информацию о страницах, которые посещал человек и т.д. Вся эта информация накапливается и предоставляется различным сервисам, облегчающим жизнь человека. Добавление к этим данным сведений о банковских реквизитах, медицинских данных формирует достаточно полное досье на человека [2].

Уязвимости системы "Умный дом"

В ходе анализа технологии концепции "Интернет вещей" более подробно рассматриваются уязвимости системы "Умный дом". Умный дом – это автоматизированное строение современного типа, организованное для удобства людей при помощи высокотехнологичных устройств. Это может быть не только жилой дом, но также и государственное учреждение, стадион и даже аэропорт.

В умном доме одно устройство может управлять поведением других устройств по заранее выработанным алгоритмам.

Главной особенностью интеллектуального здания является объединение отдельных устройств в единый управляемый комплекс [3].

При анализе уязвимостей системы "Умный дом" было выявлено следующее:

1. Отсутствие механизма аутентификации санкционированного пользователя.

Управление компонентами системы "Умный дом" должно вестись только после аутентификации пользователя и его дальнейшей авторизации. Ввиду того, что управление наиболее часто производится со смартфона или с другого портативного устройства, соединяющегося посредством беспроводной связи, возникает угроза перехвата идентификационных и (или) аутентификационных данных третьими лицами. Перехват может быть реализован через внедрение вредоносного программного обеспечения в устройства системы "Умный дом", использование существующих уязвимостей программного обеспечения устройств, прослушивание канала связи управляющего устройства (например, смартфона пользователя системы "Умный дом") с устройствами системы "Умный дом" и т.д. Отсутствие механизма аутентификации санкционированного пользователя подтверждается существованием программных средств, с помощью которых можно получить несанкционированный доступ к устройствам системы "Умный дом".

Примерами таких программных средств являются Shodan [2] и Censys [4]. Их практическое применение представлено в статье "IoT Privacy and Security Challenges for Smart Home Environments", п. 4.3 "Vulnerability Example" [5].

2. Полноценных антивирусных систем, обеспечивающих комплексную защиту от вредоносного программного обеспечения, разработанных специально для систем умного дома, не существует [6]. Более того, программный код, свойственный вирусам для систем "Умного дома", не опознается большинством сканеров сигнатур [7].

Рассмотрим основные уязвимости в программном обеспечении систем "Умного дома", которыми пользуются злоумышленники для внедрения вредоносных программ:

♦ отсутствие возможности блокировки подключений неавторизованных устройств;

♦ отсутствие контроля над широковещательной рассылкой датаграмм в сети "Умного дома";

♦ отсутствие проверки подлинности управляющей программы, передающей пакеты в сеть "Умного дома".

3. Необходимость наличия защищенных каналов связи.

Использование симметричных криптографических систем, дистанционное управление устройствами (например, со смартфона), обновление программного обеспечения устройств, преимущественное использование беспроводной связи для коммуникации устройств друг с другом – все это требует наличия защищенных каналов связи в системе "Умный дом". Недобросовестная реализация протоколов защиты информации на одном из устройств может привести к компрометации всех данных, циркулирующих в системе. Так, каналам связи свойственны следующие уязвимости:

– канал Bluetooth является крайне ненадежным и легко может принять файл с вирусом от злоумышленника, не запросив аутентификационных данных;

– по каналу Wi-Fi злоумышленник может авторизоваться во внутренней сети Wi-Fi "Умного дома" и внедрить вредоносное программное обеспечение;

– уязвимости HTTP-канала, по которому устройства из системы "Умный дом" связываются с внешней сетью Интернет, хорошо изучены и могут позволить злоумышленнику получить контроль над "Умным домом", даже не находясь в его локальной сети;

– через канал GSM злоумышленник может отправить управляющие команды "Умному дому", подменив свой номер номером санкционированного пользователя;

– если сеть "Умного дома" также находится и в другой локальной сети, то вредоносное ПО также может быть внедрено из последней.

4. Потенциальные уязвимости системы "Умный дом" ввиду функционирования в ней устройств от разных производителей.

Разные компании разрабатывают аналогичные устройства с возможным использованием своих собственных внутренних (нестандартизированных) протоколов обмена данными. Ввиду этого, внедрение устройств от

разных производителей в систему "Умный дом" влечет за собой потенциальное наличие уязвимостей информационной безопасности (например, некорректная реализация защищенного соединения между двумя устройствами).

Такая проблема может быть решена приобретением готовой системы у одного производителя. Однако, во-первых, компаний, производящих полноценную систему "Умный дом", на данный момент на рынке представлено мало; во-вторых, как показали недавние исследования независимой организации AV-TEST в области информационной безопасности IoT [8], у многих производителей уровень защищенности систем "Умный дом" находится на низком уровне.

5. Наличие свойственных определенным устройствам уязвимостей.

Устройства системы "Умный дом" обладают различным функционалом и набором выполняемых задач. Соответственно, устройства имеют и различные уязвимости:

– Smart TV. Большинство современных Smart-телевизоров оснащены камерами. При недостаточной защищенности системы "Умный дом" злоумышленники могут использовать данные камеры для слежения за пользователями данной системы и помещением в целом;

– Smart fridges. Холодильники в "Умном доме" проверяют срок годности продукции, анализируют хранящуюся в нем пищу и составляют список продуктов, которые необходимо будет купить хозяину дома. Получив контроль над этими данными, нарушитель может узнать, в какое время в доме находятся люди, а когда их нет, способствуя тем самым своему последующему проникновению в дом;

– Smart Cars. Согласно последним исследованиям, злоумышленники могут получить контроль над операционными системами "умных" устройств. Таким образом, они могут осуществлять управление всеми компонентами системы;

– система автоматизированного управления домом. Она является главной системой "Умного дома", обеспечивая контроль, в том числе, за дверьми, окнами, внешними и внутренними камерами, а также сигнализациями. Получив контроль над ней, нарушитель может абсолютно бесследно произвести физическое проникновение на территорию дома.

2. Методы повышения защищенности системы "Умный дом"

На основе проведенного анализа уязвимостей системы "Умный дом" рекомендуется следующее:

– устанавливать пароль высокой сложности на профиль администратора системы;

– своевременно обновлять ПО устройств системы "Умный дом" до последней версии;

– внедрять системы слежения за несанкционированным доступом в систему "Умный дом";

– настраивать сети VPN для системы "Умный дом";

– устанавливать межсетевые экраны (файрволы) на границе локальной сети системы "Умный дом", а также настраивать антивирусное ПО под свои потребности;

– использовать решения для системы "Умный дом" от одного производителя для избежания потенциальных уязвимостей [9].

Список литературы

1. *Борисов М.В., Иванов А.П.* Актуальные угрозы информационной безопасности интернета вещей // Современные тенденции развития науки и технологий. 2017. № 1–1. С. 23–25.
2. *Shodan*: поисковик сетевых устройств в сети Интернет. URL: https://www.shodan.io.
3. *Кусакин И.И.* Программно-аппаратный комплекс автоматизированного контроля целостности инфраструктуры. жилых помещений для. социального обеспечения // XV Междунар. телекоммуникационная конф. молодых ученых и студентов "Молодежь и наука": тез. докл. В 3 ч. М.: НИЯУ МИФИ. 2012. Ч. 3. С. 156–157.
4. *Censys:* поисковик сетевых устройств в сети Интернет. URL: https://censys.io.
5. *IoTPrivacyandSecurity* Challenges for Smart Home Environments. Базель, Швейцария, 2016. URL: https://www.mdpi.com/2078-2489/7/3/44/htm (дата обращения: 04.12.2020).
6. *Касперски К.* Записки исследователя компьютерных вирусов. С-Пб.: Питер, 2006. 216 с.
7. *Аристов М.С.* Антивирусный программно-аппаратный комплекс для систем автоматизированного здания // XIV Междунар.

телекоммуникационная конф. молодых ученых и студентов "Молодежь и наука": тез. докл. В 3 ч. М.: НИЯУ МИФИ, 2011. Ч. 3. С. 151–152.
8. *AV-TEST:* Test: Smart Home Kits Leave the Door Wide open – for Everyone. URL: https://www.avtest.org/en/news/test-smart-home-kits-leave-the-door-wide-open-for-everyone (дата обращения: 04.12.2020).
9. *Безопасный* умный дом: сложная технология, полезная каждому. URL: http://news.ifmo.ru/ru/startups_and_business/star tup/news/5832/ (дата обращения: 04.12.2020).

Vulnerabilities in Smart Home system

A. V. Volvach, N. S. Poddubnaya
Moscow State Technical University of Civil Aviation; 20, Kronstsdt blv., Moscow, 125493, Russia
poddubnaya1999@bk.ru; +79852120431

The article considers the existing vulnerabilities in the Smart Home system. The characteristic vulnerabilities in information security of some devices included in the Smart Home system are determined. The methods to improve information security of Smart Home systems are proposed.

Keywords: *authentication; information protection; information security; unauthorized access; vulnerability.*