Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 681.518.5:004.056

На правах рукописи

КОСТЮЧЕНКО
Владислав Владимирович

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ СИСТЕМ «УМНЫЙ ДОМ»

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2019

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **АЛЕФИРЕНКО Виктор Михайлович,** кандидат технических наук, доцент, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **СВИТО Иван Антонович,** кандидат физико-математических наук, старший научный сотрудник НИЛ энергоэффективных материалов и технологий учреждения образования «Белорусский государственный университет»

Защита диссертации состоится «5» февраля 2019 г. года в $9^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Современные умные дома имеют доступ к конфиденциальной информации и владеют правом управления большинством домашней электроники и техники. В связи с этим существует риск, что управление системой, а также удаленный контроль над всеми подключенными устройствами, может быть перехвачено злоумышленником. Самыми распространенными атаками злоумышленников являются удаленный перехват контроля над зданием и получение конфиденциальной информации. Предметами атаки могут стать беспроводные модули в сети, такие как смарт-розетки, умные колонки, электронные дверные замки, электронные счетчики и сервера хранения информации.

Анализ информации о различных системах автоматизации жилых помещений и моделирование схожих условий с применением технических и программных средств позволяет определить основные векторы атаки на системы «Умный дом» и способы их предотвращения.

Одной из основных проблем в безопасности умных устройств является незащищенность каналов связи, как во внешней части сети, так и во внутренней, включая каналы связи между умными устройствами и датчиками, что в дальнейшем позволяет удаленно перехватывать управление и контролировать все параметры и данные в умных домах.

На сегодняшний день существует большое количество работ в области исследования безопасности умных домов. Наиболее значимые результаты были получены российскими учеными, которые проводили исследования в области систем безопасности, построенных по технологиям «Умный дом» (А. В. Снегуров, Е. А. Ткаченко, А. Д. Кравченко). Среди зарубежных авторов особый интерес вызывают работы Б. Фулади, С. Ганун, Вай Ли, Си Ху в которых представлено описание некоторых механизмов безопасности сенсорных сетей.

Применение методов оценки рисков и поиска каналов утечки информации, обнаружение проблем конфиденциальности и безопасности систем, моделирование и предложение методов повышения защищенности систем приводит к улучшению качества защиты современных умных систем автоматизации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Системы «Умный дом» постоянно развиваются и становятся всё более распространенными, так как повышают комфорт жителей и облегчают их повседневную жизнь. Важнейшими вопросами для таких систем являются вопросы безопасности и конфиденциальности данных. Однако эти вопросы до сих пор должным образом не исследованы по причине многообразия систем и стандартов. В связи с этим актуальность темы исследования довольно вы-

сока, поскольку исследовательских работ по данной тематике не так много, а систем и стандартов автоматизации выпускается все больше.

Степень разработанности проблемы

Исследования безопасности систем «Умный дом» осуществлялись на основе анализа и моделирования системы «Умный дом», на основании методик и работ зарубежных авторов

Одним из недостатков современных работ является неполное рассмотрение особенности уязвимостей систем, построенных на базе свободно распространяемых программных комплексов.

Предложенное исследование направлено на устранение этого недостатка на основе исследования моделирования атак на проникновение в систему «Умный дом» с открытым исходным кодом, использующего открытые стандарты связи.

Цель и задачи исследования

Целью диссертации является поиск вероятных уязвимостей систем и сетей «Умных домов», а также моделирование различных атак на систему «Умный дом» и рекомендации по устранению найденных уязвимостей.

Поставленная цель работы определяет **следующие основные задачи**:

1. Провести обзор и анализ существующего программного обеспечения, оборудования и системы управления связью для умных домов, которые в настоящее время доступны на рынке;

2. Выявить основные сильные и слабые стороны систем «Умный дом» путем использования методологии оценки риска *OCTAVE* для умных домов;

3. Выполнить моделирование вероятных векторов атак злоумышленника, обработать полученные результаты и предложить возможные пути улучшения безопасности умных систем.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 1-39 81 01-2012 специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы зарубежных ученых в области защиты информации, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в исследовании уязвимостей систем «Умный дом», угрожающих безопасности и нарушающих конфиденциальность данных пользователей.

Теоретическая значимость работы заключается в детальном анализе существующих умных систем и сравнении их технологической и программной баз в контексте безопасности.

Практическая значимость диссертации заключается в исследовании найденных уязвимостей в системах и сетях умных домов и предлагаемых методах их устранения.

Основные положения, выносимые на защиту

1. Систематизация механизмов взаимодействия устройств современных систем «Умный дом», основанная на анализе доступной технической документации и спецификации протоколов связи.
2. Методология оценки риска, выявляющая слабые стороны различных систем «Умный дом», незащищённые сетевые коммуникации и небезопасные умные устройства.
3. Экспериментально выявленные уязвимости сетевых коммуникаций и умных устройств путем моделирования системы «Умный дом» и проведения атак на группу устройств и рекомендации по устранению проблем безопасности систем «Умный дом».

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на II Международной научно-практической конференции «Научные исследования и современное образование» (г. Чебоксары, Чувашская Республика, 2018 г.); 54-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Беларусь, 2018 г.); XVI Белорусско-Российской научно-технической конференции «Технические средства защиты информации» (г. Минск, Беларусь, 2018 г.), а также вошли в сборник научных трудов «Актуальные научные исследования в современном мире» выпуск 32 часть 2 (г. Переяслав-Хмельницкий, Украина, 2017 г.) и в сборник научных трудов «Актуальные научные исследования в современном мире» выпуск 35 часть 2 (г. Переяслав-Хмельницкий, Украина, 2017 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 6 печатных работах. В их числе 5 статей в сборнике научных трудов и 1 тезис доклада на научной конференции.

Общий объем публикаций по теме диссертации составляет 31 страницу.

Структура и объем работы

Диссертация состоит из перечня условных обозначений и терминов, введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен обзор современного состояния проблемы безопасности умных домов и различных интеллектуальных систем, обычно используемых на базе системы «Умный дом», проводится сравнительный анализ существующих систем так же, кратко сравниваются популярные стандарты защиты связи внутри сети умного дома.

Во второй главе представлен анализ безопасности системы «Умный дом» в контексте методологии анализа рисков *OCTAVE* в системах «Умный дом», а также, демонстрируется контекстная модель контроля доступа применимая к системам «Умный дом».

В третьей главе представлен эксперимент по моделированию системы «Умный дом» на основе архитектуры *CoSSMic* и проведению атак по выявленным уязвимым каналам связи.

В приложении представлены таблицы со сравнительным анализом систем «Умный дом», руководство по установке *CoSSMic*, публикации автора и акт внедрения.

Общий объем диссертационной работы составляет 161 страницу. Из них 70 страниц основного текста, 33 иллюстрации на 17 страницах, 8 таблиц на 10 страницах, библиографический список из 116 наименований на 10 страницах, список собственных публикаций соискателя из 6 наименований на 1 странице, 6 приложений на 80 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы безопасности умных домов, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе приведен обзор современного состояния систем «Умный дом», рассмотрены используемые технологии, программные средства и инженерные решения. Определяются основные концепции современных систем «Умный дом».

Из анализа следует, что современный умный дом нацелен на повышение качества жизни путем развертывания полностью автоматизированного управления приборами и оказание дополнительной помощи жильцам. Такой дом позволяет повысить энергоэффективность за счет адаптивной эксплуатации устройств в каждом конкретном случае, повысить удобство пользования

домашним оборудованием, вести своевременный учет расхода коммунальных услуг, автоматически экономить электроэнергию путем управления энергопотреблением, предоставлять функциональную мультимедийную базу, расширенные возможности по обеспечению безопасности здания и полный удаленный контроль над техникой. Пользователи и устройства постоянно связаны в расширенный коммуникационный сетевой комплекс.

Проанализированы особенности эксплуатации и функциональной наполненности существующих на данный момент умных систем. Проведено сравнение предоставляемых возможностей различными системами, используемых стандартов связи, поставляемого программного обеспечения и многофункциональных датчиков.

При проведении анализа выявлено, что большинство существующих систем имеют разрозненные протоколы связи, не используют общепринятые стандарты безопасности, имеют небезопасные предустановки и настройки.

Во второй главе представлен анализ безопасности системы «Умный дом» в контексте методологии анализа рисков *OCTAVE*.

Для анализа рисков в методике *OCTAVE* предлагается подход из восьми шагов, объединенных в четыре фазы (рисунок 1).

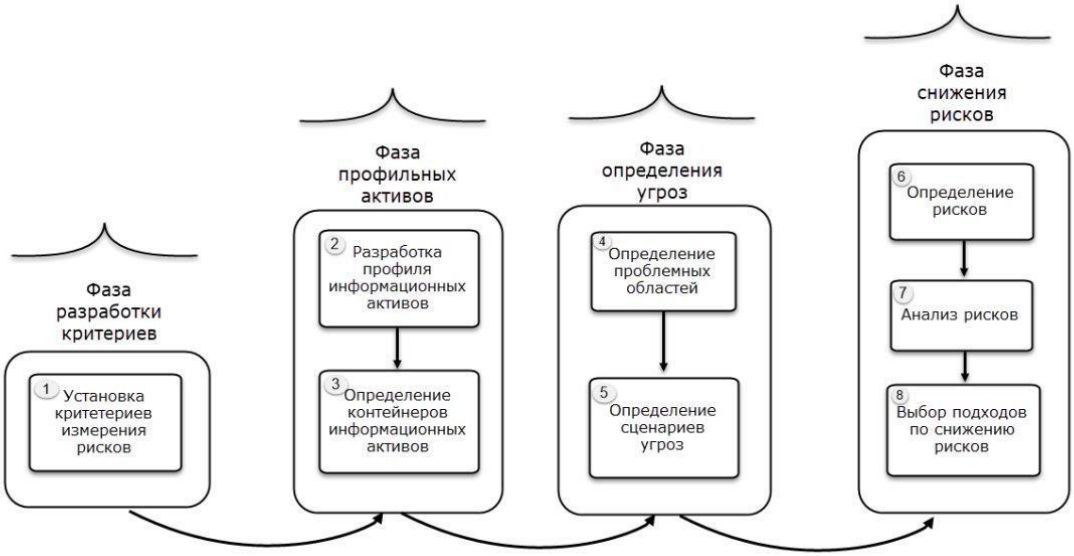

Рисунок 1 – Технологическая схема OCTAVE Allegro из восьми этапов, которые подразделяются на четыре основные группы

Анализ риска включает в себя следующие этапы: идентификацию риска (определение активов, определение угроз, определение существующих мер и средств контроля и управления, выявление уязвимостей, определение последствий) и установление значения риска (оценка последствий, оценка вероятности инцидента, установление значений уровня рисков). Оценка рисков должна идентифицировать риски, определить количество и приоритеты рисков на основе критериев для принятия риска и целей, значимых для обеспечения безопасности системы.

Общий алгоритм действий группы анализа рисков, основанный на методике *OCTAVE* выглядит следующим образом:

На шаге 1 необходимо определить критерии оценки рисков информационной безопасности, то есть совокупность качественных показателей, которая позволит установить значения оценки риска и последствия реализации риска. Без введения таких критериев невозможно оценить зависимость системы от тех или иных рисков.

Шаг 2 начинается с составления перечня информационных активов и определения их профиля. Профиль актива представляет собой входные данные для следующих шагов и основой для выявления угроз и рисков.

Далее выполняется шаг 3. Информационные активы могут храниться не только в самой системе «Умный дом», но и вне ее пределов. Домовладелец может допускать к обслуживанию своей инфраструктуры другие организации-поставщики услуг. Если такой поставщик услуг не выполняет требования безопасности активов, к обслуживанию которых он допущен, то это само по себе несет риск. Риск может содержаться в самом факте хранения, передачи или обработке актива в постороннем месте. Это нарушает защиту информационного актива. Еще большую угрозу несет привлечение таким поставщиком услуг субподрядчиков, о которых владелец актива может и не знать. Таким образом, для получения адекватного профиля актива важно определить все места хранения, передачи и обработки актива – контейнеры, а также находится ли он в зоне прямого управления организацией. Местом хранения актива может являться техническое средство, программное обеспечение, бумажный носитель или сотрудник организации. Причем, люди здесь особенно важны, так как при получении защищаемой информации они становятся «контейнерами» актива. Такие риски необходимо своевременно выявлять.

На шаге 4 выявляются проблемные области в информационной безопасности умного дома. Целью шага 4 является не составление полного перечня всех возможных угроз, а оперативное определение тех угроз, которые сразу очевидны для аналитика.

В шаге 5, на основе выявленных проблемных областей, составляются сценарии угроз. Этот шаг позволяет учесть вероятности реализации угроз, что помогает на более поздних шагах разработать мероприятия по снижению риска. Как правило, в этом случае используется качественная шкала, и вводятся три уровня вероятности реализации угрозы: высокая, средняя и низкая.

На шаге 6 после определения угроз и выявления последствий их реализации, определяют риски информационной безопасности. Необходимо определить, как именно риск будет воздействовать на систему «Умный дом» в целом, при этом риск определяется для каждого актива, чтобы оценить его критичность для функционирования. Для каждого риска определяется не менее одного последствия.

На шаге 7 определяется количественная мера ущерба, который будет нанесен системе «Умный дом» при реализации угрозы. Это относительная оценка, которая позволяет расставить риски по их приоритету. На заключи-

тельном шаге выбираются меры обработки определенных рисков с учетом их приоритета.

В третьей главе представлен эксперимент по моделированию атак на систему «Умный дом» с использованием *CoSSMic* платформы. Описаны основные компоненты системы *CoSSMic* и современные технологии, которые были выбраны для развертывания прототипа.

Общая архитектура *CoSSMic* платформы представлена ниже на рисунке 2:

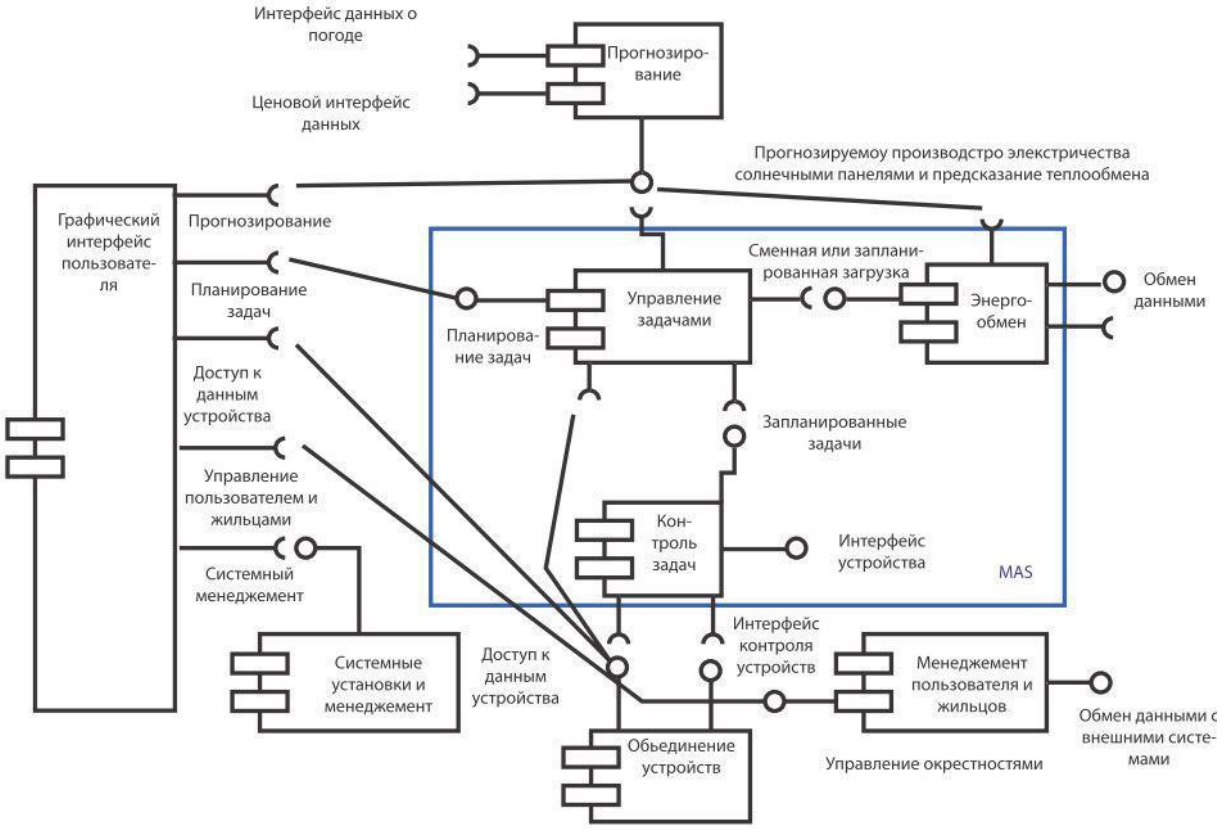

Рисунок 2 – CoSSMic платформа

Эта платформа в настоящее время реализует конфигурацию *All in Home*. В текущем развертывании все основные компоненты системы находятся на домашнем шлюзе, а облачный сервер используется только для согласования энергопотребления между различными умными домами. Домашний шлюз контролирует основные компоненты, которые отвечают за управление умным домом, такие как интеграция устройства и *Multi Agent System* (*MAS*). Электрические устройства соединены с домашним шлюзом через специальные драйверы.

Далее производится настройка виртуальный среды *CoSSMic*. В качестве тестовой среды используется *Raspberry Pi* 2 Модели *B*. Кроме *Raspberry P*i, также необходимо следующее оборудование: вспомогательное оборудование для *Raspberry Pi:* блок питания, кабель *HDMI*, *SD* карты (16 Гб), Ethernet кабель; монитор или телевизор; клавиатура; *HomeMatic* беспроводная смарт розетка: *HM-ES-PMSw1-PI;*модуль *USB CC1101 V*3; лампа для тестирования ре-

зультатов; *PC*, смартфон или планшет с браузером. Необходимое программное обеспечение: подготовленный образ *Raspbian Jessie*, содержащий большинство обновлений, внесенных в ОС; *PuTTY; Win32DiskWriter*. Программные компоненты: *EmonCMS; CUL* драйвер.

Перед подключением вышеуказанных составляющих к *Raspberry Pi* подготовленный образ записывается на SD-карту и выполняются дальнейшие настройки *CoSSMic*. Также используется удлинительный кабель для питания *HomeMatic* и *Raspberry Pi*. Это оборудование может быть подключено непосредственно к розетке питания. Лампа подключается к смарт-розетке *HomeMatic* и *USB* CC1101 к *Raspberry Pi* через его *USB* порт. Теперь можно получить доступ к веб-приложению из браузера на ПК или смартфоне, введя следующий *URL*-адрес в адресной строке: *http*://129.241.208.197/*emoncms*. Войдем в систему с именем *UK02* и паролем *uktestpass25*, которые задаются во время установки *EmonCMS*.

После настройки оборудования и программного обеспечения требуется запустить систему, которая будет имитировать действия злоумышленника. Для этого воспользуемся следующим оборудованием и программным обеспечением: операционной системой *Kali Linux*, аппаратным приёмопередатчиком на 868 МГц, сканером безопасности *OWASP ZAP*, для захвата основных данных с целью осуществления основных атак используем *TCPDump*, инструментом *Wireshark* в качестве анализатора протоколов.

Захват учетных данных пользователя осуществляется при запуске готовуй модели умного дома. Используется сетевой перехватчик *Wireshark* и анализатор *TCPdump*. Искомая конфиденциальная информация, отправляется в виде простого текста по сети. Это позволяет злоумышленнику легко перехватить эти данные, обнаружив сетевой трафик и осуществив сниффинг атаку. Результаты атаки представлен ниже на рисунке 3:

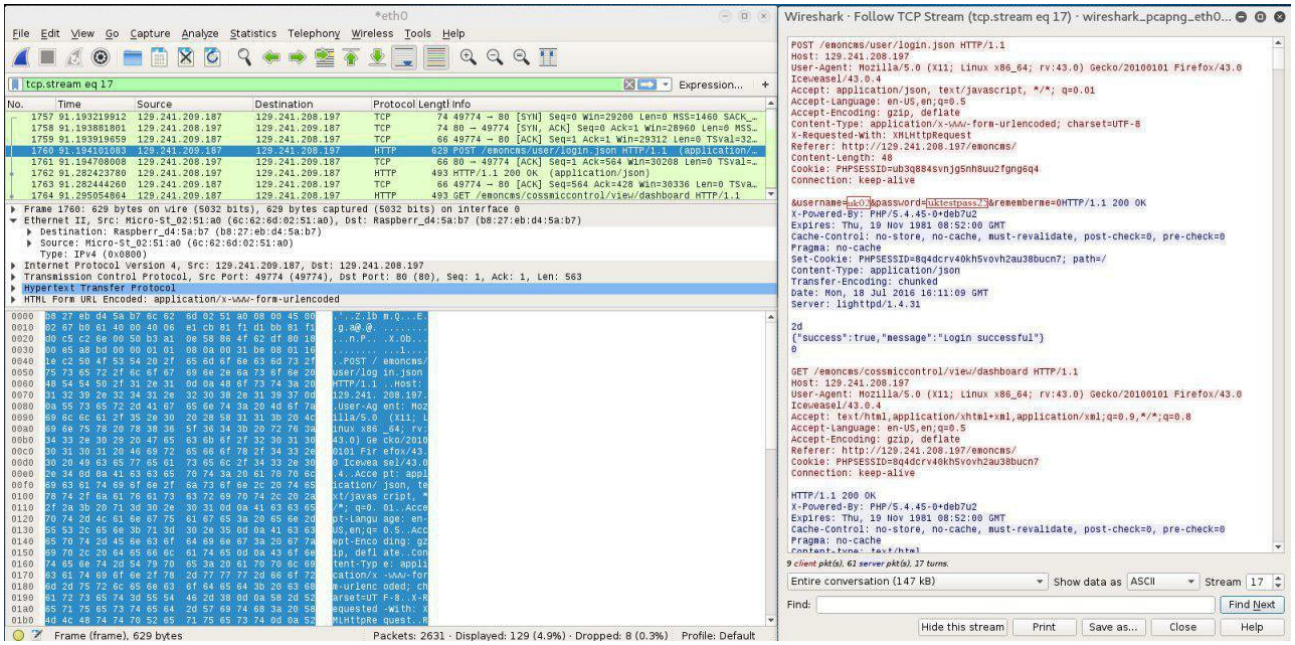

Рисунок 3 – Диалоговое окно программы Wireshark: «Сниффинг учетных данных пользователя»

Теперь, после получения знаний об активной учетной записи в системе, становится легко обойти механизм аутентификации и войти в умный дом, не будучи санкционированным пользователем.

Далее рассматривается *ClickJacking* атака. Параметр *X-FRAME-OPTIONS* заголовка не задан на некоторых веб-страницах согласно результатам анализа *ZAP*.

Смоделировать *ClickJacking* атаку можно путем запуска сценария, как показано ниже на рисунке 4:

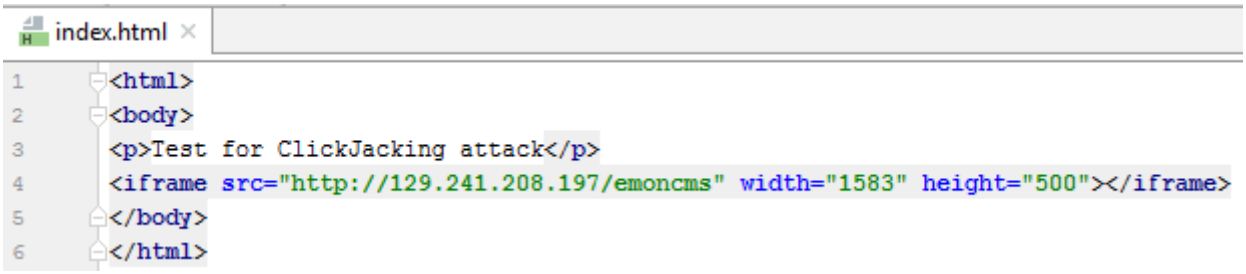

Рисунок 4 – Диалоговое окно программы PyCharm: «Скрипт для моделирования ClickJacking атаки»

Веб-интерфейс *CoSSMic* может быть встроен в другой сайт, что делает его уязвимым для *ClickJacking* атак

Среди возможных уязвимостей найдена проблема удаленного управления устройствами без авторизации. Злоумышленник может легко управлять устройствами, подключенными к *HomeMatic* смарт-розетке, будучи неавторизованным в системе. Кроме того, всеми устройствами, подключенными к смарт-розетке, можно управлять с помощью *HTTP GET* запроса. Атакующий может ввести *URL* в браузере, как показано на рисунке 5, и таким образом включить/отключить смарт-розетку.

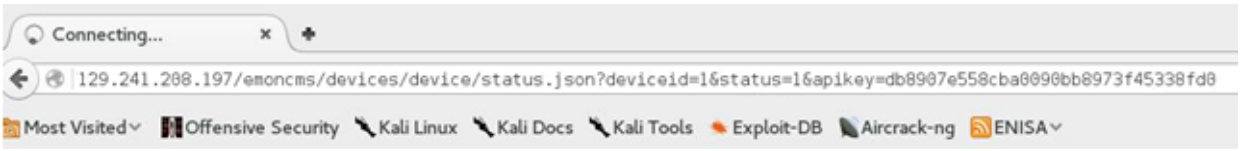

Рисунок 5 – Окно адресной строки браузера: «API-ключ добавлен в URL»

Когда злоумышленник введет этот *URL*, он сделает систему недоступной. Параметр *status* в *URL*-адресе принимает в качестве значения символ, который не является допустимым значением для ввода. Статус может принимать только цифры в качестве значений. Наблюдение показывает, что смарт-розетка выключается, как показано на рисунке 6, когда параметру *status* было присвоено значение 0, и включается, как показано на рисунке 7, когда параметру *status* было присвоено любое другое число (не только 1). Авторизованному пользователю не нужно переключать устройство через *URL*-адрес, поскольку для этого он может использовать кнопку в веб-

интерфейсе. Злоумышленнику не нужно входить в систему, так как он может использовать *API* ключи от сниффинг атаки. После этого система не будет реагировать на запросы пользователей, и домашний шлюз нужно физически перезагружать, чтобы восстановить функционирование и доступ к системе.

Злоумышленник может легко перехватить и прослушать трафик между домашним шлюзом (*Raspberry Pi*) и умным штекером *HomeMatic HM-ES-PMSw1-PI*, так как соединение между смарт-розеткой *HomeMatic* и умным домом не зашифровано.

Пакетные данные для удалённого управления смарт-розетками могут быть получены с помощью *Linux* терминала.

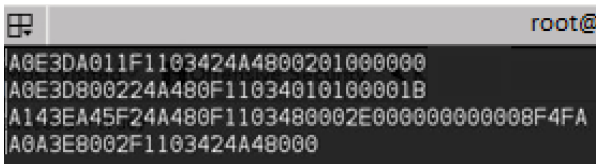

Рисунок 6 – Диалоговое окно программы Terminal Linux: «Пакетные данные, полученные после команды выключения»

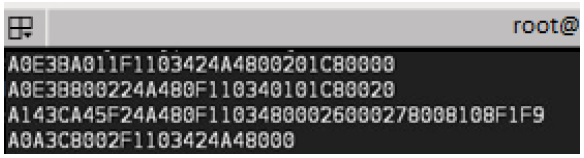

Рисунок 7 – Диалоговое окно программы Terminal Linux: «Пакетные данные, полученные после команды включения»

Продемонстрированные атаки показывают, как злоумышленник может перехватить контроль и удаленно управлять большей частью систем «Умный дом», имеет возможность незаметного проникновения в помещение, управление электроэнергией, может контролировать и подменять данные в системе учета и брать на себя несанкционированное полное управление системой «Умный дом».

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен обзор и анализ существующего программного обеспечения, оборудования и систем управления связью для умных домов, которые в настоящее время доступны на рынке. Выявлено, что в настоящее время в отечественных и зарубежных источниках недостаточно освещен вопрос безопасности и конфиденциальности систем «Умный дом».

2 Проведен анализ безопасности системы «Умный дом» в контексте методологии анализа рисков *OCTAVE*, выявлены основные сильные и слабые стороны технологий и продуктов, представленных на рынке.

3. Выполнено моделирование системы «Умный дом», проведены основные возможные атаки на систему, обработаны полученные результаты и предложены возможные пути улучшения безопасности умных систем.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в компанию ООО «ЛюкАндВит» как демонстрационное руководство по тестированию на проникновение в системы «Умный дом».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в сборниках научных трудов

1. Алефиренко, В. М. Уязвимости систем «Умный дом» и причины их возникновения / В. М. Алефиренко, В. В. Костюченко // Актуальные научные исследования в современном мире : сборник научных трудов XXXII-ой Международной науч. конф., 26-27 декабря 2017г. / Переяслав-Хмельницкий, 2017. – Вып. 12 (32), ч. 1. – С. 117–122.

2. Алефиренко, В. М. Проблемы конфиденциальности и безопасности в системах «Умный дом» / В. М. Алефиренко, В. В. Костюченко // Актуальные научные исследования в современном мире : сб. научных трудов XXXV Международной науч. конф., март 2018 г. - Переяслав-Хмельницкий, 2018. – Вып. 3 (35), ч. 1. – С. 196 – 204.

3. Костюченко, В. В. Проблемы аутентификации и контроля доступа в системах «Умный дом» / В. В. Костюченко, В. М. Алефиренко // Научные исследования и современное образование : материалы II Междунар. науч.-практ. конф., Чебоксары, Российская Федерация, 26 март 2018 г. / редкол.: О.Н. Широков [и др.] – Чебоксары: ЦНС «Интерактив плюс», 2018. – С. 229-234.

4. Костюченко, В. В. Особенности безопасной эксплуатации системы «Умный дом» / В. В. Костюченко // материалы 54-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 23-27 апреля 2018 г. / БГУИР». – Минск, 2018. – С. 36-37.

5. Костюченко, В. В. Угрозы безопасности системы «Умный дом» / В. В. Костюченко // материалы 54-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 23-27 апреля 2018 г. / «БГУИР». – Минск, 2018. – С. 38-41.

Тезисы конференций

6. Алефиренко, В. М. Проблемы конфиденциальности и безопасности голосовых ассистентов / В. М. Алефиренко, В. В. Костюченко // Технические средства защиты информации : тезисы докладов XVI Белорусско-российской научно-технической конференции, Минск, 5 июня 2018 г. – Минск: БГУИР, 2017. – С. 12.

РЭЗЮМЭ

Касцючэнка Уладзіслаў Уладзіміравіч

Методыка забеспячэння функцыянальнай надзейнасці электронных модуляў на базе мікракантролераў пры ўздзеянні разрадаў статычнага электрычнасці

Ключавыя словы: бяспека, “разумны дом”.

Мэта працы: даследаванне ўразлівасцяў сістэм і сетак “разумных дамоў”, а таксама мадэляванне верагодных нападаў.

Атрыманыя вынікі і іх навізна: праведзены агляд праграмнага забеспячэння, абсталявання і сістэм кіравання сувяззю для “разумных дамоў”. Праведзены аналіз бяспекі сістэмы “разумны дом” у кантэксце метадалогіі аналізу рызык OCTAVE, выяўлены асноўныя моцныя і слабыя бакі тэхналогій і прадуктаў, прадстаўленых на рынку. Выканана мадэляванне сістэмы “разумны дом”, праведзены асноўныя магчымыя атакі на сістэму і сетку, апрацаваны атрыманыя вынікі і прапанаваны магчымыя шляхі паляпшэння бяспекі разумных сістэм.

Ступень выкарыстання: вынікі ўкаранёны ў кампанію ТАА “ЛюкАндВіт” як дэманстрацыйнае кіраўніцтва па тэставанні на пранікненне ў сістэмы “разумных дамоў”.

Вобласць ужывання: хатняя аўтаматызацыя, абарона дадзеных, пошук уразлівасцяў.

РЕЗЮМЕ

Костюченко Владислав Владимирович

Исследование безопасности систем «Умный дом»

***Ключевые слова*:** безопасность, «умный дом».

***Цель работы*:** исследование уязвимостей систем и сетей «умных домов», а также моделирование вероятных атак.

***Полученные результаты и их новизна*:** проведен обзор программного обеспечения, оборудования и систем управления связью для «умных домов». Проведен анализ безопасности системы «умный дом» в контексте методологии анализа рисков OCTAVE, выявлены основные сильные и слабые стороны технологий и продуктов, представленных на рынке. Выполнено моделирование системы «умный дом», проведены основные возможные атаки на систему и сеть, обработаны полученные результаты и предложены возможные пути улучшения безопасности умных систем.

***Степень использования*:** результаты внедрены в компанию ООО «ЛюкАндВит» как демонстрационное руководство по тестированию на проникновение в системы «Умный дом».

***Область применения*:** домашняя автоматизация, защита данных, поиск уязвимостей.

SUMMARY

Kactsiuchenka Uladzislau Uladzimiravich

The method for ensuring the functional reliability of electronic modules based on microcontrollers when exposed to static discharges electricity

Keywords: security, smart home.

***The object of study*:** to study the vulnerabilities of systems and networks of smart homes, as well as the modeling of possible attacks.

The results and novelty: a review of the software, equipment and communication management systems for smart homes. The security analysis of the smart home system was conducted in the context of the OCTAVE risk analysis methodology, and the main strengths and weaknesses of the technologies and products on the market were identified. The smart home system was simulated, the main possible attacks on the system and network were carried out, the results obtained were processed and possible ways to improve the security of smart systems were proposed.

Degree of use: the results are implemented in the LucAndVit LLC as a demonstration guide for testing for penetration into the systems of smart homes.

Sphere of application: home automation, data protection, vulnerability scan.