БАЗОВЫЕ ШАГИ ЗАЩИТЫ ИНТЕРНЕТА ВЕЩЕЙ

Алевтина Александровна Мурадова
ТУИТ имени Мухаммада аль-Хорезми, PhD, доцент кафедры «Телекоммуникационный инжиниринг»
Email: a.muradova1982@inbox.ru

АННОТАЦИЯ

В статье представлены базовые шаги защиты Интернета вещей. Показаны 5 основных правил безопасного пользования смарт-устройствами и защиты Интернета вещей. Каждый шаг представлен основными техническими моментами при подключении устройств: определение параметров конфиденциальности данных, проверка наличия обновлений встроенного ПО, загрузка решений по безопасности и защиты смарт-устройств.

Ключевые слова: *Интернет вещей, защита и безопасность IoT, IoT-устройства, смарт-устройства, IoT-приложения.*

ABSTRACT

This article presents the basic steps to secure the Internet of Things. Shows 5 basic rules for safe use of smart devices and protecting the Internet of Things. Each step covers the basic technical aspects of connecting devices: defining data privacy settings, checking for firmware updates, downloading security solutions and protection for smart devices.

Keywords: *Internet of things, IoT protection and security, IoT devices, smart devices, IoT applications.*

ANNOTATSIYA

Ushbu maqola Internet ashyolar xavfsizligini ta'minlash bo'yicha asosiy qadamlarni taqdim etadi. Smart qurilmalardan xavfsiz foydalanish va internet ashyolarini himoya qilishning 5 ta asosiy qoidalarini ko'rsatadi. Har bir qadam qurilmalarni ulashning asosiy texnik jihatlarini qamrab oladi: ma'lumotlar maxfiyligi sozlamalarini aniqlash, proshivka yangilanishlarini tekshirish, xavfsizlik yechimlarini yuklab olish va aqlli qurilmalar uchun himoya.

Kalit so'zlar: *Internet ashyolari, IoT himoyasi va xavfsizligi, IoT qurilmalari, aqlli qurilmalar, IoT ilovalari.*

ВВЕДЕНИЕ

Устройства Интернета вещей (IoT) стали неотъемлемой частью жизни каждого, упрощая выполнение повседневных дел. Использование голосового помощника помогает записать заметку или поставить напоминание о встрече, подключение смартфона к камерам видеонаблюдения и смарт-звонкам обеспечивает удобное управление системой дома, а смарт-телевизоры позволяют насладиться просмотром любимых фильмов [1]. С ростом популярности смарт-устройств увеличивается интерес к ним со стороны киберпреступников, которые постоянно ищут новые способы атак пользователей. Примеры устройств интернета вещей включают умные мобильные телефоны, умные холодильники, умные часы, фитнес-трекеры, умные пожарные сигнализации, умные дверные замки, умные велосипеды, медицинские датчики, умные системы безопасности, а также виртуальные помощники, такие как Alexa и Google Home.

ЛИТЕРАТУРА И МЕТОДОЛОГИЯ

Широкое распространение этих устройств приводит к тому, что в случае взлома одного из них компания-производитель не сможет оперативно отозвать все устройства и обновить систему защиты. Кроме того, хакеры могут через одно устройство проникнуть во всю сеть. Один девайс предоставит

несанкционированный доступ к широкому спектру конфиденциальных данных - от банковских реквизитов до медицинских записей, и даже к важным корпоративным сведениям, учитывая, что многие люди используют одни и те же устройства дома и на работе. Ключевая особенность «интернета вещей» - связанность. Концепция IoT основана на принципе M2M. Это означает, что электронные устройства могут «общаться» друг с другом без посредничества человека. IoT - это автоматизация наивысшего уровня. В IoT для обмена информацией через интернет используются TCP/IP-протоколы. Интернет вещей усиливает проблему конфиденциальности и безопасности данных, полученных от устройств, подключенных к интернету. Последствия хакерских атак могут быть необратимыми [2].

Представим 5 основных правил безопасного пользования смарт-устройствами и защиты Интернета вещей. **1. Защищайте Wi-Fi роутер.** Для безопасности Интернет-соединения следует обеспечить надежную защиту роутера, который является основным устройством Интернета вещей. Большинство пользователей после установки роутера оставляют настройки по умолчанию, что является достаточно распространенной ошибкой. Это может представлять большую угрозу безопасности ваших подключенных устройств. Поэтому следует немедленно сменить пароли для подключения к роутеру и для доступа к его настройкам. При смене пароля выберите вариант WPA2 (или WPA 3 на более новых роутерах). Кроме этого, не забывайте обновлять встроенное программное обеспечение до последней версии, хотя многие из роутеров делают это автоматически, однако время от времени следует проверять актуальность версий. **2. Шифруйте веб-трафик.** Еще одним способом повышения безопасности онлайн и защиты Интернета вещей является шифрование веб-трафика. Самый простой метод - создать виртуальную частную сеть (VPN), которая будет работать как зашифрованный туннель для вашего веб-трафика. Это позволит не только защитить ваши данные от посторонних лиц, но и в случае необходимости - получить доступ к ним из любой точки мира. Также вы можете настроить отдельную сеть для всех

подключенных девайсов, чтобы снизить риски заражения. **3. Позаботьтесь о безопасности смартфона.** Теперь мобильные устройства обладают функционалом компьютеров и используются не только для звонков, но и для фотосъемки, хранения файлов, получения и отправки электронной почты. Большинство этих задач предусматривает доступ к личным данным и подключение к Интернету, ваш смартфон должен быть надежно защищен. Для большинства смартфонов доступны решения по безопасности, которые помогают предотвратить проникновение угроз на устройство. Для дополнительной защиты также следует зашифровать все конфиденциальные данные на смартфоне. В случае получения доступа к устройству киберпреступники не смогут прочитать ваши личные данные [3]. **4. Обновляйте устройства**. Регулярное обновление устройств - базовое правило кибербезопасности. Любые исправления безопасности и обновления следует применять сразу после их выхода, своевременно не исправив определенную уязвимость, вы рискуете стать жертвой атак киберпреступников. Поэтому обращайте внимание на запросы обновлений и своевременно устанавливайте доступные исправления. **5. Защищайте смарт-телевизор.** Сегодня трудно найти телевизор, который не обладает смарт-функциями. Соответственно такие устройства тоже могут быть скомпрометированы киберпреступниками. В частности, злоумышленники могут использовать уязвимости для удаленного управления телевизором или инфицировать устройство вредоносным программным обеспечением [4].

РЕЗУЛЬТАТЫ

Чтобы защитить смарт-телевизор, сначала следует правильно настроить его. Прежде всего необходимо определить параметры конфиденциальности для данных, которые может собирать ваш провайдер, а также включить функцию родительского контроля для защиты детей от нежелательного контента. Кроме этого, важно проверить наличие обновлений

встроенного программного обеспечения, и конечно загрузить решение по безопасности для защиты смарт-телевизора [5].

ОБСУЖДЕНИЕ

Поскольку количество девайсов, подключенных к сети, постоянно растет, а их функциональные возможности совершенствуются, каждый пользователь должен позаботиться о защите Интернета вещей от потенциальных киберугроз. Ведущие технологические компании до сих пор не приложили достаточно усилий по разработке решений для обеспечения безопасности IoT-приложений. Если за эту важнейшую задачу не возьмутся гиганты индустрии, то обязанности лягут на плечи множества стартап-компаний, которые в значительной степени обеспечивают нынешний рост сектора IoT. К 2025 году более половины продуктов IoT будут производиться небольшими компаниями, существующими менее трех лет. Можно представить, что лишь часть этих компаний будет в силах обеспечить нормальный уровень безопасности своих изделий [6].

ЗАКЛЮЧЕНИЕ

Что необходимо для обеспечения действительно прочной защиты устройств IoT. Во-первых, необходимо поощрять производителей активнее сотрудничать с поставщиками ПО, аппаратного обеспечения и в целом с экосистемой отрасли. Старшие партнеры могут стать для новичков рынка ценным источником опыта и знаний по применению существующих стандартов и элементов безопасности. Во-вторых, нужно развивать образование. В пример можно привести создание лабораторий безопасности на базе Microsoft, Breed Reply и Indiegogo [7]. В этих лабораториях даже небольшие разработчики могут получить доступ к передовому оборудованию и сделать свой вклад в развитие систем безопасности. Работающие в этих лабораториях узнают, что вопросы безопасности должны быть первоочередными на всех этапах IoT-проекта - от идеи до серийного выпуска и даже после и во время эксплуатации. В нашем

мире все больше предметов можно подключить к интернету, а значит, все больше предметов становятся потенциально подвержены взлому. Возможно, мы никогда не решим эту фундаментальную проблему, но, объединив усилия, мы можем создать безопасный интернет вещей, которого заслуживает мир.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Мурадова, А.А. (2023). Надежность и безопасность интернет вещей, *Multidisciplinary Scientific Journal SCHOLAR*, Vol.1,27, 109-117.

2. Мурадова, А.А. (2023). Вызовы и будущие тенденции надежного интернет вещей. *Multidisciplinary Scientific Journal SCHOLAR*, Vol.1,29, 55–65.

3. Peterson, G., Shenoi, S., & Alabdulsalam, S. (2018). Internet of Things Forensics - Challenges and a Case Study. *Advances in Digital Forensics XIV,* 35-48.

4. Тягай, Е. Д. (2017). Интернет вещей и охрана интеллектуальной собственности в бизнесе: новые вызовы времени. *Журнал Суда по интеллектуальным правам*, № 15, 57-64.

5. Черняк, Л. (2012). Платформа Интернета вещей. *Открытые системы. СУБД*, № 7, 44.

6. Бурыкин, А. (2020). Кибер-физические системы. Жизнь после пандемии. *Сноб*., 13 мая.

7. Sicari, S. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, Vol. 76, 146-164.