УДК 004

Золотова Евгения Георгиевна, ФГБОУ ВО «Уфимский государственный нефтяной технический университет», студент, zolotova.evgeniya2003@mail.ru

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ ЗАЩИЩЕННОСТИ WI-FI СЕТЕЙ

Аннотация. В статье рассматриваются актуальные угрозы безопасности беспроводных сетей Wi-Fi, анализируются уязвимости протоколов WPA2 и WPA3, а также предлагаются рекомендации по повышению защищенности. На основе анализа данных за 2020–2023 гг. выявлены ключевые риски, включая атаки типа KRACK, перехват данных через публичные точки доступа и уязвимости в IoT-устройствах. Особое внимание уделено российскому контексту: нормативно-правовым аспектам и отечественным разработкам в области защиты беспроводных сетей. Результаты исследования подчеркивают необходимость комплексного подхода, сочетающего технологические решения и обучение пользователей.

Ключевые слова: Wi-Fi, кибербезопасность, WPA3, KRACK, IoT, аутентификация.

Abstract. The article examines current threats to the security of wireless Wi-Fi networks, analyzes the vulnerabilities of the WPA2 and WPA3 protocols, and offers recommendations for improving security. Based on the analysis of data for 2020–2023, key risks were identified, including KRACK-type attacks, data interception through public access points, and vulnerabilities in IoT devices. Particular attention is paid to the Russian context: regulatory aspects and domestic developments in the field of wireless network security. The results of the study emphasize the need for an integrated approach combining technological solutions and user training.

Keywords: Wi-Fi, cybersecurity, WPA3, KRACK, IoT, authentication.

С распространением беспроводных технологий и увеличением количества мобильных устройств возрастает значимость вопросов безопасности Wi-Fi сетей. Практически каждая сфера деятельности, от домашнего использования до крупных корпоративных сетей, требует надёжной защиты информации, передаваемой по беспроводным каналам.

Wi-Fi представляет собой беспроводную локальную сеть, использующую радиоволны для передачи данных и предоставления доступа в Интернет [1].

Далее в статье рассмотрим угрозы безопасности Wi-Fi.

Несанкционированный доступ к сети открывает возможность для перехвата сетевого трафика, что приводит к компрометации конфиденциальности и нарушению целостности данных. Злоумышленник также может злоупотреблять сетевыми ресурсами, потребляя пропускную способность и снижая общую производительность сети [2].

DDoS-атака, или распределенный отказ в обслуживании, представляет собой попытку вывести из строя целевую систему (сервер, сервис, сеть) путём перегрузки её трафиком, генерируемым множеством источников. В отличие от обычной DoS-атаки, трафик поступает не из одного, а из множества мест, что значительно усложняет защиту. Для организации DDoS-атак часто используются ботнеты – сети скомпрометированных устройств, управляемых злоумышленником. Эти устройства, зараженные вредоносным ПО, по команде начинают отправлять запросы на целевой ресурс, приводя к его перегрузке и отказу в обслуживании [3].

Man-in-the-Middle (MITM) — атака «человек посередине», вид кибератаки позволяет злоумышленнику перехватывать и, возможно, изменять данные, передаваемые между двумя сторонами. Он может пассивно собирать информацию или активно вмешиваться в процесс обмена, что может привести к краже данных, изменению сообщений или даже полному захвату контроля над соединением [4].

Перехват сеанса — это тип атаки, при которой злоумышленник захватывает управление сеансом пользователя. Этот вид атаки также называют перехватом файлов cookie или перехватом TCP. Он может произойти, когда человек делает выбор товара в интернет-магазине или проверяет свой банковский баланс. Чаще всего злоумышленники нацеливаются на сеансы браузеров и веб-приложений, чтобы получить доступ к личным данным и паролям [5].

Key Reinstallation Attack (KRACK) [6] — это атака на протокол безопасности WPA2, используемый в Wi-Fi сетях. Она позволяет злоумышленнику перехватывать и расшифровывать данные, передаваемые между устройством и точкой доступа, без необходимости взламывать пароль сети. Атака основана на уязвимости в 4-этапном рукопожатии WPA2, которое выполняется при подключении устройства к Wi-Fi.

Принцип работы KRACK заключается в том, что злоумышленник может перехватить и повторно использовать сообщения при установлении защищенного соединения между устройством и маршрутизатором. В ходе аутентификации используется 4-этапный процесс, в котором происходит обмен ключами. При правильном использовании этих ключей атакующий может заставить устройство повторно установить сессионный ключ, тем самым получая доступ к зашифрованным данным, отправляемым по сети.

Как защититься от данной атаки?

1. Обновить прошивку роутера и устройства.

2. Использовать WPA3 (новый стандарт, устойчивый к KRACK).

3. Всегда использовать HTTPS/VPN (чтобы злоумышленник не смог прочитать данные).

KRACK показал фундаментальную уязвимость WPA2. Хотя современные устройства уже защищены, важно обновлять ПО и переходить на WPA3 для большей безопасности.

Современное состояние проблемы защищенности Wi-Fi сетей остается актуальным, несмотря на применение различных мер безопасности и технологий. Основные аспекты, влияющие на защищенность Wi-Fi сетей, можно рассмотреть в нескольких направлениях:

1. Социальная инженерия. Применение методов социальной инженерии по-прежнему является распространенной угрозой. Пользователи могут случайно подключаться к фальшивым сетям или вводить пароли на поддельных страницах.

2. Логирование и конфиденциальность. С ростом требований к конфиденциальности пользователей возникают опасения по поводу сбора и хранения данных в сетях Wi-Fi. Уязвимости в системах безопасности могут позволить злоумышленникам перехватывать данные о пользователях.

3. IoT и умные устройства. Увеличение числа подключенных устройств (IoT) также создает риски. Многие из этих устройств не имеют достаточных мер безопасности, что может привести к их использованию в сложных атаках.

4. Необходимость регулярных обновлений. Защищенность Wi-Fi сетей требует регулярного обновления прошивок и программного обеспечения для устранения известных уязвимостей. Но не все пользователи и организации соблюдают эти рекомендации.

5. Образование пользователей. Важным аспектом остается просвещение пользователей о методах защиты, рисках и безопасности. Большинство атак происходит из-за невнимательности или незнания со стороны пользователей.

Защищенность Wi-Fi сетей представляет собой важную проблему в условиях постоянного роста числа киберугроз. Понимание основ угроз и методов защиты позволяет пользователям и организациям принимать осознанные меры для защиты своих данных и систем. В современных

условиях никто не застрахован от атак, однако, следуя рекомендациям по безопасности, можно значительно снизить риск возникновения инцидентов.

С развитием технологий безопасности, в том числе и в области Wi-Fi, необходимо постоянно следить за новыми угрозами и методами защиты, чтобы эффективно противостоять потенциальным атакам.

Литература

1. https://skillbox.ru/media/code/chto-takoe-wifi-obyasnyaem-prostymi-slovami/

1. Канатьев К.Н., Большаков В.Н., Куприков О.Д., Горошков Д.Б., Баулин Е.И. "Анализ угроз безопасности беспроводной сети и разработка оптимальных методов их предупреждения" Инновации и инвестиции. 2022. №3. С. 116-123.

2. DDoS-атака [Электронный ресурс] – Режим доступа: https://encyclopedia.kaspersky.ru/glossary/ddos-distributed-denial-of-service-attack/ (дата обращения 01.04.2025)

3. Man-in-the-Middle: советы по обнаружению и предотвращению [Электронный ресурс] – Режим доступа: https://habr.com/ru/companies/varonis/articles/526632/ (дата обращения 11.04.2025)

4. Попукайло В.С., Бугаенко Е.А. Анализ угроз и источников возникновения сетевых уязвимостей // Актуальные проблемы науки и образования в условиях современных вызовов. 2023. С. 73-78.

5. Что такое KRACK? [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/krack (дата обращения 15.09.2024)