Интернет вещей: обзор проблем безопасности

Автор: Максим Бобровский 19.09.2017

В [предыдущей статье](https://business-online.su/blog/internet-veschey/) об Интернете вещей (IoT) мы познакомились с его историей, перспективами развития, возможностями и, самое главное, пришли к простому выводу – **Internet of Things должен сделать мир по-настоящему открытым**. Он должен стать той технологией, которая поможет решить множество проблем, стоящих перед каждым из нас в отдельности и перед человечеством в целом, начиная от автоматизации быта и заканчивая защитой окружающей среды от экологических катастроф.

Многие преимущества «открытого мира» мы можем оценить уже сегодня – интернет позволяет нам делиться информацией, получать образование, совершать покупки, знакомиться с другими странами, общаться с близкими и наслаждаться произведениями искусства, не покидая своей квартиры. Интернет размывает границы – национальные, географические, культурные, коммуникационные – и с этой точки зрения является безусловным благом, так как обеспечивает взаимодействие всех структур общества.

С другой стороны, всеобщая интернетизация стала благоприятной средой для совершения преступлений, которые происходят в киберпространстве, но, благодаря все той же открытости, имеют последствия для реальной жизни как отдельного человека, так и целых государств. Речь идет о краже личных данных, хакерских атаках, взломах серверов национальных комитетов и министерств…

То же относится и к Интернету вещей, который есть не что иное, как один из этапов развития всемирной паутины. IoT становится объединением физической и цифровой реальности, превращением интернета в «сеть сетей», которая включает в себя все объекты окружающего мира – не только привычные девайсы, но и предметы, казалось бы, не созданные для роли «интернет-узлов»: кофеварки и холодильники, дорожные светофоры и уличные видеокамеры, водосчетчики и сантехнические устройства, медицинское и промышленное оборудование.

**Как сегодня обстоит дело с безопасностью Интернета вещей?** Каковы последствия создания глобальной сети, охватывающей все сферы нашей жизни? Воображение рисует пугающие перспективы: перепрограммирование тормозов автомобиля, удаленное отключение кардиостимуляторов, блокирование датчиков утечки газа в «умном» доме – неужели без должной защиты все это становится возможным? Ответов на эти вопросы пока нет, ведь мы находимся только в начале пути.

Проблемы безопасности IoT – отчеты экспертов

**Что такое Интернет вещей в контексте безопасности?**В общем смысле это совокупность цифровых устройств, которые обмениваются данными друг с другом и работают автономно, без участия человека.

Этих двух факторов вполне достаточно, чтобы задуматься над теми угрозами, которые несет с собой превращение предметов в интернет-узлы. И нужно сказать, что экспертные исследования проблем безопасности IoT не заставили себя ждать – уже в 2008 г. (именно этим годом датируется появление Интернета вещей как явления) «сеть сетей» фигурирует в отчете Национального разведывательного совета США в качестве одной из шести потенциально разрушительных технологий.

Спустя 7 лет, в начале 2015 года, компания OpenDNS представила неутешительные результаты исследования, проведенного в корпоративных сетях, которые используют «интернет-вещи». К слову, бренд OpenDNS принадлежит компании Cisco, мировому лидеру в области информационных технологий, с которым, в частности, связаны и общепринятая формулировка термина «Интернет вещей», и популяризация этого явления в целом.

Итак, компания OpenDNS неоднозначно заявила: **безопасного IoT не существует**. Инфраструктура, которая используется для подключения устройств в корпоративные сети, не контролируется ни пользователями, ни IT-специалистами. Вот лишь некоторые выкладки из экспертного отчета:

* Только 35% компаний используют отдельную wi-fi сеть для потенциально небезопасных «интернет-вещей»
* Видеокамеры, медицинские гаджеты, фитнес-браслеты и другое оборудование передают данные за пределы корпоративной сети
* Большинство телевизоров, интегрированных в IoT, не имеют сертификатов безопасности
* Жесткие диски используют для хранения данных небезопасные облачные серверы

В это же время компания HP независимо от OpenDNS провела собственное исследование, но не в коммерческом, а в потребительском секторе. Результаты оказались аналогичными – и в этом случае было выявлено множество уязвимостей, начиная от применения дефолтных паролей и заканчивая незащищенным веб-интерфейсом, который используют большинство устройств, подключенных к Интернету вещей. Кроме того, было выявлено, что почти все исследуемые девайсы собирают личную информацию пользователей без их ведома.

Есть и более свежие данные – в начале текущего года авторитетный интернет-журнал TechRepublic предсказал повышение количества киберпреступлений из-за плачевного состояния системы безопасности «сети сетей». Специалисты выделили несколько критериев, которые могут привести к настоящему хаосу в инфраструктуре Internet of Things. Вот главные из них:

* **Быстрорастущий парк IoT-устройств**. Сегодня к сети подключается около 6 000 000 новых «вещей» ежедневно! Если учесть, что каждый девайс имеет не одну «дыру» в системе безопасности, а несколько, то ситуация складывается действительно устрашающая.
* **Слабая защищенность огромных массивов пользовательских данных**. Добавим, что для корректной работы многие IoT-устройства собирают не только пароли, но и информацию другого типа, начиная от имени пользователя и заканчивая фактами из биографии. Очевидно, что там, где хранятся множества взаимосвязанных данных, требуется и надежная защита. Интернет вещей пока этим похвастать не может.
* **Возможность быстро создать мощный ботнет из миллионов устройств**, подключенных друг к другу. До появления IoT эта проблема стояла не так остро, что связано, прежде всего, с потерей «автономии» предметов физического мира – с наступлением эры Internet of Things «интернет-вещи» уже не работают сами по себе, а интегрированы в единую коммуникационную структуру.

Это теория. А что на практике?

Очевидно, что **проблемы безопасности Интернета вещей требуют немедленного поиска решений**, что и подтверждает наш обзор. И опасения экспертов, к сожалению, оправданы – IoT в его современном виде дает большие возможности для деятельности киберпреступников. Приведем лишь три реальных примера.

**Пример 1**. В феврале 2016 года инженеры из компании Panasonic взломали… унитаз. Устройство самопроизвольно спускало воду и таким образом пугало посетителя, находившегося в помещении. Все это происходило в рамках эксперимента, где требовалось доказать наличие уязвимостей в системе «умного» дома. Случай довольно забавный, но и вполне характерный – если можно подобрать пароль к унитазу (в буквальном смысле), то кто даст гарантию, что другие «вещи» из IoT защищены более надежно?

**Пример 2**. В сентябре 2016 года блог журналиста Брайана Кребса, имеющего репутацию одного из самых известных IT-специалистов по киберпреступлениям, подвергся масштабной хакерской атаке (665 гигабит в секунду). Эту крупнейшую в истории Интернета вещей DDoS-атаку организовали злоумышленники, объединившие в ботнет сотни тысяч устройств, интегрированных в IoT. И это уже совсем не шутка.

**Пример 3**. Участники конференции Positive Hack Days шестой год подряд участвуют в конкурсе по конкурентной разведке, что добавляет фактов в неутешительную статистику – взломать ту или информационную систему сегодня совсем не сложно, а физическое расширение Интернета вещей делает этот процесс еще проще.

В текущем году авторы конкурса придумали простую легенду, согласно которой все сотрудники некой IT-фирмы исчезли. Задача конкурсантов – распутать это странное дело. Расследование началось с анализа исходного кода сайта компании, что помогло выяснить фамилию одного из «пропавших» дизайнеров, его e-mail и обнаружить профиль в социальных сетях. Цепочка следующих действий выглядела так: анализ чекинов и публикаций пользователя, выявление его интересов и связанных профилей, получение доступа к access-логам сервера социальной сети, установление VoIP-шлюза и подключение к Skype-группе «пропавших» разработчиков, определение и взлом аккаунтов в профессиональных сервисах, получение информации об IP-адресе роутеров, доступ к платежным сервисам пользователей и так далее – до победного конца.

Что характерно, все участники конкурса справились хотя бы с одним этапом, а 9 человек из 66 выполнили более 50% заданий.

**Вывод прост**: чем больше мы оставляем «следов» в цифровом мире, тем более уязвимы для несанкционированного доступа к нашим данным.

Как защитить Интернет вещей?

Для повышения безопасности IoT предлагается много решений, но большинство из них можно свести к следующим:

1. **Во-первых**, требуется единая стандартизация, которая установит регламенты для каждой из областей Интернета вещей. Первый шаг к этому уже сделан – в октябре 2016 года появилась информация о планах Еврокомиссии по обязательной сертификации предметов физического мира, интегрированных в IoT. Подробностей этой программы пока нет, но в качестве одного из вариантов называется необходимость чипирования «вещей», подключенных к глобальной сети. В контексте IoT речь идет о тех устройствах, которые сами по себе не представляют ценности для преступников, но могут быть использованы для хакерских атак и других криминальных активностей – холодильниках, телевизорах, видеокамерах, принтерах и пр.
2. **Во-вторых**, нужно уходить от «кроссплатформенности», которая сегодня является одним из главных критериев не только Интернета вещей, но и цифровой реальности в целом. Другими словами, каждая категория устройств, встроенных в «сеть сетей», должна прийти к использованию двух-трех платформ, не более. Например, все стиральные машинки должны быть оснащены микроконтроллерами с типовыми, а не разными, прошивками, видеокарты должны использовать одинаковые драйверы... Пока это кажется фантастикой, но именно в этом направлении должны работать и производители аппаратного оборудования, и разработчики операционных систем, и поставщики ПО.
3. И, **в-третьих**, нужно обратить внимание на производительность самого программного обеспечения. Это касается не только необходимости «латать дыры» в эффективности используемых приложений, но и улучшения их масштабируемости, что особенно важно, учитывая непрерывность процесса включения в IoT новых и новых устройств.

**В заключение**хочется сказать, что IoT находится только в начале своего развития, и было бы наивно полагать, что на этом пути не возникнут препоны и препятствия. Одним из них является уязвимость Интернета вещей. Несмотря на всю сложность ситуации, у нас есть серьезные основания для оптимизма – этой проблемой заинтересованы не только экспертное сообщество, но и политические институты, и коммерческие структуры, и обычные потребители.

Именно так, сообща, мы приблизим качественно новую эпоху в развитии информационного пространства. Эпоху безопасного Интернета вещей.