УДК 004.056

ОЦЕНКА УЯЗВИМОСТЕЙ ПРОТОКОЛОВ ЗАЩИТЫ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ В УСЛОВИЯХ ПЛОТНОЙ ГОРОДСКОЙ ЗАСТРОЙКИ

Клешнев Н.А., Костюков А.В., Ударцев Д.В., студенты гр. ИБт-241, II курс
Научный руководитель: Хакимов П.Е., ассистент
Кузбасский государственный технический университет имени Т.Ф. Горбачева
г.Кемерово

Беспроводные локальные сети стандарта IEEE 802.11 прочно вошли в повседневную жизнь городского населения. Их повсеместное распространение в жилых кварталах, офисных комплексах и общественных пространствах крупных городов порождает среду, в которой десятки и сотни точек доступа работают в непосредственной близости друг от друга. Плотная городская застройка формирует специфические условия распространения радиосигнала — многолучевое отражение от стен зданий, дифракция на углах конструкций, затухание в перекрытиях. Все эти физические явления существенно влияют на реальную картину угроз безопасности беспроводных сетей. Цель настоящей работы — проанализировать уязвимости основных протоколов защиты Wi-Fi (WEP, WPA, WPA2, WPA3) с учётом факторов, характерных именно для плотной городской среды, и оценить практическую реализуемость атак в таких условиях.

Прежде чем переходить к рассмотрению уязвимостей протоколов, необходимо подробно охарактеризовать среду, в которой эти протоколы функционируют. Город с многоэтажной застройкой создаёт целый ряд физических эффектов, напрямую определяющих возможности потенциального злоумышленника.

Многолучевое распространение представляет собой первый значимый фактор. Радиоволны диапазонов 2,4 ГГц и 5 ГГц активно отражаются от бетонных и кирпичных стен, металлических каркасов, стеклянных фасадов. В результате приёмник получает несколько копий одного и того же сигнала с различной задержкой и фазой. Как отмечает Раппапорт [1], такое распространение приводит к замираниям (fading), которые могут как ослаблять, так и усиливать сигнал в конкретных точках пространства. Для атакующего это означает, что даже на значительном расстоянии от точки доступа уровень принимаемого сигнала может оказаться достаточным для перехвата трафика — например, через стену соседнего здания или с улицы.

Второй важный фактор — высокая плотность сетей. По данным сервиса Wigle.net за 2024 год, в центральных районах крупных российских городов при однократном сканировании обнаруживается от 40 до 120 точек доступа в радиусе 50 метров [2]. Подобная насыщенность создаёт значительную интерференцию в перекрывающихся каналах. С одной стороны, это затрудняет ста-

бильный перехват трафика конкретной сети, с другой — предоставляет злоумышленнику обширное поле для выбора целей и увеличивает вероятность обнаружения слабо защищённой точки доступа. Кроме того, пользователи, страдающие от нестабильного соединения, нередко прибегают к упрощению настроек безопасности — используют короткие пароли, отключают дополнительные механизмы защиты.

Третий фактор — физическая близость клиентских устройств к чужим точкам доступа. В многоквартирном доме Wi-Fi-адаптер ноутбука свободно «видит» сети соседей через одну-две стены. Согласно рекомендациям МСЭ [3], затухание сигнала на частоте 2,4 ГГц при прохождении через типовую межкомнатную перегородку из пенобетона составляет порядка 5–8 дБ, через несущую железобетонную стену — от 15 до 25 дБ. При типичной мощности бытового передатчика 20 дБм (100 мВт) сигнал остаётся пригодным для декодирования через 2–3 перегородки. Злоумышленник, находящийся в том же подъезде или соседнем здании, располагает вполне достаточным уровнем сигнала для проведения различных атак.

Протокол WEP был определён в первоначальном стандарте IEEE 802.11 в 1997 году. Он использовал потоковый шифр RC4 с ключами длиной 40 или 104 бита, а вектор инициализации (IV) имел длину всего 24 бита и передавался в открытом виде. Малое пространство IV — около 16,7 миллионов значений — приводило к неизбежному повторению ключевых последовательностей при сколько-нибудь интенсивном трафике.

Уже в 2001 году Флурер, Мантин и Шамир описали атаку (FMS-атака), позволяющую восстановить ключ WEP путём статистического анализа захваченных пакетов [4]. Позднее Тьюс, Вайнман и Пышкин предложили усовершенствованный подход (PTW-атака), сокративший число требуемых перехваченных кадров до 40–80 тысяч [5]. На практике с помощью общедоступного набора утилит aircrack-ng ключ WEP восстанавливается за несколько минут при наличии достаточного объёма трафика.

Несмотря на то что WEP давно признан устаревшим и небезопасным, он до сих пор изредка встречается в эксплуатации — как правило, на забытом оборудовании с заводскими настройками. В условиях городской застройки атака на WEP не представляет существенных трудностей: вечерний трафик типичного домохозяйства (потоковое видео, загрузка обновлений) генерирует необходимый объём данных за 10–20 минут, а физическая близость через стену обеспечивает устойчивый приём сигнала.

Протокол WPA, представленный Wi-Fi Alliance в 2003 году, стал промежуточным решением на пути к стандарту IEEE 802.11i. WPA использовал протокол TKIP (Temporal Key Integrity Protocol), который решил проблему повторного использования ключей за счёт механизма попакетного формирования и проверки целостности MIC (Michael). Однако в основе оставался шифр RC4, и в 2009 году Тьюс и Бек продемонстрировали атаку, позволяющую расшифровывать отдельные короткие пакеты и внедрять поддельные кадры в сеть, защищённую TKIP [6].

WPA2, основанный на полноценном стандарте IEEE 802.11i (2004), заменил TKIP на CCMP (Counter Mode with CBC-MAC Protocol), использующий блочный шифр AES-128. Криптографически CCMP считается надёжным — прямых атак на сам шифр не известно. Тем не менее режим WPA2-Personal (PSK) подвержен серьёзной практической уязвимости: атаке по словарю на этапе четырёхстороннего рукопожатия (4-way handshake). Злоумышленник перехватывает обмен кадрами EAPOL между клиентом и точкой доступа, после чего в офлайн-режиме подбирает пароль, сравнивая вычисленные значения MIC с перехваченными [7]. Скорость перебора определяется вычислительными ресурсами: современная видеокарта NVIDIA RTX 4090 обеспечивает около 2,5 миллионов проверок WPA2-PSK в секунду при использовании программы hashcat [8]. Если пароль представляет собой словарное слово, номер телефона или короткую числовую комбинацию, он подбирается за часы или даже минуты.

В 2017 году Ванхоеф и Писсенс опубликовали атаку KRACK (Key Reinstallation Attacks), которая эксплуатировала недостаток в реализации четырёхстороннего рукопожатия: принудительная повторная установка уже использованного ключа позволяла обнулить счётчик nonce и повторно использовать ключевой поток [9]. Атака затрагивала практически все существовавшие реализации WPA2 и требовала присутствия злоумышленника в зоне радиодоступности жертвы. В плотной городской застройке это условие выполняется почти тривиально — достаточно находиться в соседней квартире или на лестничной клетке. После публикации атаки большинство производителей выпустили исправления, однако значительная часть бытовых маршрутизаторов не получает обновлений и остаётся уязвимой.

Для перехвата рукопожатия злоумышленник может форсировать переподключение клиента, отправив деаутентификационный кадр (deauth-атака). Защитный механизм IEEE 802.11w (Management Frame Protection) противодействует такой атаке, но он включён по умолчанию только в WPA3, а в настройках WPA2 активируется редко.

Стандарт WPA3, анонсированный Wi-Fi Alliance в 2018 году, призван устранить основные слабости предшественника. В режиме WPA3-Personal применяется протокол SAE (Simultaneous Authentication of Equals), основанный на обмене Dragonfly — протоколе класса PAKE (Password-Authenticated Key Exchange). SAE обеспечивает свойство прямой секретности (forward secrecy): даже если пароль впоследствии станет известен злоумышленнику, ранее перехваченный трафик не может быть расшифрован. Помимо этого, SAE устойчив к офлайн-атакам по словарю, так как каждая попытка проверки пароля требует интерактивного взаимодействия с точкой доступа [10].

Тем не менее WPA3 не лишён уязвимостей. В 2019 году Ванхоеф и Ронен описали группу атак Dragonblood, включающую побочный канал по времени отклика и атаку понижения протокола (downgrade), при которой злоумышленник вынуждает клиентское устройство переключиться на WPA2 [11]. В условиях городской застройки атака понижения реализуется путём со-

здания поддельной точки доступа (evil twin) с тем же SSID, но объявляющей поддержку только WPA2. Клиентское устройство, потеряв связь с легитимной точкой из-за кратковременного затухания сигнала, может автоматически подключиться к поддельной — после чего к нему становятся применимы все атаки на WPA2.

Распространённость WPA3 пока остаётся невысокой. Большинство бытовых точек доступа, поддерживающих WPA3, работают в переходном режиме WPA3/WPA2 transition mode, что сохраняет возможность атаки понижения. Полноценная миграция на WPA3-only затруднена наличием устаревших клиентских устройств, не поддерживающих новый протокол.

Анализ, проведённый в предыдущих разделах, показывает, что плотная городская застройка существенно снижает барьер для проведения атак на беспроводные сети. Физическая близость к целевой точке доступа — ключевое требование для большинства атак — обеспечивается самой архитектурой многоквартирных домов и офисных зданий.

Отдельного внимания заслуживает атака Evil Twin, которая эффективна вне зависимости от используемого протокола шифрования. Злоумышленник создаёт точку доступа с идентичным SSID и, как правило, более мощным сигналом, подавляя легитимную точку деаутентификационными кадрами. В городской среде, где пользователь привык видеть множество окружающих сетей и нередко подключается к открытым точкам в кафе и торговых центрах, порог бдительности заметно снижен. По данным «Лаборатории Касперского» за 2023 год, около 28% пользователей в российских городах хотя бы раз подключались к неизвестной открытой Wi-Fi-сети .

Физические условия плотной застройки позволяют разместить поддельную точку доступа в соседнем помещении, на лестничной клетке, в подвале здания или даже в припаркованном автомобиле рядом с окнами целевого объекта. Мощность сигнала атакующего при этом может оказаться сопоставимой или превышающей мощность легитимной точки доступа, что существенно повышает вероятность автоматического подключения клиентских устройств.

Наибольшую практическую угрозу в городских условиях, таким образом, представляют два типа атак: атака по словарю на WPA2-PSK (ввиду массовой распространённости этого протокола и частого использования слабых паролей) и атака Evil Twin (ввиду физической доступности и низкого порога бдительности пользователей).

На основании проведённого анализа сформулированы следующие рекомендации для пользователей и администраторов беспроводных сетей, эксплуатируемых в условиях плотной городской застройки:

Полный отказ от использования протоколов WEP и WPA (TKIP). Оборудование, не поддерживающее хотя бы WPA2-AES, подлежит обязательной замене на современные модели.

Установка паролей WPA2/WPA3 длиной не менее 16 символов, включающих буквы верхнего и нижнего регистра, цифры и специальные знаки.

Категорически не рекомендуется использовать в качестве паролей номера телефонов, даты рождения, словарные слова и их транслитерацию.

Активация механизма IEEE 802.11w (Protected Management Frames) на оборудовании, поддерживающем данную функцию, для противодействия деаутентификационным атакам.

Переход на WPA3 при обновлении оборудования. Желательно использовать режим WPA3-only, если все клиентские устройства поддерживают новый протокол, избегая переходного режима WPA3/WPA2.

Снижение мощности передатчика до минимально достаточного уровня. В условиях квартиры многоэтажного дома мощность 10–14 дБм обычно обеспечивает устойчивое покрытие внутри помещения, но существенно сужает зону приёма за его пределами, уменьшая поверхность атаки.

Применение WPA2/WPA3-Enterprise с RADIUS-сервером в корпоративных сетях, расположенных в офисных зданиях с высокой концентрацией соседних беспроводных сетей.

Отключение автоматического подключения к ранее известным SSID на клиентских устройствах и обязательное использование VPN при работе в публичных беспроводных сетях.

Условия плотной городской застройки формируют специфическую и во многом благоприятную для злоумышленника среду функционирования беспроводных локальных сетей. Физическая близость множества точек доступа и клиентских устройств, многолучевое распространение сигнала и его проникновение через строительные перегородки существенно упрощают перехват трафика и проведение атак различного типа. Протоколы WEP и WPA (TKIP) полностью скомпрометированы и не должны использоваться ни при каких обстоятельствах. WPA2-PSK остаётся доминирующим протоколом в бытовых сетях, однако его безопасность критически зависит от длины и сложности используемого пароля. WPA3 устраняет ряд фундаментальных слабостей предшественника, но пока распространён незначительно и уязвим к атаке понижения в переходном режиме. Только комплексный подход, сочетающий грамотный выбор протокола, надёжный пароль, ограничение мощности сигнала и повышение осведомлённости пользователей, позволяет добиться приемлемого уровня защищённости беспроводных сетей в условиях плотной городской среды.

Список литературы:

1. Отчёт «Лаборатории Касперского» о безопасности публичных Wi-Fi-сетей в России // Kaspersky Daily. — URL: https://www.kaspersky.ru/blog/moscow-wifi-insecure/12975/ (дата обращения: 04.03.2026).

2. Rappaport T. S. Wireless Communications: Principles and Practice / T. S. Rappaport. — 2nd ed. — Upper Saddle River : Prentice Hall, 2002. — 707 p. — URL: https://telkom2013.wordpress.com/wp-content/uploads/2014/02/wireless-comm-princip-n-practice-theodoresrappaport.pdf (дата обращения: 04.03.2026).

3. WiGLE.net — Wireless Network Mapping // WiGLE. — URL: https://wigle.net/ (дата обращения: 04.03.2026).

4. ITU-R P.2040-3. Effects of building materials and structures on radio-wave propagation above about 100 MHz. — Geneva : ITU, 2023. — 32 p. — URL: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.2040-3-202308-S!!PDF-E.pdf (дата обращения: 04.03.2026).

5. Fluhrer S. R., Mantin I., Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4 // Selected Areas in Cryptography. — Springer, 2001. — P. 1–24. — URL: https://link.springer.com/chapter/10.1007/3-540-45537-X_1 (дата обращения: 04.03.2026).

6. Tews E., Weinmann R.-P., Pyshkin A. Breaking 104 bit WEP in less than 60 seconds // Information Security Applications. — Springer, 2007. — P. 188–202. — URL: https://eprint.iacr.org/2007/120.pdf (дата обращения: 04.03.2026).

7. Тип шифрования Wi-Fi — какой выбрать: WEP, WPA2-PSK, WPA3 Personal-Enterprise для защиты безопасности сети. — URL: https://wifika.ru/tip-shifrovaniya-wifi-wpa2-psk.html (дата обращения: 04.03.2026).

8. Неожиданная мощь GeForce RTX 4090. Восемь таких видеокарт могут подобрать пароль из восьми символов методом перебора всех комбинаций всего лишь за 48 минут // iXBT. — URL: https://www.ixbt.com/news/2022/10/18/geforce-rtx-4090-48.html (дата обращения: 04.03.2026).

9. WPA3 – крупнейшее обновление безопасности Wi-Fi за последние 14 лет. — URL: https://nag.ru/material/33569 (дата обращения: 04.03.2026).

10. WPA3 – новый уровень безопасности Wi-Fi 802.11. — URL: https://www.atraining.ru/wpa3-802-11-2018/ (дата обращения: 04.03.2026).

11. Уязвимость Dragonblood // Хакер. — URL: https://xakep.ru/2019/04/12/dragonblood/ (дата обращения: 04.03.2026).