УДК: 004.35

WI-FI – ДОМАШНИЙ И ОБЩЕСТВЕННЫЙ ДОСТУП. ОСОБЕННОСТИ И ОПАСНОСТИ.

Четыркин Е.А., студент гр. 21401, IV курс
Научный руководитель: Субаева А.К., д.э.н., доцент
Чистопольский филиал «Восток» Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ
г. Чистополь

Wi-Fi представляет собой стандарт беспроводной передачи данных, который обеспечивает связь между электронными устройствами, такими как ПК, мобильные телефоны и планшеты, посредством использования радиочастотного спектра (ультракоротких радиоволн).

Для создания сети обычно используют роутеры или маршрутизаторы с беспроводными адаптерами. Их главное различие заключается в способе подключения к кабелю интернет-провайдера: роутер — напрямую, маршрутизатор — через модем. Данные устройства оборудованы антенными модулями, предназначенными для передачи радиосигнала. Эти антенны могут быть интегрированы в корпус модема или маршрутизатора, либо представлять собой внешние компоненты. В случае внешних антенн, их ориентация может быть изменена для оптимизации качества связи с подключаемыми устройствами [1].

Повсеместная интеграция беспроводных технологий передачи данных в инфраструктуру городской среды обусловила трансформацию моделей потребления интернет-трафика. Наличие публичных точек доступа в объектах массового скопления людей является стандартом сервиса, обеспечивающим удаленный доступ к информационным ресурсам. Однако экстенсивное расширение поверхности атаки при одновременной низкой осведомленности пользователей о принципах функционирования беспроводных сетей формирует устойчивый вектор роста инцидентов, связанных с утечкой аутентификационных данных и конфиденциальной информации [2].

Следует учитывать, что злоумышленники осведомлены о распространенной практике повторного использования учетных данных пользователями. Следовательно, совпадение имени пользователя и пароля, используемых для доступа к незначительным онлайн-ресурсам (например, форумам), с учетными данными для критически важных систем (банковские приложения, корпоративные сети) представляет собой серьезную уязвимость. Передача таких конфиденциальных данных в незашифрованном виде открывает возможности для несанкционированного доступа. Большинство

веб-ресурсов, требующих аутентификации, применяют протокол HTTPS для обеспечения безопасности соединений [3].

Проведенный анализ архитектуры беспроводных сетей позволяет выделить ряд принципиальных отличий между домашним и публичным доступом, которые детерминируют специфику моделей угроз для каждого типа сетей (таблица 1).

Таблица 1 – Сравнительный анализ параметров домашних и публичных сетей WI-FI

Параметр сравнения	**Домашняя (частная) сеть**	**Публичная (общественная) сеть**
Контроль среды	Полный контроль со стороны владельца	Отсутствие контроля, недоверенная среда
Тип аутентификации	WPA2-PSK / WPA3-PSK (персональный ключ)	Open (без шифрования) / WPA2-PSK (общий ключ)
Изоляция клиентов	Отсутствует (не требуется)	Отсутствует (критическая уязвимость)
Временной горизонт угрозы	Долговременный (накопление данных)	Кратковременный (сессионный перехват)

Домашняя сеть работает в безопасных условиях, потому что она находится у вас под контролем. К ней подключено ограниченное количество ваших устройств (телефоны, ноутбуки, телевизоры). Основная защита такой сети — это шифрование (кодирование) данных, которые передаются по воздуху. Для них используются специальные протоколы защиты (WPA).

Протокол WPA2 с общим паролем имеет ряд основных проблем. Люди ставят простые пароли. Если пароль слишком короткий или простой (например, «12345678» или «пароль»), злоумышленник может легко его подобрать с помощью специальных программ или угадать. Даже если он просто перехватит момент вашего подключения к сети, он сможет потом на своем компьютере спокойно перебирать варианты пароля, пока не найдет нужный [4].

Уязвимость KRACK - это техническая ошибка в самом протоколе WPA2. Из-за нее хакер, находящийся рядом с вашим домом, может заставить ваш роутер и телефон заново договориться о ключе шифрования и расшифровать ваши данные, даже не зная пароля от вашего Wi-Fi [5].

Также важно помнить, что домашняя сеть работает постоянно. Если хакер один раз получит к ней доступ (например, через слабый пароль), у него будет много времени, чтобы изучить все ваши устройства, узнать, какие данные вы передаете, и перейти от зараженной лампочки к вашему ноутбуку с важными файлами.

Самая большая проблема публичных сетей в том, что любой человек, подключившийся к тому же Wi-Fi, что и вы, технически может попытаться атаковать ваш телефон или ноутбук, потому что вы находитесь в одной «комнате».

Ключевым условием безопасной работы в публичных сетях является принятие модели «нулевого доверия» к внешней среде. Наиболее релевантными угрозами для данного типа доступа выступают:

- атака «человек посередине» (MITM). Хакер встает между вами и точкой доступа;

- фальшивая точка доступа (Злой двойник). Хакер создает свою сеть с таким же названием, как у кафе, например «Cafe_Free_WiFi». Ваш телефон, который помнит это название, может подключиться к сети хакера автоматически;

- перехват трафика (Сниффинг). Если сеть открытая (без пароля), любой человек со специальной программой может видеть, какие данные передаются по воздуху. Особенно легко украсть данные с сайтов, где нет значка замка в адресной строке (не используется протокол HTTPS).

Проведенный анализ позволяет показать различие моделей угроз для частных и публичных беспроводных сетей, что обусловливает необходимость применения специфических защитных механизмов (таблица 2).

Таблица 2 – Дифференцированные рекомендации по обеспечению безопасности

Категория мер	**Для домашних сетей**	**Для публичных сетей**
Аутентификация и шифрование	Использование WPA3, генерация парольных фраз с высокой энтропией	Использование VPN (Virtual Private Network) для шифрования всего трафика на прикладном уровне
Обновление ПО	Регулярное обновление firmware роутера	Обновление ОС и браузера
Сетевые настройки	Сегментация сети (VLAN) для изоляции IoT-устройств	Деактивация функции автоматического подключения к открытым сетям
Пользовательские практики	Мониторинг списка подключенных устройств (DHCP-клиентов)	Принудительное использование HTTPS (расширение HSTS)

Применение дифференцированного подхода к обеспечению безопасности в зависимости от типа доступа позволяет минимизировать риски

компрометации конфиденциальной информации при использовании беспроводных технологий.

Предоставление бесплатного Wi-Fi представляет собой баланс между доступностью для пользователей и потенциальными рисками для безопасности данных. В связи с этим, использование общедоступных точек доступа Wi-Fi следует рассматривать как крайнюю меру. При наличии более безопасных альтернатив, таких как использование мобильного интернета вашего оператора связи или подключение к домашней сети Wi-Fi, предпочтительнее выбрать именно их для выполнения необходимых онлайн-задач.

Таким образом, проведенное исследование демонстрирует принципиальное различие моделей угроз для домашних и публичных сетей Wi-Fi, обусловленное степенью контроля над средой передачи данных, типом аутентификации и временным горизонтом эксплуатации уязвимостей. Если для частных сетей основными рисками являются компрометация парольной фразы и эксплуатация протокольных уязвимостей с возможностью долговременного накопления данных, то в публичных сетях доминируют угрозы, связанные с недоверенной средой: атаки «человек посередине», создание фальшивых точек доступа и перехват незашифрованного трафика. Исходя из этого, для обеспечения безопасности беспроводных технологий необходимо применять разные меры. В домашних условиях следует сосредоточиться на сегментации трафика и внедрении современных протоколов шифрования (WPA3). При работе в публичных сетях же обязательно нужно принять модель "нулевого доверия", использовать VPN и контролировать безопасность на уровне приложений (HTTPS). Игнорирование этих различий и использование единых стратегий защиты значительно повышает риски компрометации конфиденциальных данных пользователей.

Список литературы:

1. Как избежать рисков безопасности в публичных сетях Wi-Fi. [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/preemptive-safety/public-wifi-risks (Дата обращения 16.03.2026)

2. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2023. - 1008 с.

3 ФГУП «ЗащитаИнфоТранс». Центр кибербезопасности ФГУП «ЗащитаИнфоТранс» сообщает: экспериментально подтверждена критическая уязвимость сетей Wi-Fi (KRACK) [Электронный ресурс] // ФГУП «ЗащитаИнфоТранс» : официальный сайт. – 2017. – 20 октября. – URL: https://www.z-it.ru/news/detail/95(Дата обращения 16.03.2026)

4. Гордейчик, С.В. Безопасность беспроводных сетей Wi-Fi / С.В. Гордейчик. - М.: Горячая линия - Телеком, 2020. - 288 с.

5. Что такое Wi-Fi: объясняем простыми словами. [Электронный ресурс] URL: https://skillbox.ru/media/code/chto-takoe-wifi-obyasnyaem-prostymi-slovami/(Дата обращения 16.03.2026)