Тип работы: ВКР (Выпускная квалификационная работа)

Предмет: Информационные ресурсы

ВВЕДЕНИЕ

В настоящее время предъявляются очень высокие требования к комфортности среды обитания:
1. Требования к эстетике;
2. Климатические требования (к температурному режиму, чистоте воздуха и др.);
3. Общебытовые (вода, газ, электричество, радио, телевидение, интернет, телефонная связь, наличие кухонных машин и систем гигиены саун и ванн);
4. Требования к безопасности и контролю за ней (безопасность жилища, хозяев дома и их близких);
5. Требования к надежности сложных систем (компьютеры, домашние кинотеатры, посудомоечные, стиральные машины, СВЧ-печи и др.)
Комплексное управление всеми указанными ресурсами реализуется в системах умного дома, которые получили широкое распространение. Так как данные системы являются программно управляемыми, актуальной задачей становится обеспечение их информационной безопасности.
Цель работы: разработка политики информационной безопасности для системы управления умным домом.
Задачами работы являются:
- анализ теоретических аспектов использования систем умного дома и их классификация;
- анализ вопросов обеспечения информационной безопасности при работе с системами умного дома;
- анализ угроз безопасности систем «умный дом»;
- обзор методов противодействия угрозам информационной безопасности;
- разработка алгоритмов противодействия угрозам информационной безопасности системам умного дома;
- разработка требований к обеспечению безопасности системы умного дома от перехвата информации посредством устройств съема информации.
Объект исследования: системы «умный дом».
Предмет исследования: системы обеспечения безопасности для систем «Умный дом».
Методы исследования: изучение литературных источников, нормативно-правовой базы, изучение технической документации средств защиты информации, анализ функционала систем умного дома, сравнения, включенного наблюдения.

1.Общая характеристика системы «Умный дом»

Термин "умный" дом появился в начале 1970-х годов с развитием информационных технологий и их

интеграции с системами жизнеобеспечения. На тот период под умным домом подразумевалось "здание, обеспечивающее продуктивное и эффективное использование рабочего пространства...".
Технология «Умный дом» обеспечивает управление следующими компонентами инженерных систем:
- Электроснабжение, что предполагает рациональное расходование электроэнергии (использование датчиков движения, двухаршинных систем и запуск оборудования на низком тарифе и др.);
- Освещение;
- Газоснабжение;
- Водоснабжение (включая системы очистки воды) и канализация;
- Вентиляция;
- Системы видеонаблюдения;
- Система контроля доступа;
- Управление телефонной связью;
- Телевидение;
- Системы очистки воздуха;
- Системы внешнего обогрева;
- Холодильные системы.
Интегрированное управление всеми указанными системами производится из единого центра управления с использованием специализированного программного и аппаратного обеспечения.
Одним из компонент системы «Умный дом» является дистанционный пульт «Умный Дом», заменяющий пульты управления от различных видео-, аудиоустройств, кондиционеров, спутниковых ресиверов. Также с использованием дистанционного пульта осуществляется управление осветительными приборами, в которых реализованы различные сценарии освещения. Также возможно использование настенных пультов управления.
Связь между помещениями осуществляется в режиме селектора.
Средства коммуникации внутри системы реализованы с использованием ресурсов Интернета, в том числе мессенджеров, средств электронной почты, мобильных сервисов.
При входе в умный дом необходимо с помощью него снять систему с охраны, а при уходе из дома — устанавливать систему на охрану. Также в системе реализована возможность просмотра протокола сообщений о событиях, произошедших за время отсутствия, ввода номера телефонов экстренных служб [3].
Управление системой «Умный дом» может осуществляться с использованием персонального компьютера, мобильных устройств, а также специализированных управляющих систем.
Наиболее распространенные технологии управления системой «Умный дом»:
- X10. Данная система определяет технологии и протокол передачи управляющих сигналов электронными модулями, к которым подключены бытовые приборы, с использованием обычной электропроводки или беспроводных каналов;
- 1-Wire, предполагающая использование специализированых микроконтроллеров и домашней электрической сети;
- Ethernet, управление в рамках которой производятся по протоколу TCP/IP.
Вместе с этим, система «умный дом», как и любая система, использующая информационные технологии, имеет свои уязвимости, связанные с возможностью ошибок в ее функционировании, которые могут быть обусловлены различными факторами: ошибками в прошивках устройств, ошибками при обновлениях ПО, несанкционированным доступом извне. Угрозы информационной безопасности при использовании TCP/IP предполагает возможность функционирования вредоносного ПО. Таким образом, при нарушении требований информационной безопасности в системе «Умный дом» возможны ситуации, при которых как минимум нарушается нормальная жизнедеятельность жильцов дома и, как максимум, могут возникать опасности пожаров, затоплений, выхода из строя электроприборов. Кроме того, актуальной угрозой также являются возможные действия злоумышленников, которые посредством программных или аппаратных средств могут получить доступ к управлению системой и, например, отключит сигнализацию, систему видеонаблюдения или охраны и, таким образом, вывести из строя систему безопасности дома. Таким образом, при установке системы «Умный дом» необходимо также учитывать требования к обеспечению информационной безопасности ее компонент.

2.Анализ теоретических аспектов информационной безопасности технологических систем

2.1. Обзор протоколов, используемых в системах типа «Умный дом»

Основными типами используемых протоколов в системах типа «Умный дом» являются:

- ZigBee;
- Z-wave;
- Bluetooth Smart Low Energy.

Рассмотрим особенности функционирования данных систем.

1. ZigBee

Протокол беспроводной связи ZigBee может использоваться для решения большого количества задач, среди которых значится и автоматизация домов. Тем не менее, за десять лет своего существования этот универсальный стандарт так и не стал по-настоящему популярным. Увы, создатели протокола попытались реализовать полный комплекс задач для системы «Умный дом», что привело к появлению ряда проблем безопасности, к которым можно отнести [5]:

- Проблемы совместимости оборудования, что приводит к некорректной работе компонент системы разных производителей;
- Проблемы при использовании различных профилей компонентами системы – отказ системы при одновременной активации различных профилей.

Перспективное развитие системы: использование IP-протокола.

Сетевая архитектура данного стандарта спроектирована с поддержкой топологии «звезда», петлевых и древовидных кластерных топологий (гибрид между «звездой» и «петлей»). Петлевая архитектура сети обладает возможности автоконфигурирования и автовосстановления, поскольку включает в себя разветвленную сеть маршрутов передачи данных. Сеть может работать в импульсном режиме, либо с гарантированном таймслотом. Таймслот обеспечивает возможность повторного посыла данных с высоким приоритетом.

Многопетлевая топология сети родилась в следствие реализации поддержки разнородных физических и логических устройств, подчиняющихся спецификации ZigBee. Это снижает стоимость если не всех, то многих сетевых устройств.

Согласно протоколу ZigBee, существует два типа физических устройств: полнофункциональные устройства, называемые FFD (full function device), и устройства с ограниченной функциональностью, называемые RFD (reduced function device). Полнофункциональные устройства обычно соединяются вместе через линии электросети. Они могут действовать как сеть и осуществлять сетевую координацию, а также обнаруживать в сети другие полнофункциональные устройства и устройства с ограниченной функциональностью.

Протокол ZigBee описывает логические устройства, такие как сетевые координаторы, маршрутизаторы и конечные устройства. Функция координации сети предполагает в инициализацию беспроводной сети ZigBee, а также управление сетевыми узлами и хранение информации от них. Маршрутизаторы ZigBee производят передачу сообщений между соседними узлами. Конечные устройства сети ZigBee могут быть только краевыми узлами, поскольку не участвуют в маршрутизации сообщений. Применяемое в данном протоколе ПО используется в качестве дополнения к компьютерным программам, лежащим в основе 802.15.4.

2. Z-Wave

Z-Wave представляет собой запатентованный беспроводной протокол связи, разработанный для домашней автоматизации, в частности для задач системы умного дома. Технология применяет маломощные и миниатюрные радиочастотные модули, встраиваемые в бытовую электронику и различные устройства, такие как освещение, отопление, системы контроля доступа, развлекательные системы и бытовую технику. Данный стандарт представляет собой беспроводную радио технологию, разработанную специально для дистанционного управления. В отличие от Wi-Fi и других IEEE 802.11 стандартов передачи данных, предназначенных в основном для больших потоков информации, Z-Wave использует диапазон частот до 1 ГГц и оптимизирован для передачи простых управляющих команд (например, включить/выключить, изменить громкость, яркость и т. д.). Выбор низкого радиочастотного диапазона для Z-Wave обуславливается малым количеством потенциальных источников помех.

Преимуществами Z-Wave являются [6]:

- Малое энергопотребление;
- Низкая стоимость;
- Возможность встраивания в различные бытовые устройства;
- Совместимость устройств Z-Wave различных типов;

Технология Z-Wave использует сетевые решения типа mesh, в рамках которых каждый узел или устройство может производить приём и передачу управляющих сигналов для других устройств сети с использованием промежуточных соседних узлов. Mesh представляет собой самоорганизующуюся сеть с маршрутизацией, зависимой от внешних факторов — например, при возникновении преграды между двумя ближайшими узлами сети, сигнал пойдет через другие узлы сети, находящиеся в радиусе действия.
Протокол Z-Wave также определяет класс «устройств-монтажников» (Installers), применяемых для централизации процесса установки сети, а также устройств «мостов» (Bridge), соединяющих вместе разнородные сети. Определяя несколько классов устройств с пониженной функциональностью, разработчики протокола Z-Wave стремились снизить стоимость системы, поэтому пожертвовали простотой коммуникации равноправных узлов ЛВС. Подобная «сделка» вполне понятна, если принять во внимание сложность маршрутизации. Но учитывая то, что различные устройства обладают разнличными возможностями, пользователи сети должны обладать знаниями о том, как работает такая сеть. Наиболее серьезным ограничением для пользователя сети Z-Wave является требование к однотипности мастер-контроллеров.
3. Bluetooth Smart Low Energy
Bluetooth Low Energy (или Bluetooth Smart) — версия, экономящая заряд аккумулятора. При этом радиус действия ограничен 10 м, а скорость передачи данных — 1 Мбит/с, но при передаче потребляется не более 10 мА.
Большая часть нововведений Bluetooth 4.1 относится к защите от помех. Сейчас Bluetooth является стандартным компонентом смартфонов и планшетов; вскоре в эти устройства начнут внедряться и LTE-модули.
К сожалению, Bluetooth использует нелицензируемый частотный диапазон 2,45 ГГц (наряду с 2,6 ГГц), а также диапазон LTE в России и в других странах. Это может привести к взаимным помехам (см. диаграмму). Проблема заключается в том, что пользователь никак не может повлиять на сигнал LTE.
От разработчиков Bluetooth требовались определенные действия, чтобы избежать помех. И именно это было сделано в новой версии.
Для минимизации помех в Bluetooth 4.1 будет встроен фильтр диапазона LTE. Если передатчик LTE создает помехи для передаваемых по Bluetooth данных, Bluetooth 4.1 моментально на это отреагирует.
Таким образом, большая часть протоколов, используемых системой, основаны на функционировании беспроводных сетей и радиоканалов. Основными угрозами функционирования подобных систем являются:
- наведение радиопомех;
- прослушивание.
В рамках данной работы проведем анализ вопросов обеспечения безопасности функционирования системы.

2.2. Обеспечение информационной безопасности при эксплуатации инженерных систем «умный дом»

Защита системы умного дома представляет собой компоненты защиты радиоканала, а также защиты протокола TCP/IP, используемого некоторыми устройствами системы.
Основной целью обеспечения безопасности систем автоматизации является поддержание их в рабочем состоянии, в первую очередь, предотвращение проникновения чужеродного программного обеспечения – вирусов и другого вредоносного ПО [3].
Компонентами управления инженерными системами умного дома являются программные продукты различного вида. Как известно, любая информационная система должна включать в свой состав компоненты информационной безопасности. Для каждой из информационной систем необходимо сформулировать модели угроз и модели злоумышленников, в соответствии с которыми строится архитектура информационной безопасности. В случае систем управления умным домом в качестве угроз информационной безопасности могут выступать [2]:
- активность злоумышленников;
- недокументированные возможности установленного ПО;
- активность вредоносного ПО;
- нарушения функциональности ПО;
- внешние атаки на информационную систему управления инженерными системами умного дома;
- отключение и нестабильная работа системы электроснабжения;
- активность атмосферного электричества;
- нарушение в системе разграничения доступа и др.

В качестве злоумышленников могут выступать как внешние заказчики, недобросовестные производители микроконтроллеров, так и инсайдеры – сотрудники предприятия.
Рассмотрим принципы существующих подходов к обеспечению информационной безопасности управления инженерными системами умного дома.
Практика показывает, что необходимость защиты управления инженерными системами умного дома может быть связана с [2]:
- повсеместным внедрением систем Windows и связанных с этим типовых угроз;
- отсутствием блокировки системы на физическом уровне, что создает угрозы запуска не предусмотренного технологией работы программного обеспечения и нарушения функциональности управления инженерными системами умного дома;
- отсутствие разделения задач, связанных с функционированием системы умного дома и использования домашнего Интернета в рамках одной локальной сети (зачастую вероятны ситуации, в которых и система «Умный дом» и домашние мобильные устройства и компьютеры, работающие в Интернете, работают в одной подсети и при проникновении вредоносного ПО на домашний компьютер оно же начинает влиять на функционал умного дома);
- множественностью точек входа в сеть на программно-сетевом уровне (зачастую для сетей с системой «умный дом» характерна ситуация, когда к оборудованию умного дома можно получить доступ с устройств, не связанных с системой, например, при включенном беспроводном доступе и получении к нему доступа от злоумышленников);
- ошибками в настройках парольной защиты;
- ошибками при обновлении программного обеспечения, что может приводить к некорректной работе устройств и, в случае отсутствия необходимой защиты, даже к выходу их из строя;
- необходимостью наличия инженерно-технической защиты.
Основной целью информационной безопасности (ИБ) управления инженерными системами умного дома является поддержание необходимого уровня безопасности, а также поддержка непрерывности работы оборудования.
Так как в настоящее время, как было сказано выше, сети умного дома в своей архитектуре сопряжены с Windows-сетями, то основными путями проникновения зловредного ПО в систему являются характерные пути для Windows-систем [3]:
- файлообменныке сети, FTP;
- уязвимости в сетевом ПО;
- использование внешних носителей информации (USB, CD/DVD);
- использование мобильных устройств.
Защита от угрозы безопасности производится в 6 этапов, сформулированных на основе стандартов NIST, ISA, а также стандартов промышленной ИБ, которые в настоящее время находятся в процессе интеграции в единый международный стандарт IEC 62443. Они описывают не только механизмы безопасности, предназначенные для систем управления, но и требования к поставщикам таких систем. Уже существуют системы сертификации для поставщиков систем ИБ для инженерных систем.
Реализация политик безопасности на уровне сети должна присутствовать как фундамент внедрения систем ИБ умного дома.
Этап 1. Обеспечение безопасности периметра сети.
В рамках данного этапа предполагается установка безопасности периметра сети, для контроля тех точек, где чужеродное ПО может проникнуть в систему автоматизации умного дома. Как видно из рисунка 1, в типичной системе управления корпоративные сети находятся в модели Пердью на уровнях 3 и выше, в то время как сети систем управления и полевые шины – на уровнях 2 и ниже.

1. Умный дом: новейшие технологии. [Электронный ресурс]. Режим доступа: http://koffkindom.ru/umnyj-dom-novejshie-texnologii-dlya-realnoj-zhizni.htm
2. Умный дом своими руками. [Электронный ресурс]. Режим доступа: http://kakpravilnosdelat.ru/umnyj-dom-svoimi-rukami/
3. 6 шагов к информационной безопасности. [Электронный ресурс]. Режим доступа: http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp
4. Программные закладки в бизнес-приложениях. [Электронный ресурс]. Режим доступа: http://bezopasnik.org/article/31.htm

5. Протокол ZigBee. [Электронный ресурс]. Режим доступа: http://www.ferra.ru/ru/digihome/review/SmartHome-ZigBee/
6. Умный дом на базе Z-Wave. [Электронный ресурс]. Режим доступа: https://geektimes.ru/post/257630/
7. Протоколы системы умного дома. [Электронный ресурс]. Режим доступа: http://bacnet.ru/knowledge-base/articles/index.php?ELEMENT_ID=746
8. Источник питания для системы «Умный дом». [Электронный ресурс]. Режим доступа: http://smartron.ru/katalog/smartron/smarthome/domashnjaja-avtomatika/knx-eib/sistemnoe/istochnik-pitaniia-knx-eib-230v-30v-nagruzka-do-640ma-funktsiia-ibp-do-dvukh-akkumuliatorov-12v-12a-ch
9. Устройство системы грозозащиты. [Электронный ресурс]. Режим доступа: http://www.rmnt.ru/story/electrical/682949.htm
10. Сборно-разборные экранирующие камеры. [Электронный ресурс]. Режим доступа: http://faradey.ru/catalog/ekranirovannyie-pomeshheniya/sborno-razbornaya-kamera/
11. Грибунин В.Г., Чудовский В.В. Реализация требований комплексной системы защиты информации. – М.: Академия, 2017. – 533 с.
12. Королев Е. Н. Администрирование операционных систем : учебное пособие / Е. Н. Королев. - Воронеж : Воронежский государственный технический университет, 2017. - 85 с.
13. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск : ОмА МВД России, 2016. - 87 с.
14. Белобородова Н. А. Информационная безопасность и защита информации : учебное пособие / Н. А. Белобородова; Минобрнауки России, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования "Ухтинский гос. технический ун-т" (УГТУ). - Ухта : УГТУ, 2016. - 69 с.
15. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки : [учебное пособие] / А. В. Кондратьев. - Москва : Горячая линия - Телеком, 2016. - 304 с.
16. Смычёк М.А. Информационная безопасность и защита информации : учебное / М.А. Смычёк. - Нижний Новгород : Нижегородский государственный технический университет, 2016. – 125с.
17. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с
18. Никифоров С. Н. Защита информации: учебное пособие / С.Н. Никифоров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный архитектурно-строительный университет. - Санкт-Петербург : СПбГАСУ, 2017. – 76 с.
19. Никифоров С. Н., Ромаданова М. М. Защита информации. Пароли, скрытие, удаление данных: учебное пособие / С. Н. Никифоров, М. М. Ромаданова. - Санкт-Петербург : СПбГАСУ, 2017. - 107 с.
20. Никифоров С. Н. Защита информации: защита от внешних вторжений : учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 82 с
21. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. - Саратов: Профобразование, 2017. - 702 с
22. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С.. - Тамбов : ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017.