

MUNICIPAL AUTONOMOUS GENERAL EDUCATION INSTITUTION GYMNASIUM No.  
16 OF THE CITY OF TYUMEN

DEVELOPMENT OF PRACTICAL RECOMMENDATIONS FOR DATA  
PROTECTION AGAINST THE “EVIL TWIN” THREAT IN PUBLIC WI-FI NETWORKS

Supervisor:  
Yulia Yu. Myshko  
Informatics Teacher, MAOU Gymnasium No. 16

Author:  
Student of Grade 10-Zh  
Saveliy A. Golubev

TYUMEN, 2026

## **Brief Annotation**

This project presents a theoretical and practical analysis of the “Evil Twin” attack against public Wi-Fi networks. All stages of the attack — including the deployment of a rogue access point and the interception of data — were reproduced experimentally in an isolated environment (Kali Linux, airgeddon). Based on the results obtained, a set of practical recommendations for users was developed, aimed at protecting personal data: the use of a VPN, disabling automatic connection to networks, applying two-factor authentication, and verifying HTTPS. The work is intended to improve digital literacy and to foster safe behavioral habits.

## **Abstract**

This work is dedicated to the study of a personal-data security threat in public Wi-Fi networks known as the “Evil Twin” attack. The aim of the project is a comprehensive analysis of the attack’s mechanics, its practical reproduction in an isolated laboratory environment, and the development — based on the obtained results — of accessible recommendations for users. The theoretical part examines the architecture and vulnerabilities of open wireless networks, presents a detailed step-by-step breakdown of the attack scenario, and provides a comparative analysis with other types of wireless threats. In the experimental part, using a Kali Linux virtual environment and the airgeddon framework, all stages of the attack were successfully reproduced: from the deployment of a rogue access point to the interception of credentials through a phishing captive portal. On the basis of the conducted analysis, a set of practical security rules has been formulated, including the prioritized use of a VPN, control of automatic Wi-Fi connections, two-factor authentication, and other measures. The work has a strongly applied focus and can serve as a basis for raising digital literacy among a wide range of users.

## Contents

|                   |   |
|-------------------|---|
| INTRODUCTION..... | 4 |
|-------------------|---|

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| CHAPTER 1. THEORETICAL ANALYSIS OF THE “EVIL TWIN” THREAT .....                              | 5  |
| 1.1. Architecture and vulnerabilities of public wireless networks .....                      | 5  |
| 1.2. Mechanism and step-by-step breakdown of the “Evil Twin” attack .....                    | 6  |
| 1.3. Potential damage, consequences, and real-world cases .....                              | 6  |
| 1.4. Comparative analysis with other attacks on wireless networks .....                      | 7  |
| 1.5. Legal and ethical aspects of vulnerability research .....                               | 7  |
| CHAPTER 2. EXPERIMENTAL SIMULATION OF THE THREAT IN A CONTROLLED ENVIRONMENT .....           | 9  |
| 2.1. Design and setup of an isolated laboratory environment .....                            | 9  |
| 2.2. Experimental methodology and overview of the toolset .....                              | 9  |
| 2.3. Detailed report on the practical demonstration .....                                    | 10 |
| 2.4. Analysis of issues and solutions during the laboratory setup .....                      | 10 |
| 2.5. Detailed examination of the captive portal’s operation .....                            | 11 |
| 2.6. Extended scenario: simulating the attack against a network with a shared password ..... | 11 |
| CHAPTER 3. DEVELOPMENT OF A SET OF RECOMMENDATIONS FOR PROTECTING PERSONAL DATA .....        | 12 |
| 3.1. Systematic analysis of the results and identification of key countermeasures .....      | 12 |
| 3.2. Development and justification of practical security rules for the user .....            | 12 |
| 3.3. Technical means of detecting an Evil Twin attack for advanced users .....               | 13 |
| 3.4. Comparative analysis of protection solutions: VPN, Tor, personal hotspot .....          | 13 |
| 3.5. The role of device manufacturers and public Wi-Fi providers in protection .....         | 13 |
| Conclusion .....                                                                             | 14 |
| List of references .....                                                                     | 15 |
| Appendix A .....                                                                             | 16 |
| Appendix B .....                                                                             | 18 |

## INTRODUCTION

In the contemporary digital reality, public Wi-Fi networks have become a standard element of infrastructure. Their main advantage — accessibility — is at the same time their main source of risk. Data transmitted over such networks is often not protected by sufficient

encryption, which makes it an easy target for attackers. One of the most widespread attacks is “Evil Twin”. The simplicity of its execution contrasts sharply with its high potential for harm, which makes a detailed analysis of this threat critically important for building digital literacy.

Project goal: to conduct a comprehensive analysis of the Evil Twin threat by reproducing it in a controlled environment, and, on the basis of the results obtained, to develop practical recommendations for protecting personal data for ordinary users.

Project objectives:

1. Study the theoretical foundations of public Wi-Fi networks, their vulnerabilities, and analyze the Evil Twin attack mechanism in detail.
2. Set up a safe, isolated laboratory environment for the lawful simulation of a cyberattack.
3. Carry out a hands-on demonstration of all stages of the attack using specialized software (Kali Linux OS, airgeddon framework).
4. Analyze the success of the demonstration and identify the key user mistakes that make the attack possible.
5. Systematize the conclusions in the form of clear, practice-oriented recommendations and a printable user guide.

Object of research: the security of personal data in open wireless networks.

Subject of research: the technology and methods of carrying out an Evil Twin attack, and effective ways to counter it.

Research hypothesis: it can be assumed that a live demonstration of an Evil Twin attack in a controlled environment will allow not only a detailed analysis of its mechanism, but also the development of the most effective and user-friendly recommendations for protection, thereby raising the level of digital literacy.

Review of existing research: the problem of public Wi-Fi vulnerability is actively investigated in the field of cybersecurity. In the works of various specialists (for example, the articles of M. J. Ryan on wireless attacks, and research from Russian experts at “Roskachestvo”), Evil Twin is highlighted as one of the most widespread social engineering attacks because of how easy it is to execute. The present project builds on this research while shifting the focus from a theoretical description toward an applied educational simulation and the creation of preventive materials.

Research methods: the following methods were applied: 1) theoretical analysis of academic literature and specialized sources; 2) modeling — reproducing the attack in an isolated virtual environment (Kali Linux, VirtualBox); 3) a practical experiment using penetration-testing tools (the airgeddon framework); 4) analysis and synthesis of the obtained data to formulate conclusions and recommendations.

The applied significance of the work lies in the creation of an illustrative educational resource that helps people grasp the seriousness of the threat. The key practical deliverable is a set of recommendations and a printable user guide that allow even a person without a cybersecurity background to substantially improve their level of protection on public networks.

## **CHAPTER 1. THEORETICAL ANALYSIS OF THE “EVIL TWIN” THREAT**

### **1.1. Architecture and vulnerabilities of public wireless networks**

Public Wi-Fi networks are based on the IEEE 802.11 family of standards. Unlike home networks, which usually rely on protected access (WPA2/WPA3) with a unique password, public hotspots use simplified models. The most common ones are:

Open networks: do not use encryption at the data link layer. All traffic is transmitted over the air in cleartext.

Networks with shared authentication (Captive Portal): after connecting to an open network, the user is redirected to a web page (portal) where they must accept terms of service or enter a code. However, traffic before authentication — and, crucially, the traffic of many other users after authentication — often remains unencrypted.

Networks with a shared password (WPA2-Personal): the password is known to every visitor of the venue, which negates its cryptographic value. Once an attacker obtains it, they can not only join the network but also carry out more sophisticated attacks against other clients.

The key vulnerability lies in the very nature of the radio channel: data transmitted over the air can be received by any device within range. Without end-to-end encryption — such as that provided by HTTPS or a VPN — data packets are easily intercepted. Moreover, public networks rarely use Client Isolation, which in theory allows connected devices to interact with each other, opening up an additional attack vector.

## **1.2. Mechanism and step-by-step breakdown of the “Evil Twin” attack**

The Evil Twin attack is a classic variant of the Man-in-the-Middle (MitM) attack adapted for wireless environments. Its success rests on two factors: the technical ability to deploy an access point, and user psychology. The stages are described in detail below:

1. Reconnaissance stage. The attacker uses a wireless adapter that supports monitor mode together with sniffing software (for example, `airodump-ng` from the Aircrack-ng suite). The goal is to scan the radio spectrum and build a list of available networks (their SSIDs — Service Set Identifiers), broadcast channels, and signal strengths. Popular SSIDs are of particular interest: `Free_McCafe_WiFi`, `MTS_FREE`, `Airport_Free`.

2. Evil Twin deployment stage. Using the same or another adapter in master mode, the attacker creates a new wireless network. Its SSID and security parameters (open or with a known password) exactly mirror those of the legitimate target. The signal strength of the rogue access point is often artificially boosted so that it appears “more attractive” to devices that automatically connect to the strongest known network.

3. Forced reconnection stage (Deauthentication Attack). To “lure” clients away from the legitimate access point onto the rogue one, the attacker injects forged management frames — deauthentication packets — into the air. These packets, crafted using tools such as `aireplay-ng`, are spoofed to appear as commands from the legitimate access point and force the target device to drop its connection. After losing the link, the user’s device immediately searches for an available network and — finding the “twin” with a strong signal and a familiar name — connects to it automatically.

4. Traffic interception and analysis stage. After the victim has connected to the Evil Twin, all of their network traffic passes through the attacker’s machine. Using analysis tools such as Wireshark or ettercap, the attacker can passively “listen in” on the session. If the user visits sites that rely on the unprotected HTTP protocol, cookies, form data (logins and passwords), and browsing history become exposed.

5. Active interference and phishing stage. To work around transport-layer encryption (HTTPS), the attacker can go further. They may use ARP spoofing within their fake network to route the victim’s traffic through their proxy servers. This allows them to:

- Downgrade connection security (SSL stripping), turning HTTPS requests into HTTP.

- Modify website content on the fly, injecting malicious code.

- Most effectively, deploy a phishing captive portal that closely imitates the network operator’s login page, an email service (Gmail, Yandex), or a social network. A trusting user enters their credentials, which are then directly stored on the attacker’s side.

## **1.3. Potential damage, consequences, and real-world cases**

A successful Evil Twin attack leads to the complete compromise of a user’s digital session. The consequences cascade:

Credential theft: passwords for email, social networks, messengers, and corporate systems.

Financial losses: interception of bank-card data, access to online banking, theft of e-wallet credentials.

Theft of personal information: confidential correspondence, photos, documents.

Device compromise: the ability to deliver and install malicious software through spoofed update pages.

Legal risks: unlawful actions may be performed in the victim's name.

Beyond direct damage, the attack creates long-term risks. Compromised credentials are often tested against other services (credential stuffing), leading to multiple-account takeovers. Intercepted session cookies may grant access to accounts even without a password. In a corporate environment, an employee connecting to an Evil Twin can become the entry point of a chain attack against the organization's entire internal network.

In 2017, at the Black Hat security conference, a report was presented demonstrating how, using a device worth less than \$100, one could automatically deploy Evil Twins for the most common public SSIDs around the world. In Russia, "Roskachestvo" has repeatedly included this threat in its recommendations, emphasizing its social-engineering nature: the attack does not target cryptography, it targets the user.

#### **1.4. Comparative analysis with other attacks on wireless networks**

To fully understand the specifics of Evil Twin, it is important to view it in the context of other widespread Wi-Fi attacks:

WPS (Wi-Fi Protected Setup) attack: exploits vulnerabilities in the simplified-pairing mechanism. Unlike Evil Twin, it requires the presence of a password-protected network with WPS enabled. Modern routers have become more resilient to this attack.

Brute-force and dictionary attacks: aimed at directly breaking the network's encryption key. Effective only against weak passwords and require significant computing resources and time.

Pixie Dust attack: a modern method that exploits weak random-number generation in the WPS implementation of certain chipsets. Like the WPS attack, it applies only to a limited range of devices.

Eavesdropping in open networks: passive interception of traffic without setting up any attack infrastructure. Evil Twin is an active extension of this technique — the attacker is no longer just listening, but routing traffic through themselves, gaining far greater control.

Key distinction of Evil Twin: the attack does not try to break the network's cryptography. It bypasses cryptography by creating a new, unprotected access point that the user chooses themselves. This shifts the focus from technical complexity to user manipulation, making the attack universal and independent of the encryption strength of the target network.

#### **1.5. Legal and ethical aspects of vulnerability research**

Conducting any active security testing, even for research purposes, is regulated by law. In Russia, Articles 272 ("Unauthorized access to computer information") and 273 ("Creation, use, and distribution of malicious computer programs") of the Criminal Code can be applied to actions that disrupt networks or violate data confidentiality without the owner's consent.

The ethical-hacking methodology applied in this project is based on the following principles:

1. Explicit authorization: all actions are performed only against infrastructure owned by the researcher or for which written permission has been obtained.
2. Full isolation: the use of virtual environments and network modes (NAT, Internal Network) that exclude any impact on third-party systems.
3. Educational purpose: a clear definition of the activity's goal as raising awareness and developing defensive measures, not causing harm or seeking profit.
4. Data confidentiality: the impermissibility of intercepting, storing, or analyzing real user data even in an isolated environment. Only test datasets are used.

This project fully complies with these principles: the laboratory testbed is physically and logically isolated from external networks, and all manipulations are performed on test data using equipment owned by the researcher.

Conclusion to Chapter 1: The Evil Twin attack therefore represents a complex threat that skillfully combines the exploitation of fundamental vulnerabilities of open Wi-Fi networks (lack of encryption, weak authentication) with the manipulation of behavioral patterns of users (trust in familiar network names, the habit of automatic connection, inattentiveness when entering data). Thanks to the availability of off-the-shelf software, its technical execution has become trivial, which is what determines its widespread occurrence and high level of danger. Understanding its mechanism and how it differs from other attacks is the first and necessary step toward building effective protection.

## **CHAPTER 2. EXPERIMENTAL SIMULATION OF THE THREAT IN A CONTROLLED ENVIRONMENT**

### **2.1. Design and setup of an isolated laboratory environment**

To make the research lawful, ethical, and safe, it was necessary to build a testbed that fully excluded any impact on real networks and the public internet. The following architecture was chosen:

Host system: a personal computer running Windows 10/11.

Virtualization software: Oracle VM VirtualBox 7.0 — cross-platform open-source software for running guest operating systems.

Guest OS for the attacker: Kali Linux 2024.1 Rolling Release — a Debian-based distribution that comes preloaded with hundreds of penetration-testing tools, including those required for working with wireless networks.

Critically important network configuration: the network adapter of the Kali Linux virtual machine was configured in “Internal Network” mode. In this mode, the virtual machine can only communicate with other virtual machines connected to the same internal network and is fully isolated from the host’s physical network interfaces (Wi-Fi, Ethernet). This creates a clean “sandbox” testbed.

Role of the victim: for clarity, a physical Android smartphone was used. Within the model, it was meant to connect to the access point created by the virtual machine.

### **2.2. Experimental methodology and overview of the toolset**

The methodology was based on sequentially reproducing the stages of the attack within the isolated environment. The primary tool selected was the airgeddon framework (version 11.22). Its advantages for an educational project:

Integration: combines many separate utilities (Aircrack-ng, Hostapd, Bettercap, SSLstrip, etc.) under a single text menu.

Interactivity: walks the operator step by step through every stage of the attack with hints.

Automation: automatically handles routine tasks such as discovering interfaces and checking dependencies.

The stages of the experiment matched the theoretical model from Chapter 1 exactly, which allowed direct verification of theory by practice.

### 2.3. Detailed report on the practical demonstration

The course of the experiment was recorded step by step, with mandatory screenshots saved (see Appendix A).

1. Preparation and reconnaissance in airgeddon. After launching the script (``sudo bash airgeddon.sh``), the virtual wireless adapter (typically ``wlan0``) was selected from the list. Using the built-in function it was switched into monitor mode, which allowed all wireless packets in the air to be captured. Since the environment was isolated, the air was empty. This is the expected outcome and confirms the cleanness of the experiment.

2. Creating a fake access point (Fake AP). In the main menu, the “Fake Access Point” option was chosen. The system offered to create a new access point from scratch. The SSID ``Free_Public_Lab`` was entered. To imitate a public network, encryption was disabled (Open mode). The “hide my MAC address” option was enabled for anonymity within the lab.

3. Deploying the phishing captive portal. In the next step the key feature — “Captive Portal” — was activated. From the list of templates, a variant imitating a typical public-network login page with “Username” and “Password” fields was selected. Airgeddon automatically configured the web server (lighttpd) and the traffic-redirection rules (iptables) for intercepting HTTP requests.

4. Simulating the victim’s behavior. On the physical smartphone, the Wi-Fi network search was activated. The newly created ``Free_Public_Lab`` network appeared in the list. A manual connection was made to it (status: “Connected, no internet”). This simulated the moment when a user decides to take advantage of “free” Wi-Fi.

5. Recording the attack’s success. When attempting to open any website (for example, google.com) in the smartphone’s browser, an automatic redirect occurred to the local IP address of the virtual machine, where the phishing page was loaded. The following test data were entered: username ``test_user``, password ``Sup3rSecret!``. In less than a second, a bright notification appeared in the airgeddon terminal: “Credentials captured!”, followed by an exact record of the intercepted data. The experiment took about 15 minutes from launching the virtual machine to capturing credentials.

To keep the experiment clean it was important to ensure that the smartphone had no alternative path to the internet. In the access-point settings on Kali Linux, bridging with any other network interfaces was explicitly disabled. After data interception, the script was correctly stopped through the airgeddon menu, which guaranteed the access point’s shutdown and the reset of all iptables rules, returning the virtual environment to its original safe state.

### 2.4. Analysis of issues and solutions during the laboratory setup

Deploying the practical environment involves technical challenges, the analysis of which is important for the reproducibility of the experiment:

Issue 1: lack of monitor mode on virtual adapters. VirtualBox’s standard virtual network adapters (Intel PRO/1000) do not emulate wireless interfaces. Solution: use an external USB adapter that supports monitor mode (for example, on a Ralink RT3070 chipset) and pass it through to the virtual machine via USB passthrough. For the sake of simplicity and guaranteed isolation, this project chose to simulate the attack in a purely virtual environment by creating an access point “from scratch”, which airgeddon also allows.

Issue 2: the need to disable Network Manager in Kali Linux. The network-management service can conflict with manual interface management through airgeddon. Solution: stop the service with ``sudo systemctl stop NetworkManager`` before launching the script.

Issue 3: dependency checks. Airgeddon automatically checks for dozens of required utilities (hostapd, dnsmasq, lighttpd, etc.). Solution: run the script as a superuser and confirm the installation of all missing packages, which can take 5–10 minutes.

## 2.5. Detailed examination of the captive portal's operation

The captive portal is the key element of the demonstration that turns passive interception into active credential harvesting. In airgeddon, it relies on a stack of several services:

1. Hostapd: creates and manages the access point itself, configuring its parameters (SSID, channel).
2. Dnsmasq: acts as the DHCP server (assigning IP addresses to connected clients) and the DNS server. It is what redirects all of the client's DNS queries to the IP address of the virtual machine.
3. Lighttpd or Apache: a lightweight web server that serves the phishing page from the directory `/var/www/html/`.
4. Iptables: the Linux firewall. Configures NAT (Network Address Translation) rules that redirect all of the client's HTTP traffic (port 80) to the web server on port 80 of the virtual machine. This causes any attempt to open a website to be "intercepted".

Process logic: when a victim tries to open `http://google.com`, the following happens:

Dnsmasq returns the local IP of the virtual machine instead of Google's real address.

The victim's browser sends an HTTP request to this local address.

Iptables intercepts this request and forwards it to the lighttpd web server.

Lighttpd serves the prepared phishing page to the victim.

The submitted data is sent via a POST form back to the server, where a special script (part of airgeddon) logs and displays them on screen.

## 2.6. Extended scenario: simulating the attack against a network with a shared password

To complete the picture, a scenario was tested in which the legitimate network was emulated by a second virtual machine (for example, running Ubuntu) configured as a protected access point with the known password `PublicPassword123`. The goal was to show that Evil Twin works in this case as well.

1. On the router virtual machine, a protected `Cafe_Network` (WPA2) was deployed.
  2. On Kali Linux, after the reconnaissance stage, airgeddon was used to create a "twin" with an identical SSID `Cafe_Network` and the same password.
  3. A deauthentication attack was launched against the client (a third virtual machine), which had been preconnected to the legitimate network.
  4. After the client reconnected to the "twin", its traffic was likewise fully intercepted.
- Important conclusion: knowing the password of a public network does not protect against Evil Twin — it only makes it easier for the attacker to create a convincing copy.

Conclusion to Chapter 2: the practical experiment in a controlled environment brilliantly confirmed the theoretical analysis. The Evil Twin attack was successfully reproduced from start to finish using publicly available automated tools. This proves that no advanced professional knowledge of network security is required to carry it out — basic command-line skills and the ability to follow instructions are sufficient. The key success factor within the model was the simulation of trusting user behavior, which once again underscores the social-engineering essence of this threat. Working in "Internal Network" mode proved its effectiveness as an absolutely safe and legal method of studying cyberattacks. Understanding technical details such as the operation of the captive portal allows for a deeper grasp of the threat's mechanism and, consequently, more effective countermeasures against it.

## **CHAPTER 3. DEVELOPMENT OF A SET OF RECOMMENDATIONS FOR PROTECTING PERSONAL DATA**

### **3.1. Systematic analysis of the results and identification of key countermeasures**

Analysis of the successful demonstration makes it possible to clearly identify the points where defensive measures should be applied. The vulnerable chain looks as follows: existence of a twin → connection to it → transmission of unprotected data. Accordingly, the protection strategy must be multi-layered and break this chain at the earliest possible stages.

1. Connection prevention (the first and most important layer). It is necessary to eliminate the very possibility of a device connecting to a rogue access point.

2. Data protection if the connection has occurred (the second layer). If a connection to a rogue network does happen, the intercepted data must be made useless to the attacker.

3. Damage minimization (the third layer). Even if data has been compromised, the scale of potential damage must be limited.

### **3.2. Development and justification of practical security rules for the user**

Based on the conducted analysis, the following set of recommendations addressed to ordinary users has been formulated:

Rule 1. Prioritized use of a VPN (Virtual Private Network). This is the most effective measure, implementing the second layer of protection. A high-quality VPN service delivers all of the user's internet traffic through an encrypted "tunnel" to its server. Even after connecting to an Evil Twin, the attacker will see only a stream of encrypted data between the victim's device and the VPN server, which they cannot decrypt. Recommendation: install and activate a trusted VPN provider's application before connecting to any public network.

Rule 2. Strict control of Wi-Fi connections. Implements the first layer of protection.

Disable the "Connect to open networks automatically" setting on smartphones and laptops.

Manually remove from the list of saved networks those that are no longer in use (for example, networks of hotels and cafes from other cities).

Verify the network before connecting: confirm the exact name (SSID) and password with the venue's staff. Networks with almost identical but not exact names are suspicious (for example, `Starbucks\_Free\_WiFi` instead of the official `Google Starbucks`).

Rule 3. Mindful use of the internet on public networks. Combines the first and third layers.

Without an active VPN, avoid any actions that require authentication: logging into email, social networks, banking, making purchases.

For confidential operations, prefer mobile internet (4G/5G). Cellular networks provide built-in encryption between the device and the operator's tower, which makes them significantly safer than public Wi-Fi.

Rule 4. Strengthening account security (the third layer).

Use two-factor authentication (2FA) everywhere. Even if the login and password are intercepted, the attacker will need a one-time code from an SMS or an authenticator app (Google Authenticator, Microsoft Authenticator), which blocks access.

Use a password manager that creates and stores unique strong passwords for each service. This prevents the "domino effect" when a single password is compromised.

Rule 5. Technical checks (a supplementary measure).

Always pay attention to the HTTPS protocol. The browser address bar should display a padlock icon and the `https://` prefix. However, it is important to understand that a phishing site deployed on an Evil Twin may also have a valid HTTPS certificate (especially with free Let's Encrypt certificates). Therefore HTTPS does not replace VPN and vigilance.

Rule 6: regular software updates. Operating systems and browsers regularly receive security updates that close vulnerabilities which can be exploited even within an Evil Twin attack (for example, code injection via a browser vulnerability). Enabling automatic updates is basic digital-security hygiene.

### **3.3. Technical means of detecting an Evil Twin attack for advanced users**

In addition to preventive measures, it is useful to know the signs by which an attack can be suspected:

RSSI (Received Signal Strength Indicator) analysis: the presence of two access points with the same SSID but sharply different signal levels. Mobile applications such as Wi-Fi Analyzer make such duplicates visible.

BSSID (Basic Service Set Identifier) check: the BSSID is the MAC address of the access point. The legitimate AP and the twin will have different ones. After connecting to a network, you can check its BSSID in the device's Wi-Fi settings and compare it with the known legitimate one (for example, posted on an information board).

Network-activity monitoring: the unexpected appearance of networks with names matching frequently used ones (for example, a second `Airport\_Free` suddenly showing up at an airport) should raise suspicion.

Use of a VPN with DNS-leak protection: high-quality VPN services have built-in mechanisms that block DNS queries going outside of the VPN tunnel. If, with the VPN active, the browser suddenly displays a phishing page, this is a clear sign of an attack, since the request bypassed the encryption.

### **3.4. Comparative analysis of protection solutions: VPN, Tor, personal hotspot**

VPN (recommended solution): provides end-to-end encryption, high speed, and broad service compatibility. It may require a paid subscription. The choice should fall on providers with a transparent privacy policy (no-logs) and modern protocols (WireGuard, OpenVPN).

Tor network: provides maximum anonymity through multi-layer encryption and the routing of traffic through several servers. Drawbacks: low speed, blocking of many services (banking, video streaming), unsuitability for everyday use on public networks as a primary tool.

Creating your own hotspot from a smartphone: using mobile internet (4G/5G) and sharing it as Wi-Fi to a laptop. An effective alternative to a VPN if mobile data allowance permits. It protects you because the device connects to a trusted access point (your phone) rather than to a public one.

### **3.5. The role of device manufacturers and public Wi-Fi providers in protection**

Protection is not only the user's responsibility. Technological measures on the network side could significantly reduce the risks:

Mandatory use of WPA3-Enterprise: this standard implies individual credentials for each user, which makes the creation of a "twin" meaningless without compromising the authentication server.

Adoption of 802.11w (Protected Management Frames): this protects management frames (including deauthentication frames) from spoofing, which blocks the key stage of forcibly reconnecting the victim.

Informing users: public Wi-Fi providers can place short security instructions on their login portals or recommend specific VPN services.

Conclusion to Chapter 3: effective protection against threats such as Evil Twin is a combination of disciplinary and technical measures, in which the human factor plays a key role. The most critical of these are the use of a VPN to encrypt traffic and the mindful control of wireless connections. The recommendations developed are practical in nature and aim to build sustainable digital habits that reduce the risk of a successful attack to a minimum, turning the user from the “weak link” into an active participant in their own security. The extended analysis shows that understanding not only how to defend, but also how the mechanisms of attack and detection work, significantly increases the user’s digital resilience.

## **Conclusion**

Within this individual project, the stated goal was achieved: a complete cycle of analysis was carried out for the modern Evil Twin cyberthreat — from theoretical study to a clear practical demonstration in a safe, isolated environment.

Main results of the work:

At the theoretical level, the attack mechanism was studied in detail and the key vulnerabilities of public networks that make it possible were identified.

At the practical level, a laboratory environment based on a Kali Linux virtual machine was successfully set up, and the full sequence of the attack was demonstrated using the

automated airgeddon framework, including the creation of a rogue access point and the instant interception of test credentials from a phishing page.

Based on the analysis of the demonstration's success and the identified points of intervention, a set of practical recommendations for ordinary users was developed and summarized in the form of a printable user guide.

Conclusion: the Evil Twin attack represents a serious and easily executable threat to the security of personal data in public spaces. Counteracting it lies not in the realm of complex technical solutions, but in the realm of raising digital literacy and developing safe behavioral habits. The practical significance of the project lies in the creation of an accessible educational resource that explains the essence of the threat in clear terms and offers concrete, achievable steps for protection, thereby contributing to the formation of a safer digital environment for all users.

### **List of references**

1. v1s1t0r1sh3r3. Airgeddon — Multi-use bash script for Linux systems to audit wireless networks [Electronic resource] // GitHub. — URL: <https://github.com/v1s1t0r1sh3r3/airgeddon>
2. Kali Linux Documentation [Electronic resource] // Kali.org. — URL: <https://www.kali.org/docs/>
3. Public Wi-Fi network security: the Evil Twin threat and methods of protection [Electronic resource] // Habr.
4. Cybersecurity glossary: the “Evil Twin” attack [Electronic resource] // Roskachestvo. — URL: <https://rskrf.ru/glossary/zloy-dvoynik-evil-twin/>
5. GOST R 7.0.5-2008. Bibliographic reference. General requirements and rules for compilation.

## **Appendix A**

Selecting the wireless interface wlan0mon (option 2).

The next step to begin the attack is to choose the “Evil Twin” attack option (option 7).

Then, after several settings, the target is selected. In the search window, aircgeddon will display the list of captured Wi-Fi networks.

After the target has been selected, press option 2 (Deauth aireplay attack) to perform a DoS attack using the aireplay tool. In this case the wireless card will broadcast deauthentication packets to all devices connected to the chosen access point.

Now we need to capture the handshake file. To do that, we wait for a user to connect. After a successful capture the program asks where to save the file. It will later be used to verify whether the password entered by the victim on the captive portal is correct.

After choosing the language for the captive portal, we simulate the victim connecting to the captured Wi-Fi.

The victim is automatically redirected to the captive portal, where the Wi-Fi password must be entered. We enter the password ‘Letmein456’ (the real network password) and click Submit.

Then we return to our Linux machine. A message has appeared showing the password entered by the victim. It can later be used to connect to the access point. In addition, this window shows all of the victim’s actions — successful and unsuccessful password attempts — which are compared against the previously captured handshake.

## **Appendix B**



## 6 ПРАВИЛ БЕЗОПАСНОСТИ В ПУБЛИЧНОМ WI-FI

Разработано на основе исследования  
атаки "Evil Twin"