Системы безопасности умных домов

Автор статьи: АБАХТИМОВ АЛЕКСЕЙ АЛЕКСАНДРОВИЧ, студент 1-ого курса Московского политехнического университета, направление «Управление в технических системах», кафедра «СМАРТ»-технологии.

Научный руководитель: ЛУШИНА ОЛЬГА ВЛАДИМИРОВНА, преподаватель кафедры «Инфокогнитивные технологии» Московского политехнического университета

Аннотация. В статье освещается проблема информационной безопасности интеллектуальной собственности пользователя системы «умный дом». Проводится анализ и сравнение качества обеспечиваемой информационной безопасности двух фундаментальных конфигураций, используемых в построении системы «умного дома». Рассматривается вариант решения проблемы информационной безопасности при помощи совмещения двух подходов к построению системы «умного дома».

Ключевые слова: информационная безопасность, интернет вещей, умный дом.

Централизованные системы

Централизованная система умного дома – такой способ организации, где система состоит из элемента управления, центрального контролера и управляемого оборудования, объединенных в единую телекоммуникационную сеть для приема и передачи сигналов или команд управления. «Сердцем» всей системы является контроллер (логический модуль) с большим, но часто ограниченным количеством выходов, к которому подключаются все датчики и устройства ввода/вывода данных. Он является звеном, которое позволяет подключать множество дополнительных устройств, сообщающихся друг с другом при помощи адресации и пересылки, происходящей в центральном логическом модуле, а не при обращении к другому устройству напрямую с помощью шинного интерфейса, как это происходит в децентрализованных системах. Есть отдельные случаи реализации системы, где отдельные компоненты также имеют свои контроллеры, которые позволяют делать структуру организации всей системы более сложной, но одновременно и более гибкой. Однако мы не рассматриваем данную конфигурацию ввиду того, что дополнительные иерархические уровни системы способны лишь запутать нас, но не привнести новый смысл в исследование. Как правило, именно на центральном контроллере и находится основная программа, управляющая взаимодействием всей системы

УД. Такой подход обеспечивает комфорт в управлении всеми инженерными системами в едином интерфейсе.

Отдельные реализации построения централизованных систем УД за счет специальных преобразователей ЦЛУ позволяют легко интегрировать в среду с единой платформой инородные устройства от других производителей. Централизованная среда позволяет создавать сложные сценарии, так как устройствам необязательно постоянно сообщаться друг с другом с целью получения каких-либо данных – они уже хранятся в едином общем блоке, центральном контроллере, и любому устройству достаточно просто обратиться к нему для получения информации о любом другом устройстве. Это позволяет создавать сложные программные алгоритмы для получения каких-либо особых данных, требующих особых расчетов и порядка взаимодействия между устройствами сети.

Децентрализованные системы

Децентрализованная среда умного дома – способ организации сети, где каждый её модуль обладает независимостью. Децентрализованный подход подразумевает реализацию системы с распределенной логикой исполнения команд и ответов на запросы. В отличие от централизованного подхода, в децентрализованном отсутствует центральный контроллер, некое центральное логическое устройство, являющееся центром, обрабатывающим все поступающие с устройств данные и обрабатывающее их согласно заложенной в него программе. В этом случае система состоит из датчиков, сенсоров и активаторов. Датчики обнаруживают изменение каких-либо характеристик в доме, движения или изменения заданных в программе параметров, и реагируют на эти изменения набором команд, посылающимися исполняющим устройствам, которые включаются активаторами. Здесь каждое исполнительное устройство имеет свой процессор и свой модуль памяти. В частном случае компоненты осуществляют передачу последовательно и асинхронно. Конфликты при передаче сообщений разрешаются расстановкой приоритетов согласно установкам конкретного протокола связи. Предназначенная для передачи информация собирается в пакеты (блоки данных заданного размера) и через шину передается приемнику или группе приемников. Сообщение получают все абоненты, подключенные к шинному интерфейсу, но реагируют на него только те, кому оно адресовано.

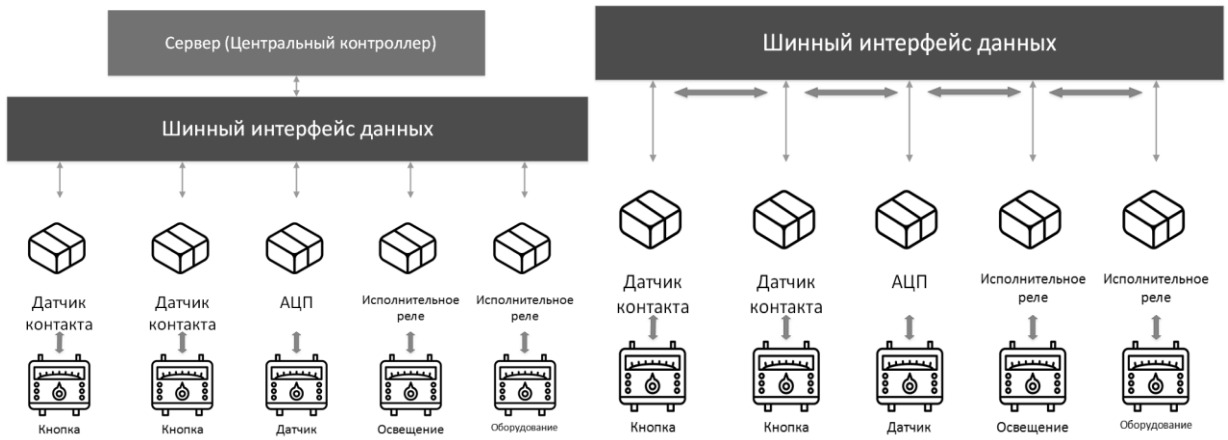

Рисунок 1-2. Структурные схемы двух фундаментальных подходов к построению систем УД. 1 – структура децентрализованной системы, 2 – структура централизованной системы

В следующей таблице приводится краткое описание недостатков и преимуществ функционирования и работы сетей, рассматривается степень удобства их масштабируемости и перенастройки.

Тип системы	**Преимущества подхода**	**Недостатки подхода**
Централизованная	1. Поддержка сложных сценариев 2. Совместимость с широким спектром устройств 3. Дешевизна периферийных устройств 4. Единый интерфейс для управления разнородными устройствами	1. Низкая надежность 2. Относительно высокая цена контроллера 3. Сложное программирование системы и дороговизна услуг написания программы «со стороны»
Децентрализованная	1. Высокая популярность => огромное разнообразие доп. оборудования и лёгкость в обслуживании 2. Легкая масштабируемость систем 3. Большой выбор управляющих панелей 4. Энергонезависимая память отдельных компонентов сети 5. Автономная работа каждого модуля	1. Необходимость настройки каждого компонента системы 2. Крайняя степень сложности составления сложных сценариев 3. Высокая стоимость отдельных компонентов сети 4. (В частном случае) Более низкая скорость обработки данных

Таблица 1. Сравнение производительности двух подходов к построению систем УД и примеры компаний, ведущих разработки систем на базе одного из подходов

Безопасность

Система “умный дом” представляет собой объект информатизации подверженный угрозам информационной безопасности. Вопрос защиты интеллектуальной собственности особенно актуален для технологии «умный дом», так как наличие уязвимостей в системе такого типа ставит под угрозу личные данные пользователя, а также его жизнь. Обилие решений от разных производителей на рынке становится барьером для установления единых стандартов по мерам защиты информации УД, например, из-за различий в используемых протоколах на том или ином уровне или из-за несопоставимого между собой ПО. В силу того, что технология “умный дом” не имеет единой методологии для построения системы, оценка и обеспечение информационной безопасности являются сложно выполняемыми, так как требуется индивидуальный подход к каждой системе. Для осуществления единого метода оценки и сравнения качества информационной безопасности систем УД предложено использовать условное деление всех систем на централизованные и децентрализованные (т.е. по структуре и организации сети УД).

Под угрозой безопасности информации будем понимать совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Под уязвимостью понимается свойство информационной системы, обусловливающее возможность реализации угроз безопасности для обрабатываемой в этой системе информации. Для определения рода каждой из потенциальных угроз воспользуемся наиболее популярной моделью безопасности, предложенной Зальцером (Saltzer) и Шредером (Schroeder) еще в 1974 году, носящей название Триада «Конфиденциальность, Целостность, Доступность» (КЦД). Хотя данная модель в условиях современных реалий перестает быть универсальной и не подходит для классификации множества современных информационных угроз в отличие от ряда усовершенствованных, более полных и актуальных на настоящее время моделей, в контексте исследования основных уязвимостей системы УД будет достаточно использования классической триады Зальцера-Шредера.

В соответствии с этой моделью любое правонарушение в сфере информационной безопасности можно отнести к одной из следующих групп: нарушение конфиденциальности, нарушение целостности, нарушение доступности информации,

Угрозы информационной безопасности УД по природе возникновения можно разделить на две категории: угрозы, обусловленные человеческим фактором и естественные угрозы. В частности,

угрозы первой группы различаются по способу осуществления: целенаправленные (преднамеренные) и случайные (непреднамеренные). Нам интересны лишь преднамеренные угрозы, обусловленные человеческим фактором.

Предложенный способ обеспечения безопасности системы умного дома

Рекомендуемое решение, которое удовлетворяет конечной цели исследования, – найти безопасную и производительную конфигурацию сетей УД, – это гибридный (смешанный) вариант построения сети (т.е. включающий в свою структуру элементы централизованного и децентрализованного подходов к построению систем УД).
«Хаб» (центральный логический модуль, центральный контроллер, сервер, станция) – центральное логическое устройство, обрабатывающее данные и осуществляющее работу системы по заданному сценарию

Д1, Д2, Д3 – исполнительные устройства и/или сенсоры, являющиеся элементами первой основной подсистемы централизованного типа построения, отвечающие за ресурсосбережение и функционал так называемого «мультирума», т.е. за функционал, основной целью которого является улучшения качества проживания пользователя в целом.

Д4, Д5, Д6, Д7 - исполнительные устройства и/или сенсоры, являющиеся элементами второй основной подсистемы децентрализованного типа построения, отвечающие за обеспечение физической и материальной безопасности пользователя и его окружения путём реагирования на получение основных сведений от ПДУ о потенциальной угрозе для основной централизованной системы в соответствии с предписанным алгоритмом работы для каждого конкретного датчика. Чаще всего эти датчики представлены в виде классических элементов системы охранной безопасности: видеокамеры, аудио-прослушивание, экстренный вызов спецслужб, блокирование проходов, дверей, окон, имитация присутствия.

Угроза взлома – совокупность факторов вредоносного характера (атака, перехват данных, попытка взлома), представляющих актуальную угрозу для корректного функционирования системы и хранящихся в ней данных (см. триада КЦД).

Пара «ОДУ-ПДУ» (отправитель данных об угрозе и получатель данных об угрозе) – два устройства-представителя двух основных подсистем, связанные между собой по обособленному каналу связи, защищенному каким-либо протоколом, устойчивым к большинству видов внешнего вмешательства в работу системы. После регистрации Угрозы взлома пакет

минимального приемлемого размера, содержащий основные данные об угрозе и злоумышленнике (зависит от конкретной реализации, в частности – от используемых производителем технологий классификации угроз и методов их обнаружения на начальной стадии) передаётся по закрытому защищенному каналу от ОДУ к ПДУ. При технология, реализующая собой логику ОДУ может быть встроена случайно в один из рядовых датчиков централизованной системы. ПДУ – модуль децентрализованной системы, отсылающий на все элементы своей системы релевантную для каждого конкретного элемента информацию об угрозе.

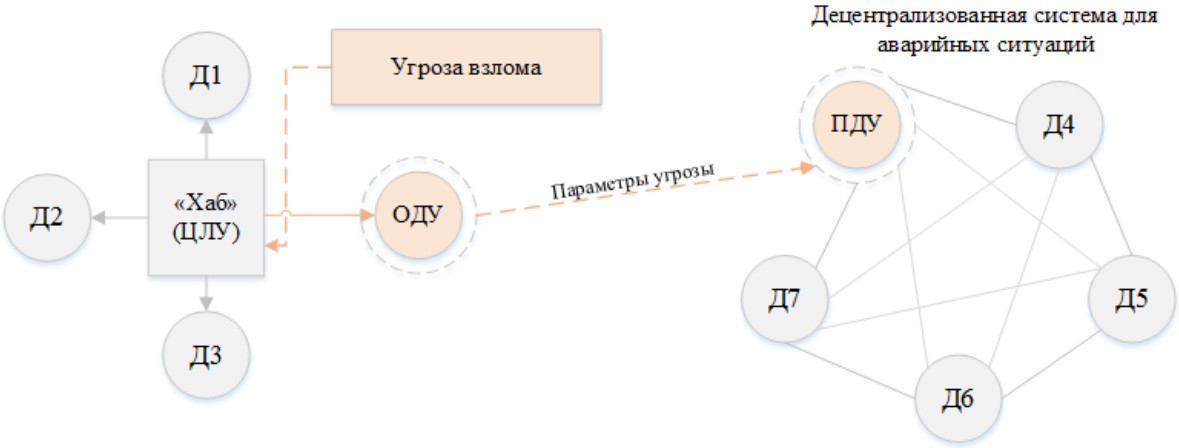

Рисунок 3. Первый этап реагирования всей системы на внешнюю угрозу

Алгоритм взаимодействия элементов общей сети в случае аварийной ситуации (детектировании потенциальной угрозы для системы):

1. Угроза зарегистрирована встроенными методами защиты ЦЛУ (определены производителем оборудования);

2. Параметры потенциальной угрозы подсистемы 1 с помощью специального передатчика «ОДУ» пересылаются на приёмник «ПДУ» подсистемы 2 в соответствии с протоколами связи, заданными для обособленного защищенного скрытого канала связи между подсистемами;

3. Элементы подсистемы 2 становятся доступными для работы и действуют либо по заданному алгоритму, либо ждут действий со стороны человека (в соответствии с заложенной логикой). Элементы централизованной системы перестают работать автономно и работают в режиме ручного управления (классическое включение с помощью нажатия на кнопку, например).

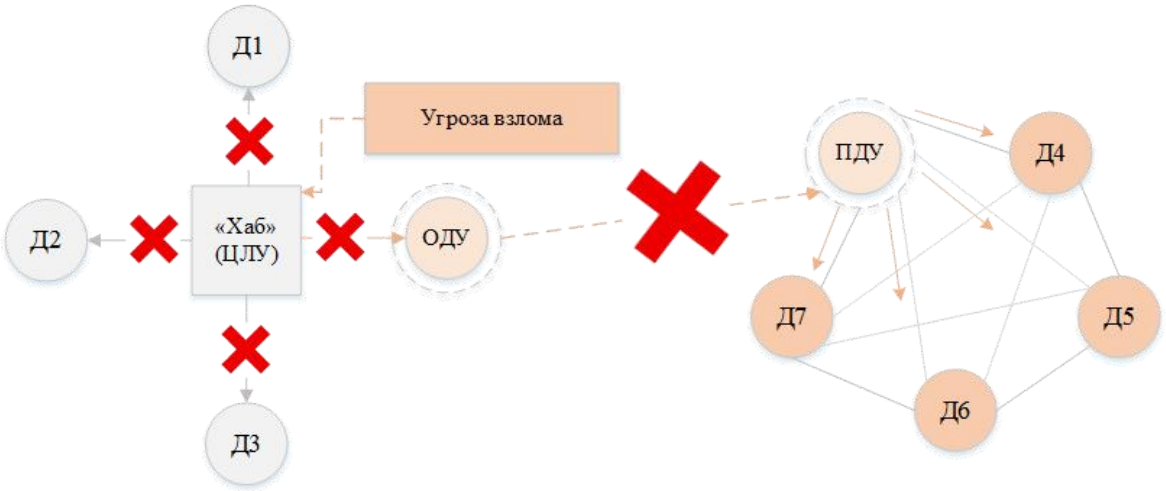

Рисунок 4. Второй этап реагирования всей системы на внешнюю угрозу

Заключение

В статье была освещена актуальность проблем информационной безопасности систем технологии «умный дом», а также отражён текущий уровень уязвимости технологии «умного дома» к самым распространенным угрозам. Рассмотрев два типа систем технологии «умный дом», автор предложил гибридную структуру сети с совмещением двух фундаментальных подходов к построению систем с целью разделения функционала на две подсистемы (первая отвечает за функционал так называемого «мультирума» и ресурсосбережение, вторая – за охранную систему). Полученная структурная схема с топологией, чья эффективность определяется повышенным уровнем безопасности системы умного дома, может являться одним из вариантов решения актуальной проблемы, но далеко не единственным. Важность решения проблемы невысокого уровня текущей защиты интеллектуальной собственности владельцев «умных домов» сложно переоценить, и с учетом представленной выше статистики, можно сделать вывод о том, что для полномасштабного интегрирования высоких технологий в каждую рядовую семью у нас еще не предпринято мер, предоставляющих гарантию постоянной и бесперебойной защиты интеллектуальной собственности пользователя.

Список литературы

1. Снегуров, А. В. Риски информационной безопасности систем, построенных по технологии «Умный дом» / А. В. Снегуров, Е. А. Ткаченко, А. Д. Кравченко // Восточно-Европейский журнал передовых технологий. - 2011. - № 3(52). - С. 30-34.
2. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения : ГОСТ Р 53114-2008. - Введ. 2009-10-01.
3. Таненбаум Э., Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. -5-е изд. - СПб: Питер, 2012. -960 с.
4. Малыш В.Н., Букреев Д.С. Анализ угроз информационной безопасности системы «умный дом»//Труды международного симпозиума «Надежность и качество». 2012.–Т.1.
5. КурчееваГ.И., Денисов В.В. Угрозы для информационной безопасности в высокоорганизованных системах типа «Умный город»//Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, No3(2016)
6. Wireless Technologies for Ambient Assisted Living and Health Care: Systems and Applications, Chapter: Security in Smart Home Environment, Publisher: Medican Information Science Reference, Editors: A. Lazakidou, K. Siassiakos, k. Ioannou
7. G. Mantas, D. Lymberopoulos, and N. Komninos, “Security in Smart Home Environment,” 2011.
8. International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 39, February 2019 / Internet of Things (IoT) of Smart Home: Privacy and Security. Editors: Zaied Shouran, Ahmad Ashari, Tri Kuntoro Priyambodo.