Тип работы: Отчет по практике

Предмет: Педагогика

Содержание Введение 3 1.Общая характеристика системы «Умный дом» 5 2.Анализ теоретических аспектов информационной безопасности технологических систем 8 2.1. Обзор протоколов, используемых в системах Интернета вещей 8 2.2. Обеспечение информационной безопасности при эксплуатации инженерных систем Интернета вещей 12 Заключение 18 Список использованных источников 19

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.)
3

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.

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;
4

- Холодильные системы. Интегрированное управление всеми указанными системами производится из единого центра управления с использованием специализированного программного и аппаратного обеспечения.

2.Анализ теоретических аспектов информационной безопасности технологических систем 2.1. Обзор протоколов, используемых в системах Интернета вещей 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
5

между «звездой» и «петлей»). Петлевая архитектура сети обладает возможности автоконфигурирования и автовосстановления, поскольку включает в себя разветвленную сеть маршрутов передачи данных.

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. 2.2. Обеспечение информационной безопасности при эксплуатации инженерных систем Интернета вещей

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].
6

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
7

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.

Список использованных источников

1. Умный дом: новейшие технологии. [Электронный ресурс]. Режим доступа: http://koffkindom.ru/umnyj-dom-novejshie-texnologii-dlya-realnojzhizni.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-informacionnojbezopasnosti-asu-tp
8

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/domashnjajaavtomatika/knx-eib/sistemnoe/istochnik-pitaniia-knx-eib-230v-30v-nagruzka-do640ma-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. Сосински Б., Дж. Московиц Дж. Windows 2008 Server за 24 часа. – М.: Издательский дом Вильямс, 2008. 11. NIST SP800-122 «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)», BS10012:2009 «Data protection – Specification for a personal information management system», ISO 25237:2008 «Health informatics – Pseudonymization» 12. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с 13. Гук М. Аппаратные средства локальных сетей. Энциклопедия. – СПб.: Питер, 2010. – 576с. 14. Иопа, Н. И. Информатика: (для технических специальностей): учебное пособие– Москва: КноРус, 2011. – 469 с. 15. Акулов, О. А., Медведев, Н. В. Информатика. Базовый курс: учебник – Москва: Омега-Л, 2010. – 557 с.
9

16. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия Интернет-университет информационных технологий - ИНТУИТ.ру, 2012 17. Могилев А.В.. Информатика: Учебное пособие для вузов - М.: Изд. центр "Академия", 2011 18. Партыка Т.Л. Операционные системы и оболочки. - М.: Форум, 2011 19. Под ред. проф. Н.В. Макаровой: Информатика и ИКТ. - СПб.: Питер, 2011 20. Новиков Ю. В., Кондратенко С. В. Основы локальных сетей. КуПК лекций. – СПб.: Интуит, 2012. – 360с.