УГРОЗЫ И ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ ПРИ ЭКСПЛУАТАЦИИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ, ПРИМЕНЯЕМЫХ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Нассо Д.М.[1], Способ С.П.[2]

1 Военная академия связи имени маршала Советского Союза Буденного С.М., г. Санкт-Петербург, г. Дамаск, Сирийская Арабская Республика, hjsm19112019@gmail.com

2 Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь, sposob@mail.ru

Abstract. Threats and problems arising from the operation of internet of things devices used in the service sector the educational process.

На основании характеристик устройств Интернета вещей определяются *угрозы и проблемы*, которые возникают при эксплуатации, а именно:

Плохая безопасность приложений и конечных точек: Плохо защищенные приложения и конечные устройства делают системы уязвимыми для кибератак. Одна из основных причин заключается в том, что большинство производителей устройств – это те же производители, которые производили устройства до появления IoT, а теперь они сделали свои устройства умными, чтобы подключаться к IoT, но не учли вопросы безопасности, потому что для них это несущественная функция.

Лёгкая авторизация / аутентификация: Большинство устройств, выпускаемых на коммерческом рынке, поставляются с процессорами настолько маленькими, что они предназначены только для выполнения очень простых задач и не могут обрабатывать что-то вроде авторизации или аутентификации, для которых требуется процессор большего размера.

Отсутствие физической безопасности: Большинство устройств Интернета вещей находятся в городских условиях и доступны для общественности. Это увеличивает риск физической атаки. Мы не имеем в виду, что какой-то преступник может повредить систему в буквальном смысле, но хакеры могут легко получить доступ к системе IoT, которая находится в открытом доступе, с целью кражи данных и нарушения работы устройств [1].

Чрезмерное количество конфиденциальных данных: Интеллектуальное устройство – это устройство, которое имеет некоторые базовые встроенные функции, такие, как микрофон, камера, ночное видение и т.д., которые необходимы для приема, передачи данных и взаимодействия с пользователем. Эти функции действуют как глаза и уши устройства и непрерывно записывают терабайты данных, иногда без ведома пользователя, использующего данные устройства. Такие данные могут быть очень конфиденциальными, и, если попадут в чужие руки, могут нарушить конфиденциальность пользователя и стать серьезной угрозой безопасности. Это одна из основных причин того, что люди не могут доверять системам Интернета вещей, и были сотни сообщений о случаях, когда сборщики данных злоупотребляли информацией и нарушали многие законы о конфиденциальности данных [3].

Небезопасные учетные данные по умолчанию: Интернет-вещь обычно поставляется с именем пользователя по умолчанию и паролем по умолчанию, который вы используете для первого входа в систему на устройстве. Это имя пользователя и пароль по умолчанию называются учетными данными по умолчанию и могут представлять огромную угрозу безопасности. Некоторые из устройств IoT даже по сей день поставляются с жестко запрограммированными паролями и именами пользователей, что означает, что эти учетные данные никогда не могут быть изменены и иногда отпечатываются на устройстве. Это делает устройство уязвимым не только для кибератак, но и для физических атак, когда кто-то может получить доступ к имени пользователя или паролю по умолчанию. Некоторые пользователи вовсе не меняют этих учетных данных, что делает их устройства ещё менее безопасными. Хакеры всегда пытаются получить доступ к устройствам, используя имя пользователя и пароль по умолчанию [2]. Получается, устройство Интернета вещей, которое изначально предполагалась приносить пользу и в некой степени быть помощником человеку, превращается в предателя, которые открывают злоумышленнику доступ к персональной информацию через *уязвимые места*:

– IPv6;

– питание сенсоров;

– стандартизация архитектуры и протоколов, сертификация устройств;

– обеспечение защиты информации;

– учетные записи по умолчанию, низкая надежность механизмов аутентификации;

– отсутствие сопровождения продуктов от производителя для решения проблем безопасности;

– невозможность обновить программноаппаратной составляющей;

– использование открытых протоколов и лишних открытых портов;

– зависимость безопасности сети от конкретных устройств;

– использование слабозащищенных мобильных технологий

–использование незащищенной облачной инфраструктуры;

– использование уязвимого программного обеспечения.

В связи с чем в Банке данных угроз безопасности информации ФСТЭК выделяют следующие уязвимости Интернета вещей:

- BDU:2019-00533 Уязвимость программной платформы Java Platform, позволяющая удаленному нарушителю нарушить конфиденциальность и целостность защищаемой информации;

- BDU:2021-01080 Уязвимость интерфейса командной строки (CLI) платформы Azure IoT, позволяющая нарушителю повысить свои привилегии;

- BDU:2021-05533 Уязвимость компонента Windows Hyper-V Discrete Device Assignment (DDA) операционной системы Windows, позволяющая нарушителю вызвать отказ в обслуживании;

- BDU:2019-01032 Уязвимость набора инструментов для разработки программного обеспечения Azure IoT SDK, связанная с ошибками процедуры подтверждения подлинности сертификата, позволяющая нарушителю осуществить атаку типа «человек посередине»;

- BDU:2019-00573 Уязвимость программного обеспечения промышленного интернета вещей IIoT Monitor, связанная с ошибками при использовании криптографии, позволяющая нарушителю раскрыть защищаемую информацию;

- BDU:2021-01204 Уязвимость базы данных для интернет вещей IoT Apache IoTDB, связанная с наличием открытого порта JMX 31999, позволяющая нарушителю выполнить произвольный код.

Проанализировав угрозы, уязвимые места и проблемы Интернета вещей, можно сделать вывод, что защита информации должна обеспечиваться уже на этапе разработки Интернета вещей. В связи с чем дают следующие *рекомендации для производителей и разработчиков ПО*:

– убедиться, что с сотрудниками проведены беседы в области кибербезопасности, и они обучены навыкам в области защиты информации;

– обеспечить совместимость данных с доверенной автоматизированной системой установки обновлений;

– провести проверку кода во время процесса установки – это уменьшит количество ошибок в конечной версии продукта, а также выявит любые попытки злоумышленника внедрить вредоносное программное обеспечение или обойти аутентификацию.

Первый и самый важный шаг, который необходимо сделать производителям и разработчикам приложений, – это осознать важность безопасности в устройствах IoT и начать рассматривать ее как приоритет, а не функцию. Все новые производимые устройства Интернета Вещей и все разрабатываемые приложения Интернета Вещей должны быть защищены от начала до конца и не допускать утечки данных. Как пользователь, мы можем сделать для обеспечения безопасности приложений и конечной точки следующее:

- при покупке устройств или установке приложения мы должны убедиться, что оно от надежного производителя или разработчика. Большинство брендов на рынке надежны с точки зрения безопасности, проблема возникает только тогда, когда производители с местных рынков пытаются продвинуть свой продукт, не уделяя внимания безопасности [4].

Второй наиболее важный шаг, который необходимо предпринять, - это необходимость аутентификации и авторизации при использовании интеллектуальных устройств, подключенных к Интернету Вещей. Производители и разработчики должны убедиться, что их устройства и приложения поддерживают безопасную авторизацию и аутентификацию. Пользователи также должны убедиться, что устройство, которое они покупают, имеет эту встроенную функцию. Для устройств, которые уже работают, но не поддерживают даже базовые функции, такие, как аутентификация и авторизация, могут использоваться вторичные приложения и устройства, которые обеспечивают дополнительную безопасность в форме аутентификации или авторизации. Пользователь также должен убедиться, что он не приобретает устройства с жестко заданными учетными данными по умолчанию, чтобы сразу при получении устройства сменить логины и пароли.

С точки зрения данных, пользовательские данные являются одним из основных компонентов, которые увеличивают риск и должны передаваться безопасным способом. Сборщики данных и поставщики должны сделать безопасность данных своим главным приоритетом и обеспечить безопасную передачу данных с одного устройства на другое. Приложение, используемое в системах Интернета Вещей, должно иметь встроенные функции для записи отклонений в данных и последующего сообщения об этом, чтобы пользователь мог принять соответствующие меры. Так же необходимо создать многоуровневую систему для защиты системы Интернета Вещей, которая сама по себе является сложной взаимосвязанной системой.

Характерные особенности - Применимость в совершенно различных областях. Место, где IoT встречается с пользователем. Вернемся к алгоритмам шифрования. Они затрагивают, в первую очередь, уровень "вещей" и большей частью связаны с ним. Ведь датчики, получают данные, которые нужно передать. Без шифрования, данные можно было бы перехватить просто прослушивая канал. Проблемы, решаемые алгоритмами шифрования: конфиденциальность, целостность, авторства сообщения.

Литература

1. Карачев О. Интернет вещей: что это и с чем его едят // Chëza. 2016. URL: http://chezasite.com/news/chto-takoe-internet-veshei-82180.html (дата обращения: 14.04.16).

2. Кириллова Э. Что такое M2M, кому это нужно и как будет развиваться // Rusbase. 2014. URL: http://rusbase.com/howto/m2m/

3. Портер М., Хеппельман Дж. Революция в конкуренции. "Умные" технологии изменяют конкурентную борьбу // Harvard Business Review. 2016. URL: http://hbr-russia.ru/special/ptc-iot/.

4. Портер М., Хеппельман Дж. Революция в конкуренции. "Умные" технологии перекраивают компании // Harvard Business Review. 2016. URL: http://hbr-russia.ru/special/ptc-iot/.

5. Шилина М.Г. Интернет коммуникация в инфосфере: Монография. - Москва: 2013. – 231.

6. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З "Об информации, информатизации и защите информации".