УДК 62-52

АНАЛИЗ СИСТЕМ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ “УМНЫЙ ДОМ” АНАЛИЗ БЕЗОПАСНОСТИ УМНЫХ ДОМОВ

Черников Н. И., студ.; Чернышев Н. Н., доц., к.т.н., доц.
(ГОУ ВПО «Донецкий национальный технический университет», г. Донецк, ДНР)

Под «умным» зданием следует понимать систему, которая обеспечивает безопасность и ресурсосбережение (в том числе комфорт) для всех пользователей. В простейшем случае она должна уметь распознавать конкретные ситуации, происходящие в здании, и соответствующим образом на них реагировать: одна из систем может управлять поведением других по заранее выработанным алгоритмам. Кроме того, от автоматизации нескольких подсистем обеспечивается синергетический эффект для всего комплекса.

Это проще понять, если представить, например, что система отопления никогда не сможет работать против системы кондиционирования. А отопление осуществляется не только по погоде, но и с учётом целого ряда других факторов. От силы ветра, по предсказанию, от времени суток (ночью комфортная температура меньше).

Можно считать, что это наиболее прогрессивная концепция взаимодействия человека (пользователей) с жилым пространством, когда в автоматизированном режиме в соответствии с внешними и внутренними условиями задаются и отслеживаются режимы работы всех инженерных систем и электроприборов.

В этом случае исключается необходимость пользоваться несколькими пультами при просмотре ТВ, десятками выключателей при управлении освещением, отдельными блоками при управлении вентиляционными и отопительными системами, системами видеонаблюдения и охранной сигнализации, моторизированными воротами и прочим.

Умный дом — система домашних устройств, способных выполнять действия и решать определенные повседневные задачи без участия человека. Домашняя автоматизация рассматривается как частный случай интернета вещей, она включает доступные через интернет домашние устройства, в то время как интернет вещей включает любые связанные через интернет устройства в принципе.

Наиболее распространенные примеры автоматических действий в "умном доме" - автоматическое включение и выключение света, автоматическая коррекция работы отопительной системы или кондиционера и автоматическое уведомление о вторжении, возгорании или протечке воды.

Домашняя автоматизация в современных условиях — чрезвычайно гибкая система, которую пользователь конструирует и настраивает самостоятельно в зависимости от собственных потребностей. Это предполагает, что каждый владелец умного дома самостоятельно определяет, какие устройства и где установить и какие задачи и как они будут исполнять.

На рисунке 1 приведена схема компонентов умного дома.

Основные вызовы для домашней автоматизации касаются отрасли безопасности данных.

Острота проблемы безопасности данных зависит от применения устройств. Чем серьезнее потенциальные последствия, тем опаснее взлом. Если для автоматизации в промышленности или медицинских учреждениях риски могут быть чрезвычайно велики, то для домашней автоматизации, отвечающей за управление светом или системой датчиков, они значительно ниже.

Однако даже при обычной домашней автоматизации есть риски нарушения безопасности данных, так как шифрования данных WPA,WPA2,WPE не дают гарантии безопасности умного дома.

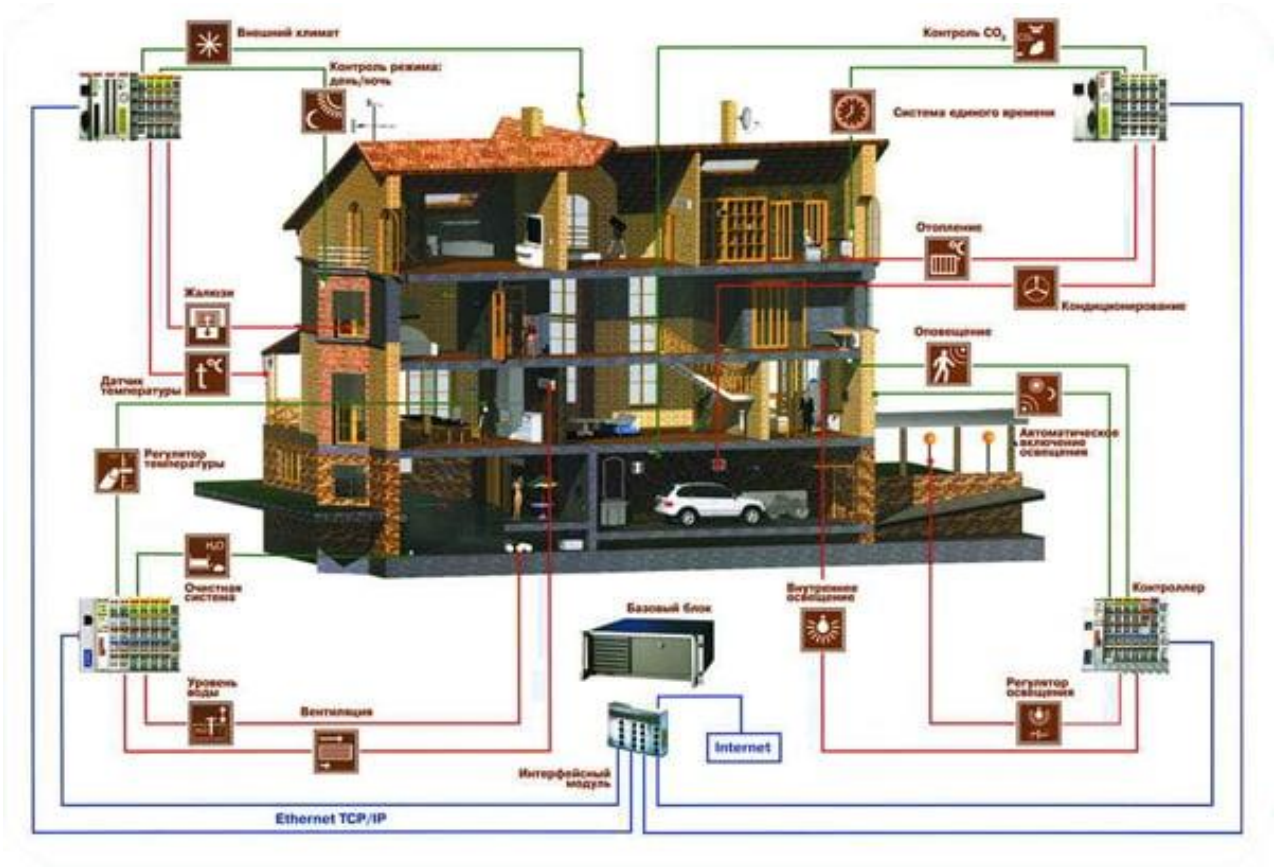

Рисунок 1 – Схема взаимодействия компонентов умного дома

Из-за того, что все элементы цепочки имеют доступ в Интернет, это делает их уязвимыми к атакам извне и подвергает опасности не только информацию пользователя, но также его здоровье. Все это меняет парадигму мышления, которая гласит: «Мой дом – островок безопасности».

Однако безопасность – это 100% требование для умного дома, кто бы что ни говорил. Сегодня в его состав могут входить системы наблюдения, системы мониторинга (в том числе здоровья) и системы безопасности, к которым можно получить удаленный доступ. Их просто необходимо защищать от злоумышленников.

Недостаточно надежная проверка подлинности. Системы, несмотря на то, что обладали облачными и мобильными интерфейсами, не требовали установки паролей достаточной длины и сложности. Также ни одна из систем не блокировала учетную запись после определенного числа неудачных попыток ввода пароля – получается, что отсутствовала банальная защита от перебора.

Проблемой так же является отсутствие шифрования при передаче данных. Хотя во всех системах реализованы механизмы шифрования на транспортном уровне, такие как SSL/TLS, многие облачные подключения остаются уязвимыми для атак.

Перечень ссылок

1. Нестеров, А. Л. Проектирование АСУТП: метод, пособие / А. Л. Нестеров. – Санкт-Петербург: ДЕАН, 2006. - Кн. 1. - 552 с.

2. Вермишев, Ю. Х. Основы автоматизации проектирования / Ю. Х. Вермишев. - Москва: Радио и связь, 1988. - 278 с.

3. Гудвин, Г. К. Проектирование систем управления / Г. К. Гудвин, С. Ф. Гребе, М. Э. Сальгадо; пер. с англ. А. М. Епанешникова. – Москва: БИНОМ Лаборатория знаний, 2004. – 911 с.