

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ГИМНАЗИЯ №16 ГОРОДА ТЮМЕНИ

РАЗРАБОТКА ПРАКТИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ДАННЫХ ОТ
УГРОЗЫ “EVIL TWIN” В ПУБЛИЧНЫХ WI-FI СЕТЯХ

Научный руководитель:
Мышко Юлия Юрьевна
Учитель информатики МАОУ Гимназии №16

Работу выполнил:
учащийся 10 Ж класса
Голубев Савелий Александрович

ТЮМЕНЬ, 2026

Краткая аннотация

В проекте проведён теоретический и практический анализ атаки «Evil Twin» на публичные Wi-Fi сети. В ходе эксперимента в изолированной среде (Kali Linux, airgeddon) смоделированы все этапы атаки, включая создание ложной точки доступа и перехват данных. На основе полученных результатов разработаны практические рекомендации для пользователей, направленные на защиту персональных данных: использование VPN, отключение автоматического подключения к сетям, применение двухфакторной аутентификации и контроль HTTPS. Работа ориентирована на повышение цифровой грамотности и формирование безопасных поведенческих привычек.

Аннотация

Работа посвящена исследованию угрозы безопасности персональных данных в публичных Wi-Fi сетях, известной как атака «Evil Twin» («злой двойник»). Целью проекта является комплексный анализ механизма атаки, её практическое моделирование в изолированной лабораторной среде и разработка на основе полученных результатов доступных рекомендаций для пользователей. В теоретической части рассмотрены архитектура и уязвимости открытых беспроводных сетей, детально разобран поэтапный сценарий атаки, а также проведён сравнительный анализ с другими типами угроз. В экспериментальной части с использованием виртуальной среды Kali Linux и фреймворка airgeddon успешно воспроизведены все этапы атаки: от развёртывания поддельной точки доступа до перехвата учётных данных через фишинговый портал. На основе проведённого анализа сформулирован комплекс практических правил безопасности, включающий приоритетное использование VPN, контроль автоматического подключения к сетям, применение двухфакторной аутентификации и другие меры. Работа имеет ярко выраженную практическую направленность и может служить основой для повышения цифровой грамотности широкого круга пользователей.

Оглавление

ВВЕДЕНИЕ.....	5
ГЛАВА 1. ТЕОРЕТИЧЕСКИЙ АНАЛИЗ УГРОЗЫ “EVIL TWIN”.....	6
1.1. Архитектура и уязвимости публичных беспроводных сетей	6
1.2. Механизм и поэтапный разбор атаки “Evil Twin”	6
1.3. Потенциальный ущерб, последствия и реальные кейсы	7
1.4. Сравнительный анализ с другими атаками на беспроводные сети	8
1.5. Правовые и этические аспекты исследования уязвимостей	8
ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНОЕ МОДЕЛИРОВАНИЕ УГРОЗЫ В КОНТРОЛИРУЕМОЙ СРЕДЕ	10
2.1. Проектирование и организация изолированной лабораторной среды.....	10
2.2. Методика проведения эксперимента и обзор инструментария	10
2.3. Подробный отчёт о практической демонстрации	10
2.4. Анализ проблем и решений при настройке лабораторного стенда	11
2.5. Детальный разбор работы фишингового портала (Captive Portal)	11
2.6. Расширенный сценарий: моделирование атаки на сеть с общим паролем.....	12
ГЛАВА 3. РАЗРАБОТКА КОМПЛЕКСА РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	13
3.1. Системный анализ результатов и выявление ключевых контрмер	13
3.2. Разработка и обоснование практических правил безопасности для пользователя	13
3.3. Технические средства детектирования атаки "Evil Twin" для продвинутых пользователей..	14
3.4. Сравнительный анализ решений для защиты: VPN, Tor, собственный хот-спот	14
3.5. Роль производителей устройств и провайдеров публичного Wi-Fi в защите	15
Заключение	16
Список использованных источников	17
Приложение А	18
Приложение Б.....	22

ВВЕДЕНИЕ

В современной цифровой реальности публичные сети Wi-Fi превратились в стандартный элемент инфраструктуры. Их основное преимущество - доступность - одновременно является главным источником риска. Данные, передаваемые через такие сети, зачастую не защищены достаточным шифрованием, что делает их лёгкой мишенью для злоумышленников. Одной из наиболее распространённых атак является «Evil Twin» («Злой двойник»). Простота её реализации контрастирует с высоким потенциалом ущерба, что делает детальный анализ этой угрозы крайне важным для формирования цифровой грамотности.

Цель проекта: провести комплексный анализ угрозы «Evil Twin», смоделировав её в контролируемой среде, и на основе полученных результатов разработать практические рекомендации по защите персональных данных для рядовых пользователей.

Задачи проекта:

1. Изучить теоретические основы работы публичных Wi-Fi сетей, их уязвимости и детально разобрать механизм атаки «Evil Twin».
2. Организовать безопасную, изолированную от реальных сетей среду для легального моделирования кибератаки.
3. Провести практическую демонстрацию всех этапов атаки с использованием специализированного программного обеспечения (ОС Kali Linux, фреймворк airgeddon).
4. Проанализировать успешность демонстрации, выявив ключевые ошибки пользователей, делающие атаку возможной.
5. Систематизировать и оформить выводы в виде понятных, практико-ориентированных рекомендаций и наглядной памятки.

Объект исследования: безопасность персональных данных в открытых беспроводных сетях.

Предмет исследования: технология и методы реализации атаки «Evil Twin», а также эффективные способы противодействия ей.

Гипотеза исследования: Можно предположить, что наглядная демонстрация реализации атаки «Evil Twin» в контролируемых условиях позволит не только детально проанализировать её механизм, но и выработать наиболее эффективные и понятные пользователям рекомендации по защите, тем самым повысив уровень цифровой грамотности.

Анализ существующих исследований: Проблема уязвимости публичных Wi-Fi сетей активно исследуется в области кибербезопасности. Так, в работах специалистов (например, в статьях М. Дж. Райана, посвящённых беспроводным атакам, и в исследованиях российских экспертов из «Роскачества») «Evil Twin» выделяется как одна из наиболее распространённых социально-инженерных атак благодаря простоте исполнения. Данный проект опирается на эти исследования, смещая фокус с теоретического описания на практическое учебное моделирование и создание профилактических материалов.

Методы и методика исследования: В работе применялись следующие методы: 1) теоретический анализ научной литературы и специализированных источников; 2) моделирование – воссоздание атаки в изолированной виртуальной среде (ОС Kali Linux, VirtualBox); 3) практический эксперимент с использованием инструментария тестирования на проникновение (фреймворк airgeddon); 4) анализ и синтез полученных данных для формулирования выводов и рекомендаций.

Практическая значимость работы заключается в создании наглядного образовательного материала, который позволяет понять серьёзность угрозы. Ключевым практическим результатом является комплект рекомендаций и памятка, позволяющие даже неискущённому в кибербезопасности человеку существенно повысить уровень своей защиты в публичных сетях.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЙ АНАЛИЗ УГРОЗЫ “EVIL TWIN”

1.1. Архитектура и уязвимости публичных беспроводных сетей

Публичные сети Wi-Fi основаны на семействе стандартов IEEE 802.11. В отличие от домашних сетей, где обычно используется защищённый доступ WPA2/WPA3 с уникальным паролем, публичные хот-споты применяют упрощённые модели. Чаще всего встречаются:

Открытые сети (Open Networks): Не используют шифрования на уровне соединения (Data Link Layer). Весь трафик передаётся в эфир в открытом виде.

Сети с общей аутентификацией (Captive Portal): После подключения к открытой сети пользователь перенаправляется на веб-страницу (портал), где необходимо принять условия или ввести код. Однако трафик до аутентификации и, что критично, трафик многих других пользователей после неё часто остаётся незашифрованным.

Сети с общим паролем (WPA2-Personal): Пароль известен всем посетителям заведения, что сводит на нет его криптографическую ценность. Злоумышленник, получив пароль, может не только подключиться, но и проводить более сложные атаки на других клиентов сети.

Ключевая уязвимость заключается в самой природе радиоканала: данные, передаваемые по воздуху, могут быть приняты любым устройством в радиусе действия. Без сквозного шифрования (end-to-end encryption), которое обеспечивают HTTPS или VPN, пакеты данных легко перехватываются. Более того, в публичных сетях редко используется изоляция клиентов (Client Isolation), что в теории позволяет подключённым устройствам взаимодействовать друг с другом, создавая дополнительный вектор для атаки.

1.2. Механизм и поэтапный разбор атаки “Evil Twin”

Атака «Evil Twin» («Злой двойник») является классической разновидностью атаки «человек посередине» (Man-in-the-Middle, MitM), адаптированной для беспроводных сред. Её успех основан на двух факторах: технической возможности создания точки доступа и психологии пользователя. Рассмотрим этапы детально:

1. Этап разведки (Reconnaissance). Злоумышленник использует беспроводной адаптер, поддерживающий «режим монитора» (monitor mode), и программное обеспечение для sniffинга (например, `airodump-ng` из комплекта Aircrack-ng). Цель - просканировать радиоэфир и составить список доступных сетей (их SSID - Service Set Identifier), каналов вещания и мощности сигнала. Особый интерес представляют популярные SSID: `Free\_McCafe\_WiFi`, `MTS\_FREE`, `Airport\_Free`.

2. Этап развёртывания двойника (Evil Twin Deployment). Используя тот же или другой адаптер в режиме точки доступа (master mode), атакующий создаёт новую беспроводную сеть. Её SSID и параметры безопасности (открытая или с известным паролем) в точности копируют легитимную цель. Часто мощность сигнала поддельной точки искусственно усиливается, чтобы она выглядела более «привлекательной» для устройств, которые автоматически подключаются к сети с самым сильным сигналом из известных.

3. Этап принудительного переподключения (Deauthentication Attack). Чтобы «переманить» клиентов с легитимной точки доступа на поддельную, злоумышленник отправляет в эфир поддельные управляющие фреймы - деаутентификационные пакеты (deauth packets). Эти пакеты, сфабрикованные с помощью инструментов вроде `aireplay-ng`, маскируются под команды от легитимной точки доступа и принудительно разрывают соединение целевого устройства с ней. Устройство пользователя, потеряв связь, немедленно начинает поиск доступной сети и, найдя «двойника» с мощным сигналом и знакомым именем, автоматически подключается к нему.

4. Этап перехвата и анализа трафика (Traffic Interception & Analysis). После того как жертва подключилась к «злому двойнику», весь её сетевой трафик проходит через компьютер атакующего. Используя инструменты анализа трафика, такие как Wireshark или ettercap, злоумышленник может пассивно «прослушивать» сессию. Если пользователь посещает сайты, использующие незащищённый протокол HTTP, перехвату становятся доступны cookies, данные форм (логины, пароли), история просмотров.

5. Этап активного вмешательства и фишинга (Active Interference & Phishing). Для противодействия шифрованию на транспортном уровне (HTTPS) атакующий может пойти дальше. Он может использовать ARP-спуфинг в рамках своей ложной сети, чтобы перенаправлять трафик жертвы через свои прокси-серверы. Это позволяет:

Снижать уровень безопасности соединения (SSL stripping), переводя HTTPS-запросы в HTTP.

Подменять содержимое сайтов на лету, внедряя вредоносный код.

Наиболее эффективно - развернуть фишинговый портал (Captive Portal), который с высокой точностью имитирует страницу входа в сеть провайдера, почтовый сервис (Gmail, Яндекс) или социальную сеть. Доверчивый пользователь вводит свои учётные данные, которые напрямую сохраняются у атакующего.

1.3. Потенциальный ущерб, последствия и реальные кейсы

Успешная атака «Evil Twin» ведёт к полной компрометации цифровой сессии пользователя. Последствия носят каскадный характер:

Кража учётных данных: Пароли от электронной почты, социальных сетей, мессенджеров, корпоративных систем.

Финансовые потери: Перехват данных банковских карт, доступ к интернет-банкингу, реквизиты электронных кошельков.

Кража личной информации: Конфиденциальная переписка, фото, документы.

Компрометация устройств: Возможность загрузки и установки вредоносного программного обеспечения через подменённые страницы обновлений.

Юридические риски: От лица жертвы могут быть совершены противоправные действия.

Помимо прямого ущерба, атака создаёт долгосрочные риски. Скомпрометированные учётные данные часто проверяются на других сервисах (credential stuffing), что ведёт к взлому нескольких аккаунтов. Перехваченные сессионные куки могут позволить доступ к аккаунтам даже без пароля. В корпоративной среде подключение сотрудника к "Evil Twin" может стать началом цепочки атаки на всю внутреннюю сеть организации.

В 2017 году на конференции по безопасности Black Hat был представлен отчёт, демонстрирующий, как с помощью устройства стоимостью менее \$100 можно автоматически развёртывать «злых двойников» для самых распространённых публичных SSID по всему миру. В России «Роскачество» неоднократно включало эту угрозу в свои рекомендации, подчёркивая её социально-инженерную составляющую: атака рассчитана не на взлом шифра, а на обман человека.

1.4. Сравнительный анализ с другими атаками на беспроводные сети

Для полного понимания специфики "Evil Twin" важно рассмотреть её в контексте других распространённых атак на Wi-Fi сети:

Атака на WPS (Wi-Fi Protected Setup): Эксплуатирует уязвимости в механизме упрощённого подключения. В отличие от "Evil Twin", требует наличия сети, защищённой паролем, и активированной функции WPS. Современные роутеры стали более устойчивы к этой атаке.

Перебор паролей (Brute-force) и атаки по словарю: Нацелены на прямое взламывание ключа шифрования сети. Эффективны только против слабых паролей и требуют значительных вычислительных ресурсов и времени.

Атака с использованием Pixie Dust: Современный метод, эксплуатирующий слабую генерацию случайных чисел в реализации WPS некоторых чипсетов. Как и атака на WPS, применима к ограниченному кругу устройств.

Подслушивание (Eavesdropping) в открытых сетях: Пассивный перехват трафика без создания инфраструктуры атаки. "Evil Twin" является активным развитием этой техники, где атакующий не просто слушает, а перенаправляет трафик через себя, получая гораздо больший контроль.

Ключевое отличие "Evil Twin": Атака не пытается взломать криптографию сети. Она обходит её, создавая новую, незащищённую точку доступа, которую пользователь выбирает сам. Это смещает фокус с технической сложности на манипуляцию пользователем, что делает атаку универсальной и не зависящей от силы шифрования целевой сети.

1.5. Правовые и этические аспекты исследования уязвимостей

Проведение любых активных тестов безопасности, даже в исследовательских целях, регулируется законодательством. В России статьи 272 ("Неправомерный доступ к компьютерной информации") и 273 ("Создание, использование и распространение вредоносных компьютерных программ") Уголовного кодекса РФ могут быть применены к действиям, нарушающим работу сетей и конфиденциальность данных без согласия владельца.

Методология этичного тестирования (Ethical Hacking), применённая в данном проекте, основана на следующих принципах:

1. Явное разрешение: Все действия проводятся только в отношении инфраструктуры, принадлежащей исследователю или на которую получено письменное разрешение.

2. Полная изоляция: Использование виртуальных сред и режимов сети (NAT, Внутренняя сеть), исключающих воздействие на сторонние системы.

3. Образовательная цель: Чёткое определение цели деятельности как повышение осведомлённости и разработка защитных мер, а не причинение вреда или извлечение выгоды.

4. Конфиденциальность данных: Недопустимость перехвата, хранения или анализа реальных пользовательских данных даже в изолированной среде. Использование исключительно тестовых наборов.

Данный проект полностью соответствует этим принципам, так как лабораторный стенд физически и логически изолирован от внешних сетей, а все манипуляции проводятся с тестовыми данными на оборудовании, находящемся в собственности исследователя.

Вывод по главе 1: Таким образом, атака «Evil Twin» представляет собой комплексную угрозу, которая искусно сочетает в себе эксплуатацию фундаментальных уязвимостей открытых Wi-Fi сетей (отсутствие шифрования, слабая аутентификация) и манипуляцию поведенческими паттернами пользователя (доверие к знакомым именам

сетей, привычка к автоматическому подключению, невнимательность при вводе данных). Её техническая реализация благодаря доступному программному обеспечению стала тривиальной, что и определяет её широкую распространённость и высокую опасность. Понимание её механизма и отличий от других атак является первым и необходимым шагом для построения эффективной защиты.

ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНОЕ МОДЕЛИРОВАНИЕ УГРОЗЫ В КОНТРОЛИРУЕМОЙ СРЕДЕ

2.1. Проектирование и организация изолированной лабораторной среды

Для легального, этичного и безопасного исследования требовалось создать стенд, полностью исключаящий воздействие на реальные сети и интернет. Была выбрана следующая архитектура:

Хост-система: Персональный компьютер под управлением Windows 10/11.

Средство виртуализации: Oracle VM VirtualBox 7.0 - кроссплатформенное ПО с открытым исходным кодом, позволяющее запускать гостевые операционные системы.

Гостевая ОС для атаки: Kali Linux 2024.1 Rolling Release - дистрибутив на базе Debian, предварительно укомплектованный сотнями инструментов для тестирования на проникновение, включая необходимые для работы с беспроводными сетями.

Критически важная сетевая настройка: Сетевой адаптер виртуальной машины Kali Linux был сконфигурирован в режиме «Внутренняя сеть» (Internal Network). В данном режиме виртуальная машина может общаться только с другими виртуальными машинами, подключёнными к той же внутренней сети, и абсолютно изолирована от физических сетевых интерфейсов хоста (Wi-Fi, Ethernet). Это создаёт чистый «песочничный» полигон.

Роль жертвы: Для наглядности использовался физический смартфон Android. В рамках модели он должен был подключаться к точке доступа, созданной виртуальной машиной.

2.2. Методика проведения эксперимента и обзор инструментария

Методология основывалась на последовательном воспроизведении этапов атаки в рамках изолированной среды. Основным инструментом был выбран фреймворк airgeddon (версия 11.22). Его преимущества для учебного проекта:

Интеграция: Объединяет множество разрозненных утилит (Aircrack-ng, Hostapd, Bettercap, SSLstrip и др.) под единым текстовым меню.

Интерактивность: Пошагово ведёт оператора через все этапы атаки с подсказками.

Автоматизация: Автоматически решает типовые задачи, такие как поиск интерфейсов, проверка зависимостей.

Этапы эксперимента чётко соответствовали теоретической модели из Главы 1, что позволяло напрямую верифицировать теорию практикой.

2.3. Подробный отчёт о практической демонстрации

Ход эксперимента был зафиксирован пошагово с обязательным сохранением скриншотов (см. Приложение А).

1. Подготовка и разведка в airgeddon. После запуска скрипта (`'sudo bash airgeddon.sh'`) из списка был выбран виртуальный беспроводной адаптер (обычно `'wlan0'`). С помощью встроенной функции он был переведён в режим монитора, что позволило захватывать все беспроводные пакеты в эфире. Поскольку среда была изолированной, эфир был пуст. Это ожидаемый результат, подтверждающий чистоту эксперимента.

2. Создание поддельной точки доступа (Fake AP). В главном меню была выбрана опция «Fake Access Point». Система предложила создать новую точку с нуля. В качестве SSID было введено имя `'Free_Public_Lab'`. Для имитации публичной сети шифрование было отключено (режим Open). Была активирована опция «Скрыть мою MAC-адрес» для анонимности в рамках лаборатории.

3. Развёртывание фишингового портала (Captive Portal). На следующем шаге была активирована ключевая функция - «Captive Portal». Из списка шаблонов был выбран

вариант, имитирующий типичную страницу входа в публичную сеть с полями «Имя пользователя» и «Пароль». Airgeddon автоматически настроил веб-сервер (lighttpd) и правила перенаправления трафика (iptables) для перехвата HTTP-запросов.

4. Имитация поведения жертвы. На физическом смартфоне был включен поиск Wi-Fi сетей. В списке появилась созданная сеть 'Free_Public_Lab'. На неё было выполнено ручное подключение (статус: «Подключено, без доступа к Интернету»). Это моделировало момент, когда пользователь решает воспользоваться «бесплатным» Wi-Fi.

5. Фиксация успеха атаки. При попытке открыть любой сайт (например, google.com) в браузере смартфона автоматически произошло перенаправление на локальный IP-адрес виртуальной машины, где была загружена фишинговая страница. В поля были введены тестовые данные: Логин: 'test_user', Пароль: 'Sup3rSecret!'. Менее чем через секунду в окне терминала airgeddon появилось яркое уведомление: «Credentials captured!», а ниже - точная запись перехваченных данных. Эксперимент занял около 15 минут от запуска виртуальной машины до перехвата данных.

Для чистоты эксперимента было важно убедиться, что смартфон не имеет альтернативных путей в интернет. В настройках точки доступа на Kali Linux был явно отключён мост (bridging) с любыми другими сетевыми интерфейсами. После перехвата данных работа скрипта была корректно остановлена через меню airgeddon, что гарантировало отключение точки доступа и сброс всех правил iptables, возвращая виртуальную среду в исходное безопасное состояние.

2.4. Анализ проблем и решений при настройке лабораторного стенда

Развёртывание практической среды сопряжено с техническими вызовами, анализ которых важен для воспроизводимости эксперимента:

Проблема 1: Отсутствие режима монитора у виртуальных адаптеров. Стандартные виртуальные сетевые адаптеры VirtualBox (Intel PRO/1000) не эмулируют беспроводные интерфейсы. Решение: Использование внешнего USB-адаптера с поддержкой мониторного режима (например, на чипсете Ralink RT3070) и его "проброс" в виртуальную машину через функцию USB passthrough. В рамках данного проекта для простоты и гарантии изоляции было принято решение имитировать атаку в чисто виртуальной среде, создавая точку доступа "с нуля", что airgeddon также позволяет.

Проблема 2: Необходимость отключения Network Manager в Kali Linux. Служба управления сетями может конфликтовать с ручным управлением интерфейсами через airgeddon. Решение: Остановка службы командой 'sudo systemctl stop NetworkManager' перед запуском скрипта.

Проблема 3: Проверка зависимостей. Airgeddon автоматически проверяет наличие десятков необходимых утилит (hostapd, dnsmasq, lighttpd и др.). Решение: Запуск скрипта от имени суперпользователя и подтверждение установки всех недостающих пакетов, на что может уйти 5-10 минут.

2.5. Детальный разбор работы фишингового портала (Captive Portal)

Фишинговый портал - ключевой элемент демонстрации, превращающий пассивный перехват в активное получение данных. Его работа в airgeddon обеспечивается связкой нескольких служб:

1. Hostapd: Созёт и управляет самой точкой доступа, задавая её параметры (SSID, канал).

2. Dnsmasq: Выполняет роль DHCP-сервера (выдаёт IP-адреса подключённым клиентам) и DNS-сервера. Именно он перенаправляет все DNS-запросы клиента на IP-адрес виртуальной машины.

3. Lighttpd или Apache: Лёгкий веб-сервер, который обслуживает фишинговую страницу, размещённую в директории '/var/www/html/'.

4. Iptables: Межсетевой экран Linux. Настраивает правила NAT (Network Address Translation), которые перенаправляют весь HTTP-трафик (порт 80) клиента на веб-сервер на 80-м порту виртуальной машины. Это вызывает "перехват" любой попытки открыть сайт.

Логика процесса: Когда жертва пытается открыть `http://google.com`, происходит следующее:

Dnsmasq возвращает ей локальный IP виртуальной машины вместо реального адреса Google.

Браузер жертвы отправляет HTTP-запрос на этот локальный адрес.

Iptables перехватывает этот запрос и перенаправляет его на веб-сервер lighttpd.

Lighttpd отдаёт жертве подготовленную фишинговую страницу.

Введённые данные отправляются формой POST обратно на сервер, где специальный скрипт (часть airgeddon) логирует их и выводит на экран.

2.6. Расширенный сценарий: моделирование атаки на сеть с общим паролем

Для полноты картины был протестирован сценарий, где легитимная сеть имитировалась второй виртуальной машиной (например, с ОС Ubuntu), настроенной как защищённая точка доступа с известным паролем `PublicPassword123`. Цель - показать, что "Evil Twin" работает и в этом случае.

1. На виртуальной машине-роутере была поднята защищённая сеть `'Cafe_Network'` (WPA2).

2. На Kali Linux с помощью airgeddon после этапа разведки был создан "двойник" с идентичным SSID `'Cafe_Network'` и таким же паролем.

3. Была запущена деаутентификация клиента (третья виртуальная машина), который был заранее подключен к легитимной сети.

4. После переподключения клиента к "двойнику" его трафик также был полностью перехвачен. Важный вывод: Знание пароля от публичной сети не защищает от "Evil Twin", а лишь упрощает атакующему задачу по созданию правдоподобной копии.

Вывод по главе 2: Практический эксперимент в контролируемой среде блестяще подтвердил теоретические выкладки. Атака «Evil Twin» была успешно воспроизведена от начала до конца с использованием общедоступных автоматизированных средств. Это доказывает, что для её осуществления не требуется углублённых профессиональных знаний в области сетевой безопасности - достаточно базовых навыков работы в командной строке и следования инструкциям. Ключевым фактором успеха в рамках модели стала имитация доверчивого поведения пользователя, что ещё раз подчёркивает социально-инженерную суть данной угрозы. Работа в режиме «Внутренняя сеть» доказала свою эффективность как абсолютно безопасный и законный метод изучения кибератак. Понимание технических деталей, таких как работа фишингового портала, позволяет глубже осознать механизм угрозы и, следовательно, более эффективно противодействовать ей.

ГЛАВА 3. РАЗРАБОТКА КОМПЛЕКСА РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Системный анализ результатов и выявление ключевых контрмер

Анализ успешной демонстрации позволяет чётко идентифицировать точки приложения защитных мер. Уязвимая цепочка выглядит так: Наличие двойника -> Подключение к нему -> Передача незащищённых данных. Соответственно, стратегия защиты должна быть многоуровневой и разрывать эту цепочку на как можно более ранних этапах.

1. Профилактика подключения (первый и самый важный уровень). Необходимо исключить возможность соединения устройства с поддельной точкой доступа.

2. Защита данных в случае подключения (второй уровень). Если подключение к ложной сети всё же произошло, необходимо сделать перехваченные данные бесполезными для злоумышленника.

3. Минимизация ущерба (третий уровень). Даже если данные были скомпрометированы, нужно ограничить масштаб потенциального ущерба.

3.2. Разработка и обоснование практических правил безопасности для пользователя

На основе проведённого анализа сформулирован следующий комплекс рекомендаций, адресованный рядовому пользователю:

Правило 1. Приоритетное использование VPN (Virtual Private Network). Это наиболее эффективная мера, реализующая второй уровень защиты. Качественный VPN-сервис доставляет весь интернет-трафик пользователя в зашифрованном «туннеле» до своего сервера. Даже подключившись к «Evil Twin», атакующий увидит лишь поток зашифрованных данных между устройством жертвы и сервером VPN, который он не может расшифровать. Рекомендация: Установить и активировать приложение доверенного VPN-провайдера до подключения к любой публичной сети.

Правило 2. Жёсткий контроль подключений к Wi-Fi. Реализует первый уровень защиты.

Отключить функцию «Подключаться к открытым сетям автоматически» в настройках Wi-Fi смартфона и ноутбука.

Вручную удалять из списка сохранённых сетей те, которые больше не используются (например, сети отелей, кафе из других городов).

Перед подключением верифицировать сеть: уточнить точное название (SSID) и пароль у сотрудника заведения. Подозрительны сети с почти идентичными, но не точными именами (например, `Starbucks\_Free\_WiFi` вместо официального `Google Starbucks`).

Правило 3. Осознанное использование интернета в публичных сетях. Совмещает первый и третий уровни.

Без активного VPN избегать любых действий, требующей аутентификации: вход в почту, соцсети, банкинг, совершение покупок.

Для конфиденциальных операций предпочитать мобильный интернет (4G/5G). Сотовые сети обеспечивают встроенное шифрование между устройством и вышкой оператора, что делает их значительно безопаснее публичного Wi-Fi.

Правило 4. Повышение уровня безопасности аккаунтов (третий уровень).

Повсеместно использовать двухфакторную аутентификацию (2FA). Даже если логин и пароль будут перехвачены, злоумышленнику потребуется одноразовый код из SMS или приложения-аутентификатора (Google Authenticator, Microsoft Authenticator), что блокирует доступ.

Использовать менеджер паролей, который создаёт и хранит уникальные сложные пароли для каждого сервиса. Это предотвращает «эффект домино» при компрометации одного пароля.

Правило 5. Технические проверки (вспомогательная мера).

Всегда обращать внимание на протокол HTTPS. В адресной строке браузера должен быть значок замка и префикс `https://`. Однако важно понимать, что на фишинговом сайте, развёрнутом на «Evil Twin», также может стоять валидный HTTPS-сертификат (особенно с бесплатными сертификатами Let's Encrypt). Поэтому HTTPS не заменяет VPN и бдительность.

Правило 6: Регулярное обновление программного обеспечения. Операционные системы и браузеры регулярно получают обновления безопасности, закрывающие уязвимости, которые могут быть использованы для более изощрённых атак даже в рамках "Evil Twin" (например, внедрение кода через уязвимость в браузере). Включение автоматических обновлений - базовая гигиена цифровой безопасности.

3.3. Технические средства детектирования атаки "Evil Twin" для продвинутых пользователей

Помимо превентивных мер, полезно знать признаки, по которым можно заподозрить атаку:

Анализ RSSI (Received Signal Strength Indicator): Наличие двух точек доступа с одинаковым SSID, но с резко различающимся уровнем сигнала. Мобильные приложения типа `WiFi Analyzer` позволяют видеть такие дубликаты.

Проверка BSSID (Basic Service Set Identifier): BSSID - это MAC-адрес точки доступа. У легитимной точки и "двойника" они будут разными. Подключившись к сети, можно проверить её BSSID в настройках Wi-Fi устройства и сравнить с известным легитимным (например, указанным на информационном стенде).

Мониторинг сетевой активности: Неожидаанные появления сетей с именами, совпадающими с часто используемыми (например, в аэропорту внезапно появляется вторая сеть `Airport\_Free`), должны вызывать подозрения.

Использование VPN с функцией "Защита от утечек DNS": Качественные VPN-сервисы имеют встроенные механизмы, которые блокируют DNS-запросы, идущие вне VPN-туннеля. Если при подключённом VPN браузер вдруг показывает фишинговую страницу - это явный признак атаки, так как запрос прошёл в обход шифрования.

3.4. Сравнительный анализ решений для защиты: VPN, Tor, собственный хот-спот

VPN (Рекомендуемое решение): Обеспечивает сквозное шифрование, высокую скорость, широкую поддержку сервисов. Может иметь платную подписку. Выбор должен падать на провайдеров с прозрачной политикой приватности (no-logs) и современными протоколами (WireGuard, OpenVPN).

Сеть Tor: Обеспечивает максимальную анонимность за счёт многослойного шифрования и маршрутизации трафика через несколько серверов. Недостатки: Низкая скорость, блокировка многих сервисов (банкинг, потоковое видео), непригодность для повседневного использования в публичных сетях как основное средство.

Создание собственной точки доступа (Hotspot) со смартфона: Использование мобильного интернета (4G/5G) и раздача его как Wi-Fi на ноутбук. Эффективная альтернатива VPN, если мобильный трафик позволяет. Защищает, так как устройство подключается к доверенной точке доступа (ваш телефон), а не к публичной.

3.5. Роль производителей устройств и провайдеров публичного Wi-Fi в защите

Защита - это не только ответственность пользователя. Технологические меры на стороне сетей могли бы значительно снизить риски:

Обязательное использование WPA3-Enterprise: Этот стандарт предполагает индивидуальные учётные данные для каждого пользователя, что делает создание "двойника" бессмысленным без компрометации сервера аутентификации.

Внедрение технологии 802.11w (Protected Management Frames): Защищает управляющие фреймы (включая деаутентификационные) от подделки, что блокирует ключевой этап принудительного переподключения жертвы.

Информирование пользователей: Провайдеры публичного Wi-Fi могут размещать на порталах входа краткие инструкции по безопасности или рекомендовать конкретные VPN-сервисы.

Вывод по главе 3: Эффективная защита от угроз типа «Evil Twin» - это комплекс дисциплинарных и технических мер, где человеческий фактор играет ключевую роль. Наиболее критичными являются использование VPN для шифрования трафика и осознанный контроль подключений к беспроводным сетям. Разработанные рекомендации носят практический характер и направлены на формирование устойчивых цифровых привычек, которые сводят риск успешной атаки к минимуму, превращая пользователя из «слабого звена» в активного участника обеспечения собственной безопасности. Расширенный анализ показывает, что понимание не только как защищаться, но и как работают механизмы атаки и детектирования, значительно повышает цифровую устойчивость пользователя.

Заключение

В рамках данного индивидуального проекта была достигнута поставленная цель: проведён полный цикл анализа современной киберугрозы «Evil Twin» — от теоретического изучения до наглядной практической демонстрации в безопасной, изолированной среде.

Основные результаты работы:

На теоретическом уровне детально изучен механизм атаки, выявлены ключевые уязвимости публичных сетей, делающие её возможной.

На практическом уровне успешно организована лабораторная среда на базе виртуальной машины Kali Linux и продемонстрирована полная последовательность атаки с помощью автоматизированного фреймворка `airgeddon`, включая создание поддельной точки доступа и мгновенный перехват тестовых учётных данных с фишинговой страницы.

На основе анализа успешности демонстрации и выявленных точек приложения усилий был разработан комплекс практических рекомендаций для рядовых пользователей, обобщённых в формате наглядной памятки.

Вывод: Атака «Evil Twin» представляет собой серьёзную и легко реализуемую угрозу безопасности персональных данных в публичных пространствах. Противодействие ей лежит не в области сложных технических решений, а в области повышения цифровой грамотности и выработки безопасных поведенческих привычек. Практическая значимость проекта заключается в создании доступного образовательного материала, который в понятной форме объясняет суть угрозы и предлагает конкретные, выполнимые шаги для защиты, способствуя тем самым формированию более безопасной цифровой среды для всех пользователей.

Список использованных источников

1. Вислоухий Шериф (v1s1t0r1sh3r3). Airedaddon – Multi-use bash script for Linux systems to audit wireless networks [Электронный ресурс] // GitHub. – URL: <https://github.com/v1s1t0r1sh3r3/airgeddon>
2. Kali Linux Documentation [Электронный ресурс] // Kali.org. – URL: <https://www.kali.org/docs/>
3. Безопасность публичных сетей Wi-Fi: угроза Evil Twin и методы защиты [Электронный ресурс] // Хабр.
4. Глоссарий по кибербезопасности: Атака «Злой двойник» (Evil Twin) [Электронный ресурс] // Роскачество. – URL: <https://rskrf.ru/glossary/zloy-dvoynik-evil-twin/>
5. ГОСТ Р 7.0.5-2008. Библиографическая ссылка. Общие требования и правила составления.

Приложение А

Выбираем беспроводной интерфейс wlan0mon(цифра 2).

```
***** Interface selection *****
Select an interface to work with:
-----
1. eth0 // Chipset: Advanced Micro Devices, Inc.
2. wlan0mon // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
-----
*Hint* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means the translation has been automatically generated and is still pending of review
-----
> 2_ I
```

Следующим шагом для начала атаки будет выбор варианта атаки “Evil Twin”(цифра 7).

```
Select an option from menu:
-----
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
-----
4. DoS attacks menu
5. Handshake tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
-----
11. About & Credits
12. Options and language menu
-----
```

Далее после нескольких настроек идет выбор цели. В окне поиска airgeddon отобразит список захваченных сетей WIFI.

```
***** Select target *****
```

N.	BSSID	CHANNEL	PWR	ENC	ESSID
1)	3A:43:3D:BF:B1:90	6	43%	WPA2	Airport-WiFi
2)	AC:A2:13:A8:52:6C	1	24%	WPA2	MolnarWIFI
3)	C8:3A:35:48:5C:A0	1	33%	WPA2	Robert_WIFI
4)	38:43:7D:BF:B1:90	6	42%	WPA2	SkyNet
5)	AC:22:05:59:50:FC	1	32%	WPA2	UPCB3A8A22
6)	3A:43:1D:BF:B1:90	6	43%	WPA2	UPC Wi-Free
7)	AE:22:15:59:50:FC	1	32%	WPA2	UPC Wi-Free

```
(*) Network with clients
-----
Select target network:
> 1_
```

После выбора цели нужно нажать цифру 2(Deauth aireplay attack), чтобы выполнить DoS-атаку с помощью инструмента aireplay. В этом случае беспроводная карта рассылать пакеты деаутентификации всем устройствам, подключенным к выбранной точке доступа.

```
Select an option from menu:
-----
0. Return to Evil Twin attacks menu
-----
1. Deauth / disassoc amok mdk4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack
-----
*Hint* If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface
n monitor mode will be needed to be able to perform it
-----
> 2_
```

Теперь нам нужно захватить файл рукопожатия(Handshake). Для этого нужно ждать подключения пользователя. После успешного перехвата программа спросит куда сохранить этот файл. Позже он будет использоваться для проверки правильности ввода пароля жертвой на странице портала захвата.

```
Don't close any window manually, script will do when needed. In about 20 seconds maximum you'll know if you've
got the Handshake
Press [Enter] key to continue...

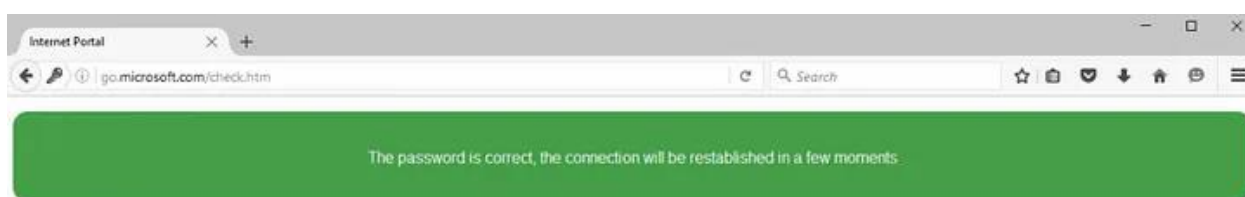
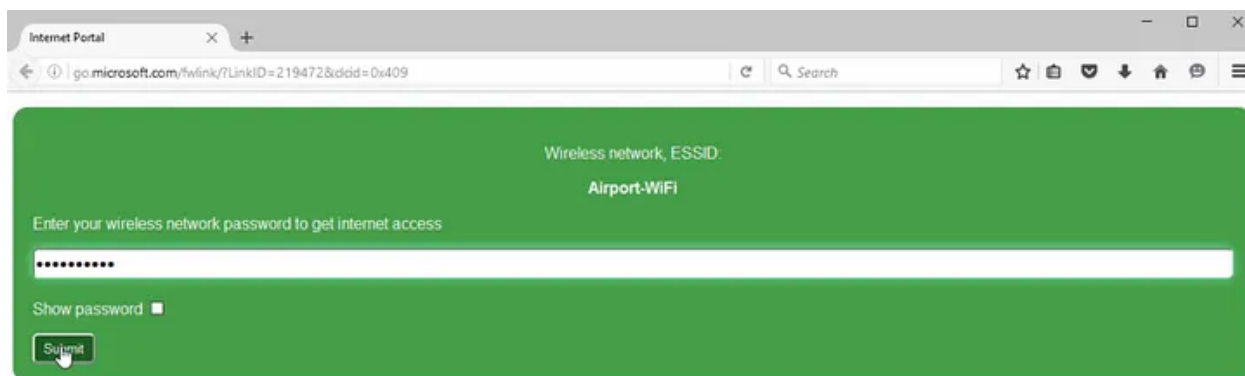
Wait. Be patient...
Congratulations!!

Type the path to store the file or press [Enter] to accept the default proposal [/root/handshake-3A:43:3D:BF:B
1:90.cap]
>
```

Далее после выбора языка для портала, имитируем подключение жертвы к захваченному WIFI.



Жертву автоматически перебрасывает на captive portal, где нужно ввести пароль от WIFI. Введем пароль 'Letmein456'(реальный пароль от сети) и нажмем Submit.



Далее вернемся в нашу Linux-машину. Появилось сообщение, в котором отображается введенный жертвой пароль. В дальнейшем его можно использовать для подключения к точке доступа. Помимо этого на данном окне видны все действия жертвы, удачные/неудачные вводы пароля, которые сравниваются с полученным ранее рукопожатием.



Приложение Б



6 ПРАВИЛ БЕЗОПАСНОСТИ В ПУБЛИЧНОМ WI-FI

Разработано на основе исследования
атаки "Evil Twin"