

АНАЛИЗ ТЕХНОЛОГИИ «ИНТЕРНЕТ ВЕЩЕЙ» (IOT) И ЕЕ РОЛЬ В «УМНОМ ДОМЕ»

© Л.К. Хаджиева, Х.Х. Мальцагов

ГГНТУ им. акад. М.Д. Миллионщикова, Грозный, Россия

В данной публикации рассмотрена технология «интернет вещей» и ее роль в проекте «Умный дом» и в системе безопасности, которую они могут предоставить, а также о ее актуальности в современном мире. Количество и качество возможностей умного дома зависит только от желания и финансовых возможностей владельца. Кто-то может устанавливать всевозможные датчики температуры, газа, движения, автоматическое освещение и шторы, кто-то может ограничиться умным чайником. Самая важная и актуальная для человека функция умного дома – это безопасность, которую он может обеспечить, для этого могут, например, использоваться электронные замки, которые открываются со смартфона владельца или по паролю, камеры видеонаблюдения, датчики движения. Все это возможно благодаря технологии интернет вещей, которая связывает все устройства в доме в единую сеть.

Ключевые слова: интернет вещей (IoT), умный дом, конфиденциальность и безопасность.

Кевин Эштон, соучредитель Центра авторизации в Массачусетском технологическом институте, впервые упомянул интернет вещей в презентации, которую он сделал в Procter&Gamble (P & G) в 1999 году. Желая довести радиочастотный идентификатор (RFID) до сведения высшего руководства P & G, Эштон назвал свою презентацию «InternetofThings», используя новый тренд 1999 года: интернет. В книге профессора Массачусетского технологического института Нила Гершенфельда «*When Things Start to Think*» (Когда все начинают мыслить), также опубликованной в 1999 году, не использовался точный термин, но было дано четкое представление о том, куда движется IoT.

В первую очередь следует заметить, что IoT не является технологией в прямом смысле этого слова. IoT – это концепция, идея вычислительной сети физических объектов, имеющих технологии для взаимодействия друг с другом и/или с внешней средой. В отличие от обычного интернета, который лишь способ объединения компьютеров, это – попытка выйти за его пределы. Таким образом, IoT можно назвать следующим шагом развития «физического» интернета (Подразумевается сам интер-

нет, а не Web), цель которого – объединить все системы ради обеспечения дополнительной выгоды для конечного потребителя [4].

Самым распространенным примером интернета вещей является «умный дом». Умными называют дома, в которых за безопасностью, энергосбережением и комфортом следит программное обеспечение, объединяющее бытовые приборы в единую систему с помощью технологии передачи данных. Представьте, что дом самостоятельно управляет освещением и выключает свет в комнате, если в ней не находится человек, следит за протечками водосточных труб и состоянием качества воздуха, предупреждает о возможности возгорания, автоматически поливает домашние растения и кормит домашних питомцев, если Вы задержались на работе или уехали в командировку. С такой системой Вы можете быть уверены, что Ваш дом находится в безопасности, а неожиданная протечка под ванной не вызовет потоп у соседей.

Иногда интернет вещей даже в домашней автоматизации сталкивается с необходимостью криптозащиты соединения, и рядовым проектом тут будет, собственно, защита жилища. Существует несколько проектов, реализующих

управление замком входной двери, но «золотая середина» так и не найдена, да и разработчики не всегда осмеливаются полностью доверить свою жизнь и здоровье микроконтроллеру, поэтому большинство решений всё ещё предполагают использование обычного замка, а электронный является лишь дополнением.

IoT эволюционировал от межмашинного взаимодействия (M2M), то есть от машин, соединяющихся друг с другом через сеть без участия человека. M2M означает подключение устройства к облаку, управление им и сбор данных.

Интернет вещей также является естественным расширением SCADA (диспетчерский контроль и сбор данных), категории программных приложений для управления процессами, сбора данных в режиме реального времени из удаленных мест для управления оборудованием и условиями. Системы SCADA включают в себя аппаратную и программные части. Аппаратное обеспечение собирает и передает данные на компьютер, на котором установлено программное обеспечение SCADA, где они затем обрабатываются и своевременно представляются. Эволюция SCADA такова, что системы SCADA последнего поколения превратились в системы IoT первого поколения.

Интернет вещей представляет людям большее удобство работы и жизни, а также позволяет получить полный контроль над своей жизнью. В дополнение к использованию интеллектуальных устройств для автоматизации домов, IoT имеет важное значение для бизнеса. IoT предоставляет компаниям в режиме реального времени взгляд на то, как на самом деле работают системы их компаний, обеспечивая понимание всего, от производительности машин до цепочки поставок и логистических операций.

IoT позволяет компаниям автоматизировать процессы и снизить трудозатраты. Также сокращается объем отходов и улучшается качество предоставляемых услуг, делая производство и доставку товаров менее дорогостоящими, а также обеспечивая прозрачность операций с клиентами.

IoT затрагивает все отрасли, включая здравоохранение, финансы, розничную торговлю и

производство. Умные города помогают горожанам сократить отходы и потребление энергии, а подключенные датчики даже используются в сельском хозяйстве, чтобы помочь отслеживать урожайность сельскохозяйственных культур и крупного рогатого скота и прогнозировать модели роста.

Таким образом, IoT является одной из наиболее важных технологий в повседневной жизни, и она будет продолжать набирать обороты, поскольку все больше компаний осознают потенциал подключенных устройств для поддержания их конкурентоспособности [1].

На данный момент IoT – это часть окружающего нас мира. Многие повседневные для нас вещи имеют IoT, из банального благодаря IoT работают умные часы, фитнес-трекеры, системы умного дома, веб-маячки, умные часы и множество других окружающих нас вещей. Одним из первых устройств, которые получили возможность подключаться к сети, был торговый автомат Coca-Cola, установленный в Университете Карнеги-Меллона. Так, уже в 1982 году он передал данные о том, сколько бутылок с напитком сейчас находится в автомате, как долго они стоят, а также отобразил информацию о том, холодная или теплая газировка. Со временем многие стали все больше задумываться о технологиях, позволяющих устройствам соединяться друг с другом. Используя эту технологию, перспектива создания вычислительной среды, которая может самостоятельно решать определенные проблемы и обмениваться информацией без вмешательства человека, становится реальной. К этому времени был сформирован запрос на такую технологию – как обычными людьми, так и в промышленности, где автоматизация была одной из самых важных задач с 19-го века. Надежной предпосылкой для межмашинного взаимодействия было постоянно ускоряющееся развитие высоких технологий в 1970-х и 1980-х годах (появление микропроцессора, персонального компьютера, графического интерфейса и эволюция интернета).

Для удобства классификации Роб Ван Краенбург ввел 4 уровня InternetofThings – по «охвату территории»:

BAN (BodyAreaNetwork) – все, что так или иначе находится на человеке: умные часы, футболки, кроссовки, очки и так далее.

LAN (LocalAreaNetwork) – по сути это умный дом: различные устройства в доме, объединенные в одну сеть.

WAN (WideAreaNetwork) – умные города: общественный транспорт, объединенный в одну сеть и имеющий выход в интернет; электростанции, объединенные в одну сеть и автоматически перераспределяющие нагрузку, и так далее.

VWAN (VeryWideAreaNetwork) – умная планета, где каждое устройство может взаимодействовать с любым другим.

То есть по сути интернет вещей можно рассматривать как объединение мелких сетей в более крупные, и, наконец, в одну глобальную общепланетарную сеть:

С первым уровнем (носимые устройства) все понятно, третий и четвертый уровни (масштабы города и планеты) развиты достаточно слабо, а вот второй уровень – умный дом – сейчас активно развивается: о нем и поговорим [5].

Умный дом – это среда, в которой разнообразные электронные устройства объединены в сеть, чтобы облегчить и сделать более удобной жизнь человека. Это может быть связано с различными преимуществами, облегчающими повседневную жизнь и работу пользователей, которые обеспечиваются растущими технологиями и устройствами интернета вещей (IoT), оснащенными датчиками, камерами или исполнительными механизмами и способными либо накапливать информацию из окружающей среды и предоставлять ее жильцам. Основные функции умных домов включают мониторинг в режиме реального времени, дистанционное управление, безопасность от злоумышленников, газовую / пожарную сигнализацию и так далее. Поскольку в «умных домах» обрабатываются конфиденциальные и персональные данные, необходимо внедрить решения для обеспечения безопасности и конфиденциальности, чтобы защитить данные пользователей / предприятий от злоумышленников, и при этом стараться гарантировать предоставление надежных услуг [2].

Основным предметом рассмотрения в данной статье будет система безопасности умного дома.

Первым барьером безопасности является обеспечение надежной защиты доступа на участок и внутри дома. Дом защищен с помощью надежных электронных замков, для открытия которых необходимо набрать секретный код, прикрепить электронный ключ или даже палец для сканирования отпечатка пальца. Используя специальный пульт дистанционного управления или команду с мобильного устройства, владелец открывает ворота. Удобная система домофона позволяет контролировать доступ на территорию посторонних лиц и открывать дверь только при необходимости.

Для защиты и оповещения владельца и службы экстренной помощи используются различные типы беспроводных датчиков, список которых включает в себя:

Пожарные датчики реагируют на дым, тепло и угарный газ. В случае пожарной тревоги система «умный дом» автоматически блокирует окна и двери, чтобы перекрыть поток свежего воздуха и предотвратить дальнейшее распространение огня, и включает средства пожаротушения. «Умный дом» отправляет сообщение владельцу, отключает газ и электричество и уведомляет экстренную службу о пожаре. Чтобы предупредить об опасности людей в доме, система активирует пожарную сигнализацию.

Если обнаружены утечки газа, газовые датчики блокируют газовую трубу на входе в дом, включают вентиляционную систему и отправляют предупреждение владельцу.

Датчики воды могут заблокировать подачу воды в случае утечки и отправить владельцу сообщение о произошедшей аварии.

Датчики движения активируются, когда нет хозяев. При срабатывании датчика освещение автоматически включается, и беспроводные камеры начинают запись. Владелец отправляет уведомление, чтобы он мог видеть в реальном времени, что происходит в доме. По запросу владельцев, при срабатывании датчика движения система может активировать сигнал тревоги и вызвать службу безопасности.

Датчики целостности периметра информируют о несанкционированном проникновении на территорию или в дом, например, через разбитое окно или открытую входную дверь. Когда эти датчики срабатывают, система включает в себя систему сигнализации, освещение и видеокамеры, а также уведомляет владельца об инциденте и службу безопасности. В некоторых случаях «умный дом» обеспечивает не только пассивную, но и активную защиту имущества, автоматически открывая вольер со сторожевой собакой, подавая напряжение на особо охраняемые зоны и даже выпуская специальный газ, чтобы временно обездвигнуть злоумышленника.

Видеонаблюдение может быть установлено как один из компонентов «умного дома», либо отдельно. Однако в сочетании с другими элементами системы «умный дом» (различные датчики, возможность автоматического включения освещения, блокировки окон и дверей, отправки оповещений и т. д.) видеонаблюдение позволяет отслеживать все, что происходит в доме в режиме реального времени и в записи, и как внутри дома, так и на другой стороне земного шара.

Согласно статистике, наибольшее количество краж происходит в отсутствие владельцев. Опытные преступники быстро определяют, находится ли кто-то дома, и могут воспользоваться кратковременным или длительным отсутствием собственников для совершения преступления. Поэтому современные системы безопасности предлагают запрограммировать «умный дом» для создания эффекта присутствия: в доме открываются и закрываются шторы, включается и выключается свет, звучит музыка, а когда звонит дверной звонок, будет громко лаять сторожевая собака.

Безопасность детей также можно контролировать на расстоянии. В этом поможет система «радионяня», которая с помощью скрытой или открытой видеокамеры принимает все, что происходит с маленьким членом семьи, помогая работающим родителям в режиме реального времени проверять, все ли в порядке.

Система «умный дом», заказанная под ключ в специализированной фирме, стоит достаточно дорого – цены начинаются в среднем

от 3 000-5 000 долларов для квартиры и гораздо дороже для частного дома. Стоимость зависит от площади жилища и набора необходимых функций. Однако, если посчитать, сколько денег можно сэкономить, защитив свой дом от различного рода проблем и неприятностей, цена профессиональной системы уже не будет казаться такой высокой [3].

Для людей, которые неплохо разбираются в технике, есть отличный альтернативный вариант – собрать «умный дом» самостоятельно, заказав комплект или отдельные компоненты системы на Ebay или Alibaba. В российских интернет-магазинах можно приобрести комплект «умный дом за час», цена которого начинается от 25-30 тысяч рублей.

К сожалению, безопасность самой системы «умный дом» на сегодняшний день ограничена техническими возможностями.

Умный дом включает в себя огромное количество IoT-устройств, собирающих и обрабатывающих данные. Они дают пользователям определённые возможности по контролю за апартаментами как в ручном, так и автоматическом режиме. В «умной среде» устройства периодически обмениваются данными по сети. Это происходит либо напрямую от устройства к устройству, либо через облако.

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.

Нельзя исключать, что с ростом числа умных устройств начнет расти и количество взломов систем управления. Злоумышленники, получившие доступ к таким системам, могут при помощи электронного ключа открыть дверь или окно, получить доступ к банковским

счетам жителей умного дома. Более того, преступники смогут вручную вызвать сбой медицинских устройств.

Компания HP провела исследование рынка интеллектуальных систем, в ходе которого выяснила, что практически все системы имеют проблемы с безопасностью.

Первая проблема – 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.

Еще одна проблема оказалась связана с конфиденциальностью. Все системы собирали какие-либо виды персональной информации: имена, адреса, номера телефонов и кредитных карт. Это вызывает определенную озабоченность, поскольку создает угрозу кражи учетных данных.

Стоит также отметить, что ключевой особенностью многих домашних систем безопасности является использование видео, просмотр которого доступен через различные интерфейсы. Конфиденциальность подобных данных тоже находится под вопросом.

Наконец, последней проблемой эксперты назвали отсутствие шифрования при переда-

че данных. Хотя во всех системах реализованы механизмы шифрования на транспортном уровне, такие как SSL/TLS, многие облачные подключения остаются уязвимыми для атак.

Задавшись этими вопросами, компании Google, Samsung Electronics, SiliconLabs и некоторые другие объединились с целью разработать новый беспроводной сетевой стандарт специально для умных домов. Он получил название Thread. Thread использует IPv6 и построен на стандарте IEEE 802.15.4, а основным его достоинством является именно безопасность. Одновременно в сети могут находиться до 250 устройств, которые защищаются шифрованием уровня банковской системы.

Еще одна особенность Thread – это прозрачность. Пользователь видит список всех подключенных устройств, благодаря которому ему легко определить, что с чем связано. В настоящий момент есть ряд решений для умных домов (ZigBee и 6LowPAN), которые легко могут начать поддерживать предложенный стандарт без аппаратных изменений – в их случае нужно просто обновить программное обеспечение.

Умные устройства все больше входят в нашу жизнь, среди предметов нашего постоянного ношения почти всегда в этот список входят смартфон, часы и многие другие вещи. В таких условиях защита хранимой и передаваемой информации становится особенно важной.

ЛИТЕРАТУРА

1. Интернет вещей [Электронный ресурс]: учебное пособие / Росляков А.В., Ваняшин С.В., Гребешков А.Ю. 2015. 135 с.
2. Концепция «Умный город» [Электронный ресурс]: монография / Волков А.А., Седов А.В., Чельшков П.Д. 2015. 92 с.
3. Роуз Дэвид Будущее вещей: Как сказка и фантастика становятся реальностью [Электронный ресурс]. Роуз Дэвид М.: Альпина нон-фикшн, 2019. 352 с.
4. [https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT-Contributor\(s\): Linda Rosencrance, Sharon Shea and Ivy Wigmore](https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT-Contributor(s):LindaRosencrance,SharonSheaandIvyWigmore)
5. <https://habr.com/ru/company/gsgroup/blog/394343/> - Холдинг GS Group- IoT: Вопросы безопасности умного дома- 19 мая 2016
6. https://www.iguides.ru/main/gadgets/other_vendors/internet_veshchey_i_umnyy_dom_chno_eto_i_kak_poyavilos/ - Интернет вещей и умный дом – что это такое -ЕГОР МОРОЗОВ | 6 МАРТА, 2017

ANALYSIS OF THE TECHNOLOGY “INTERNET OF THINGS” (IOT) AND ITS ROLE IN THE “SMART HOUSE” PROJECT

© L.K.Khadzhieva, Kh.Kh Malcagov

GSTOU named after acad. M.D. Millionshchikov, Grozny, Russia

This publication discusses the technology of the “Internet of things” and its role in the “Smart Home” project, and in the security system that they can provide, as well as its relevance in the modern world. The quantity and quality of the capabilities of a smart home depends only on the desire and financial capabilities of the owner. Someone can install all kinds of sensors for temperature, gas, movement, automatic lighting and curtains, someone can be limited to a smart kettle. The most important and relevant function of a smart home for a person is the security that it can provide, for this, for example, electronic locks can be used that open from the owner’s smartphone or password, video surveillance cameras, motion sensors. All this is possible thanks to the Internet of Things technology, which connects all the devices in the house into a single network.

Keywords: Internet of Things (IoT), Smart Home, Privacy and Security

REFERENCES

1. Roslyakov, A.V., Vanyashin, S.V. and Grebeshkov, A.Yu. (2015) *Internet veshchei* [Elektronnyi resurs]: uchebnoe posobie. [Internet of things [Electronic resource]: a tutorial]. p. 135.
2. Volkov, A.A., Sedov, A.V. and Chelyshkov, P.D. (2015) *Kontseptsiya «Umnyi gorod»* [Elektronnyi resurs]: monografiya. [The concept of “Smart City” [Electronic resource]: monograph]. p. 92.
3. Rouz Devid M. (2019) *Rouz Devid Budushchee veshchei: Kak skazka i fantastika stanovyatsya real’nost’yu* [Elektronnyi resurs]. [Rose David The Future of Things: How Fairy Tale and Fiction Come True [Electronic Resource].]: Alpina Non-Fiction. p. 352.
4. [https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT-Contributor\(s\): Linda Rosencrance, Sharon Shea and Ivy Wigmore](https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT-Contributor(s):LindaRosencrance,SharonSheaandIvyWigmore)
5. <https://habr.com/ru/company/gsgroup/blog/394343/> - Kholding GS Group- IoT: Voprosy bezopasnosti umnogo doma- 19 maya 2016.
6. https://www.iguides.ru/main/gadgets/other_vendors/internet_veshchey_i_umnyy_dom_chno_eto_i_kak_poyavilos/ - Internet veshchei i umnyi dom – chto eto takoe -EGOR MOROZOV. 6 MARTA, 2017. [The Internet of things and smart home - what is it - Egor Morozov. MARCH 6, 2017].