БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 4 (103). – 20–36

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2021-4-20-36

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ»*

И.Л. РЕВА[1], А.Б. АРХИПОВА[2], Р.В. САМОЙЛЕНКО[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: reva@corp.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: ro999@yandex.ru*

Идея умных домов существует уже несколько десятилетий и с тех пор неоднократно описывалась разными авторами. Однако в определениях последних 20 лет почти всегда присутствуют три аспекта. Во-первых, домашние устройства должны быть подключены не только друг к другу, но также и к Интернету. Во-вторых, необходим интеллектуальный способ управления системой, например, центральный шлюз или интеллектуальные приложения для смартфонов. Наконец, в системе должна быть определенная степень домашней автоматизации. Программно-аппаратный комплекс, удовлетворяющий данным требованиям, можно назвать системой «умного дома». Важное практическое значение имеет сейчас система обеспечения безопасности «умного дома», которая должна включать в себя меры по защите IT-инфраструктуры, обеспечивающие личную безопасность жителей, их здоровья, санитарного состояния помещения, а также сохранность материальных ценностей. Из этого следует, что довольно актуальной является проблема отсутствия тщательного исследования угроз информационной безопасности и проработки защиты всего программно-аппаратного комплекса системы «умный дом». При решении данной задачи в статье проведен анализ основных типов и характеристик системы «умный дом», выявлены их ключевые уязвимости. Также проведено исследование уязвимостей аппаратного обеспечения системы «умный дом». Проведена качественная оценка рисков информационной безопасности умного дома и выработаны защитные меры для их снижения; разработан и исследован прототип фрагмента системы безопасности «умный дом». При экспериментальном исследовании угроз и уязвимостей

* Статья получена 01 ноября 2021 г.

разработанного прототипа фрагмента системы «умный дом» была подробно изучена угроза перехвата критически важной информации системы. По результатам разработки и исследования «Инспектора безопасности» были сделаны выводы об эффективности применения модуля обнаружения вторжения.

Ключевые слова: информационная безопасность, безопасность системы «умный дом», модель угроз, оценка рисков, инспектор безопасности, система обнаружения вторжения, система безопасности, критически важная информационная система

ВВЕДЕНИЕ

Процессы цифровизации потребностей населения страны обусловлены чрезвычайно стремительным распространением и развитием устройств IT-инфраструктуры, которые успешно применяются для обеспечения комфортного быта граждан в многоквартирных и частных домах.

IT-технологии дают возможность создать умный дом, который представляет собой комплекс программно-аппаратных систем, непосредственно управляющих всеми компонентами инженерных коммуникаций, реализованных в жилом помещение. Согласно исследованиям компании IDC, на 2020 год объем мирового рынка устройств для умного дома составил 801,5 млн штук, увеличившись по сравнению с 2019 годом на 4,5 %. В отчете IDC отмечено, что рынок оборудования для умного дома будет сохранять положительную динамику до 2025 года и к концу периода превысит 1,4 млрд единиц [1]. Однако важно учитывать, что информация, хранящаяся и используемая в системах автоматизации жилого помещения, является частью индивидуальной критической информационной инфраструктуры, поэтому чем больше растет популярность умного дома, тем серьезнее становится проблема информационной безопасности такого комплекса.

Важное практическое значение обеспечения безопасности умного дома имеют меры по защите IT-инфраструктуры, обеспечивающие личную безопасность жителей, их здоровья, санитарного состояния помещения, а также сохранность материальных ценностей.

Из этого следует, что довольно актуальной является проблема отсутствия тщательного исследования угроз информационной безопасности и проработки защиты всего программно-аппаратного комплекса системы «умный дом». Всё больше появляется случаев, когда реальные устройства были скомпрометированы, что демонстрирует важность обеспечения высокой безопасности в этой области. Fernandes использовали несколько уязвимостей в Samsung SmartThings с сопутствующими приложениями, например, чтобы отключить определенные функции и вызвать ложную пожарную тревогу [2]. Schwartz провели тестирование методом «черного ящика» на 16 устройствах умного

дома и восстановили пароли на восьми из них [3]. Более того, были дополнительные сообщения о взломах реальных пользователей и компаний. Эти атаки варьируются от получения доступа к радионяням до доступа к внутренним серверам казино через аквариумный термометр. Поэтому очевидной становится работа, связанная с исследованием вопросов в области защиты информации устройств умного дома.

1. ОСНОВНАЯ ИДЕЯ

Идея умных домов существует не менее 70 лет и с тех пор неоднократно определялась разными авторами [4–8]. Однако в определениях последних 20 лет почти всегда присутствуют три аспекта. Во-первых, домашние устройства должны быть подключены не только друг к другу, но также и к Интернету. Во-вторых, необходим интеллектуальный способ управления системой (например, центральный шлюз или интеллектуальные приложения для смартфонов). Наконец, в системе должна быть определенная степень домашней автоматизации.

Программно-аппаратный комплекс, удовлетворяющий данным требованиям, можно назвать системой «умный дом».

В умных домах в основном используются три разных типа устройств – датчики, исполнительные механизмы и смешанные устройства. Датчики (например, термометры, датчики света или кнопочные переключатели) предоставляют информацию о реальном мире в сеть умного дома. Приводы (например, лампочки, интеллектуальные замки или кофеварки) берут за основу эту информацию и выполняют действия в соответствии с некоторыми предустановленными правилами автоматизации или ручными инструкциями. Наконец, смешанные устройства – это более мощные устройства с датчиками и исполнительными механизмами (например, развлекательные системы или системы наблюдения). В дополнение к этому в большинстве типов умных домов есть центральный шлюз, который соединяет дом и позволяет устройствам обмениваться данными. Персональные компьютеры и смартфоны обычно не считаются устройствами умного дома.

Если рассматривать систему «умный дом» как объект защиты информации, то его можно представить как помещение, оборудованное комплексом средств вычислительной техники, с использованием информационных технологий, которые способны функционировать автоматически, решая задачу обеспечения комфортного и безопасного проживания человека (рис. 1).

Вышеуказанная IT-система способна анализировать потребности человека и подстраиваться под них путем формирования и сохранения условий для повседневной жизнедеятельности человека, а также обеспечения личной

защищенности, уменьшения вероятности причинения вреда здоровью граждан и их материальным ценностям. Из этого можно сделать вывод, что целью управления системой «умный дом» является поддержание условий проживания, которые отвечают всем требованиям безопасности, а также обеспечение необходимого уровня комфорта, что достигается путем проактивного управления инженерными коммуникациями внутри здания, в том числе посредством взаимодействия с окружающей средой.

Рис. 1. Типовая система «умный дом»

Fig. 1. Typical Smart Home System

2. СТРУКТУРА УМНОГО ДОМА

Использование программно-аппаратного комплекса «умный дом» дает возможность гарантировать комфортную и высокоэффективную эксплуатацию, избежать риска причинения ущерба, вызывающего отказ или поломки всех систем жизнеобеспечения здания.

Выше подчеркивалось, что понятие «умный дом» объединяет в себе помещения в зданиях разнообразного назначения с целостной IT-системой кон-

троля состояния всех подсистем, обеспечивающих безопасность и комфортное нахождение в здание.

На рис. 2 более подробно изображена структура системы «умный дом».

Рис. 2. Структура и основные модули системы «умный дом»

Fig. 2. Smart home system structure and main modules

Есть несколько способов объединить все системы жизнеобеспечения и создать умный дом, удобный для эксплуатации конечным пользователем. Наиболее популярны четыре архитектуры, используемые для умных домов, каждая из которых имеет свои недостатки и преимущества [9].

3. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ УМНОГО ДОМА

В этом разделе проанализированы различные атаки на систему «умный дом» и классифицированы по требованиям безопасности, на которые они нацелены. Мы ориентируемся на три основных требования:

– конфиденциальность;

– целостность;

– доступность.

Согласно статистическим исследованиям компании Dr.WEB, за последние годы прослеживается динамично увеличение атак на подобные системы, результат приведен на рис. 3.

В контексте анализа умного дома под конфиденциальностью подразумевается такое состояние IT-системы управления умным домом, при котором отсутствует возможность утечки информации через подсистемы. Пример реализации угрозы – утечка персональной информации или утечка информации о конфигурации IT-систем умного дома.

Рис. 3. Динамика зафиксированных атак на устройства интернета вещей согласно статистическим исследованиям компании Dr.WEB

Fig. 3. Dynamics of recorded attacks on the Internet of Things devices according to the statistical studies of Dr.WEB

Целостность информации – это достоверность и полнота информации, получаемая системой от различных датчиков и устройств, установленных в системе. Например, при получении неверной информации о присутствии в помещении человека происходит ложное срабатывание системы контроля доступа.

Доступность информации применительно к умному дому – это состояние информации или ресурсов IT-системы, при котором субъекты или сама система, имеющие права доступа, могут реализовать различные действия в соответствии со сценарием работы (выключать / включать датчики, открывать замки и т. д.).

Проанализировав все возможные варианты угроз информационной безопасности умного дома, можно составить перечень наиболее возможных, тем самым создав модель угроз (табл. 1), которая в дальнейшем будет использоваться для оценки рисков.

Таблица 1

Table 1

Модель угроз информационной безопасности умного дома

Smart home information security threat model

№	Тип атаки	Уязвимость	Возможные последствия
1	Хакерские атаки на центральный сервер	Подключение сети умного дома к Интернету. Отсутствие (неэффективность) механизмов защиты периметра сети	Нарушение работы либо выход из строя центрального сервера, а следовательно, и всей системы. Нарушение конфиденциальности, целостности и доступности информации (КЦД)

Продолжение табл. 1

Continuation of the Tab. 1

№	Тип атаки	Уязвимость	Возможные последствия
2	Влияние вирусных и троянских программ на работу системы	Подключение сети умного дома к Интернету. Отсутствие (неэффективность) механизмов защиты периметра сети	Сбои в ПО системы, а следовательно, нарушение работы либо вывод из строя аппаратуры системы. Нарушение КЦД информации, находящейся внутри сети
3	Перехват информации, передаваемой по проводным и беспроводным каналам связи	Возможность доступа злоумышленника к проводным каналам или к зоне устойчивого перехвата радиосигналов сети. Отсутствие (неэффективность) механизмов защиты трафика	Нарушение конфиденциальности информации, передаваемой по каналу. Возможен захват управления системой
4	Доступ злоумышленника с правами администратора на центральный сервер с помощью хищения паролей и других реквизитов разграничения доступа	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
5	Доступ к сети неавторизованных пользователей	Отсутствие (неэффективность) механизмов аутентификации и идентификации	Нарушение КЦД информации, находящейся внутри сети
6	Наличие нарушителей в числе обслуживающего персонала (охранники, наладчики, уборщики и др.)	Отсутствие (неэффективность) организационных мероприятий по отбору и контролю за персоналом	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного обслуживания оборудования. Уровень опасности зависит от степени доступа инсайдера к системе
7	Ошибки пользователя	Отсутствие (неэффективность) механизмов защиты системы от неправильных действий пользователей	Нарушение КЦД информации. Возможны сбои в системе из-за неправильного использования оборудования

Окончание табл. 1

End of the Tab. 1

№	Тип атаки	Уязвимость	Возможные последствия
8	Кража (злоумышленный вывод из строя аппаратуры) системы «умный дом»	Отсутствие (неэффективность) – физической охраны объекта	Нарушение КЦД информации
9	Перебои в сети электропитания	Отсутствие системы автономного электропитания	Дезорганизация работы системы
10	Стихийные бедствия (пожар и др.)	Отсутствие (неэффективность) механизмов защиты	Дезорганизация работы системы
11	Поломка аппаратуры системы	Низкая надежность оборудования, низкая квалификация персонала	Нарушение КЦД информации
12	Ошибки программного обеспечения	Использование нелицензионного ПО, низкая квалификация персонала, отсутствие (неэффективность) тестирования закупаемого ПО	Нарушение КЦД информации
13	Утечка информации через побочные электромагнитные излучения и наводки (ПЭМИН)	Наличие ПЭМИ компьютерной техники. Выход проводников, в которых могут быть наводки излучений, за пределы контролируемой зоны	Нарушение конфиденциальности информации, обрабатываемой на ЭВМ
14	Утечка информации по акустоэлектрическому каналу	Наличие акустоэлектрических преобразователей (датчики ОС, ПС)	Нарушение конфиденциальности информации

4. ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УМНОГО ДОМА

Угрозы информационной безопасности IT-системы «умный дом» в первую очередь зависят от выбранных способов и технологий построения данной системы, так как на определение возможных угроз влияет состав оборудования. Для оценки рисков информационной безопасности умного дома использовались угрозы, представленные в предыдущих разделах. Их реализа-

ция может привести к нарушению информационной безопасности умного дома, построенного по классической технологии.

При оценке рисков системы умного дома использовался качественный метод для обоснования и оценки угроз, их привязки к уязвимостям системы, определения вероятности их возникновения и потенциального влияния на всю систему умного дома. Во время проведения оценки рисков оценивалась соответствующая вероятность и воздействие, связанные с каждой идентифицированной угрозой, по пятиуровневой шкале (1–5), после чего рассчитывалось значение риска.

Для анализа применялся подход на основе анализа угроз безопасности информационных систем, уязвимостей и уровней риска. Следовательно, архитектура умного дома рассматривается по аналогии с информационной системой и, таким образом, разделяется на подкатегории, содержащие программное обеспечение, оборудование, информацию (или данные), протоколы связи (включая радиосвязь) и людей (в качестве конечных пользователей или представителей, например поставщиков).

При анализе можно разделить систему на следующие шесть частей:

- подключенные датчики / устройства (S);
- внутренний шлюз (GW);
- облачный сервер (CS);
- API (API);
- мобильное устройство;
- приложения для мобильных устройств.

Каждая из вышеперечисленных частей была проанализирована в поисках уязвимостей и угроз, связанных с оборудованием, программным обеспечением, информацией, коммуникациями и человеческими аспектами в структурированном виде. Если риск был идентифицирован, ему присваивался уникальный дескриптор (идентификатор).

Каждый риск представлен следующими шестью атрибутами: уникальным идентификатором, объяснением уязвимости, объяснением угрозы, значением вероятности, значением стоимости последствий и в результате значением риска. Значения как вероятности, так и последствий рассчитываются с использованием анализа статистических данных атак на информационную систему. Значения риска были рассчитаны путем умножения средней вероятности и значений последствий, что дает значение риска в диапазоне 1…25. Однако самые низкие значения риска, измеренные в этом исследовании, составили 3,5, а самые высокие – 15,44. Более подробная информация о значениях риска, вероятности и последствий представлена в табл. 2.

Таблица 2

Table 2

Минимальное и максимальное значения вероятности, последствий и риска

Minimum and maximum values of probability, consequences and risk

Исследуемый параметр	Минимум	Максимум
Значение вероятности	1.0	4,75
Значение последствий	2.0	4.0
Значение риска	3.5	15,44

Исходя из значений риска каждый риск можно отнести к одному из следующих трех классов серьезности: низкий, средний, высокий. Классы серьезности были определены следующим образом:

- низкий, если значение риска < 6, т. е. событие маловероятно или риск имеет незначительное влияние;
- средний, если значение риска ≥ 6 и значение риска < 10;
- высокий, если значение риска ≥ 10.

Таким образом, что касается пятиуровневой шкалы, низкий риск требует, чтобы один из факторов вероятность / воздействие был низким или, если они равны, оба должны быть ниже 2,5. Средний риск включает два самых высоких значения для одного из факторов вероятности / воздействия, только если другой фактор ниже 3,0. Высокий риск требует, чтобы оба фактора были выше 3. Из 32 рисков 9 были классифицированы как низкие, 19 как средние и 4 как высокие по степени серьезности. В табл. 3 показана классификация серьезности каждого риска, разделенного на шесть категорий подсистем, а также на пять категорий угроз. Категория угроз, которая включает в себя большинство рисков, – это категория, связанная с программным обеспечением, которая включает 13 рисков. Категории угроз, касающиеся информации, коммуникации и человека, содержат по 5 рисков каждая, в то время как аппаратные угрозы содержат 4 риска. Наиболее серьезные риски встречаются в категории людей.

В табл. 3 представлена классификация серьезности риска на низкий / средний / высокий на основе соответствующего значения риска. Риски разделены на пять столбцов, по одному для каждой категории угроз, и шесть строк, по одной для каждой категории подсистем.

Таблица 3

Table 3

Классификация серьезности риска

Classification of risk severity

Идентификатор	Программное обеспечение	Аппаратное обеспечение	Информация	Передача данных	Человек
Датчики / устройства	0 / 0 / 0	0 / 1 / 0	1 / 0 / 0	1 / 0 / 0	N / A
Шлюз	0 / 3 / 0	0 / 1 / 0	0 / 2 / 0	0 / 1 / 0	N / A
Облачный сервер	0 / 1 / 0	1 / 0 / 0	1 / 0 / 0	0 / 1 / 0	N / A
Мобильные устройства	1 / 0 / 0	1 / 0 / 0	1 / 0 / 0	1 / 0 / 0	N / A
Программы	0 / 3 / 1	0 / 0 / 0	0 / 0 / 0	0 / 0 / 0	N / A
API	0 / 4 / 0	0 / 0 / 0	0 / 0 / 0	1 / 0 / 0	N / A
Общее	1 / 11 / 1	2 / 02 / 0	3 / 2 / 0	3 / 2 / 0	0 / 2 / 3

5. РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОТОТИПА ФРАГМЕНТА ЗАЩИТЫ СИСТЕМЫ «УМНЫЙ ДОМ»

В этом разделе описывается процесс разработки модуля безопасности для обнаружения вредоносной активности в сети умного дома, так как выявление атак является первоочередной и наиболее проблемной задачей. Модуль мы называли «Инспектор безопасности», он интегрирован с популярной платформой Smart Hub, использующей открытый исходный код. Описана структура Security Supervisor (Инспектор безопасности) и то, как она взаимодействует с Home Assistant на абстрактном уровне, также описана фактическая реализация системы защиты.

При создании прототипа фрагмента защиты системы «умный дом», был использован интеллектуальный концентратор в качестве места для размещения диспетчера безопасности. Было проанализировано несколько умных хабов и выбран Home Assistant из-за его популярности, доступности и открытости. Таким образом, был разработан диспетчер безопасности так, чтобы он соответствовал архитектуре Home Assistant, даже несмотря на то что общие

принципы программного обеспечения можно адаптировать к любой системе интеллектуального концентратора.

Как уже отмечалось выше, модуль ориентирован на обнаружение угроз безопасности системы «умный дом», в дальнейших исследованиях при успешных испытаниях «Инспектора безопасности» планируется изучить возможные реакции системы на обнаруженные атаки и разработать оптимальный способ их предотвращения.

Home Assistant имеет простую модульную архитектуру программного обеспечения (рис. 4) [13]. Он состоит из центрального ядра, пользовательского интерфейса, домашней автоматизации и компонентов для связи с интеллектуальными устройствами в доме. На рис. 4 заштрихованные области – части исходного кода Home Assistant, а незаштрихованные – внешние библиотеки и физические устройства.

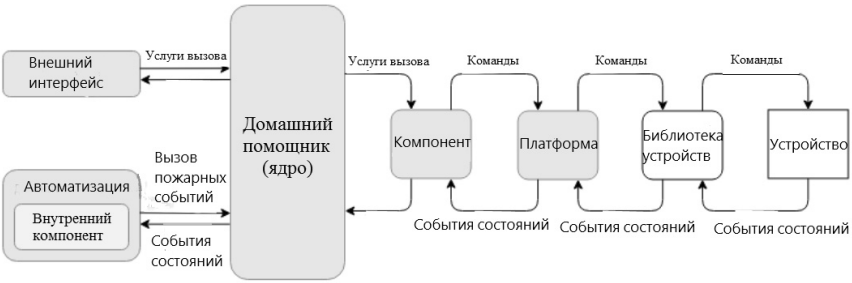

Рис. 4. Архитектура домашнего помощника [13]

Fig. 4. Home Assistant Architecture [13]

Ядро Home Assistant состоит из Event Bus и State Machine. Event Bus позволяет другим частям Home Assistant активировать и прослушивать события, чтобы сообщать об изменениях друг другу. State Machine хранит текущее состояние умного дома, и изменения состояний упрощаются с помощью событий, отправляемых по шине EventBus.

Связь с устройствами умного дома осуществляется через компоненты и платформы. Компоненты объекта – это элементы, которые обеспечивают связь с определенным типом устройства (например, светом или переключателем). Они содержат общие функции для типа устройства. Платформы расширяют компоненты сущности, чтобы они были совместимы с устройствами определенных марок. Фактическая связь с устройством осуществляется через внешние сторонние библиотеки. Платформы передают команды, состояния и события этим библиотекам через вызовы API. Модульность, обеспечивае-

мая компонентами сущностей и платформами, упрощает разработчикам добавление поддержки для большего количества устройств.

Заключительная часть Home Assistant – это домашняя автоматизация, управляющая пользовательскими настройками и внутренними компонентами, которые используют триггеры событий вместе с информацией из ядра для активации команд. Примером автоматизации может быть включение света, когда пользователь приходит домой, а на улице темно.

ЗАКЛЮЧЕНИЕ

Результатом настоящей работы является исследование защищенности IT-систем умного дома путем выявления угроз и уязвимостей информационной безопасности умного дома, а также применения натурного моделирования для проверки работоспособности предлагаемых решений по защите умного дома.

Для достижения указанной цели в ходе работы были решены следующие задачи:

- при решении задачи анализа основных типов и характеристик системы «умный дом» были выявлены их ключевые уязвимости, проведено исследование уязвимостей аппаратного обеспечения системы;
- проведена качественная оценка рисков информационной безопасности умного дома и выработаны защитные меры для их снижения;
- разработан и исследован прототип фрагмента системы «умный дом»;
- при экспериментальном исследовании угроз и уязвимостей разработанного прототипа фрагмента системы «умный дом» была подробно изучена угроза перехвата критически важной информации системы.

По результатам разработки и исследования Инспектора безопасности были сделаны выводы об эффективности применения модуля обнаружения ботнета. Также следует подчеркнуть оптимальное использование ресурсов прототипом безопасности, что доказывает оптимальность подбора комплектующих для создания модуля обнаружения. В дальнейших исследованиях запланировано усовершенствование модуля обнаружения вредоносной активности и разработка полноценной системы для предотвращения атак на программно-аппаратный комплекс «умный дом».

СПИСОК ЛИТЕРАТУРЫ

1. IDC forecasts double-digit growth for smart home devices as consumers embrace home automation and ambient computing [Прогноз продаж умных

устройств]. – IDC, 2021. – URL: https://www.idc.com/getdoc.jsp?containerId=prUS47567221 (accessed: 03.12.2021).

2. *Fernandez E., Jung J., Prakash A.* Security analysis of new intelligent home applications // Proceedings of the IEEE Symposium on Security and Privacy (SP). – San Jose, CA, 2016. – P. 636–654. – DOI: 10.1109/SP.2016.44.

3. Opening Pandora's box: effective techniques for reverse engineering IoT devices / O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, Y. Oren // Smart Card Research and Advanced Applications, CARDIS 2017. – Cham: Springer, 2018. – P. 1–21. – DOI: 10.1007/978-3-319-75208-2_1.

4. *Полоцкий Р.Е.* Что такое «умный дом»? // Алгоритм безопасности. – 2017. – № 4. – С. 4–7.

5. *King N.* Smart home – definition. – Intertek Research & Testing Centre, 2003. – URL: https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf (accessed: 03.12.2021).

6. Организация информационного взаимодействия элементов системы «умный дом» / В.С. Афонин, А.Г. Зрюмова, А.А. Кузнецов, Р.А. Забеляев, Р.А. Дьякин // Ползуновский альманах. – 2017. – № 4-3. – С. 170–172.

7. *Robles R.J., Kim T.-h.* Applications, systems and methods in intelligent home technologies: a review // International Journal of Advanced Science and Technology. – 2010. – Vol. 15. – P. 37–48.

8. *Sandström G.* Smart homes and user values: long-term evaluation of IT-services in residential and single family dwellings: Doctoral thesis. – Stockholm: KTH, 2009. – 164 p. – URL: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A281689&dswid=-7783 (accessed: 08.12.2021).

9. *Росляков А.В.* Интернет вещей. – Самара: ПГУТИ, 2014. – 342 с.

10. *Снегуров А.В., Ткаченко Е.А., Кравченко А.Д.* Риски информационной безопасности систем, построенных по технологии «Умный дом» // Восточно-Европейский журнал передовых технологий. – 2011. – Т. 4, № 3. – С. 30–34.

11. *Fall K.*, *Stevens W.* TCP/IP illustrated. Vol. 1. The protocols. – 2nd ed. – Upper Saddle Rive: Addison-Wesley, 2012. – 1056 p. – (Addison-Wesley Professional Computing Series).

12. Overview of intrusion detection in the internet of things / B. Bogaz, R.S. Miani, G.G. Garpelon, S.T. Kawakani, S.C. de Alvarenga // Journal of Network and Computer Applications. – 2017. – Vol. 84. – P. 25–37. – URL: http://www.sciencedirect.com/science/article/pii/S1084804517300802 (accessed: 08.12.2021).

13. *Anderson R.* Security engineering: a guide to building dependable distributed systems. – 3rd ed. – New York: Wiley, 2020. – 1232 p.

Рева Иван Леонидович, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность, информационные технологии, приборостроение. E-mail: reva@corp.nstu.ru

Архипова Анастасия Борисовна, кандидат технических наук, доцент кафедры защиты информации Новосибирского государственного технического университета. Основные направления научных исследований: программное обеспечение научных задач, управление в социально-экономических системах, информационная безопасность. E-mail: arhipova@corp.nstu.ru

Самойленко Роман Вадимович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность. E-mail: Cherkaev@corp.nstu.ru

DOI: 10.17212/2782-2230-2021-4-20-36

Analysis of threats to information security and data protection in the "Smart house systems"*

I.L. Reva[1], A.B. Arhipova[2], R.V. Samoylenko[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: reva@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*

[3] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: ro999@yandex.ru*

The idea of smart homes has been around for several decades and has been described by different authors many times since then. However, there are almost always three aspects in the definitions of the last 20 years. First, home devices must be connected, not only to each other, but also to the Internet. Second, an intelligent way to manage the system is needed, such as a central gateway or smart smartphone apps. Finally, there must be some degree of home automation in the system. A hardware and software complex that meets these requirements can be called a "smart home" system. The system of ensuring the security of the "smart home" is now of great practical importance, which should include measures to protect the IT infrastructure, ensuring the personal safety of residents, ensuring their health, the sanitary condition of the premises, as well as the safety of material assets. It follows from this that the problem of the lack of a thorough study of information security threats and the elaboration of protection of the entire software and hardware

* *Received 01 November 2021.*

complex of the "smart home" system is quite urgent. When solving this problem, an analysis of the main types and characteristics of smart home systems was carried out, and their key vulnerabilities were identified. Also, a study of vulnerabilities in the hardware of smart home systems was carried out; A qualitative assessment of the information security risks of a "smart home" has been carried out and protective measures have been developed to reduce them; A prototype of a fragment of the "smart home" security system has been developed and studied. In an experimental study of threats and vulnerabilities of the developed prototype of a fragment of the "smart home" system, the threat of interception of critical information of the system was studied in detail. Based on the results of the development and research of the Security Inspector, conclusions were drawn about the effectiveness of the use of the intrusion detection module.

Keywords: information security, smart home security, threat model, risk assessment, security inspector, intrusion detection system, security system, critical information system

REFERENCES

1. *IDC forecasts double-digit growth for smart home devices as consumers embrace home automation and ambient computing*. IDC, 2021. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS47567221 (accessed 03.12.2021).

2. Fernandez E., Jung J., Prakash A. Security analysis of new intelligent home applications. *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2016, pp. 636–654. DOI: 10.1109/SP.2016.44.

3. Shwartz O., Mathov Y., Bohadana M., Elovici Y., Oren Y. Opening Pandora's box: effective techniques for reverse engineering IoT devices. *Smart Card Research and Advanced Applications, CARDIS 2017*. Cham, Springer, 2018, pp. 1–21. DOI: 10.1007/978-3-319-75208-2_1.

4. Polotskii R.E. Chto takoe "umnyi dom"? [What is a smart home]. *Algoritm bezopasnosti*, 2017, no. 4, pp. 4–7.

5. King N. *Smart home – definition*. Intertek Research & Testing Centre, 2003. Available at: https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf (accessed 03.12.2021).

6. Afonin V.S., Zryumova A.G., Kuznetsov A.A., Zabelyaev R.A., D'yakin R.A. Organizatsiya informatsionnogo vzaimodeistviya elementov sistemy "umnyi dom" [Organization of information interaction of elements of the smart home system]. *Polzunovskii al'manakh = Polzunov Almanac*, 2017, no. 4-3, pp. 170–172.

7. Robles R.J., Kim T.-h. Applications, systems and methods in intelligent home technologies: a review. *International Journal of Advanced Science and Technology*, 2010, vol. 15, pp. 37–48.

8. Sandström G. *Smart homes and user values: long-term evaluation of IT-services in residential and single family dwellings*. Doctoral thesis. Stockholm, KTH, 2009. 164 p. Available at: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A281689&dswid=-7783 (accessed 08.12.2021).

9. Roslyakov A.V. *Internet veshchei* [Internet of things]. Samara: PGUTI Publ., 2014. 342 p.

10. Snegurov A.V., Tkachenko E.A., Kravchenko A.D. Riski informatsionnoi bezopasnosti sistem, postroennykh po tekhnologii "Umnyi dom" [Risk of information security systems based on technology "smart house". *Vostochno-Evropeiskii zhurnal peredovykh tekhnologii = Eastern-European Journal of Enterprise Technologies*, 2011, vol. 4, no. 3, pp. 30–34.

11. Fall K., Stevens W. *TCP/IP illustrated*. Vol. 1. *The protocols*. 2nd ed. Upper Saddle Rive, Addison-Wesley, 2012. 1056 p.

12. Bogaz B., Miani R.S., Garpelon G.G., Kawakani S.T., Alvarenga S.C. de. Overview of intrusion detection in the internet of things. *Journal of Network and Computer Applications*, 2017, vol. 84, pp. 25–37. Available at: http://www.sciencedirect.com/science/article/pii/S1084804517300802 (accessed 08.12.2021).

13. Anderson R. *Security engineering: a guide to building dependable distributed systems*. 3rd ed. New York, Wiley, 2020. 1232 p.

Для цитирования:

Рева И.Л., Архипова А.Б., Самойленко Р.В. Анализ угроз информационной безопасности и защита данных в системах «умный дом» // Безопасность цифровых технологий. – 2021. – № 4 (103). – С. 20–36. – DOI: 10.17212/2782-2230-2021-4-20-36.

For citation:

Reva I.L., Arkhipova A.B., Samoylenko R.V. Analiz ugroz informatsionnoi bezopasnosti i zashchita dannykh v sistemakh "Umnyi dom" [Analysis of threats to information security and data protection in the "Smart house systems"]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2021, no. 4 (103), pp. 20–36. DOI: 10.17212/2782-2230-2021-4-20-36.