Угрозы информационной безопасности систем типа «Умный дом», возникающие при управлении системой через Интернет

А. Д. Бондарева[1], Е. Н. Созинова[2], Д. А. Заколдаев[3], М. Жакиш[4]
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
[1]Bondareva.AD@yandex.ru, [2]s.ekaterina-nik@mail.ru, [3]d.zakoldaev@mail.ru, [4]zhakishmadina@gmail.com

***Аннотация*. В статье приведена общая схема построения систем типа «Умный дом». Были исследованы возможные угрозы информационной безопасности при управлении системой через Интернет. Определены основные объекты, на которые направлены атаки, а также возможная мотивация действий нарушителя.**

Ключевые слова: Умный дом; Интернет; угрозы информационной безопасности

В век расцвета информационных технологий создается множество различных устройств для облегчения жизни человека. Современный рынок техники включает огромное количество так называемых «умных» устройств, имеющих возможность выполнения дополнительных функций, помимо той, для которой они предназначены.

Большую популярность сейчас получает система «Умный дом» (УД), в которую входят такие приборы как: умные чайники, плиты, утюги, кофеварки, водонагреватели, розетки и цоколи, а также охранные и пожарные системы со множеством новейших датчиков. Неоспоримым преимуществом «Умный дом» является возможность управления всеми его устройствами, объединенными в общую сеть, с помощью только одного пульта. Такой пульт может быть реализован в виде различных панелей, компьютера, а также смартфона. Также «Умный дом» может управляться через Интернет, именно эта возможность так привлекает пользователей данной системы.

Однако Интернет является незащищенным каналом связи, что создает опасность как перехвата передаваемой информации, так и возможных компьютерных атак. Это может нанести большой финансовый и материальный ущерб владельцу «Умный дом».

Вследствие данной причины, в целях понимания опасности использования данного способа управления системой «Умный дом» целесообразно исследовать актуальные проблемы управления УД через сеть Интернет с точки зрения информационной безопасности (ИБ).

Для решения поставленной задачи представляется целесообразным исследовать структуру управления «Умный дом».

В общем случае «Умный дом» строится по принципу подключения всех устройств, датчиков и инженерных систем к центральному контроллеру (ЦК). Часто ЦК подключается к серверному компьютеру, с которого и осуществляется управление. Пользователь взаимодействует с ЦК или сервером через панель оператора, представленную в виде различных устройств.

При удаленном управлении ЦК или сервер должны подключаться к сети Интернет, для чего используется маршрутизатор. В таком случае команды, данные о состоянии системы УД и другая защищаемая информация пользователя передается через сеть общего пользования с использованием открытых протоколов передачи данных. Общую схему построения «Умный дом» можно представить в виде рисунка [1, 2].

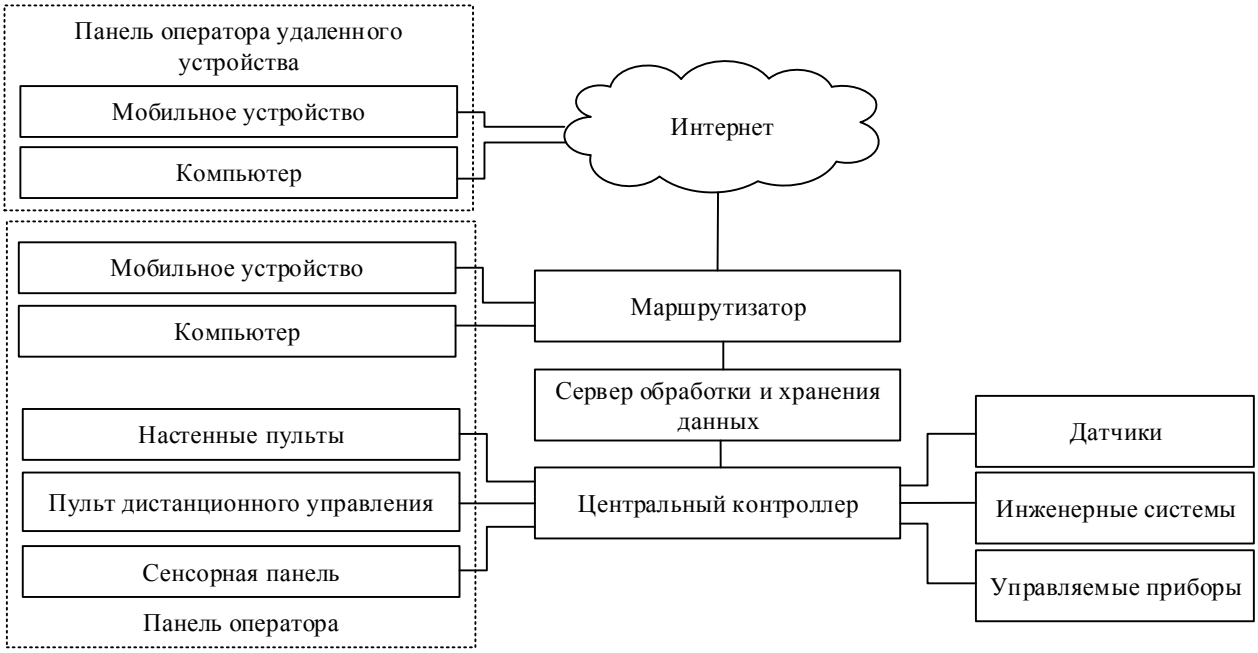

Рис. 1. Общая схема построения системы «Умный дом»

Из представленной схемы можно сделать вывод, что при реализации атаки через Интернет объектами, на которые направлены атаки являются:

- панель оператора – как основные устройства управления, так и удаленные;
- информационных поток между удаленным устройством и серверным компьютером;
- сервер обработки и хранения данных;
- центральный контроллер (в случае, если управление осуществляется через Wi-Fi без серверного компьютера);

Немаловажной является цель нарушителя, осуществляющего данные атаки. В соответствии с методикой определения угроз безопасности информации в информационных системах [3] мотивацией действий нарушителя может быть:

- нарушение правильного функционирования системы;
- получение конфиденциальной информации пользователя, содержащейся в мобильных устройствах, компьютерах и на сервере, а также ее изменение или уничтожение;
- физический доступ в помещение, в котором установлена система «Умный дом»;
- причинение имущественного ущерба;
- выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;
- любопытство или желание самореализации.

В общем случае можно сказать, что цель нарушителя - нарушить безопасность информации. Под безопасностью информации понимают такое состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, целостность и доступность [4]. Таким образом, вся деятельность нарушителя направлена на нарушение этих свойств, а именно на получение защищаемой информации или доступа к ней, искажение информации или блокирование доступа легитимных пользователей.

В рамках исследования проблем информационной безопасности, связанных с управлением УД через Интернет, целесообразно принимать во внимание только угрозы, осуществляемые из сети Интернет. Примеры данных угроз представлены в таблице.

ТАБЛИЦА I ПРИМЕРЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ УПРАВЛЕНИИ УД ЧЕРЕЗ ИНТЕРНЕТ

Нарушаемое свойство	Пример угрозы	Пояснения
Конфиденциальность	Угроза восстановления аутентификационной информации учётной записи пользователя в системе	Данная угроза опасна тем, что нарушитель может «подобрать» пароль к легальной учетной записи пользователя системы, и управлять «Умным домом» по собственному разумению и в своих целях.
	Угроза получения сведений о владельце беспроводного устройства управления УД	При управлении системой УД через беспроводное устройство, например, смартфон, нарушитель может получить данные о местонахождении владельца системы, что позволит ему осуществить попытку физического проникновения в помещение, в котором установлена система, во время отсутствия там владельца.
	Угроза перехвата данных, передаваемых по вычислительной сети	Нарушитель может «прослушивать сетевой трафик» для сбора и анализа сведений о системе, а также получать передаваемые по сети данные.
	Угрозы «фарминга» или «фишинга»	Скрытное (или реализованное в виде рекламы) перенаправление пользователя на поддельный сайт, на котором от пользователя требуется ввести защищаемую информацию.
Конфиденциальность	Угроза подмены содержимого сетевых ресурсов	Несанкционированный доступ к защищаемым данным пользователей сети путём скрытной подмены содержимого хранящихся или передаваемых по сети данных.
	Угроза несанкционированного доступа к системе по беспроводным каналам	Доступ нарушителя к информации из-за слабостей протоколов используемых для авторизации пользователей при подключении к точке беспроводного доступа.
	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Осуществляется нарушителем для получения сведений о возможности установления соединения с системой по данным портам, конфигурации самой системы.
	Угроза определения топологии вычислительной сети	Угроза заключается в возможности «сканирования сети» нарушителем для получения сведений о топологии сети, по которой построена система «Умный дом». Эти сведения могут быть использованы в дальнейшем при попытках реализации других угроз.
Конфиденциальность, целостность	Угроза неправомерного ознакомления с защищаемой информацией	Сюда относится получение нарушителем конфиденциальной личной информации пользователя, хранящейся в системе, что может позволить ему воспользоваться ею в целях собственной выгоды.
	Угроза перехвата банковской информации третьими лицами	В случае реализации данной угрозы, злоумышленник получит доступ к финансам владельца системы «Умный дом».
	Угроза неправомерных действий в каналах связи	Опасна возможностью нарушения работы системы или получением третьими лицами конфиденциальной информации. Означает вмешательство в информационный поток, передаваемый по каналу связи.
Конфиденциальность, доступность	Угроза подмены беспроводного клиента или точки доступа	Получение нарушителем защищаемой информации, передаваемой в ходе автоматического подключения к доверенным субъектам сетевого взаимодействия, подменённым нарушителем.
Доступность	Угроза приведения системы в состояние «отказ в обслуживании»	Отказ системой в доступе легальным пользователям, (например, при лавинообразном увеличении числа сетевых соединений с данной системой).
	Угроза деавторизации санкционированного клиента беспроводной сети.	Данная угроза заключается в том, что нарушитель может отключить панель оператора от сети и лишить его возможности управления системой на некоторое время.
Целостность, доступность	Угроза перехвата управления системой	Угроза заключается в возможности нарушителя осуществить несанкционированный доступ к системе и получении права управлять системой «Умный дом». Это может быть возможно, например, при наличии уязвимостей в протоколах сетевого/локального обмена данными.
Конфиденциальность, целостность, доступность	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Внедрения вредоносного кода в систему при посещении зараженных сайтов с управляющего устройства или серверного компьютера.
	Угроза некорректного использования функционала программного обеспечения	При получении доступа к управлению системой, нарушитель может использовать ее функции, чтобы оказывать на нее деструктивное воздействие. Например: отключить охранную сигнализацию и открыть электронный замок на входной двери, или включить все электроприборы в доме, вызвав этим скачок напряжения, который в свою очередь может вызвать возгорание или повреждение техники.
	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Нарушитель может осуществлять перехват трафика беспроводной сети, если подключится к беспроводной сети, (например, в полуавтоматическом режиме без ввода ключа шифрования).

Для реализации данных угроз, необходимо наличие слабых мест в системе и ее программном обеспечении. Основными уязвимостями УД являются:

- недостаточно надежные пароли (включая установленные по умолчанию пароли на доступ), позволяющие нарушителю обойти ограничения безопасности;

- отсутствие шифрования передаваемых данных, в том числе передача пароля в открытом виде, позволяющая нарушителю перехватить пароль;
- недостаточная проверка входных данных, позволяющая нарушителю получить доступ на чтение к произвольным системным ресурсам и оказать влияние на доступность системы;
- ошибки управления регистрационными данными, позволяющая нарушителю получить учетные данные пользователей;
- недостатки процедуры авторизации, позволяющая нарушителю получить доступ к устройству с привилегиями администратора или просматривать диагностическую информацию;
- недостатками процедуры аутентификации, позволяющая нарушителю выполнить произвольные команды и получить полный контроль над сервером;
- обратимость метода кодирования пароля, позволяющая нарушителю получить пароль доступа к контроллеру;
- уязвимость, вызванная переполнением буфера на стеке, позволяющая нарушителю повысить свои привилегии и выполнить произвольный код;
- выход операции за границы буфера в памяти, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации;
- недостатки разграничения доступа, позволяющие нарушителю выполнить произвольный код;

В результате проведенного исследования, следует сделать следующий вывод: несмотря на то, что управление системой «Умный дом» через Интернет, несомненно, является очень удобным для пользователя, оно несет в себе ряд угроз финансам и имуществу владельца системы. Кроме этого, нарушение работы УД может привести к опасности для жизни и здоровья людей, находящихся в помещении, в котором эта система установлена.

Эти угрозы нужно в обязательном порядке идентифицировать, проанализировать и оценить. В противном случае, наличие самой системы УД можно считать бессмысленной, а управление УД через Интернет может принести больше вреда, чем пользы.

В общем случае пользователю «Умного дома» надлежит принять ряд мер:

- выбирать более «сложные» пароли;
- не следует подключаться к системе через незащищенные сети общего пользования;
- в случае использования серверного компьютера при построении системы УД следует установить на него антивирусное программное обеспечение;
- по возможности, отказаться от хранения конфиденциальной информации на сервере.

Если планируется использовать определенные устройства для управления через Интернет, то при настройке УД следует рассмотреть следующие варианты:

- привязка MAC-адресов удаленных устройств, что не позволит подключаться остальным пользователям к данной сети, тем самым ее обезопасит;
- использование VPN-виртуальных частных сетей.

Производителям систем УД следует при разработке своих устройств предусмотреть использование двухфакторной аутентификации и защищенных протоколов передачи данных.

Список литературы

[1] А.Д. Бондарева, Е.Н. Созинова, К.А. Фаязов "Модель защищаемой информации в системах типа "Умный дом" // Научно-технический вестник Поволжья. №6 2017г. – С. 173-175. URL: http://ntvp.ru/files/%D0%9D%D0%A2%D0%92%D0%9F_2017_6.php (дата обращения: 10.02.2018)

[2] Д.В. Байгозин, Д.Н. Первухин, Г.Б. Захарова "Разработка принципов интеллектуального управления инженерным оборудованием в системе "Умный дом" // Известия Томского политехнического университета. Инжиниринг ресурсов.URL: https://elibrary.ru/item.asp?id=11901101 (дата обращения: 15.02.2018)

[3] Методика определения угроз безопасности информации в информационных системах. Проект. URL: https://fstec.ru/component/attachments/download/812 (дата обращения: 13.02.2018)

[4] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/gost-r-50922-2006 (дата обращения: 13.02.2018)

[5] Банк данных угроз безопасности информации URL: https://bdu.fstec.ru/threat (дата обращения: 15.01.2018)