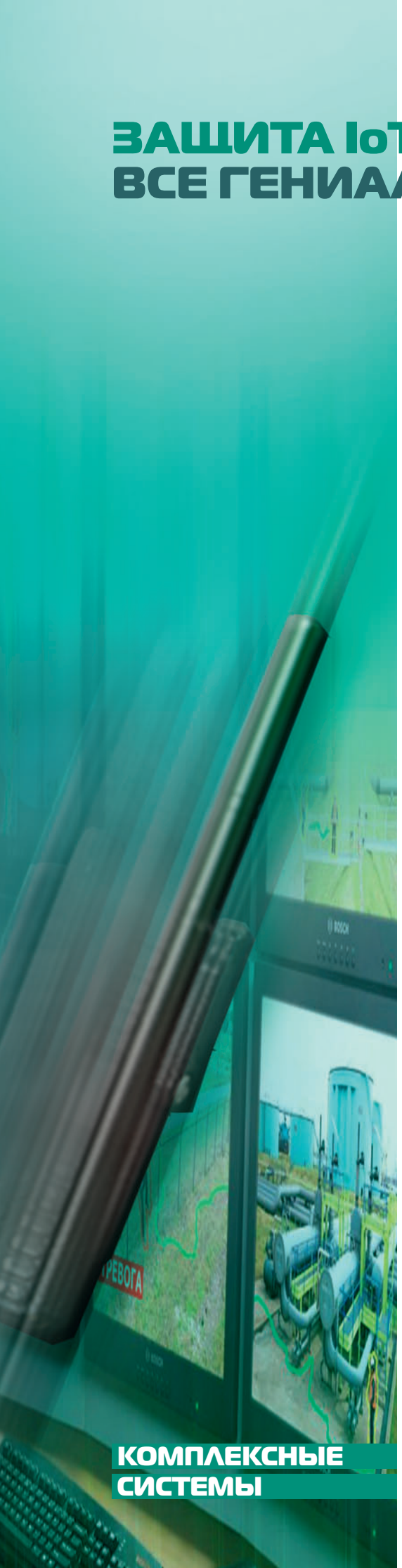
ЗАЩИТА IoT-УСТРОЙСТВ: ВСЕ ГЕНИАЛЬНОЕ ПРОСТО!

Кочиева Диана Батрадзовна
менеджер по маркетинговому контенту «Окей-Телеком»



КОМПЛЕКСНЫЕ СИСТЕМЫ

Каждая вторая статья об Интернете вещей начинается с прогноза: к 2020 году число подключенных к сети устройств достигнет отметки в 20,4 млрд (по данным консалтинговой компании Gartner на январь 2017). Результаты многочисленных исследований подогревают ожидания светлого будущего. Концепция Интернета вещей – IoT стремительно завоевывает рынок и уже сегодня является одним из главных трендов мира IT.

Мы привыкли говорить о преимуществах, которые дает Интернет вещей. Потребительский сектор после массового внедрения технологии станет жить в «умных городах» и работать на «умных предприятиях». Только представьте, с работы жителей «умных домов» будет ждать наполненная ванна с водой нужной температуры, а свет в квартире будет включаться по одному только щелчку пальцев или вовсе без него, это кому как нравится: чувствовать себя властелином датчиков или забыть об их существовании. Благодаря Интернету вещей жизнь уже в самом ближайшем будущем обещает не только стать комфортнее, но и начать походить на сказку – чем дальше, тем страшнее (см. британский фантастический телесериал «Черное зеркало»).

А мониторинг систем на производствах, если говорить о промышленном Интернете вещей (IIoT), позволяет предупреждать выход из строя оборудования, сокращать расход потребляемой электроэнергии на предприятиях и в точности рассчитывать необходимые ресурсы на решение тех или иных задач. Одним словом, долгожданная оптимизация!

В погоне за мировыми трендами и лучшей жизнью мы совсем забыли подумать о безопасности используемых технологий.

Как сказал в интервью Илье Стечкину, эксперту по маркетингу высокотехнологичных компаний, сопредседатель совета директоров фонда US-MAC (бизнес-акселератор; фонд помогает компаниям выйти на американский рынок) Крис Берри: «…Мы все, представители индустрии высоких технологий, не уделяли этому вопросу достаточного внимания в течение последних пятидесяти лет, и сейчас платим за это невнимание очень высокую цену. Я все еще верю, что существуют подходы к обеспечению безопасности информации, защите компьютерных сетей, защите устройств, о которых мы даже не подозреваем».

ОБ УСТРОЙСТВАХ IoT

Интернет вещей – это многоуровневая система, которая включает в себя «умные» устройства, среду передачи данных, сетевые протоколы, систему управления, хранилище и инструменты анализа данных.

Сегодня устройством Интернета вещей принято считать любой прибор, способный считать показания из окружающей среды и передать их в базу данных, где они будут сохранены и, в ряде случаев, проанализированы. Поэтому обязательным условием является подключение smart-устройства к компьютерной сети тем или иным способом. Когда речь идет об IoT, под сетью можно понимать интранет того или иного предприятия, то есть локальную, а не глобальную сеть.

Это могут быть как устройства, изначально спроектированные для использования в рамках концепции IoT, так и модифицированные продукты. К последним можно отнести, например, бытовые приборы. Обычная микроволновка, подключенная к сети, становится полноценным участником Интернета вещей.

Здесь важно отметить, что концепция IoT, на самом деле, новое имя для совокупности проектов в сфере автоматизации и диспетчеризации. Проекты эти уже много лет используются на производствах. Другой вопрос, что сфера применения технологий расширилась – теперь они доступны и для частных, и для многоквартирных домов. Но перед разработчиками устройств с появлением термина «Интернет вещей» не встала кардинально новая задача: проектируемые под концепцию IoT устройства отвечают тем же стандартным требованиям, что и любые другие. Специального IoT-стандарта на сегодняшний день не существует. А значит, могут не учитываться риски по безопасности. Но, если в ситуации, когда датчик используется на заводе автономно, – это не представляет видимой угрозы, то при подключении устройства к глобальной компьютерной сети риски резко возрастают.

ПОЧЕМУ ЭТО ВАЖНО?

Когда «гаджеты» работают во взаимодействии с всемирной сетью, каждый рискует стать жертвой киберпреступников. Хакеры могут получить доступ к сведениям о вашем сердцебиении и количестве пройденных за день шагов, взломав

фитнес-часы. Это неприятная ситуация, но не фатальная.

Однако же, Интернет вещей не ограничивается персональными данными. Концепция внедряется повсеместно: в медицинских и государственных учреждениях, финансовых организациях, крупных компаниях… Конфиденциальность информации в этих секторах выше, а значит, речь идет о совсем других последствиях. При этом технологии используются примерно одинаковые: и в фитнес-часах, и в датчиках на металлургическом заводе, и в кардиостимуляторах в больнице. Те же самые устройства со встроенной (или не встроенной) системой защиты, которую довольно просто взломать.

Киберпреступники могут получить доступ к персональным данным, корпоративным и коммерческим тайнам, информации о денежных переводах, истории болезни… Список угроз бесконечен.

«Умные устройства сегодня являются привлекательной целью для злоумышленников, поскольку к ним довольно легко получить доступ, ведь многие пользователи не меняют стандартные настройки от производителя, включая пароли, обновления прошивок выходят нерегулярно и они редко устанавливаются владельцами на конечные устройства, – комментирует Денис Легезо, антивирусный эксперт «Лаборатории Касперского». – Наконец, подобные устройства подключены к сети в режиме 24/7. Эта угроза актуальна не только для рядовых пользователей – сегодня практически любое производство имеет выход в Интернет и использует различные сервисы, повышающие производительность, например, облачные технологии».

ПОЧЕМУ ОБ ЭТОМ НЕ ГОВОРЯТ?

Отсутствие единых стандартов – главный тормоз развития Интернета вещей сегодня. Например, существует множество протоколов передачи данных, которые используются для реализации IoT. Выбор конкретного решения зависит от рассматриваемой задачи.

Предположим, нам нужна энергоэффективная сеть. Скорость передачи данных значения не имеет. В этом случае подойдет, например, Sigfox. Но этот протокол поддерживают не все производители устройств. А значит, это сужает список вендоров, из которого мы можем выбирать. Следующая проблема, которая может перед нами встать, – это несовместимость устройств разных производителей между собой.

Поэтому на сегодняшний день совместимость устройств друг с другом и поддержка единых сетевых решений – это главная проблема, которую пытаются решить разработчики, производители и интеграторы. В этой ситуации вопросы безопасности уходят на второй план.

КАК ЗАЩИТИТЬ IoT-УСТРОЙСТВО?

Надо понимать, что устройства под Интернет вещей разрабатываются главным образом по принципу «просто в использовании». Производители выпускают на рынок тысячи устройств с минимальным функционалом (этим обусловлена низкая цена таких приборов) и одинаковыми характеристиками. В том числе, универсальными заводскими паролями.

Рассмотрим кейс. Компания закупает на фабрику 400 одинаковых сенсоров освещенности. Их подключают к Интернету. Информация о приобретенной модели сенсоров попадает к киберпреступнику. Первое, что он сделает, – найдет во всемирной сети заводской пароль к данному оборудованию. Это открытая информация.

Если сотрудники компании не сменили универсальный пароль хотя бы на одном сенсоре, то хакер может получить к нему несанкционированный доступ, не прикладывая дополнительных усилий. А через взломанный сенсор, теоретически, открывается доступ ко всей инфраструктуре предприятия. Теперь преступник может вмешаться в производственный процесс, даже остановить его.

Возникает вопрос: кто несет ответственность за произошедшее? Разработчик? Нет. Ведь в документах не прописано, что пароли разных устройств должны отличаться. А в инструкции по применению, которую, как правило, никто не читает, указана процедура изменения «заводского» пароля. И этим вопросом должен был озаботиться пользователь или инсталлятор. Равно как и вопросом своевременного обновления ПО на устройствах. Новые вирусы создаются каждый день, и тех инструментов защиты, которые были актуальны еще вчера, завтра может быть недостаточно. Для удобства можно настроить функцию автоматического обновления, если она есть.

«Ничего не мешает ставить уникальный пароль на массово тиражируемые устройства. Технически это осуществимо и не требует значительных финансовых затрат, – считает Дмитрий Белявский, ведущий специалист АО «Технический Центр Интернет». – Дело в том, что у разработчиков устройств пока нет мотивации об этом заботиться. И здесь встает вопрос квалификации среднего пользователя, которому удобнее работать с паролем по умолчанию, чем руководствоваться соображениями безопасности».

Для использования в рамках концепции IoT лучше выбирать устройства ровно с тем набором функций, которые требуются для решения задачи. Если в здании надо поставить датчики обнаружения дыма, то следует приобрести устройство, к примеру, без USB-порта. Каждый дополнительный физический разъем увеличивает риски по безопасности.

Более того, предусмотренных разработчиком средств защиты часто бывает недостаточно. В IoT-устройства лучше встраивать дополнительные механизмы обнаружения несанкционированных изменений, в том числе, физических.

«Про необходимость смены пароля, присвоенного устройству по умолчанию, говорят все чаще. И в этом действительно есть смысл. Но гораздо эффективнее еще на этапе проектирования встроить в устройство протоколы аутентификации и шифрования. При том такие, которые требуют минимального вмешательства конечного пользователя. К примеру, научить устройство автоматически обмениваться ключами с основной системой на этапе настройки и сопряжения нового устройства и основной системы, – говорит Роман Вербицкий, технический директор чешской компании «Хост-Телеком». – Но если мы действительно заботимся о безопасности Интернета вещей, как наследника систем мониторинга и диспетчеризации, то гораздо важнее минимизировать уязвимости в протоколах передачи данных. Вдруг на одно из ваших устройств уже установлено программное обеспечение, которое позволит злоумышленнику подключиться к сети удаленно. И это станет возможно не столько из-за того, что вы не сменили заводской пароль, сколько благодаря недостаточной защищенности вашей сети в целом».

ЗАКЛЮЧЕНИЕ

Все уровни организации IoT тесно взаимосвязаны. Получив доступ к «умному» устройству, можно считать отправленные данные или фальсифицировать их. Чтобы этого не произошло, требуется, как минимум, аутентификация устройства (т. е. процедура проверки подлинности пользователя или устройства, например, путем сравнения введенного им пароля или ключа с тем, что хранится в базе данных) и шифрование данных. Незащищенная сеть позволит преступнику отправить в хранилище «ложные показания». А через панель управления можно изменить политику анализа данных… Обеспечив киберпреступнику доступ к одному из уровней системы, пользователь рискует потерять контроль над всей инфраструктурой. Поэтому предусматривать уязвимости следует на всех стадиях реализации IoT, но начать с самого очевидного. Смените заводские пароли. Ведь известное правило «Все гениальное – просто!» работает даже в сложных технических вопросах.