**Умный дом**

Умный дом — это система устройств, каждое из которых выполняет свою функцию. В нее входят датчики, розетки, камеры, бытовая техника. Их подключают к единому центру управления или устанавливают по отдельности — такую систему называют децентрализованной. Обычно умным домом управляют с помощью панели, которую располагают в квартире, и предусматривают удаленный доступ со смартфона или планшета.

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 куда установить и какие задачи они будут исполнять.

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 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.

Система умного дома включает три типа устройств:

* **Контроллер (хаб)** — управляющее устройство, соединяющее все элементы системы друг с другом и связывающее её с внешним миром.
* **Датчики (сенсоры)** — устройства, получающие информацию о внешних условиях.
* **Актуаторы** — исполнительные устройства, непосредственно исполняющие команды. Это самая многочисленная группа, в которую входят умные (автоматические) выключатели, умные (автоматические) розетки, умные (автоматические) клапаны для труб, сирены, климат-контроллеры и так далее.

В большинстве современных умных домов контроллер общается с остальными устройствами системы через радиосигналы. Самые распространенные стандарты радиосвязи для домашней автоматизации — Z-Wave (частота зависит от страны, в Европе 868 МГц, в России 869 МГц) и ZigBee (868 МГц или 2,4 ГГц), Wi-Fi (2,4 ГГц), Bluetooth (2,4 ГГц). Почти все они используют шифрование данных (AES-128), в Wi-Fi применяется шифрование WPA, WPA2 или WEP.

Для связи с внешним миром контроллер, как правило, подключается к интернету.

Основные вызовы для домашней автоматизации касаются фрагментированности отрасли и безопасности данных. Острота проблемы безопасности данных зависит от применения устройств. Чем серьёзнее 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.

Производители создают устройства на собственном программном обеспечении, с собственными мобильными приложениями и контроллерами. Это усложняет взаимодействие устройств и создание единой сети из устройств различных производителей. Крайний случай представляет собой применение проприетарного софта с закрытым кодом. Работающие на таком программном обеспечении устройства зачастую вообще невозможно связать с устройствами других производителей. Некоторые протоколы, в первую очередь Z-Wave, создавались с целью преодолеть эту проблему и дать производителям возможность создавать устройства, способные взаимодействовать друг с другом. Конструировать устройства с возможностью свободного взаимодействия друг с другом стали также производители на ZigBee. Готовность производителей создавать устройства на одном и том же стандарте — один из путей решения проблемы, они объединяют свои усилия в рамках единого консорциума (например, Z-Wave Alliance) и совместно развивают стандарт. Второй путь — разработка устройств, способных взаимодействовать с разными стандартами. Некоторые производители встраивают в главный контроллер домашней сети возможность управлять устройствами на нескольких стандартах, например на Z-Wave, ZigBee, Bluetooth LE и KNX. В этом случае устройства все ещё не могут взаимодействовать напрямую, но получают возможность работать друг с другом через хаб, который переводит сигналы с одного стандарта на другой.

## **Системы безопасности**

* Датчики движения, датчики присутствия, датчики вибрации, датчики разбития стекла, датчики открытия окна или двери
* Видеонаблюдение
* Видеодомофоны и видеоглазки
* Электронные замки (умные замки, смартлоки) и модули управления воротами
* Сирены

Эти устройства позволяют сконструировать подходящую систему безопасности, от сравнительно простой до достаточно сложной.

Среди основных алгоритмов:

* регистрация нежелательного проникновения
* уведомление владельцев
* включение сирены
* запуск видеосъемки
* запирание входных или межкомнатных дверей

Вдобавок, системы безопасности умного дома интегрируются с охранными системами, по тревоге высылающими группы реагирования. В большинстве стран рынок охранных систем существует достаточно давно, в то время как системы умного дома стали широко распространяться лишь в 2010-х годах. Отдельные поставщики охранных услуг позволяют интегрировать свою сигнализацию с умными устройствами, которые устанавливает сам пользователь, либо соглашаются высылать группы реагирования по сигналам тревоги с таких устройств.

Принципом построения охраны в доме являются так называемые линии защиты.

Первая линия защиты – это, прежде всего, средства обнаружения. К ним относятся камеры наблюдения, датчики с использованием различных физических принципов, которые сообщают о проникновении и местонахождении нарушителя.

На средства слежения возлагается задача обнаружения посторонних лиц, и сообщение об этом владельцу дома или в охранные структуры милиции.

Вторая линия защиты – обеспечивает беспрепятственный проход хозяину и членам семьи, а при помощи всевозможных средств ограничивает доступ на территорию участка и в помещение дома незваным гостям. К средствам защиты относятся прочные двери при входе на территорию с дистанционно управляемыми замками, двери при входе в дом, переговорные устройства, снабжённые телекамерами. Все эти устройства помогают задержать продвижение нарушителя.

Третья линия защиты – на этом этапе охранные устройства помогают блокировать продвижение нарушителя в доме и воздействовать на его психическое состояние. К ним относятся замки, которые блокируют межкомнатные двери, психическое воздействие при помощи звука и света, а также неожиданным воздействием: дыма, газа, электротока.

Четвёртая линия защиты – предусматривает защиту сейфов и хранилищ от вскрытия. А для людей, проживающих в доме, предлагается оборудовать убежище, чтобы отсидеться на случай налёта или вооружённого нападения, до приезда милиции.

**Протокол MQTT**

MQTT расшифровывается как Message Queuing Telemetry Transport (Передача телеметрии очередью сообщений). Он был разработан специально для общения умных устройств между собой.

Протокол имеет следующие основные особенности:

* используется механизм издатель/подписчик/топик;
* асинхронный протокол;
* компактные пакеты;
* работает поверх стека TCP/IP;
* требуется меньшая пропускная способность сети и может работать в условиях нестабильного канала передачи данных.

В основе работы протокола MQTT лежит традиционная модель клиент-сервер. Согласно этой модели, есть один сервер (также называемый брокером) и много клиентов. Клиенты всегда поддерживают связь с сервером. Задачами сервера (брокера) являются фильтрация и передача сообщений для клиентов-подписчиков.

Связь между клиентами основана на механизме издатель / подписчик / топик, в котором:

* сообщениям присваивают топик;
* издатель отправляет сообщения в сеть;
* подписчик ожидает сообщения, содержащие нужный ему топик;
* брокер координирует связь между издателями и подписчиками.

Топик представляет собой строку символов в кодировке UTF‑8 и состоит из одного или нескольких уровней, которые разделены между собой символом «/».

QoS (Quality of Service – качество обслуживания): неформально, этот показатель обозначает вероятность прохождения пакета между двумя точками сети. Существуют следующие модели QoS:

* QoS 0 — на этом уровне издатель отправляет пакет брокеру без подтверждения доставки (этот уровень самый быстрый, но ненадёжный);
* QoS 1 — на этом уровне пакеты гарантированно доставляется брокеру, но существует вероятность дублирования сообщения от издателя. После получения дублированного сообщеня брокер заново делает рассылку подписчикам, издателю снова отправляет сообщение о получении. В случае если издатель не получает PUBACK сообщения от брокера, то осущуствляется повторная отправка пакета, а DUP присваивается значение “1”. Этот уровень используется по умолчанию.
* QoS 2 — гарантируется доставка сообщений подписчику и исключается вероятность дублирования отправленных пакетов. Здесь издатель отправляет пакет брокеру. Указывается уникальный PacketID, QoS=2 и DUP присваевается значение “0”. До тех пор, пока от брокера не получен ответ PUBREC издатель хранит сообщение неподтверждённым. Брокер должен ответить сообщением PUBREC, которое содержит тот же PacketID. ПРосле того, как пакет получен, издатель отправляет с тем же PacketID PUBREL. Пока брокер не получил PUBREL он хранит пакет у себя. После получения PUBREL копия сообщения удаляется, а издателю отправляется PUBCOMP об успешном завершении транзакции. Это самый надёжный уровень, но самый медленный.

**Сохраняемые сообщения**: брокер сохраняет такие сообщения после отправки, поэтому если появиться новый подписчик, интересующийся топиком этого сообщения, то оно будет отправлено ему.

## Преимущества использования MQTT для устройств:

* Является стандартом де-факто для современных облачных систем IoT. Данный протокол поддерживается абсолютно всеми современными облачными и On Premises системами IoT
* Развитая экосистема opensource решений автоматизации и диспетчеризации, в том числе: HomeAssistant, OpenHab, Wiren Board, Node Red - это позволяет оконечным устройствам легко использовать уже имеющееся ПО без необходимости разрабатывать Web- интерфейсы, мобильные приложения, Rule-engines и пр.
* ПО MQTT брокера, также, доступно в открытом исходном коде и портировано под основные ОС (https://mosquitto.org/)
* Поддержка данного протокола устройством позволяет использовать его совместно с большим кол-вом уже существующего ПО и легко интегрировать новые устройства
* Библиотеки для реализации клиентской части данного протокола, также, доступны в исходном коде и могут быть легко интегрированы в ваш проект

## Недостатки и особенности реализации MQTT:

Протокол хорошо специфицирует такие операции как подписка на информацию (топик) и публикацию информации в топик, но сам формат данных оставляет на усмотрение приложений IoT.

Это привело к тому, что разные системы используют разные форматы данных и оказываются, на деле, несовместимы между собой

Например, популярные OpenSource системы управления УД: OpenHab, HomeAssistant и IOBroker поддерживают MQTT. Но при этом напрямую, не совместимы.