**Домашняя автоматизация** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *home automation*), или **умный дом** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *smart home*) — система домашних устройств, способных выполнять действия и решать определённые повседневные задачи без участия человека. Домашняя автоматизация рассматривается как частный случай [интернета вещей](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9), 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 куда установить и какие задачи они будут исполнять.

Технологии

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](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B2%D1%8B%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D1%82%D0%B5%D0%BB%D1%8C), 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](https://ru.wikipedia.org/wiki/Z-Wave) (частота зависит от страны, в Европе 868 МГц, в России 869 МГц) и [ZigBee](https://ru.wikipedia.org/wiki/ZigBee) (868 МГц или 2,4 ГГц), [Wi-Fi](https://ru.wikipedia.org/wiki/Wi-Fi) (2,4 ГГц), [Bluetooth](https://ru.wikipedia.org/wiki/Bluetooth) (2,4 ГГц). Почти все они используют шифрование данных ([AES-128](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard)), в Wi-Fi применяется шифрование [WPA](https://ru.wikipedia.org/wiki/WPA), [WPA2](https://ru.wikipedia.org/wiki/WPA2) или [WEP](https://ru.wikipedia.org/wiki/Wired_Equivalent_Privacy).

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

Системы безопасности

[Датчики движения](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA%D0%B8_%D0%B4%D0%B2%D0%B8%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F), [датчики присутствия](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA_%D0%BF%D1%80%D0%B8%D1%81%D1%83%D1%82%D1%81%D1%82%D0%B2%D0%B8%D1%8F), датчики вибрации, датчики разбития стекла, [датчики открытия окна или двери](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%B8%D1%8F)

* [Видеонаблюдение](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B4%D0%B5%D0%BE%D0%BD%D0%B0%D0%B1%D0%BB%D1%8E%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5)
* [Видеодомофоны](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B4%D0%B5%D0%BE%D0%B4%D0%BE%D0%BC%D0%BE%D1%84%D0%BE%D0%BD) и видеоглазки
* [Электронные замки](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B7%D0%B0%D0%BC%D0%BE%D0%BA) (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](https://ru.wikipedia.org/wiki/%D0%9E%D1%85%D1%80%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), 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.

Электронные замки, видеодомофоны и видеоглазки позволяют также организовать систему контроля доступа с возможностями дистанционного управления, видеозаписи и так далее.

Управление освещением

[Умные выключатели](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B2%D1%8B%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) и [диммеры](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%B8%D0%BC%D0%BC%D0%B5%D1%80)

* Модули управления шторами, жалюзи и рольставнями
* RGB- и RGBW-контроллеры для управления [светодиодными светильниками](https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BE%D0%B4%D0%BD%D0%BE%D0%B5_%D0%BE%D1%81%D0%B2%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5), прежде всего [светодиодными лентами](https://ru.wikipedia.org/wiki/%D0%A1%D0%B2%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BE%D0%B4%D0%BD%D0%B0%D1%8F_%D0%BB%D0%B5%D0%BD%D1%82%D0%B0)
* [Датчики движения](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA%D0%B8_%D0%B4%D0%B2%D0%B8%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F) и [присутствия](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%82%D1%87%D0%B8%D0%BA_%D0%BF%D1%80%D0%B8%D1%81%D1%83%D1%82%D1%81%D1%82%D0%B2%D0%B8%D1%8F" \o "Датчик присутствия)
* Датчики освещенности

Такие устройства позволяют автоматизировать управление светом и чаще всего используются, чтобы:

* автоматически включать свет, когда люди входят в помещение, и выключать, когда выходят
* автоматически поддерживать освещенность на постоянном уровне, регулируя яркость светильников и положение жалюзи или штор
* автоматически регулировать освещенность в зависимости от сезона и времени суток или по другим заранее заданным правилам

Управление климатом]

* Датчики влажности
* Датчики температуры
* [Термостаты](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%BC%D0%BE%D1%81%D1%82%D0%B0%D1%82) для поддержания постоянной температуры или её автоматического регулирования
* [Терморегуляторы](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%BC%D0%BE%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80) для управления мощностью батарей отопления
* Климат-контроллеры, передающие команды умного дома на технику предыдущих поколений, которая управляется обычными дистанционными пультами, прежде всего на кондиционеры
* Гигростаты для поддержания постоянной влажности или её регулирования

Основная задача устройств умного дома в этом случае — автоматически регулировать работу климатических систем так, чтобы одновременно обеспечить комфортный микроклимат и сократить расходы на его поддержание. Наиболее распространенные функции умного дома здесь:

* автоматически поддерживать комфортную температуру в помещениях, где находятся люди
* автоматически снижать мощность батарей и кондиционеров в отсутствие людей и ночью
* автоматически поддерживать влажность, комфортную для людей и подходящую для помещения и предметов обстановки
* автоматически вентилировать помещения и очищать воздух, поддерживая комфортное качество воздуха

Вызовы

Основные вызовы для домашней автоматизации касаются [фрагментированности](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B0%D0%B3%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%BF%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D1%8B) отрасли и [безопасности данных](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)[[10]](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D1%8F%D1%8F_%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F#cite_note-mckinseyopport-10)[[11]](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D1%8F%D1%8F_%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F#cite_note-mckinseyfive-11).

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.

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](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D0%B5%D1%82%D0%B0%D1%80%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) с закрытым кодом. Работающие на таком программном обеспечении устройства зачастую вообще невозможно связать с устройствами других производителей.

Некоторые протоколы, в первую очередь [Z-Wave](https://ru.wikipedia.org/wiki/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](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) друг с другом стали также производители на [ZigBee](https://ru.wikipedia.org/wiki/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](https://ru.wikipedia.org/wiki/Z-Wave#Z-Wave_Alliance)) и совместно развивают стандарт.

Второй путь — разработка устройств, способных взаимодействовать с разными стандартами.[[12]](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D1%8F%D1%8F_%D0%B0%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F#cite_note-mckinseyexec-12) 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.