Моделирование и анализ информационных систем. Т. 23, № 6 (2016), с. 767–776
Modeling and Analysis of Information Systems. Vol. 23, No 6 (2016), pp. 767–776

DOI: 10.18255/1818-1015-2016-6-767-776

УДК 004.056.53

Разработка и анализ защищенности фрагмента информационно-телекоммуникационной системы, реализующей концепцию Интернета вещей

Александров В. А., Десницкий В.А.[1,2]**, Чалый Д.Ю.**[1]

получена 17 октября 2016

Аннотация. В работе исследуются вопросы разработки и реализации систем, использующих концепцию Интернета вещей. В условиях активного развития отраслей, использующих концепцию Интернета вещей, актуальна проблема информационной безопасности. Для того чтобы определить актуальные угрозы, необходимо использовать детальный анализ рисков в соответствии с действующими стандартами ГОСТ. Выбирая защитные меры, необходимо учитывать все идентифицированные актуальные угрозы информационной безопасности. В статье определяются актуальные угрозы и защитные меры, необходимые для разработки и внедрения защищенного фрагмента программно-аппаратной системы Умный дом в части контроля доступа в помещение. Решены следующие задачи: описание системы Умный дом, описание этапов оценки и обеспечения безопасности системы Умный дом; осуществление аппаратной сборки и написания программного кода для выбранного фрагмента системы; оценка безопасности выбранного фрагмента Умного дома и определение актуальных угроз; выработка рекомендаций по противодействию актуальным угрозам; программная реализация одной из актуальных угроз и программная реализация защитных мер для выбранной угрозы. Особенностью работы является комплексный подход к проектированию с использованием моделей нарушителя, анализа активов системы и оценки их защищенности.

Ключевые слова: Интернет вещей, информационная безопасность

Для цитирования: Александров В. А., Десницкий В.А., Чалый Д.Ю., "Разработка и анализ защищенности фрагмента информационно-телекоммуникационной системы, реализующей концепцию Интернета вещей", *Моделирование и анализ информационных систем*, **23**:6 (2016), 767–776.

Об авторах:
Александров Владислав Андреевич, orcid.org/0000-0003-1169-6034, магистрант,
СПБНИУ ИТМО, Кронверский пр-т, д. 49, г. Санкт-Петербург, 197101 Россия, e-mail: 2-q2@mail.ru

Десницкий Василий Алексеевич, orcid.org/0000-0002-3748-5414, канд. техн. наук, старший научный сотрудник,
ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
14 линия, 39, г. Санкт-Петербург, 199178 Россия, e-mail: vasily.desnitsky@mail.ru

Чалый Дмитрий Юрьевич, orcid.org/0000-0003-0553-7387, канд. физ.-мат. наук,
Ярославский государственный университет им. П.Г. Демидова,
ул. Советская, 14, г. Ярославль, 150003, Россия, e-mail: dmitry.chaly@gmail.com

Благодарности:
[1]Работа выполнена при финансовой поддержке РФФИ (проект №16-37-50035).
[2]Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-29-09482 офи_м, 16-37-50035).

Введение

В работе исследуются вопросы разработки и реализации систем, использующих концепцию Интернета вещей. Понятие Интернета вещей включает системы аппаратных устройств специализированного назначения, в которые встраиваются электронные модули для управления такими устройствами и организации внешних коммуникаций. Количество подключенных устройств растет с каждым годом. Так, близкий к линейному, по оценкам компании Cisco, прогнозируемый рост числа встроенных устройств обусловливает важность исследования вопросов информационной безопасности систем Интернета вещей [1]. Множество устройств Интернета вещей можно увидеть в потребительской сфере – устройства бытовой электроники, контрольные устройства физической и информационной безопасности, игровые устройства, имплантируемые медицинские устройства и другие. Такие устройства, соединенные между собой, значительно упрощают их использование и расширяют выдаваемый функционал. В целом концепция Интернета вещей, внедренная на предприятии, позволяет эффективней использовать его ресурсы путем повышения скорости реагирования на изменения. Взаимосвязь и анализ датчиков и объектов предприятия происходит с минимальным участием человека или без него. Это также способствует повышению производительности и уменьшает влияние человеческого фактора.

Цель работы состоит в разработке и исследовании защищенного фрагмента системы Умный дом, являющегося типовым примером системы Интернета вещей. Решены следующие задачи: описание системы Умный дом, описание этапов оценки и обеспечения безопасности системы Умный дом; осуществление аппаратной сборки и написания программного кода для выбранного фрагмента системы; оценка безопасности выбранного фрагмента Умного дома и определение актуальных угроз; выработка рекомендаций по противодействию актуальным угрозам; программная реализация одной из актуальных угроз и программная реализация защитных мер для выбранной угрозы. Особенностью работы является комплексный подход к проектированию с использованием моделей нарушителя, анализа активов системы и оценки их защищенности.

1. Методология разработки защищенных систем Умного дома

В настоящее время концепция Умного дома набирает все больший охват: в системах взаимосвязанных между собой программно-аппаратных устройств и сенсоров, применяемых для повышения автоматизации, физической и информационной безопасности, энергоэффективности и улучшения целевой функциональности. При этом использование концепции Интернета вещей позволяет получить такие преимущества, как модульность системы, масштабируемость системы, расширение функциональности и гибкость системы.

К основным недостаткам систем, реализующих концепцию Интернета вещей, можно отнести: (1) подверженность устройств системы множеству различных киберфизических атак, включающих сочетание в чистом виде программно-информа-

ционных воздействий и атак с использованием физических характеристик устройств и сенсоров системы, что определяет необходимость учета повышенных требований к защищенности; (2) разнородность устройств, их компонентов, используемых протоколов и технологий, что увеличивает сложность интеграции системы из отдельных компонентов; (3) высокую зависимость реализуемой защиты от бизнес-функций и особенностей системы, что затрудняет разработку универсальных средств и методик проектирования механизмов защиты для таких систем.

В соответствии с ГОСТ Р ИСО/МЭК ТО 13335-3-2007 [2] для обеспечения безопасности и выбора защитных мер для фрагмента системы Умного дома применяется детальный анализ рисков. Детальный анализ рисков включает идентификацию активов, оценку возможных угроз, которым подвержены активы, а также оценку их уязвимости. По результатам этих операций выполняется оценка рисков и последующее определение обоснованных защитных мер [3]. Результаты анализа рисков позволяют идентифицировать объекты системы или этапы в организации и использовании с высоким уровнем риска и выбрать меры обеспечения безопасности. Применение выбранных мер повышения безопасности снижает уровень идентифицированного риска до некоторого приемлемого.

2. Реализация и оценка фрагмента защищенной системы Умного дома

Разработан фрагмент системы Умного дома, нацеленный на проверку помещения на наличие в нем движения. В частности, анализируется ликвидность нахождения в контролируемом помещении при помощи политики безопасности с последующим оповещением в случае незаконного проникновения. Система включает следующие объекты: (1) центральное управляющее устройство на основе одноплатного компьютера; (2) датчик движения; (3) визуальное оповещение (светодиод).

В качестве датчика движения используется инфракрасный сенсор движения DFRobot. Микроконтроллер Raspberry Pi (RPi) используется в качестве центрального управляющего устройства системы. Небольшие размеры RPi определяют широкие возможности по его встраиванию в информационно-техническое окружение, тогда как аппаратные возможности RPi позволяют реализовать управление бизнес-функциями системы Умного дома с возможностью подключения различных сенсоров к стандартизированным пинам GPIO [4]. Наличие операционной системы Linux позволяет осуществлять программирование системы Умного дома на языках программирования высокого уровня, поддерживающих эту операционную систему.

На RPi установлен серверный модуль, написанный на Python 2.7, который получает данные с датчика движения каждые 10 миллисекунд. В случае обнаружения движения в помещении, контроллер сверяет точное значение времени и дату события с политикой безопасности, которая хранится в специальном файле. В данном файле устанавливается время и день недели, в пределах которых пользователю разрешается легально находиться в помещении.

В случае если действие было обнаружено в запрещенное в соответствии с политикой безопасности время, то RPi (1) включает предупреждающий светодиод; (2) записывает в log-файл информацию о событии (указывая дату и время); (3) от-

правляет сообщение о тревоге всем подключенным к серверу клиентам. Связь с клиентом происходит при помощи сокетов по протоколу TCP/IP. Подключение может осуществляться как в локальной сети, так и через сеть Интернет. Клиентская сторона написана также на языке Python 2.7 [5].

Клиент подключается к серверу. После прохождения аутентификации, посредством ввода пары логин/пароль, можно получить информацию с датчика движения. Пользователь может просмотреть действующую политику безопасности. Также имеется возможность изменять файл политики безопасности через клиентское приложение. В случае как законного, так и незаконного проникновения клиент получает оповещение от сервера.

Выбранный фрагмент Умного дома включает следующие активы, которые подлежат учету: (1) центральное управляющее устройство на основе одноплатного компьютера; (2) датчик движения; (3) программное обеспечение – клиент-серверное приложение, приложения для выполнения бизнес-функций системы и функций защиты; (4) файл политики безопасности Умного дома; (5) log-файл, хранящий информацию о случившихся изменениях в системе – данные об изменениях файла политики безопасности, подключенных клиентах и полученных данных от датчика.

К фрагменту Умного дома имеют доступ авторизованные пользователи, которые являются сотрудниками организации. Также имеется администратор, который имеет возможность добавлять пользователей и должен контролировать корректность работы системы. Допускается, что система используется в офисном помещении организации, в пределах одного этажа. Система предназначена для контроля периметра помещения и оповещения в случае проникновений. Все дальнейшие этапы выполняются в рамках установленных границ.

После получения перечня активов производится оценка ценности каждого из них. Ценность актива определяется его важностью для функционала системы Умного дома. Результаты проведенной оценки активов приведены в таблице 1.

Таблица 1. Оценка активов
Table 1. Evaluation of assets

Название актива	Оценка актива
центральное управляющее устройство	высокая
датчик движения	средняя
программное обеспечение	высокая
файл политики безопасности	высокая
log-файл	средняя

Для идентифицированных активов используется перечень угроз и их классификация с учетом известных типовых разновидностей угроз [3]. Далее классифицируемые угрозы сопоставляются с минимальным уровнем нарушителя, необходимым для реализации угрозы в соответствии с моделью Арбахама [6], [7]. На основе этого определяется вероятность возникновения угрозы, выраженная оценкой: «низкая», «средняя» или «высокая». Для угроз, не обусловленных преднамеренной деятельностью, основным фактором оценки будут служить данные о частоте появления угрозы.

На основании таблицы 1 составим перечень уязвимостей для исследуемой программно-аппаратной системы. При составлении перечня будем использовать примеры

общих уязвимостей [3]. Перечень уязвимостей представлен в таблице 2. Перечень уязвимостей будет неполным, но достаточным для проведения всех этапов анализа риска. Для оценки вероятности реализации покажем, какие угрозы можно осуществить, используя данную уязвимость.

Таблица 2. Оценка вероятности реализации уязвимости
Table 2. Assessment of the probability of vulnerability

Вид уязвимости	Угрозы, использующие данную уязвимость	Оценка вероятности реализации
отсутствие резервных копий	изменение целостности переданной информации (У7)	средняя
незащищенные линии связи	ошибки передачи (У1); повреждение линий (У2); перехват информации (У4); анализ трафика (У5); изменение целостности переданной информации (У7); сбои в функционировании услуг связи (например, сетевых услуг) (У8)	высокая
передача ценной информации без применения шифрования	перехват информации (У4); изменение целостности переданной информации (У7)	высокая
пересылка паролей открытым текстом	перехват информации (У4); изменение целостности переданной информации (У7)	высокая
отсутствие подтверждений посылки или получения сообщения	перехват информации (У4); изменение маршрута направления сообщений (У6); изменение целостности переданной информации (У7)	средняя
неадекватное управление сетью	ошибки передачи (У1); перегруженный трафик (У3); сбои в функционировании услуг связи (например, сетевых услуг) (У8)	высокая
недостаточная подготовка персонала	ошибки пользователей (У9)	низкая
отсутствие механизмов отслеживания	перегруженный трафик (У3); ненадлежащее использование ресурсов (10)	средняя
отказ системы вследствие отказа одного из элементов	ошибки передачи (У1); сбои в функционировании услуг связи (например, сетевых услуг) (У8)	средняя
неадекватные результаты проведения технического обслуживания	сбои в функционировании услуг связи (например, сетевых услуг) (У8)	высокая

В рамках идентификации существующих защитных мер предполагается, что фрагмент системы Умного дома будет встраиваться в организацию с уже суще-

ствующей системой безопасности. Данная программно-аппаратная система предназначена для развертывания в помещении организации, и предполагается, что физический доступ к центру управления Умного дома будет ограничен, а также что на объекте уже существует защищенная сеть. Персонал предприятия, работающий с объектами системы Умного дома, должен быть ознакомлен с правилами работы с этими объектами. Предполагается, что на предприятии имеется квалифицированный сотрудник, который будет администрировать систему Умного дома.

Для оценки рисков составим таблицу ранжирования угроз по мерам риска. Для этого определим оценку воздействия как оценку актива, на которую направлена угроза (если активов несколько, то берется значение самого ценного актива), информацию об активе получим из таблицы 1, где высокая оценка соответствует оценке 1, средняя – 2, низкая – 3. Вероятность возникновения угрозы и перечень идентифицированных угроз получим из таблицы 2. Высокая вероятность возникновения угрозы соответствует оценке 1, средняя – 2, низкая – 3. В таблице 3 проранжируем опасности. Цифрой 1 обозначена угроза с самым низким рангом, т.е. угроза с самым малым воздействием и самой низкой вероятностью возникновения.

Таблица 3. Ранжирование угроз по мерам риска
Table 3. Ranking vulnerabilities by risks

Дескриптор Угроза	Оценка воздействия (ценности актива)	Вероятность возникновения угрозы	Мера риска	Ранг угрозы
У1	2	2	4	2
У2	2	1	2	4
У3	2	1	2	4
У4	2	1	2	4
У5	2	1	2	4
У6	1	2	2	4
У7	1	1	1	5
У8	2	2	4	2
У9	2	2	4	2
У10	2	2	4	2

В таблице 3 каждой идентифицированной угрозе соответствует её ранг, в зависимости от метрики риска. Угрозы с рангом два или один считаются угрозами, риск от которых приемлем. Также необходимо учитывать существующие меры защиты, которые могут снизить ранг угрозы.

Исходя из идентифицированных защитных мер, можно считать, что риски от угрозы кражи, повреждения линий связи и нелегального проникновения злоумышленника можно считать допустимыми, так как предполагается, что за сохранностью физических объектов на предприятии/организации следит служба охраны или другая служба, на которую возложена функция охраны объекта.

Защитные меры выбираются исходя из списка угроз, уровень риска которых считается недопустимым. Защитные меры можно разделить на организационные и технические. В защитные меры для технической части необходимо включить периодическую проверку работоспособности всех элементов системы. Это необходимо

для уменьшения вероятности аппаратных сбоев. Исходя из существующих защитных мер, на предприятии должна быть организованна защищенная корпоративная сеть. Это уменьшит вероятность перегрузки трафика, изменения конфиденциальности, целостности, доступности информации, передаваемой или обрабатываемой в программно-аппаратной системе. Также во избежание изменения целостности информации, передаваемой между клиентом и сервером, необходимо применять шифрование и хеширование. Для уменьшения вероятности использования программного обеспечения несанкционированными пользователями необходимо передавать и хранить пару логин/пароль в виде результата хеш-функции.

3. Реализация

В рамках программно-аппаратной системы Умного дома рассмотрим более детально угрозу перехвата информации для получения пары логин/пароль, отправляемых в процессе аутентификации клиент-серверного взаимодействия. Способ моделирования атаки: для снифинга сетей обычно используют сетевые карты в режиме прослушивания. Предположим, что злоумышленник имеет доступ в сеть, в которой функционирует приложение клиент системы Умного дома. Для перехвата процесса сетевого взаимодействия между двумя хостами A и B подменим IP адреса взаимодействующих хостов своим IP адресом, направив сетевым хостам A и B фальсифицированные ARP-сообщения с использованием дистрибутива Debian Linux и утилит Ettercap и Wireshark. Данные средства используются для сканирования сети, задания цели атаки, отправки ARP-сообщений и анализа трафика между атакуемым компьютером и маршрутизатором. В качестве результата атаки получены пара логин/пароль и пользовательские данные (Рис. 1), определяющие правила доступа в помещения Умного дома в зависимости от времени суток и роли пользователя.

Для выбора защитных мер необходимо проследить, через какие уязвимости можно реализовать выбранную угрозу. Используя таблицу 2, можно определить, что угрозу перехвата данных можно осуществить через такие уязвимости, как наличие незащищенных линий связи и передачу ценной информации без применения шифрования.

Устранение этих уязвимостей можно осуществить несколькими способами. Основным условием проведения такой атаки является нахождение нарушителя в сети, в которой работает атакуемый компьютер. Поэтому если сеть будет защищена и злоумышленник не сможет подключиться к ней, то он не сможет провести атаку. Отметим, что при внедрении Умного дома на предприятии, как правило, нет возможности такого контроля состояния сети, поэтому этот способ не подходит. Возможно использовать маршрутизаторы с поддержкой защиты и фильтрации ARP-пакетов. Также можно использовать сети VPN или VLAN. Но все перечисленные способы требуют дополнительных настроек сети или компьютеров, что делает систему Умного дома менее гибкой. В рамках реализованного прототипа для защиты от атаки «Человек посередине» используется шифрование передаваемой информации между клиентом и сервером. При этом даже если линии связи будут не защищены, то получить информацию из перехваченных пакетов у злоумышленника не получится. Используемый протокол SSL базируется на основе асимметричной криптографии

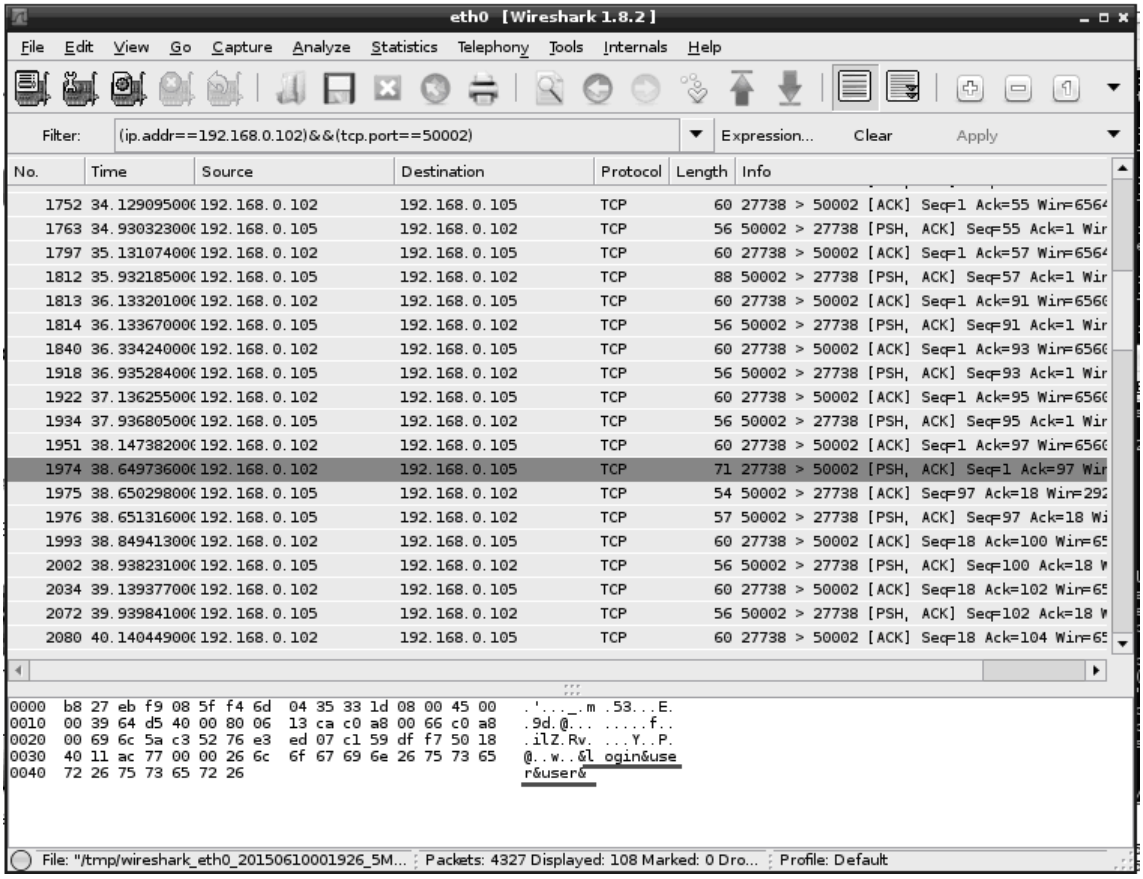

Рис. 1. Перехваченный пакет с парой логин/пароль

Fig. 1. Login/password packet captured

для аутентификации ключей обмена, используется также симметричное шифрование для обеспечения конфиденциальности, коды аутентификации сообщений – для целостности сообщений.

Для подключения протокола SSL воспользуемся библиотекой языка Python ssl. При помощи программы openSSL создадим самоподписанный сертификат для сервера, который он будет предоставлять клиентам. В openSSL сгенерируем приватный ключ с размером 1024 бит. Далее с помощью этого ключа сгенерируем самоподписанный сертификат. Теперь с помощью этого сертификата сервер может подтверждать валидность клиентов. Затем с использованием библиотеки ssl и самоподписанного сертификата создадим защищенное соединение между клиентом и сервером. Теперь вся информация, передаваемая между клиентом и сервером, будет зашифрована. После внедрения мер защиты – протокола SSL – необходимо проверить его работоспособность. Для этого смоделируем такую атаку на компьютер с использованием клиентского приложения. После отправки фальсифицированных ARP-сообщений мы получим пакеты, передаваемые между клиентом и сервером. Однако теперь сообщения зашифрованы и злоумышленник уже не может получить пару логин/пароль из этих пакетов без применения криптографического анализа.

Получить данные расписания из политики безопасности таким способом у злоумышленника теперь также не получится. При этом можно утверждать, что от угрозы перехвата информации, а в частности атаки «Человек посередине», система Умный дом защищена.

Заключение

Разработан и исследован фрагмент защищенной системы Умный дом, который является типовым примером системы Интернета вещей. Практическим результатом работы является разработанный фрагмент защищенной системы Умного дома в части функций контроля доступа в помещение. В соответствии с ГОСТ Р ИСО/МЭК 13335-1-2006 [3] и ГОСТ Р ИСО/МЭК ТО 13335-3-2007 [2] проведены и детально описаны основные этапы обеспечения безопасности построенной системы: установление границ рассмотрения; идентификация активов; оценка угроз; оценка уязвимостей; идентификация существующих мер безопасности; оценка рисков; выбор защитных мер.

Для заданного фрагмента системы проведена оценка обеспечения безопасности и определены актуальные угрозы. Также для идентифицированных актуальных угроз были разработаны защитные меры, для противодействия актуальным угрозам. Реализована одна из актуальных угроз – угроза перехвата критически важной информации системы. Реализация осуществлена путем моделирования атаки типа «Человек посередине». Далее реализованы программные меры защиты для противодействия установленной угрозе. Путём повторной попытки реализации угрозы было зафиксировано, что система Умный дом защищена от нее.

Список литературы / References

[1] Morgan S., *Internet Trends: 2007*, http://www.slideshare.net/rmesquita/morgan-stanley-technology-internet-trends.

[2] *ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий*, 2007, http://ohranatruda.ru/ot_biblio/normativ/data_normativ/51/51065.html;
[*GOST R ISO/MJeK TO 13335-3-2007. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Chast 3. Metody menedzhmenta bezopasnosti informacionnyh tehnologij*, 2007, URL: http://ohranatruda.ru/ot_biblio/normativ/data_normativ/51/51065.html, (in Russian)].

[3] *ГОСТ Р ИСО/МЭК 13335-1-2006. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий*, 2006, http://www.gosthelp.ru/gost/gost271.html;
[*Information technology. Security techniques. Part 1. Concepts and models for information and communications technology security management*, 2006, http://www.gosthelp.ru/gost/gost271.html, (in Russian)].

[4] Ричардсон М., Уоллес Ш., *Заводим Raspberry Pi*, Амперка, 2013, 230 с.; [Richardson M., Uolles S., *Zavodim Raspberry Pi*, Amperka, 2013, 230 c., (in Russian).]

[5] Лутц М., *Программирование на Python*, **2**, Символ-Плюс, 2011, 992 с.; [Lutc M., *Programmirovanie na Python*, **2**, Simvol-Pljus, 2011, 992 c., (in Russian).]

[6] Abraham D. G., Dolan G. M., Double G. P., “Transaction Security System”, *IBM Systems Journal*, **30**:2 (1991), 230–243.

[7] Десницкий В. А., Чечулин А. А., “Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами”, *Технические науки — от теории к практике*, 2014, № 39, 7–21; [Desnitsky V. A., Chechulin A. A., “Obobshhennaja model narushitelja i verifikacija informacionno-telekommunikacionnyh sistem so vstroennymi ustrojstvami”, *Tehnicheskie nauki — ot teorii k praktike*, 2014, № 39, 7–21, (in Russian).]

Alexandrov V. A., Desnitsky V.A., Chaly D.Y., "Design and Security Analysis of a Fragment of Internet of Things Telecommunication System", *Modeling and Analysis of Information Systems*, **23**:6 (2016), 767–776.

DOI: 10.18255/1818-1015-2016-6-767-776

Abstract. This paper comprises the development and implementation of systems using the concept of Internet of Things. In terms of active development of industries, use the concept of the Internet of Things, the information security problem is urgent. To create a protected module of information-telecommunication system which implements the Internet of Things concept, it is important to take into account all its aspects. To determine relevant threats, it is necessary to use the detailed risk analysis according to existing GOST standards when choosing protection measures, one must rely on identified relevant threats. Actual threats and necessary protective actions are determined in this paper for implementation of Smart House computer appliance module, in order to develop a protected part of Smart House, which is necessary for realization of room access control. We solved the following tasks in the work, namely, a description of the system Smart Home, a description of steps and evaluation system security Smart Home; implementation of hardware assembly and writing a code for the selected fragment of the system; safety evaluation of the selected fragment Smart House and identification of actual threats; make recommendations to counter current threats; software implementation of one of the most urgent threats and software implementation of protective measures for a selected threat. A feature of the work is an integrated approach to the design with the use of the intruder models, analysis of the system's assets and evaluation of their security.

Keywords: Internet of Things, information security

About the authors:
Vladislav A. Alexandrov, orcid.org/0000-0002-3748-5414, a candidate for a Master's degree,
ITMO University, 49 Kronverksky Pr., St. Petersburg 197101, Russia, e-mail: 2-q2@mail.ru

Vasily A. Desnitsky, orcid.org/0000-0002-3748-5414, PhD, senior researcher,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
39 Liniya 14-ya, Saint-Petersburg 199178, Russia, e-mail: desnitsky@mcomsec.spb.ru

Dmitry Y. Chaly, orcid.org/0000-0003-0553-7387, PhD, head of department,
P.G. Demidov Yaroslavl Stat University, 14 Str. Sovetskaya, Yaroslavl 150003, Russia, e-mail: dmitry.chaly@gmail.com

Acknowledgments:
[1]This research was financially supported by grants of RFBR (project №16-37-50035).
[2]This resear was financially supported by grants of RFBR (projects №14-07-00697, 14-07-00417, 15-07-07451, 16-29-09482 ofi_m, 16-37-50035).