# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УСТРОЙСТВ IOT С ИСПОЛЬЗОВАНИЕМ АППАРАТНОЙ И СЕТЕВОЙ ПОДДЕРЖКИ

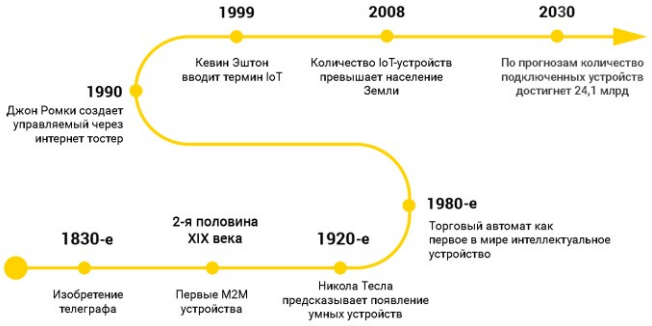
*Кабаков В.П., Чертков А.С., Способ С.А.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*подполковник Способ С.П. – магистр тех. наук*

**Аннотация.** В тезисе рассматривается информационная безопасность устройств Интернета вещей с использованием аппаратной поддержки и сетевой для эффективной работы.

*IoT – Internet of Things* (Интернет вещей) – относительно новая технология, идея о которой появилась еще в 1999 году Кевином Эштоном. В лаборатории Массачусетского университета была представлена метка *RFID* – метка идентификации, позволяющая простейшим объектом ориентировать и определять себя в пространстве с помощью радиоволн. Тогда идея о взаимодействии миллиарда устройств, находящийся на огромных расстояниях между собой казалась нереализуемой. Уже сегодня она объединяет множество устройств в сеть, позволяющую им собирать, анализировать, обрабатывать и передавать между собой данные.




Несмотря на то, что поле работы с вопросом безопасности остается огромным, сейчас существуют решения, позволяющие осуществлять развертывание *IoT* более надежно. Например, для решения проблемы устаревания программного обеспечения устройств, есть возможности эффективных стратегий автоматического обновления.

Благодаря *SOTA (Software Over the Air)* “обновление по воздуху” и *FOTA (Firmware Over the Air)* – «прошивка по воздуху», программное обеспечение подключенных устройств и настройки можно обновлять с помощью беспроводной связи.

Очень немногие устройства используют зашифрованную связь как часть своей первоначальной конфигурации. Они чаще используют обычные веб-протоколы, которые обмениваются данными в виде простого текста, что позволяет хакерам легко наблюдать за ними и выявлять слабые места. Вот почему для всего веб-трафика крайне важно использовать *HTTPS*, безопасность транспортного уровня *(TLS),* безопасный протокол передачи файлов *(SFTP)*, расширения безопасности *DNS* и другие безопасные протоколы при общении через Интернет. Устройства, которые подключаются к мобильным приложениям, также должны использовать зашифрованные протоколы, а данные, хранящиеся на флэш-накопителях, должны быть зашифрованы в качестве меры безопасности *IoT.* Только зашифровав данные, вы можете быть уверены, что вредоносное ПО не заразило устройство.

Чтобы защитить продукт компании от перенастройки, можно использовать функции аппаратного корня доверия. Например, если устройство имеет хранилище ключей, его можно использовать для шифрования потока битов или прошивки продукта, чтобы можно было запрограммировать только устройства с определенным ключом. Это эффективно, но действительно безопасно только в том случае, если устройство с ключом имеет встроенные лицензированные меры противодействия *DPA*.

Сгенерированные закрытый и открытый ключи инициируют связь, и облачный сервер с открытыми ключами отправляет каждому устройству контрольный вопрос. Если ответ правильный, предпринимаются следующие шаги для защиты связи на основе шифрования информации с помощью закрытых ключей. Обратитесь к поставщику, у которого есть инфраструктура открытых ключей *(PKI)* и *PUF* для обеспечения высочайшего уровня безопасности данных.

Другие способы реализации безопасности *IoT* включают:

– Контроль доступа к сети. *NAC* может помочь идентифицировать и инвентаризировать устройства *IoT,* подключающиеся к сети. Это обеспечит основу для отслеживания и мониторинга устройств.

– Сегментация. Устройства *IoT*, которым необходимо напрямую подключаться к Интернету, должны быть сегментированы в свои собственные сети и иметь ограниченный доступ к корпоративной сети. Сегменты сети должны отслеживать аномальную активность, где могут быть предприняты действия в случае обнаружения проблемы.

– Шлюзы безопасности. Выступая в качестве посредника между устройствами *IoT* и сетью, шлюзы безопасности обладают большей вычислительной мощностью, памятью и возможностями, чем сами устройства *IoT*, что дает им возможность реализовывать такие функции, как брандмауэры,

чтобы гарантировать, что хакеры не смогут получить доступ к устройствам *IoT*, которые они подключают.

– Управление исправлениями/непрерывное обновление программного обеспечения. Крайне важно предоставить средства обновления устройств и программного обеспечения либо через сетевые подключения, либо с помощью автоматизации. Координированное раскрытие уязвимостей также важно для скорейшего обновления устройств. Рассмотрите также стратегии окончания срока службы.

Однако в настоящий момент главная проблема у *IoT* – его уязвимость к кибератакам. Причиной тому является ежегодное увеличение количества подключенных устройств, поэтому возрастают риски несанкционированного доступа в *IoT*-систему.

Причина кроется в большом количестве заводов без централизированного управления и реализации безопасности. Например, хакеры могут изменять параметры контура управления, вмешиваться в производственную логику, изменять состояние робота и многое другое. Группа исследователей решила продемонстрировать, какой ущерб на самом деле может нанести взломанный робот. Они обнаружили уязвимости в системе робота-манипулятора и смогли запрограммировать робота так, чтобы он наносил ущерб продуктам, которые он производил на миллионы долларов.

Киберпреступники не остановятся ни перед чем, даже перед взломом медицинского оборудования. Примером является атака программы-вымогателя *WannaCry* на Национальную службу здравоохранения в 2017 году, которая затронула компьютеры, томографы и операционное оборудование и поставила под угрозу множество жизней. Вот почему безопасность устройств *IoT* имеет решающее значение.

***Список использованных источников:***

*1. “Информационная безопасность устройств IoT с использованием аппаратной поддержки” https://habr.com/ru/post/534300/*

*2. “Информационная безопасность интернета вещей (IoT)” https://center2m.ru/informatsionnaya-bezopasnost-veschey*

*3. “Что такое IoT и что о нем следует знать” https://habr.com/ru/company/otus/blog/549550/*

*4. “IoT security” IoT Security: Its importance and how to improve it | ALSO_*

*5. “Hardware security in IOT” https://embeddedcomputing.com/technology/security/hardware-security-in-the-iot*