**Оглавление**

[Введение 2](#_Toc59595603)

[1.Безопасное и эффективное управление 3](#_Toc59595604)

[2. Разработка безопасных устройств 5](#_Toc59595605)

[3.Эволюция парадигмы 6](#_Toc59595606)

[4.Контроль взаимодействий в сети 7](#_Toc59595607)

[Заключение 10](#_Toc59595608)

[Список литературы 11](#_Toc59595609)

# Введение

Интернет вещей (IoT) плотно вошел в нашу жизнь и миллиардов людей по всему миру. Однако рост количества подключенных устройств ведет к увеличению рисков безопасности: от причинения физического вреда людям до простоев и повреждения оборудования — это могут быть даже трубопроводы, доменные печи и установки для выработки электроэнергии. Поскольку ряд таких объектов и систем IoT уже подвергались нападению и был причинен внушительный ущерб, обеспечение их защиты выходит на первый план.  
В быту, когда разговор идет про IoT, как правило, имеют в виду лампочки, обогреватели, холодильники и прочую технику для дома, которой можно управлять через интернет. На самом деле, тема IoT намного шире. Под интернетом вещей мы в первую очередь понимаем подключенные к вычислительной сети автомобили, телевизоры, камеры наблюдения, роботизированное производство, умное медицинское оборудование, сеть электроснабжения и бесчисленные промышленные системы управления (турбины, клапаны, сервоприводы и т. д.). К счастью, безопасность интернета вещей можно построить на фундаменте из четырех краеугольных камней: безопасность связи, защита устройств, контроль устройств и контроль взаимодействий в сети.

Как профессиональным инженерам, нам необходимо установить адекватный и легкодостижимый минимальный уровень безопасности для любой системы IoT, где важна безопасность. Также будет полезно для всех, если одна удачно спроектированная архитектура защиты сможет применяться во многих разных областях. Однако некоторые компании могут выбрать уровень безопасности «выше и дальше», который мы здесь тоже описали. Мы очень надеемся, что ведущие производители и провайдеры услуг выйдут за пределы обозначенного минимума.

# 1.Безопасное и эффективное управление

Мы знаем, что реверс-инжиниринг устройств рано или поздно будет проведен, уязвимости будут обнаружены, а для устройств необходимо будет предоставлять обновления OTA (удаленно). Конечно, механизмы обновления OTA добавляют сложность архитектуре устройства IoT, поэтому многие инженеры стараются избегать их на свой страх и риск. К счастью, хороший механизм OTA может использоваться для многих целей, не только для исправлений программного обеспечения и функциональных обновлений, но также: Обновления конфигурации Управления телеметрией безопасности для аналитики защищенности Управления телеметрией для контроля правильности функционирования устройства Диагностики и восстановления Управления учетными данными доступа к сети (NAC) Управления правами/привилегиями и множества других задач Конечно, все вышеперечисленное должно исполняться безопасно и надежно, здесь потребуется наиболее тщательный подход к подписанию кода и организации передачи файлов.

Здорово, что существуют стандарты управления окружением software и firmware на каждом устройстве, включая конфигурацию, и многие производители, в частности, Open Mobile Alliance (OMA), поддерживают такие стандарты. Некоторые из решений масштабируются для управления миллиардами устройств. Управление безопасностью каждого устройства может предполагать управление конфигурацией с помощью хостовой защиты, которую мы рассмотрели в предыдущем разделе. Естественно, некоторые технологии безопасности предусматривают обновления OTA для контента безопасности, например, черные и белые списки, эвристика, сигнатуры IPS и данные о репутации. Также существуют технологии безопасности, основанные на политиках, которым обновления нужны только при переустановке на устройстве программного обеспечения для каких-то целей, например, для добавления функциональных возможностей.

Тем не менее оба типа технологий могут генерировать телеметрию безопасности, которая имеет большое значение при столкновении с целенаправленными атаками. Поэтому телеметрические данные безопасности всегда должны собираться от этих host-based (device-based) технологий для централизованного анализа. Разумеется, компоненты безопасности не единственные в устройстве IoT, которыми необходимо управлять безопасно и надежно. Большинство устройств генерируют телеметрию или данные с датчиков, которые нужно также безопасно и надежно собирать и передавать в места хранения и анализа.

Многие устройства уже содержат в себе функции контроля, которыми нужно аккуратно управлять через конфигурационные параметры, а те в свою очередь безопасно и надежно хранить и обновлять. К счастью, инфраструктуры управления устройствами, которые используют общепринятые безопасные протоколы, могут применяться и для защищенного управления основными функциями устройства, контентом безопасности и телеметрией устройства. Фактически подобные модели адаптируются для OTA-управления автомобилями и используются для безопасного и надежного управления торговыми автоматами. Некоторые из инфраструктур управления комбинируют агентские и безагентские протоколы управления IoT, тогда как устройства выпускаются с поддержкой стандартизированного управления для упрощения функций контроля.

А отдельные инфраструктуры управления могут дополнительно сочетать все эти методы управления с понимаем информации, полученной от сетевых снифферов. В сложившейся ситуации системы IoT должны изначально иметь встроенные возможности обновления OTA. Отсутствие этих возможностей оставит устройства подверженными угрозам и уязвимостям в течение всего срока их службы.

Разумеется, обновление OTA может применяться еще для управления конфигурациями устройств, контентом безопасности, учетными данными, а также для расширения функциональных возможностей устройств, сбора телеметрии и данных программного окружения, для доставки патчей безопасности и многого другого. Однако с дополнительной функциональностью или без нее базовые возможности обновления и управления защищенностью должны быть предусмотрены еще на этапе проектирования устройств IoT.

# 2. Разработка безопасных устройств

Одним из основных способов создания безопасных устройств – помнить о безопасности во всем, что вы делаете. В этом помогает жизненный цикл безопасной разработки - методика разработки безопасных программ. Он состоит из семи этапов:

* **Обучение.** Основополагающие концепции для создания защищенного программного обеспечения включают безопасный дизайн, моделирование угроз, безопасное кодирование, тестирование безопасности и обеспечение приватности.
* **Требования.** Начальная стадия проекта - это подходящее время для рассмотрения и определения основных вопросов безопасности и конфиденциальности вашего проекта, включая нормативные требования.
* **Проектирование.** Не все программные функции безопасны, поэтому на стадии проектирования определяются сильные стороны разрабатываемого ПО и добавляются дополнительные уровни безопасности там, где это наиболее целесообразно.
* **Реализация.** Разработка на этой стадии заключается в использовании задокументированных средств разработки, поиска и устранения устаревшего программного обеспечения и проводится анализ всех функций проекта.
* **Верификация.** На этом этапе происходит проверка кода на соответствие требованиям безопасности и конфиденциальности.
* **Выпуск.** Перед непосредственным выпуском программного продукта создается план отслеживания инцидентов безопасности и быстрого реагирования на них.
* **Реагирование.** Выполнение плана реагирования на инциденты.

# 3.Эволюция парадигмы

Большинство устройств IoT представляют из себя «закрытые системы». Покупатели не смогут добавлять программное обеспечение безопасности после того, как устройства покинут завод. Такое вмешательство аннулирует гарантию, а зачастую попросту не представляется возможным. По этой причине, защитные функции должны быть изначально встроены в устройства IoT, чтобы они были безопасными по своей архитектуре.

Для большей части индустрии ИБ такая «безопасность внутри», то есть встроенная при изготовлении устройства на заводе — это новый способ обеспечения защиты, это касается и классических технологий безопасности, таких как шифрование, проверка подлинности, проверка целостности, предотвращение вторжений и возможности безопасного обновления. Учитывая тесную связь аппаратного и программного обеспечения в модели IoT, иногда проще, чтобы программы для защиты использовали расширение функций аппаратной части и создавали «внешние» уровни безопасности.  Здорово, что многие производители чипов уже встроили функции безопасности в оборудование. Но аппаратный уровень — это всего лишь первый слой, необходимый для комплексной защиты связи и устройств.

Комплексная защита требует интеграции функций управления ключами, защиты на основе хоста, инфраструктуры OTA и аналитики безопасности, о чем мы упоминали прежде. Отсутствие даже одного из краеугольных камней в фундаменте безопасности оставит широкий простор действиям злоумышленников. Поскольку промышленный интернет и IoT привносят сетевой интеллект в физические вещи вокруг нас, мы должны внимательно относиться к вопросам их безопасности. Наша жизнь зависит от самолетов, поездов и автомобилей, которые перевозят нас, от инфраструктуры здравоохранения и гражданской инфраструктуры, которая позволяет нам жить и работать. Нетрудно представить, как незаконное манипулирование светофорами, медицинским оборудованием или бесчисленными другими устройствами может привести к плачевным последствиям. Также ясно, что простые граждане и покупатели IoT не хотят, чтобы незнакомые люди взламывали их дома или машины, чтобы кто-то причинял им вред, устраивая сбои на автоматизированных промышленных объектах. В этой ситуации мы попытаемся предложить такие рекомендации, которые сформируют целостную безопасность для IoT, одновременно сделав ее эффективной и простой в реализации.

# 4.Контроль взаимодействий в сети

Давайте заглянем немного вперед, в будущее. Сегодня бесчисленные технологии и системы IoT представляют из себя не более чем «интранет вещей». Однако поскольку все больше систем должны будут связываться друг с другом, все важнее становится знать, «чему доверять». Сертификаты устройств могут содержать информацию о происхождении и типе устройства. Тем не менее на вопросы о том, нужно ли доверять этому устройству, в конечном итоге должны будут отвечать другие службы, например, основанные на репутации, или «Справочник вещей» (Directory of Things).

Такой каталог способен не только отслеживать информацию о безопасности для каждого устройства и систем IoT, но еще отслеживать и управлять привилегиями и полномочиями, которыми устройства и системы наделяют друг друга. Фактически каждый из нас оказывается окруженным все большим количеством устройств IoT, а такие справочники могут помочь разобраться с устройствами с интересующими функциями в интересующих областях. Модель справочника делает возможным быстрый поиск удаленного устройства через каталог и, может быть, будет содействовать ускорению принятия решения об использовании данных с чужого устройства. Даже если вы никогда не видели устройство раньше, информация об устройстве, включая его возможности и репутацию, могут быть указаны в таком каталоге. Если предположить, что устройство захочет узнать, может ли оно доверять пользователю, то «Справочника вещей», возможно, будет недостаточно, и в этом случае скорее потребуется «Справочник всего» (Directory of Everything), который будет включать устройства, системы и пользователей.

Конечно, у многих людей нет умных чайников или умных холодильников… пока нет... Но у многих из нас уже есть автомобиль, который получает информацию для навигатора через интернет, Smart TV или проигрыватели Blu-ray, которые транслируют видео через интернет, фитнес-браслеты, а еще мы используем банкоматы и вендинговые аппараты. Наше взаимодействие с IoT на самом деле чаще, чем мы замечаем. В этой ситуации мы, возможно, захотим иметь наш собственный «Справочник вещей». Защищая устройства и связь, управляя программными обновлениями и выполняя аналитику безопасности для стратегической защиты от угроз, мы понимаем, что все эти меры абсолютно необходимы для защиты IoT. Концепция каталогов «чему доверять» весьма перспективна, но не является сегодня ни основополагающей технологией, ни ключевым ингредиентом в «контроле взаимодействий в сети» для большинства участников.

Мы включаем эту перспективную концепцию каталогов только для того, чтобы дать предварительный обзор стоящих перед многими компаниями вызовов, и приводим пример, как можно справиться со сложными масштабными задачами. Некоторые компании уже столкнулись с подобного рода проблемами, поскольку они несут ответственность за защиту более чем миллиарда устройств. Для них это «будущее» уже наступило, и они не одиноки.

# 

# Заключение

Как можно защитить IoT? Системы IoT бывают очень сложными, им требуются комплексные меры защиты, покрывающие уровни облаков и подключений, также необходима поддержка устройств IoT с ограниченными вычислительными ресурсами, которых недостаточно для поддержки традиционных решений безопасности. Простого универсального решения не существует, и для обеспечения безопасности недостаточно запереть двери, оставив окна открытыми.

Безопасность должна быть всесторонней, иначе атакующие просто воспользуются самым слабым звеном. Конечно, традиционные IT-системы как правило передают и обрабатывают данные из систем IoT, но сами системы IoT обладают своими уникальными потребностями в защите.

# Список литературы

1. Белунцов Macromedia Flash 5. Анимация в Интернете. Практическое руководство / Белунцов, Валерий. - М.: ДЕСС КОМ, 2001.
2. Богданов-Катьков, Н.В. Интернет для начинающих / Н.В. Богданов-Катьков, А.А. Орлов. - М.: Эксмо, 2005. - 384 c.
3. Вламис Бизнес-путь: Yahoo! Секреты самой популярной в мире интернет-компании / Вламис, Смит Энтони; , Боб. - М.: Крылов, 2003.
4. Герасевич Блоги и RSS: интернет-технологии нового поколения / Герасевич, Виталий. - М.: СПб: BHV, 2006. - 256 c.
5. Хараменских, Е.П. Интернет вещей. Исследования и область применения. Монография / Е.П. Зараменских. - М.: ИНФРА-М, 2016.
6. 10. Кастельс Галактика Интернет / Кастельс, Мануэль. - М.: Екатеринбург: У-Фактория, 2004. - 328 c.