ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ IOT

INFORMATION SECURITY IOT

Авторы: *Петросян Роберт Ашотович (МИРЭА)*
Молчанов Максим Гелаевич (МИРЭА)

Аннотация: *В наше время одной из актуальных проблем в области информационной безопасности является обеспечение защиты так называемых Интернет вещей (Internet of Things, IoT). Как показывают исследования, в последние 3-4 года наблюдается увеличение уровня потребности в таких вещах. Интернет вещей (англ. Internet of Things, IoT) открывает новые возможности для мобильных устройств, бытовой техники и программного обеспечения в области обмена и передачи информации по интернету. В данной статье описана сущность интернет-вещей. Перечислены основные уязвимости и угрозы интернет-вещей. Рассмотрены проблемы информационной безопасности интернет-вещей и их причины. Проанализированы основные виды атак на интернет вещей. Проанализированы средства, обеспечивающие безопасность данных в интернете вещей.*

Ключевые слова: *интернет вещей, информационная безопасность, угроза безопасности.*

Annotation: *Nowadays, one of the urgent problems in the field of information security is to ensure the protection of the so-called Internet of things (IOT). As studies show, in the last 3-4 years there has been an increase in the level of demand for such things. The Internet of things (eng. Internet of Things (IoT) opens up new opportunities for mobile devices, home appliances and software in the field of information exchange and transmission over the Internet. This article describes the essence of Internet things. The main vulnerabilities and threats of Internet of things are listed. The problems of information security of Internet things and their causes are considered. The main types of attacks on the Internet of things are analyzed. The tools to ensure data security in the Internet of things are analyzed.*

Keywords: *Internet of things, information security, security threat.*

В современном мире телекоммуникационные, запоминающие, идентификационные и другие устройства занимают в жизни общества главенствующее положение, в связи с наступлением так называемого «Века Информационных Технологий». Если ранее человеку было необходимо непосредственно взаимодействовать с устройством, то теперь научно-технический прогресс открывает новые возможности. В создаваемых системах предусматривается возможность взаимодействия по новой схеме «устройство-устройство», а не только «человек-устройство». Набор современных информационных и телекоммуникационных технологий, способных обеспечить данный вариант взаимодействия, получил название «Интернет Вещей».

В промышленном IoT основными разновидностями «вещей», которые надо подключать к сети, являются различные типы датчиков (сенсоров) и приводов для сбора и обмена данными, с возможностью удаленного контроля и управления [9].

К потребительскому IoT относятся: носимые устройства, умный дом, умная одежда, Smart TV, IP-камеры, умные девайсы для животных, устройства для автомобилей.

Приобретая такие устройства, люди чаще всего не задумываются, что зачастую безопасность у них не находится на должном уровне. С одной стороны, удаленное управление системами позволяет с большим комфортом организовать свое жизненное пространство; а с другой - датчики и элементы управления системами жизнеобеспечения. оказавшись в руках злоумышленника, значительно увеличивают риски в области информационной безопасности [8].

В работе [4] была предложена развернутая система классификации процессов в среде «Интернет вещей». Так, архитектура безопасности среды рассматривается как три измерения: службы безопасности, сетевой слой и домен безопасности. Причем первое измерение включает в себя: аутентификацию, управление доступом, конфиденциальность, целостность, доступность и др. Второе измерение, состоящее из физического слоя, сетевого слоя, пользовательского слоя и слоя управления, соотносится со слоями сетевой модели OSI. Третье измерение включает в себя четыре подраздела, которые характеризуют принцип работы среды «Интернета вещей». Первый подразде|л - это домен исполнительных и сенсорных устройств. Он отвечает за требования к надежности, специфику эксплуатации и др. Второй подраздел - домен доступа, в задачи которого входит определение правомерности доступа к системе не только пользователя, но и устройств между собой. Третий - сетевой домен определяет условия доступа к узлам сети, маршрутизацию информационного трафика и т.п. Последний домен приложений отвечает за безопасность информации, циркулирующей внутри среды программного обеспечения. Здесь большее внимание уделяется ошибкам в проектировании и программировании, а также особенностям работы с критически важной или персональной информацией, например с информацией о состоянии здоровья пациента [9]. Обсуждаемая классификации представлена на рис. 1.

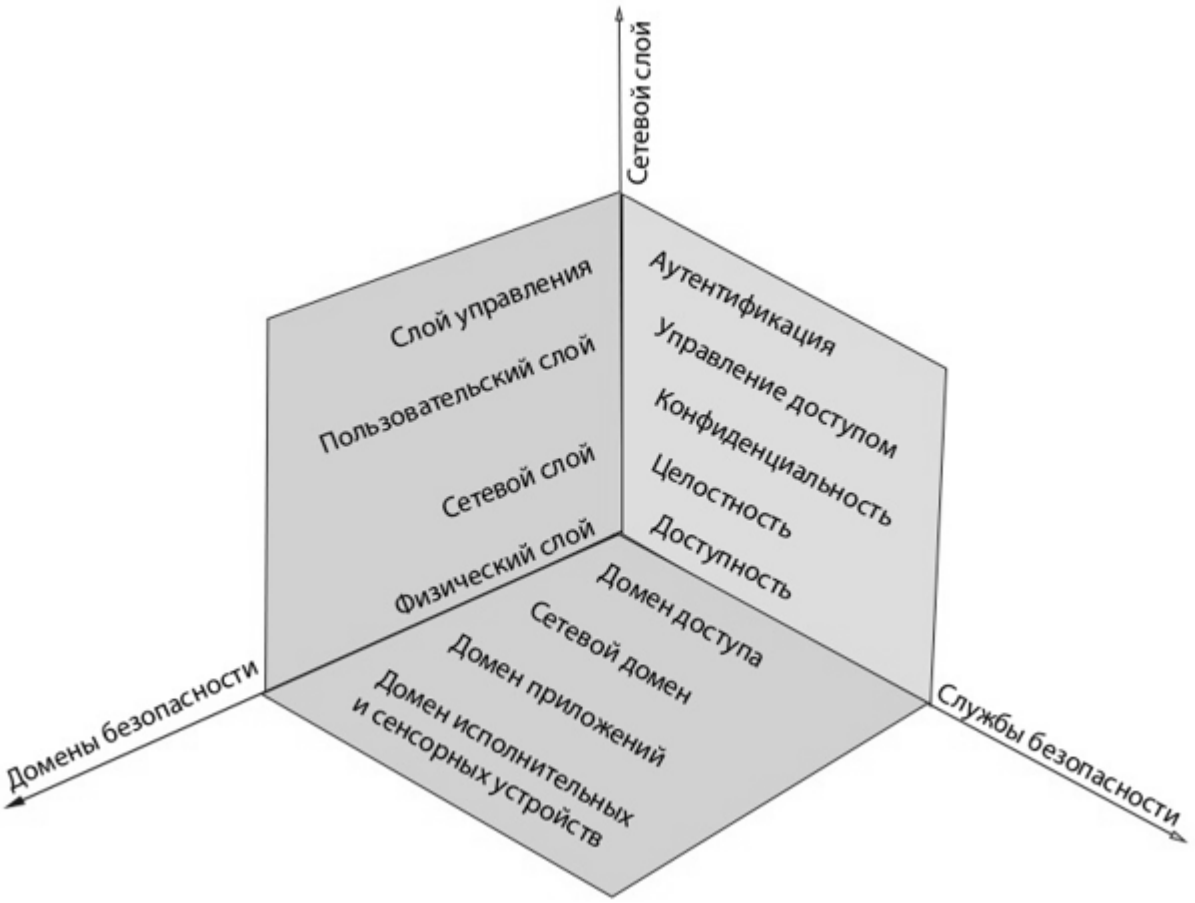

Рис. 1. Составляющие безопасности среды «Интернет вещей» авторов Li H, Zhou X

Аналитики Gartner прогнозируют, что по итогам 2017 г. во всем мире к Интернету вещей будет подключено 8,4 млрд устройств. Результаты сканирования разработанной BullGuard программой IoT Scanner 310 тыс. пользовательских сетевых устройств показали, что 4,5 % (почти 14 тыс.) из них уязвимы и могут быть без труда взломаны. Аналитики BullGuard прогнозируют, что потенциально уязвимыми являются 378 млн устройств [1].

Конфиденциальность в IoT рассматривается как серьезная проблема. IoT предоставил огромное количество данных, принадлежащих не только таким потребителям, как, например, в WorldWideWeb, но и граждан в целом, групп и организаций. Это можно использовать для установления того, что нас интересует, куда мы идем, и наших намерений. Хотя это может предоставить большие возможности для улучшения услуг, оно должно быть сопоставимо с нашим стремлением к конфиденциальности. Жизненно важно, чтобы потребители доверяли службам, с которыми они связаны, чтобы уважать их конфиденциальность. Доверие является фундаментальным элементом в формировании любых отношений и является важным фактором в принятии новых технологий.

Датчики, в том числе встроенные в мобильные устройства, собирают разнообразные данные о жизни граждан. Эти данные будут агрегированы, проанализированы, обработаны, чтобы извлечь полезную информацию для предоставления интеллектуальных и вездесущих услуг. Доверие относится к

определению того, когда и кому информация должна быть выпущена или раскрыта.

Предоставление пользователям большего контроля над сбором и использованием их личной информации рассматривается как важный аспект обеспечения доверия к распределенным системам. Предыдущие проекты, такие как Project for Privacy Preferences Project (P3P), были разработаны таким образом, чтобы пользователи могли управлять ими при использовании веб-браузеров. Протокол P3P, инициатива консорциума World Wide Web (W3C), инициированная в 2002 году, был основан на идее перевода политик конфиденциальности веб-сайтов в стандартизованную машиночитаемую информацию для обеспечения прозрачности и обеспечения возможности выбора пользователя. К сожалению, проект закончился преждевременно, и было очень мало реализаций. Существует ряд причин, объясняющих провал P3P, в центре которого - отсутствие принятия со стороны промышленности и пользователей. Конкретные причины включают отсутствие принятия вебсайтами из-за драйверов для предприятий по внедрению технологий PET (соответствие, эффективность и риск повреждения бренда), которые недостаточно значительны для достаточного количества предприятий, отсутствие заимствования браузерами и отсутствие принятия пользователями, включая культурные соображения, которые влияют на международное принятие P3P.

Для обеспечения конфиденциальности были разработаны различные технологии повышения конфиденциальности, в том числе виртуальные частные сети, безопасность транспортного уровня, расширение безопасности DNS, луковая маршрутизация и получение частной информации. Языки политики конфиденциальности - это еще один тип PET. PPL можно классифицировать как внешние (декларативные без принудительного исполнения) или внутренние (нормативные с поддержкой принудительного исполнения); P3P приходится на предшествующий класс. Другие PPL включают SAML (язык разметки безопасности), XACML (стандарт OASIS для контроля доступа), включая PPL, A-PPL и GeoXACML расширения XACML. XACL, SecPAL4P, XPref, P2U, EPAL. FlexDDPL, PSLang, ConSpec, и SLAng. Несмотря на то, что существует ряд PPL, ни один из них не стал стандартом де-факто, и широкомасштабное принятие остается проблемой.

В таблице перечислены типичные уязвимости, обнаруженные в рамках исследования, проведенного компанией HPE [2].

Распространенные уязвимости устройств Интернета вещей

Уязвимость	Примеры
Незащищенный веб-интерфейс (мобильный, облачный)	Слабые пароли; ненадежные системы восстановления паролей; отсутствие механизма блокировки учетной записи; уязвимость для атак на основе межсайтовых скриптов, подделки запросов
Слабость средств аутентификации и проверки полномочий	Необоснованное повышение привилегий, отсутствие контроля доступа

Незащищенные сетевые сервисы	Уязвимость для атак на отказ в обслуживании, переполнение буфера, нечеткое тестирование; предоставление без необходимости доступа к сетевым портам н сервисам извне
Отсутствие шифрования данных и проверки целостности данных при передаче	Передача информации без шифрования
Отсутствие обеспечения приватности	Сбор данных о пользователе без необходимости; недостаточный контроль доступа к пользовательским данным; отсутствие механизмов анонимизации конфиденциальных данных
Недостаточные возможности настройки параметров безопасности	Отсутствие схемы разграничения привилегий; отсутствие разделения прав администратора и пользователей; допустимость слабых паролей; отсутствие журнала безопасности; отсутствие вариантов выбора механизмов шифрования данных; отсутствие предупреждений пользователя о событиях безопасности
Незащищенное программное или микропрограммное обеспечение	Отсутствие механизма защищенных обновлений; файлы обновлений не шифруются; файлы обновлений не проверяются перед загрузкой; незащищенный сервер обновлений
Недостаточная физическая защищенность	Наличие доступа к ПО через порты USB; наличие съемных носителей информации

Для устройств Интернета вещей характерны следующие угрозы:

- получение несанкционированного доступа;
- внедрение вредоносных программ;
- выявления паролей;
- перехват сетевого трафика;
- сканирование открытых портов;
- удаленный запуск приложений.

При успешной реализации таких угроз злоумышленники могут получить доступ к устройству для получения информации о пользователе, подсматривать через взломанные камеры, отслеживать перемещение устройств, создавать ботнеты с сотнями шли тысячами уязвимых устройств, с помощью которых атаковывать и взламывать серверы и веб-сайты, устраивать DDoS-атаки. На этом список возможных последствий не заканчивается, его можно продолжать и продолжать.

Одна из проблем устройств интернет-вещей - это недостаточное уделение внимания обеспечению безопасности при проектировании и производстве. Ее

следствием являются ошибки в программном коде, отсутствие обновлений для выпущенных продуктов. Причина этой проблемы - это то, что более половины продуктов IoT производится небольшими компаниями, существующими менее трех лет. Можно представить, что лишь часть этих компаний в силах обеспечить нормальный уровень безопасности своих изделий [5]. Кроме того, цель производителей - это продать IoT-устройства. Результатом всего этого является то, что устройства IoT имеют очень слабую защиту или ее нет совсем, а рынок наполнен подобными уязвимыми устройствами [6]. Пока производители не уделяют должного внимания безопасности своей продукции, потребитель должен сам задуматься о защите своих данных.

Во-первых, стоит задуматься, стоит ли подключать устройство к Интернету. Может быть, эти функции не будут востребованы. Если не предполагается использовать его через сеть, то не следует подключать устройство к Интернету.

Во-вторых, будет безопаснее, если создать отдельную сеть для таких устройств, например, с помощью Wi-Fi маршрутизатора, тем самым обеспечив безопасность основной сети. В случае взлома этой сети ваш компьютер и мобильные устройства, подключенные к основной сети (которая является приоритетным интересом злоумышленников), будут в безопасности [4].

В-третьих, другим важным моментом являются смена пароля и обновление устройства. Большинство атак злоумышленников происходит путём перебора стандартных логинов и паролей производителей, поэтому при первой настройке устройства пароль, поставленный производителем, нужно изменить на уникальный. А регулярная проверка и установка обновлений позволят закрыть уязвимости, обнаруженные производителем.

Выполнение этих действий поможет уберечь устройства.

Другие проблемы связаны со спецификой таких устройств, это проблемы малых вычислительных ресурсов, что усложняет обеспечение безопасности большого числа устройств, как и отсутствие единых стандартов для их взаимодействия. Они в данный момент еще не решены.

Сможет ли Интернет вещей стать безопасным? Вероятно, да. Но лишь тогда, когда подавляющее большинство разработчиков начнет с большей ответственностью относиться к защите своих гаджетов [3]. Использование устройств интернет-вещей позволяет повысить эффективность в промышленной отрасли и улучшить качество жизни людей. Но при их использовании нужно быть осторожным.

Заключение. IoT-сети, которые становятся новой инфокоммуникацией цифровой экономики, требуют соответствующих технологий обеспечения безопасности. Рассмотренные атаки на сети Интернета вещей определяют соответствующие механизмы защиты, некоторые из которых продиктованы особено-стями IoT-сетей.

Список литературы

1. IoT-ботнет Reaper может задействовать для атак 378 млн уязвимых IoT-устройств [Электронный ресурс]. – URL: https://iot.ru/bezopasnost/iot-botnet-reaper-mozhet-zadeystvovat-dlya-atak-378-mln-uyazvimykh-iot-ustroystv
2. Ботнеты и безопасность Интернета вещей [Электронный ресурс]. – URL: https://www.osp.ru/os/2017/02/13052219/
3. Интернет вещей угрожает человечеству [Электронный ресурс]. – URL: https://hyser.com.ua/tehnology/internet-veshhej-ugrozhaetchelovechestvu-104393
4. Интернет вещи (iot) и их безопасность [Электронный ресурс]. – URL: http://www.cleper.ru/articles/description.php?n=589
5. Как обезопасить Интернет вещей? [Электронный ресурс]. – URL: https://rb.ru/story/IoT-security/
6. Новые угрозы и направления развития информационной безопасности в 2017 году [Электронный ресурс]. – URL: http://1234g.ru/novosti/infobezopasnost-2017
7. Проблемы безопасности SmartTV [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/problemy-bezopasnosti-smarttv
8. Проблемы информационной безопасности: интернет вещей [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/problemyinformatsionnoy-bezopasnosti-internet-veschey