НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ПОРІВНЯННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ АНОНІМІЗАЦІЇ ТРАФІКУ КОРИСТУВАЧА»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Слободянюк Володимир Володимирович

Керівник: к.т.н., доцент
Бойко Віктор Дмитрович

Рецензент: д.т.н., професор
Соколов Артем Вікторович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет кібербезпеки та інформаційних технологій
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Слободянюку Володимиру Володимировичу

1. Тема роботи: «Порівняння ефективності засобів анонімізації трафіку користувача»
Керівник роботи: наукова ступінь, звання ПІБ
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16 » вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз предметної області та пошук науково-технічної інформації за темою роботи	Вересень-жовтень 2024	
2	Узгодження теми з науковим керівником, формулювання мети та завдань дослідження	Листопад 2024	
3	Робота над першим розділом	Листопад-грудень 2024	
4	Робота на другим розділом	Січень-лютий 2025	
5	Робота над третім розділом	Лютий-березень 2025	
6	Уточнення подальшого обсягу роботи та його коригування	Березень-травень 2025	
7	Оформлення звітної частини	Травень 2025	
8	Захист роботи	11.06.2025	

Здобувач_____
(підпис) (прізвище та ініціали)

Керівник роботи_____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Слободянюк Володимир Володимирович "Порівняння ефективності засобів анонімізування трафіку користувача" – Кваліфікаційна робота бакалавра за спеціальністю 125 Кібербезпека, освітньою програмою Кібербезпека. Кваліфікаційна робота викладена на 53 сторінках основного тексту і 41 сторінках загального тексту, містить 3 розділи, 3 рисунки, 2 додатка та 11 використаних джерел.

Метою дослідження є порівняльний аналіз ефективності поширених засобів анонімізації користувацького трафіку, таких як OpenVPN, SOCKS5 proxy, HTTP/S proxy та SSH тунелі, за ключовими показниками продуктивності, безпеки та зручності використання.

У кваліфікаційній роботі проведено огляд сучасних підходів до анонімізації трафіку, обґрунтовано вибір досліджуваних засобів та критеріїв та їх оцінки. Розроблено методику та налаштовано тестове середовище для проведення експериментальних вимірювань. Здійснено тестування обраних засобів анонімізації за такими параметрами, як швидкість передачі даних, затримка, рівень маскування IP-адреси, наявність DNS-витоків та навантаження на ресурси сервера.

За результатами дослідження проведено аналіз отриманих даних, виявлено переваги та недоліки кожного із засобів. Сформульовано рекомендації щодо вибору оптимального засобу анонімізації залежно від конкретних потреб та пріоритетів користувача.

Результати роботи можуть бути використані користувачами для вибору захисту своєї приватності в мережі, а також системним адміністраторам при налаштування корпоративних засобів безпеки.

АНОНІМІЗАЦІЯ ТРАФІКУ, VPN, OPENVPN, SOCKS5 PROXY, HTTP PROXY, HTTPS PROXY, SSH ТУНЕЛЬ, ЗАХИСТ ДАНИХ.

ABSTRACT

Slobofianiuk Volodymyr Volodymyrovych “Comparison of the effectiveness of user traffic anonymization tools“ – Bachelor`s work in Cybersecurity, specialization 125 Cybersecurity, educational program Cybersecurity. The thesis consists of 53 pages of main text and 41 pages of total text, comprising 3 chapters, 3 figures, appendices, and references to 11 sources.

The purpose of the study is to compare the effectiveness of common means of anonymizing user traffic, such as OpenVPN, SOCKS5 proxy, HTTP/S proxy, and SSH tunnels, in terms of key performance, security, and usability indicators.

The qualification work provides an overview of modern approaches to traffic anonymization, justifies the choice of the studied tools and criteria and their evaluation. A methodology was developed and a test environment was set up for experimental measurements. The selected anonymization tools have been tested in terms of such parameters as data transfer rate, latency, IP address masking level, DNS leaks, and server resource load.

Based on the results of the study, the data obtained were analyzed, the advantages and disadvantages of each of the tools were identified. Recommendations for choosing the optimal anonymization tool depending on the specific needs and priorities of the user are formulated.

The results of the study can be used by users to choose the protection of their privacy in the network, as well as by system administrators when setting up corporate security tools.

TRAFFIC ANONYMIZATION, VPN, OPENVPN, SOCKS5 PROXY, HTTP PROXY, HTTPS PROXY, SSH TUNNEL, DATA PROTECTION.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

DoS – Denial of Service;

VPN – Virtual Private Network

IP – Internet Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

HTTP/S – HyperText Transfer Protocol/Secure

SSH – Secure Shell

SOCSK – Socket Secure

DNS – Domain Name System

VPS – Virtual Private Server

Mbps – Megabits per second

ВСТУП

В епоху цифрових технологій та глобального поширення Інтернету питання забезпечення приватності та безпеки користувацьких даних набуває надзвичайної актуальності. Щоденно мільйони користувачів передають величезні обсяги інформації, яка може стати об’єктом перехоплення, аналізу або несанкціонованого доступу з боку зловмисників, інтернет провайдерів або державних структур.

Згідно з дослідженнями, кількість зареєстрованих кібератак зросла на 300% у період з 2019 по 2024 рік. Більше того, 83% проаналізованих витоків даних призвели до розкриття персональної ідентифікаційної інформації, що свідчить про серйозну загрозу для приватності користувачів. [1]

Використання засобів анонімізації трафіку стає необхідним інструментом для захисту конфіденційності, обходу цензури та забезпечення безпечного доступу до мережевих ресурсів.

Ринок пропонує різноманітні технології анонімізації, від VPN-сервісів до проксі-сервісів та SSH-тунелів, кожна з яких має свої переваги, недоліки та специфіку застосування. Однак для пересічного користувача або навіть для системного адміністратора вибір оптимального засобу часто ускладнюється відсутністю чітких, об’єктивних даних щодо їх реальної ефективності за різними критеріями. Це зумовлює необхідність проведення порівняльного дослідження ефективності популярних засобів анонімізації трафіку.

Мета дослідження: Здійснити порівняльний аналіз обраних засобів анонімізації трафіку користувача на основі експериментальних даних та розробити рекомендації щодо їх вибору залежно від потреб користувача.

Для досягнення мети було сформульовано такі завдання:

1. Провести аналіз предметної галузі: розглянути основні загрози приватності в мережі, існуючі підходи та засоби анонімізації трафіку.

2. Вибрати та обґрунтувати методологію дослідження: визначити критерії оцінки ефективності засобів анонімізації, обрати інструментарій для тестування.
3. Вибрати та обґрунтувати програмну реалізацію тестового стенду: налаштувати серверне та клієнтське середовище, розгорнути досліджувані засоби анонімізації (OpenVPN, SOCKS5 proxy, HTTP/S proxy, SSH тунель).
4. Провести експериментальне тестування обраних засобів анонімізації за визначеними критеріями (швидкість, затримка, рівень анонімності, навантаження на сервер, зручність використання).
5. Провести аналіз отриманих результатів, порівняти ефективність досліджуваних засобів та виявити їх переваги та недоліки.
6. Сформувати висновки та надати практичні рекомендації щодо вибору засобу анонімізації трафіку.

Об’єкт дослідження: процеси передачі даних в мережі інтернет, та методи їх анонімізації за допомогою технологій OpenVPN, SOCKS5 proxy, HTTP/HTTPS proxy та SSH-тунелів.

Предмет дослідження: ефективність засобів анонімізації користувацького трафіку, що оцінюється за сукупністю показників продуктивності, безпеки та зручності використання.

1 АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ ЗАСОБІВ АНОНІМІЗАЗЦІЇ ТРАФІКУ

1.1 Постановка проблеми забезпечення анонімності користувача в мережі

Сучасний світ неможливо уявити без інтернету, який проник у всі сфери людського життя, від особистого спілкування та розваг до професійної діяльності, фінансових операцій та державного управління. Щодня мільярди користувачів генерують та обмінюються величезними обсягами даних, створюючи цифровий слід, який стає все більш детальним та всеосяжним. Ця цифрова активність, хоча й надає безпрецедентні можливості, водночас породжує серйозні виклики для конфіденційності та безпеки особистих даних.

Одним із найгучніших прикладів несанкціонованого використання персональних даних став скандал навколо компанії Cambridge Analytica та соціальної мережі Facebook, що розгорівся у 2018 році. Виявилося, що дані понад 87 мільйонів користувачів Facebook були зібрані без їхньої належної згоди через сторонній додаток-тест особистості та передані Cambridge Analytica [1, 2]. Ця компанія використовувала зібрані дані для створення психологічних профілів виборців та таргетування політичної реклами, зокрема під час президентських виборів у США 2016 року та референдуму Brexit у Великій Британії [3]. Цей інцидент продемонстрував, як легко особиста інформація, якою користувачі діляться в соціальних мережах, може бути використана для маніпуляції громадською думкою та втручання у демократичні процеси, а також підкреслив недостатній контроль користувачів над тим, як їхні дані збираються, обробляються та передаються третім сторонам.

Проблема забезпечення анонімності користувача в мережі виходить далеко за межі лише несанкціонованого використання даних великими компаніями. Щоденна онлайн-активність користувачів, така як перегляд веб-сторінок, використання соціальних мереж, онлайн-покупки та спілкування в месенджерах, залишає цифровий слід. Цей слід включає IP-адреси, дані про місцезнаходження, історію переглядів,

пошукові запити, особисті вподобання та багато іншої інформації. Збір та аналіз цих даних здійснюється різними суб’єктами:

Приклади можливих інцидентів:

1. Інтернет-провайдери (ISP): Мають доступ до всього трафіку своїх клієнтів і можуть його логувати, аналізувати або передавати третім сторонам, наприклад, на вимогу правоохоронних органів.
2. Рекламні мережі та технологічні гіганти: Збирають дані для таргетування реклами, профілювання користувачів та покращення своїх сервісів. Практики збору даних часто детально описані в політиках конфіденційності, проте користувачі не завжди їх уважно вивчають.
3. Зловмисники: Можуть перехоплювати незахищений трафік, викрадати облікові дані, фінансову інформацію, здійснювати фішингові атаки або поширювати шкідливе програмне забезпечення. Атаки типу "людина посередині" (Man-in-the-Middle, MitM) на незахищених Wi-Fi мережах є поширеною загрозою.
4. Державні структури: Можуть здійснювати моніторинг інтернет-активності з метою національної безпеки, боротьби зі злочинністю або, в деяких країнах, для здійснення цензури та придушення інакомислення

Відсутність належного рівня анонімності може призвести до низки негативних наслідків для користувачів:

1. Крадіжка особистих даних та фінансові втрати: Перехоплення логінів, паролів, даних банківських карток.
2. Втрата приватності та небажане стеження: Відстеження онлайн-поведінки, створення детальних цифрових профілів.
3. Маніпуляція та дезінформація: Використання профілів для поширення цілеспрямованої дезінформації або пропаганди.
4. Цензура та обмеження доступу до інформації: Блокування доступу до певних веб-ресурсів урядами або корпораціями. [4].

Саме тому забезпечення анонімності та захист цифрової ідентичності стає не просто бажанням, а нагальною потребою для сучасного інтернет-користувача. Це вимагає використання спеціальних технологій та інструментів, здатних приховати реальну IP-адресу, зашифрувати трафік та ускладнити відстеження онлайн-активності. Однак, різноманітність таких засобів та їхня різна ефективність у різних сценаріях використання створюють проблему вибору оптимального рішення, що й зумовлює актуальність даного дослідження.

1.2 Сучасний стан проблеми анонімізації трафіку та основні загрози

Проблема забезпечення анонімності в сучасному цифровому середовищі є багатогранною та динамічною. З розвитком технологій та зростанням обсягів переданої інформації з’являються нові методи збору, аналізу та використання даних користувачів, а також вдосконалюються інструменти, спрямовані на деанонімізацію. Розуміння поточного стану цієї проблеми та основних загроз є ключовим для обґрунтування необхідності використання та порівняння ефективності засобів анонімізації трафіку [5].

Якщо раніше збір даних переважно обмежувався аналізом логів веб-серверів та даних, добровільно наданих користувачами при реєстрації, то сьогодні арсенал методів значно розширився. До них належать:

1. Трекери та файли cookie: Веб-сайти та рекламні мережі активно використовують різноманітні трекери (включаючи сторонні файли cookie, пікселі відстеження, "цифрові відбитки" браузера – browser fingerprinting) для збору інформації про поведінку користувачів на різних ресурсах. "Цифрові відбитки" дозволяють ідентифікувати користувача навіть без використання cookie, аналізуючи унікальну конфігурацію його браузера та системи (версія ОС, встановлені шрифти, плагіни, роздільна здатність екрану тощо)

2. Аналіз метаданих: Навіть якщо сам зміст комунікації зашифрований (наприклад, у месенджерах з наскрізним шифруванням), метадані (хто, кому, коли, як довго спілкувався, з якого IP-адреси) можуть розкривати значну кількість інформації про соціальні зв’язки, інтереси та діяльність користувача.
3. нтернет речей (IoT): Зростаюча кількість підключених до Інтернету пристроїв (розумні годинники, фітнес-трекери, побутова техніка) збирають різноманітні дані про користувачів та їхнє оточення, часто з недостатнім рівнем захисту та прозорості щодо використання цих даних [6].
4. Системи глибинного аналізу пакетів (DPI - Deep Packet Inspection): Технології DPI, що використовуються інтернет-провайдерами та державними структурами, дозволяють аналізувати не лише заголовки, а й вміст мережевих пакетів, що дає змогу ідентифікувати типи трафіку (наприклад, використання VPN або Tor), блокувати певні ресурси або навіть збирати конфіденційну інформацію, якщо вона передається у незашифрованому вигляді .

На основі вищезазначених методів збору даних формується цілий спектр конкретних загроз для анонімності та приватності користувачів у мережі. Однією з фундаментальних загроз є пасивне прослуховування (Eavesdropping), що полягає у перехопленні мережевого трафіку зловмисниками або іншими зацікавленими сторонами. Якщо дані передаються у незашифрованому вигляді, їх зміст може бути легко прочитаний. Ця загроза особливо актуальна при використанні публічних Wi-Fi мереж, де зловмисник, підключений до тієї ж мережі, може використовувати доступні інструменти, такі як Wireshark, для аналізу всього трафіку, що проходить через точку доступу.

Окрім пасивного спостереження, існують і активні атаки на мережевий трафік, спрямовані на його перехоплення, модифікацію або перенаправлення. Серед них особливе місце займають атаки типу "людина посередині" (Man-in-the-Middle, MitM). При такій атаці зловмисник вбудовується в канал зв’язку між користувачем та

цільовим сервером, отримуючи можливість не тільки переглядати, але й змінювати дані, що передаються. Популярними векторами для реалізації MitM-атак є ARP-спуфінг у локальних мережах, що дозволяє перенаправляти трафік через пристрій зловмисника; створення фальшивих точок доступу Wi-Fi (відомих як "Evil Twin"), які імітують легітимні мережі для заманювання користувачів; або компрометація DNS-серверів, що дає змогу перенаправляти запити користувачів на фішингові або шкідливі сайти, навіть якщо вони вводять правильну адресу ресурсу [7].

З маніпуляціями DNS-запитами пов’язана й інша значна загроза – DNS-спуфінг та DNS-витоки (DNS Spoofing & DNS Leaks). Підміна DNS-записів, як вже зазначалося, може перенаправити користувача на шкідливий сайт. DNS-витоки, у свою чергу, виникають, коли запити на розпізнавання доменних імен, які браузер або операційна система надсилають для отримання IP-адреси сайту, відправляються повз встановлений анонімізуючий канал, наприклад, VPN-тунель (див. Рисунок 1.3). Це призводить до того, що реальний DNS-провайдер користувача (часто це інтернет-провайдер) отримує інформацію про відвідувані сайти, що може розкрити його місцезнаходження або історію веб-активності, нівелюючи частину переваг від використання засобів анонімізації.

До активних атак також належать атаки на протоколи шифрування SSL/TLS, такі як SSL Stripping або Downgrade Attacks. Метою SSL Stripping є примусове зниження рівня захисту з’єднання з безпечного HTTPS до незашифрованого HTTP, що робить трафік вразливим до перехоплення. Downgrade Attacks, у свою чергу, можуть змусити клієнта та сервер використовувати слабкіші або застарілі криптографічні алгоритми, які легше піддаються злому та розшифруванню.

Навіть якщо трафік надійно зашифрований, загрозу становлять аналіз трафіку та кореляційні атаки (Traffic Analysis & Correlation Attacks). Аналіз характеристик зашифрованого трафіку, таких як обсяг переданих даних, час відправлення та отримання пакетів, напрямки комунікації, може дозволити зробити певні висновки про діяльність користувача або тип використовуваних ним сервісів. Кореляційні атаки

є більш складним методом, що полягає у зіставленні патернів трафіку на вході та виході з анонімізуючої мережі (наприклад, Tor). Якщо атакуючий має можливість спостерігати за трафіком у різних точках мережі, він може спробувати встановити зв’язок між конкретним користувачем та ресурсом, який той відвідує, шляхом пошуку схожих за часом та обсягом потоків даних. Такі атаки особливо небезпечні, якщо атакуючий контролює значну частину мережевої інфраструктури, наприклад, велику кількість вхідних чи вихідних вузлів анонімізуючої мережі [7].

Сукупність цих загроз створює надзвичайно складне середовище, в якому забезпечення повної та абсолютної анонімності є практично неможливим завданням. Проте, свідоме використання відповідних засобів анонімізації трафіку може значно підвищити рівень захисту приватності, суттєво ускладнити відстеження онлайн-активності та зменшити ризики, пов’язані з різноманітними загрозами в цифровому просторі. Саме тому глибоке розуміння не тільки принципів роботи цих засобів, але й їхньої реальної ефективності у протистоянні сучасним викликам, що й буде досліджено в наступних розділах даної роботи, є критично важливим.

1.3 Класифікація та характеристика досліджуваних засобів анонімізації

В умовах зростаючих загроз приватності та постійного моніторингу інтернет-активності користувачі все частіше звертаються до різноманітних технологій та інструментів, спрямованих на забезпечення анонімності та захист своїх даних. Ринок пропонує широкий спектр рішень, що відрізняються за принципом дії, рівнем забезпечуваної безпеки, продуктивністю та складністю використання. Для цілей даного дослідження було обрано чотири поширені та репрезентативні засоби анонімізації, які представляють різні підходи до приховування реальної IP-адреси користувача та захисту його трафіку: OpenVPN, SOCKS5 проксі, HTTP/HTTPS проксі та SSH-тунелі. Вибір саме цих технологій зумовлений їхньою популярністю серед користувачів, доступністю (як у вигляді безкоштовних, так і платних рішень, а також

можливістю самостійного налаштування), а також тим, що вони охоплюють різні рівні мережевої моделі OSI та використовують різні механізми для забезпечення анонімності [8].

Загалом, засоби анонімізації можна класифікувати за декількома критеріями, такими як рівень мережевої моделі, на якому вони працюють, наявність та тип шифрування, ступінь централізації та архітектура. Для дослідження використовувались наступні засоби:

OpenVPN є одним з найпопулярніших та найгнучкіших протоколів для створення віртуальних приватних мереж (VPN) з відкритим вихідним кодом. VPN, за своєю суттю, створює зашифрований тунель між пристроєм користувача та віддаленим VPN-сервером. Весь інтернет-трафік користувача спрямовується через цей тунель, внаслідок чого його реальна IP-адреса маскується IP-адресою VPN-сервера, а дані захищаються від перехоплення третіми сторонами.

Ключові характеристики OpenVPN:

1. Протоколи передачі: OpenVPN може працювати як поверх протоколу TCP (Transmission Control Protocol), так і UDP (User Datagram Protocol). Використання UDP зазвичай забезпечує вищу швидкість через менші накладні витрати на встановлення та підтримання з’єднання, тоді як TCP гарантує надійну доставку пакетів і може бути ефективнішим при обході деяких мережевих обмежень або фаєрволів, які можуть блокувати UDP-трафік.
2. Шифрування та безпека: OpenVPN використовує бібліотеку OpenSSL для забезпечення криптографічних операцій. Він підтримує широкий спектр симетричних шифрів (наприклад, AES-256, Blowfish), геш-алгоритмів (наприклад, SHA-256, SHA-512) та протоколів обміну ключами (наприклад, на основі SSL/TLS). Це забезпечує високий рівень захисту даних від несанкціонованого доступу. Для автентифікації можуть використовуватися сертифікати, статичні ключі або комбінація логіна та пароля.

3. Платформенна сумісність: Клієнтське програмне забезпечення OpenVPN доступне для більшості популярних операційних систем, включаючи Windows, macOS, Linux, Android та iOS.
4. Гнучкість налаштувань: OpenVPN надає адміністраторам та користувачам широкі можливості для конфігурації параметрів безпеки, маршрутизації, стиснення даних та інших аспектів роботи VPN-тунелю.
5. Обхід цензури: Завдяки можливості працювати на різних портах та використовувати TCP, OpenVPN може бути ефективним засобом для обходу інтернет-цензури та доступу до заблокованих ресурсів, хоча деякі просунуті системи DPI можуть намагатися ідентифікувати та блокувати OpenVPN-трафік [9].

OpenVPN має низку переваг, що роблять його популярним вибором серед засобів анонімізації трафіку. По-перше, він забезпечує високий рівень безпеки завдяки надійному шифруванню. Крім того, ця технологія має відкритий вихідний код, що сприяє прозорості її роботи та дає можливість проводити незалежний аудит безпеки. OpenVPN вирізняється гнучкістю налаштувань, а також підтримкою широкого спектру операційних систем і платформ. Однією з вагомих переваг є також здатність обходити більшість фаєрволів та мережевих обмежень, що дозволяє використовувати його навіть у жорстко контрольованих мережах.

Разом з тим, OpenVPN не позбавлений недоліків. Основним з них є можливе зниження швидкості інтернет-з’єднання, яке зумовлене накладними витратами на шифрування та тунелювання трафіку. Крім того, налаштування власного OpenVPN-сервера може виявитися складним завданням для недосвідчених користувачів, хоча в інтернеті доступні численні скрипти та покрокові інструкції, що частково спрощують цей процес. Також варто враховувати, що продуктивність роботи OpenVPN залежить від обчислювальних можливостей як сервера, так і клієнтського пристрою.

SOCKS (Socket Secure) – це мережевий протокол, який дозволяє клієнтським додаткам встановлювати з’єднання з серверами через проксі-сервер. Версія SOCKS5

є найсучаснішою та найпоширенішою, вона працює на сеансовому рівні (рівень 5) моделі OSI, що робить її більш універсальною порівняно з HTTP-проксі

Ключові характеристики SOCKS5 проксі:

1. Універсальність протоколів: На відміну від HTTP-проксі, які зазвичай працюють лише з HTTP/HTTPS трафіком, SOCKS5 може перенаправляти трафік будь-яких протоколів прикладного рівня, що використовують TCP або UDP (наприклад, HTTP, HTTPS, FTP, SMTP, BitTorrent, ігровий трафік).
2. Методи автентифікації: SOCKS5 підтримує декілька методів автентифікації, включаючи відсутність автентифікації (для публічних проксі), автентифікацію за логіном/паролем, а також GSS-API.
3. Підтримка UDP: Можливість перенаправляти UDP-трафік є важливою перевагою для додатків, що використовують цей протокол (наприклад, деякі онлайн-ігри, VoIP-сервіси, DNS-запити, якщо вони налаштовані на передачу через SOCKS5).
4. Відсутність власного шифрування: Важливо розуміти, що протокол SOCKS5 сам по собі не забезпечує шифрування трафіку між клієнтом та проксі-сервером, а також між проксі-сервером та кінцевим ресурсом. Безпека переданих даних залежить від того, чи використовує шифрування сам додаток (наприклад, HTTPS). Однак SOCKS5 проксі часто використовується в поєднанні з іншими технологіями шифрування, наприклад, через SSH-тунель, що забезпечує захист трафіку.
5. Маскування IP-адреси: SOCKS5 проксі ефективно приховує реальну IP-адресу користувача, замінюючи її на IP-адресу проксі-сервера.

SOCKS5-проксі має низку переваг, які забезпечують його популярність у сфері анонімізації трафіку. Передусім, до ключових переваг можна віднести універсальність — підтримку як TCP, так і UDP з’єднань, що дає змогу обробляти різні типи трафіку. Крім того, SOCKS5, як правило, забезпечує вищу продуктивність у порівнянні з VPN, оскільки має менші накладні витрати, особливо у випадках, коли не використовується

додаткове шифрування. Також важливою особливістю є наявність механізмів автентифікації, які дозволяють обмежувати доступ до проксі-сервера.

Разом із тим, SOCKS5-проксі має і певні обмеження. Основним недоліком є відсутність вбудованого шифрування трафіку за замовчуванням, що може створювати ризики у разі використання незахищених мереж. Окрім цього, існує загроза витоку DNS-запитів, якщо останні не перенаправляються через проксі, що потенційно дозволяє розкрити інформацію про відвідувані ресурси. Також слід зазначити, що використання SOCKS5-проксі потребує окремого налаштування на рівні прикладного програмного забезпечення або операційної системи, що може ускладнити його інтеграцію для пересічного користувача.

HTTP-проксі (HyperText Transfer Protocol proxy) – це тип проксі-сервера, що працює на прикладному рівні (рівень 7) моделі OSI і спеціалізується на обробці HTTP та HTTPS запитів [Джерело: Стаття про HTTP проксі, наприклад, з MDN Web Docs або аналогічного ресурсу]. Коли користувач налаштовує HTTP-проксі у своєму браузері або системі, всі його HTTP/HTTPS запити спочатку надсилаються на проксі-сервер, а вже той, у свою чергу, звертається до цільового веб-сервера від імені користувача.

Ключові характеристики HTTP/HTTPS проксі:

1. Спеціалізація на веб-трафіку: Основне призначення – робота з HTTP та HTTPS протоколами. Деякі HTTP-проксі можуть підтримувати метод CONNECT для тунелювання HTTPS-трафіку, що дозволяє передавати зашифровані дані безпосередньо між клієнтом та кінцевим сервером, при цьому сам HTTP-проксі бачить лише запит на встановлення тунелю.
2. Кешування: HTTP-проксі часто мають можливість кешувати веб-контент (зображення, скрипти, сторінки). Це може прискорити завантаження раніше відвідуваних сторінок для користувачів, що використовують один і той же проксі, а також зменшити навантаження на мережу.

3. Фільтрація контенту: HTTP-проксі можуть використовуватися для фільтрації веб-контенту на основі URL-адрес, ключових слів або типів файлів. Це часто застосовується в корпоративних мережах або освітніх закладах для обмеження доступу до небажаних ресурсів.
4. Маскування IP-адреси: Як і інші проксі, HTTP/HTTPS проксі замінюють IP-адресу користувача на свою.
5. Шифрування: HTTPS-проксі, або HTTP-проксі з підтримкою методу CONNECT, забезпечує створення зашифрованого тунелю між клієнтом і кінцевим HTTPS-сервером. У такій конфігурації проксі-сервер не має змоги переглядати вміст переданих даних, що істотно підвищує рівень конфіденційності. Водночас слід зауважити, що навіть за умов використання зашифрованого з'єднання, проксі-сервер може фіксувати сам факт встановлення з'єднання з конкретним веб-ресурсом, що залишає можливість для здійснення аналізу метаданих [10].

Переваги та недоліки використання HTTP/HTTPS-проксі в контексті анонімізації трафіку мають як технічні, так і функціональні аспекти, що слід враховувати при виборі відповідного рішення.

Серед ключових переваг HTTP/HTTPS-проксі варто відзначити їхню простоту налаштування, особливо в середовищі веб-браузерів, що робить їх зручним інструментом для кінцевих користувачів. Крім того, підтримка кешування контенту дозволяє зменшити навантаження на мережу та потенційно підвищити швидкість доступу до часто відвідуваних ресурсів. У разі використання HTTPS-проксі забезпечується шифрування веб-трафіку між клієнтом і кінцевим ресурсом, що підвищує рівень конфіденційності.

Водночас, HTTP/HTTPS-проксі мають і низку суттєвих обмежень. По-перше, вони переважно обмежені роботою з протоколами HTTP та HTTPS, що знижує їхню універсальність порівняно з SOCKS5-проксі або VPN-рішеннями. По-друге, класичні HTTP-проксі не шифрують трафік, що створює додаткові ризики для безпеки,

особливо при передачі конфіденційної інформації. Крім того, HTTP/HTTPS-проксі є менш гнучкими в контексті підтримки нестандартних протоколів або типів трафіку.

SSH (Secure Shell) – це мережевий протокол, що дозволяє встановлювати безпечне (зашифроване) з'єднання між двома комп'ютерами в незахищеній мережі. Хоча основне призначення SSH – це безпечний віддалений доступ до командного рядка, його можливості тунелювання портів дозволяють використовувати його як ефективний засіб анонімізації трафіку [Джерело: Офіційна документація OpenSSH або авторитетний посібник з SSH].

Ключові характеристики SSH-тунелю:

1. Шифрування: Весь трафік, що проходить через SSH-тунель, надійно шифрується за допомогою криптографічних алгоритмів, підтримуваних протоколом SSH. Це забезпечує конфіденційність та цілісність даних.
2. Типи тунелювання: SSH підтримує декілька типів тунелювання: Локальне перенаправлення (-L) спрямовує трафік з локального порту клієнта через SSH-сервер на віддалений хост, що дає змогу отримати доступ до внутрішніх ресурсів. Віддалене перенаправлення (-R) працює у зворотному напрямку — з SSH-сервера на локальний порт клієнта, що корисно для надання доступу до локальних сервісів. Найбільш ефективним для анонімізації є динамічне перенаправлення (-D), яке створює локальний SOCKS-проксі та передає весь трафік через зашифрований SSH-тунель до кінцевого ресурсу.
3. Автентифікація: Для встановлення SSH-з'єднання потрібна автентифікація на SSH-сервері, зазвичай за допомогою пароля або пари криптографічних ключів (публічний та приватний).

До основних переваг SSH-тунелю слід віднести високий рівень безпеки, який забезпечується завдяки використанню криптографічних механізмів протоколу SSH. Крім того, можливість створення SOCKS-проксі (за допомогою параметра -D) дозволяє спрямовувати через тунель різноманітні типи трафіку, що робить це рішення універсальним. Важливо також, що для користувачів із базовими навичками роботи з

SSH його налаштування зазвичай не становить суттєвих труднощів.

Разом з тим, SSH-тунелі мають і певні обмеження. Продуктивність може бути зниженою порівняно з традиційними проксі-сервісами або деякими реалізаціями VPN, що пов’язано з накладними витратами на обробку трафіку через SSH. Це особливо відчутно у випадках TCP-over-TCP, коли TCP-з’єднання програми інкапсулюється в інше TCP-з’єднання тунелю, що може призводити до неефективності в разі втрат пакетів. Також для використання SSH-тунелю необхідна наявність доступу до відповідного SSH-сервера, що може бути обмежувальним чинником. Окрему увагу слід приділити проблемі DNS-витоків: за замовчуванням DNS-запити можуть обходити тунель, тому їх необхідно окремо перенаправляти через створений SOCKS-проксі або застосовувати додаткові механізми конфігурації.

Розглянувши характеристики кожного з обраних засобів, стає очевидним, що вони пропонують різні компроміси між безпекою, продуктивністю, універсальністю та простотою використання. Це підкреслює необхідність проведення експериментального порівняння їхньої ефективності для надання обґрунтованих рекомендацій користувачам.

Таким чином, на основі проведеного теоретичного аналізу сформовано підґрунтя для розробки методики експериментального дослідження, спрямованого на порівняльну оцінку обраних засобів анонімізації за визначеними критеріями, що є завданням наступного розділу даної кваліфікаційної роботи.

2 ТЕОРЕТИЧНА РОЗРОБКА МЕТОДИКИ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ АНОНІМІЗАЦІЇ

2.1 Обґрунтування вибору критеріїв оцінки ефективності

Розробка обґрунтованої та відтворюваної методики експериментального дослідження є ключовим етапом для отримання достовірних результатів порівняльного аналізу ефективності засобів анонімізації трафіку. Даний розділ присвячено теоретичному обґрунтуванню вибору критеріїв оцінки, підбору відповідного інструментарію для проведення вимірювань та формулюванню послідовності експериментальних дій.

Для всебічної та об’єктивної оцінки ефективності досліджуваних засобів анонімізації необхідно визначити набір ключових критеріїв, що відображають як технічні аспекти їхньої роботи, так і практичну цінність для кінцевого користувача. Враховуючи специфіку завдання, було виділено наступні основні параметри для порівняльного аналізу.

Першочерговим показником, що цікавить більшість користувачів, є швидкість передачі даних. Цей критерій включає швидкість завантаження та швидкість віддачі інформації, виміряні в мегабітах на секунду (Mbps). Зниження цих показників при використанні засобів анонімізації є очікуваним через накладні витрати на шифрування, тунелювання та маршрутизацію трафіку через проміжні сервери. Однак, величина цього зниження може суттєво відрізнятися для різних технологій.

Тісно пов’язаним із швидкістю є параметр затримки, що зазвичай вимірюється як час проходження сигналу до тестового сервера та назад (Ping) у Мілі секундах (ms). Високі значення затримки можуть негативно впливати на інтерактивні додатки, такі як онлайн-ігри, відеоконференції або VoIP-телефонія.

Наступним важливим аспектом є продуктивність веб-доступу. Цей критерій оцінюється за двома показниками: по-перше, загальний час повного завантаження стандартизованої тестової веб-сторінки, виміряний у секундах; по-друге, кількість

запитів на секунду, яку може обробити веб-сервер при доступі до нього через засіб анонімізації, що визначається за допомогою спеціалізованих інструментів для тестування навантаження. Ці показники дозволяють оцінити, наскільки комфортним буде перегляд веб-сайтів при використанні того чи іншого засобу [11].

Ключовим для засобів анонімізації є рівень анонімності та безпеки. Цей комплексний критерій включає перевірку фактичного маскування реальної IP-адреси користувача, виявлення потенційних DNS-витоків, що можуть розкрити інформацію про інтернет-провайдера або відвідувані ресурси, а також якісну оцінку типу шифрування трафіку, що використовується кожною технологією.

Для оцінки ресурсоємності серверної частини досліджуваних рішень, що особливо актуально при самостійному розгортанні зафіксовано навантаження на ресурси сервера. Це включає орієнтовне вимірювання використання центрального процесора у відсотках та оперативної пам’яті у мегабайтах під час активного використання каналу анонімізації.

Також проведено суб’єктивну оцінку складності налаштування та використання кожного із засобів. Хоча цей критерій не є суто технічним, він має значний вплив на доступність технології для широкого кола користувачів. Оцінка проведена за стандартизованою шкалою.

Обрана сукупність критеріїв дозволяє охопити основні аспекти функціонування засобів анонімізації та надати користувачам комплексну інформацію для прийняття обґрунтованого рішення щодо вибору найбільш відповідного інструменту

2.2 Вибір інструментів для тестування методів анонімізації трафіку

Для проведення експериментальних вимірювань за визначеними у попередньому підрозділі критеріями ефективності необхідний ретельно підібраний набір програмних та апаратних засобів. Вибір інструментарію ґрунтувався на вимогах щодо точності, доступності, можливості автоматизації вимірювань та поширеності у

практиці тестування мережевих технологій.

Апаратна складова тестового стенду передбачає використання трьох основних компонентів.

Серверна частина реалізована на базі віртуального приватного сервера (VPS). Для забезпечення відтворюваності та мінімізації впливу сторонніх факторів, обрано VPS з операційною системою Linux, зокрема дистрибутив Ubuntu актуальної версії. На цьому сервері послідовно розгорнуті серверні компоненти досліджуваних засобів анонімізації: OpenVPN сервер, SOCKS5 проксі-сервер Dante та HTTP/HTTPS проксі-сервер Squid. SSH-сервер, необхідний для реалізації SSH-тунелів, є стандартним компонентом обраної операційної системи. Конкретні апаратні характеристики VPS (кількість процесорних ядер, обсяг оперативної пам’яті, тип накопичувача) зафіксовані та враховані при аналізі навантаження.

Клієнтська частина буде представлена персональним комп’ютером з встановленою операційною системою Linux, що має стабільне підключення до мережі Інтернет. З цього комп’ютера ініційовано тестові запити та проведено вимірювання.

Для тестів продуктивності веб-доступу буде використовуватися цільовий веб-ресурс. З метою мінімізації впливу зовнішніх мережевих факторів та для вимірювання саме накладних витрат засобів анонімізації, розгорнуто простий веб-сервер Nginx з тестовою статичною сторінкою безпосередньо на тому ж VPS, де розміщуються сервери анонімізації.

Програмний інструментарій для вимірювань включає наступні утиліти та сервіси.

Для вимірювання швидкості завантаження/віддачі даних та базової затримки використано консольну утиліту speedtest-cli. Цей інструмент дозволяє проводити тести швидкості до географічно розподілених серверів мережі Speedtest.net, надаючи об’єктивні показники пропускної здатності каналу.

Для більш детального аналізу максимальної пропускної здатності мережевого каналу між клієнтською та серверною частинами застосовано інструмент iperf3. Ця

утиліта працює в клієнт-серверному режимі та дозволяє генерувати TCP або UDP трафік, вимірюючи фактичну пропускну здатність та інші параметри мережі.

Оцінка продуктивності доступу до веб-сервера здійснена за допомогою утиліти ab (Apache Benchmark), що входить до складу Apache HTTP Server. ab дозволяє симулювати навантаження на веб-сервер шляхом надсилання великої кількості одночасних запитів та вимірює такі показники, як кількість запитів на секунду та середній час відповіді.

Для оцінки часу повного завантаження веб-сторінок буде використано веб-браузер Mozilla Firefox з вбудованими інструментами розробника (Developer Tools), зокрема вкладкою "Network", яка дозволяє детально аналізувати процес завантаження всіх компонентів сторінки.

Перевірка фактичного маскування IP-адреси та виявлення потенційних DNS-витоків проведено за допомогою загальнодоступних онлайн-сервісів, таких як whatismyip.com, ipleak.net, які відображають публічну IP-адресу клієнта та використовувані ним DNS-сервери.

Для вимірювання мережевої затримки до конкретних вузлів та трасування маршруту пакетів використано стандартні системні утиліти ping та traceroute.

Моніторинг навантаження на ресурси серверної частини (CPU, RAM) під час активного тестування здійснено за допомогою системних моніторів операційної системи Linux, наприклад, утиліти htop або vmstat.

Вибір зазначеного інструментарію забезпечує можливість проведення комплексних та стандартизованих вимірювань за всіма визначеними критеріями ефективності, що є необхідною умовою для отримання об’єктивних та порівнянних результатів дослідження.

2.3 Розробка методики проведення експерименту

Для забезпечення об’єктивності та відтворюваності результатів порівняльного аналізу ефективності засобів анонімізації трафіку, розроблена уніфікована методика

проведення експериментальних вимірювань. Ця методика регламентує послідовність дій, умови проведення тестів та способи фіксації даних для кожного досліджуваного засобу анонімізації, а також для контрольних вимірювань.

Експериментальне дослідження проводилось у декілька послідовних етапів, кожен з яких спрямований на оцінку певних критеріїв ефективності. Перед початком тестування кожного засобу анонімізації здійснюється його належне налаштування на серверній та клієнтській частинах згідно з рекомендаціями розробників та найкращими практиками. Усі вимірювання для одного засобу проводяться протягом одного сеансу для мінімізації впливу можливих коливань умов мережевого підключення клієнта. Для кожного кількісного показника виконується серія з п’яти вимірювань, після чого розраховується середнє арифметичне значення, яке й використовується для подальшого аналізу та порівняння. Такий підхід дозволяє зменшити вплив випадкових флуктуацій та отримати більш стабільні та репрезентативні дані.

Перший етап дослідження передбачає проведення контрольних вимірювань без використання будь-яких засобів анонімізації. Це необхідно для отримання базових показників продуктивності інтернет-з’єднання клієнтської машини та її взаємодії з тестовим веб-ресурсом. На цьому етапі фіксуються:

1. Швидкість завантаження та віддачі даних, а також час затримки за допомогою утиліти speedtest-cli до обраного тестового сервера.
2. Максимальна пропускна здатність TCP-каналу між клієнтською машиною та серверним VPS за допомогою інструменту iperf3.
3. Продуктивність доступу до тестової веб-сторінки, розміщеної на VPS, за допомогою утиліти ab (Apache Benchmark). Визначається кількість запитів на секунду та середній час відповіді на запит при встановленій кількості загальних та одночасних запитів.

4. Час повного завантаження тестової веб-сторінки, виміряний за допомогою інструментів розробника веб-браузера. Перед кожним вимірюванням кеш браузера очищується для забезпечення чистоти експерименту.
5. Публічна IP-адреса клієнта та використовувані DNS-сервери за допомогою спеціалізованих онлайн-сервісів. Очікується відображення реальної IP-адреси та DNS-серверів інтернет-провайдера клієнта.

Наступні етапи присвячені послідовному тестуванню кожного з обраних засобів анонімізації: OpenVPN, SOCKS5 проксі, HTTP/HTTPS проксі та SSH-тунелю. Для кожного засобу процедура тестування є аналогічною, але виконується після його активації та налаштування відповідного з'єднання або проксі-сервера на клієнтській машині.

Процедура тестування для кожного засобу анонімізації включає:

1. Перевірку рівня анонімності: Після активації засобу анонімізації, за допомогою онлайн-сервісів перевіряється, чи змінилася публічна IP-адреса клієнта на IP-адресу сервера анонімізації. Також проводиться тест на наявність DNS-витоків для визначення, чи спрямовуються DNS-запити через анонімізуючий канал, чи обходять його.
2. Вимірювання швидкості передачі даних та затримки: За допомогою speedtest-cli визначаються швидкість завантаження, віддачі та пінг при роботі через активований засіб анонімізації. Важливо забезпечити, щоб тестовий сервер, обраний speedtest-cli, був відмінним від сервера, на якому розгорнуто засіб анонімізації, для коректної оцінки пропускної здатності тунелю.
3. Вимірювання максимальної пропускної здатності каналу: За допомогою iperf3 тестується пропускна здатність між клієнтом та серверним VPS, при цьому трафік спрямовується через досліджуваний засіб анонімізації.
4. Оцінка продуктивності веб-доступу: Аналогічно до контрольних вимірювань, за допомогою ab тестується продуктивність доступу до тестової веб-сторінки через засіб анонімізації. Також фіксується час повного

завантаження тестової веб-сторінки у браузері з використанням інструментів розробника.

5. Моніторинг навантаження на сервер: Під час проведення найбільш інтенсивних тестів на серверній частині за допомогою системних моніторів фіксується пікове та середнє навантаження на центральний процесор та використання оперативної пам’яті, спричинене роботою серверного компонента засобу анонімізації.
6. Фіксація особливостей налаштування та використання: У процесі налаштування та тестування кожного засобу суб’єктивно оцінюється складність його конфігурації, стабільність роботи та загальна зручність використання з точки зору кінцевого користувача.

Усі отримані кількісні дані (швидкості, затримки, час завантаження, кількість запитів, показники навантаження на сервер) заносяться до таблиць для подальшого аналізу. Якісні показники (маскування IP, наявність DNS-витоків, тип шифрування, суб’єктивна оцінка зручності) також систематизуються.

Таким чином, розроблена в даному розділі методика створює необхідне теоретико-методологічне підґрунтя для проведення експериментальної частини дослідження. Вона забезпечує стандартизований підхід до вимірювань, що дозволить отримати об’єктивні, порівнянні та відтворювані результати щодо ефективності досліджуваних засобів анонімізації трафіку, які будуть представлені та проаналізовані у наступному розділі роботи.

3 ЕКСПЕРЕМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ АНОНІМІЗАЦІЇ ТРАФІКУ

3.1 Налаштування тестового середовища та засобів анонімізації

Формування адекватного та контрольованого тестового середовища є необхідною умовою для отримання достовірних результатів експерименту. Нижче детально описано етапи підготовки серверної та клієнтської інфраструктури, а також конфігурування кожного із засобів анонімізації, що підлягають дослідженню.

Для реалізації серверної частини тестового стенду було орендовано віртуальний приватний сервер з наступними технічними характеристиками: 1 vCPU, 1 ГБ RAM, 25 ГБ SSD . В якості операційної системи було обрано дистрибутив Linux Ubuntu 24.10 x64. Після отримання доступу до сервера через протокол SSH, було проведено повне оновлення системних пакетів до актуальних версій. Наступним кроком було встановлення необхідного програмного забезпечення та утиліт, що використовуються як для функціонування досліджуваних сервісів, так і для проведення вимірювань та моніторингу. Зокрема, було інстальовано: curl, wget (для завантаження файлів), nano (текстовий редактор), net-tools (для роботи з мережевими налаштуваннями), dnsutils (для діагностики DNS), iperf3 (для тестів пропускної здатності), speedtest-cli (для тестів швидкості Інтернет-з’єднання), htop (для інтерактивного моніторингу системних ресурсів) та ufw (Uncomplicated Firewall) для налаштування правил мережевої безпеки.

Для забезпечення безпеки сервера було налаштовано фаєрвол ufw. Було встановлено політику за замовчуванням на заборону всіх вхідних з’єднань (sudo ufw default deny incoming) та дозвіл всіх вихідних (sudo ufw default allow outgoing). Додано правила, що дозволяють вхідні з’єднання для SSH (порт 22), а також HTTP (порт 80) та HTTPS (порт 443) для функціонування тестового веб-сервера. Після налаштування правил фаєрвол було активовано командою sudo ufw enable. Стан фаєрволу після конфігурації представлено у Додатку

З метою проведення тестів продуктивності веб-доступу за допомогою утиліти ab, на сервері було розгорнуто веб-сервер Nginx. Після встановлення та запуску, було створено просту тестову HTML-сторінку, яка використовувалася як цільовий ресурс для вимірювань. Доступність тестової сторінки було перевірено через веб-браузер.

Для тестування максимальної пропускної здатності каналу за допомогою iperf3, ця утиліта була запущена на сервері, слухаючи на стандартному порту 5201/TCP. Відповідне правило для дозволу вхідних з'єднань на цей порт було додано до конфігурації ufw.

Клієнтська частина тестового стенду була реалізована на персональному комп'ютері під керуванням операційної системи Linux Mint 22.1 "Xia" Cinnamon edition, На клієнтській машині було встановлено необхідні утиліти для проведення тестів (speedtest-cli, iperf3, ab, клієнтське програмне забезпечення для OpenVPN) та сучасний веб-браузер з інструментами розробника.

Для розгортання OpenVPN сервера на VPS було використано популярний скрипт автоматичного встановлення openvpn-install.sh від Angristan, завантажений з офіційного репозиторію GitHub. Після надання скрипту прав на виконання, його було запущено з правами суперкористувача. У процесі інтерактивного налаштування було обрано наступні ключові параметри: протокол UDP, стандартний порт 1194, рекомендовані DNS-сервери, а також створено клієнтський конфігураційний файл з унікальним іменем. Фрагменти діалогу налаштування представлені у Додатку. Після успішного завершення роботи скрипта, згенерований клієнтський файл .ovpn було скопійовано на клієнтську машину для подальшого використання. Сервіс OpenVPN було автоматично запущено та додано до автозавантаження. Відповідне правило для дозволу вхідного UDP-трафіку на порт 1194 було додано до ufw.

В якості SOCKS5 проксі-сервера було обрано Dante SOCKS server. Встановлення здійснювалося стандартними засобами менеджера пакетів операційної системи. Основна конфігурація сервера проводилася шляхом редагування файлу /etc/danted.conf. Було визначено мережевий інтерфейс для внутрішніх та зовнішніх

з’єднань, вказано порт прослуховування (1080). Для спрощення тестового сценарію було обрано метод автентифікації none, що дозволяє підключення без логіна та пароля (слід зазначити, що для реального використання такий підхід не рекомендується з міркувань безпеки). Дозволено проходження TCP та UDP трафіку для всіх клієнтів. Приклад конфігураційного файлу danted.conf наведено у Додатку. Після збереження конфігурації, сервіс danted було перезапущено та додано до автозавантаження. У фаєрволі ufw було відкрито TCP-порт 1080 та UDP-порт.

Для реалізації HTTP/HTTPS проксі-сервера було використано програмне забезпечення Squid. Встановлення проводилося стандартними засобами операційної системи. Конфігурація Squid здійснювалася шляхом редагування файлу /etc/squid/squid.conf. Для тестових цілей було змінено стандартні правила доступу, дозволивши підключення з будь-яких IP-адрес (правила acl all src 0.0.0.0/0 та http_access allow all). Важливо зазначити, що таке налаштування є вкрай небезпечним для використання у реальних умовах і застосовувалося виключно в рамках контрольованого експерименту. Стандартний порт прослуховування Squid (3128/TCP) було залишено без змін. Змінені фрагменти конфігураційного файлу Squid наведено у Додатку. Сервіс squid було перезапущено та додано до автозавантаження. Порт 3128/TCP було відкрито у фаєрволі ufw.

Для тестування SSH-тунелю не потребувалося додаткових налаштувань на серверній частині, оскільки SSH-сервер є стандартним компонентом встановленої ОС Ubuntu Server та вже функціонував для забезпечення віддаленого доступу. Анонімізація трафіку за допомогою SSH-тунелю реалізувалася на клієнтській машині шляхом створення динамічного перенаправлення портів. У якості LOCAL_PORT було обрано порт 8080. Таким чином, на локальній машині клієнта створювався SOCKS-проксі, що слухав на localhost:8080 і перенаправляв весь трафік через зашифроване SSH-з’єднання на віддалений VPS.

Після завершення налаштування всіх компонентів тестового середовища та досліджуваних засобів анонімізації, було розпочато етап проведення експериментальних вимірювань згідно з розробленою методикою.

3.2 Проведення експериментальних вимірювань

Після успішного налаштування тестового середовища та розгортання всіх досліджуваних засобів анонімізації було розпочато етап безпосереднього проведення експериментальних вимірювань. Усі тести виконувалися згідно з методикою, детально описаною у підрозділі 2.3 даної кваліфікаційної роботи, для забезпечення стандартизації умов та можливості коректного порівняння отриманих результатів.

Експериментальна частина дослідження проводилася в період з 30.04.2025 по 7.05.2025. Такий підхід дозволив мінімізувати вплив можливих короткострокових змін у завантаженості мережевих каналів або продуктивності серверів, що могли б спотворити результати при проведенні тестів у різні дні.

Для кожного кількісного показника (швидкість передачі даних, затримка, час завантаження сторінки, кількість запитів на секунду для ab) було проведено серію з п’яти послідовних вимірювань. Отримані значення фіксувалися, після чого розраховувалося їх середнє арифметичне. Саме ці усереднені показники використовувалися для подальшого аналізу та побудови порівняльних таблиць і графіків. Такий підхід спрямований на нівелювання випадкових флуктуацій та підвищення надійності отриманих даних.

Спочатку були проведені контрольні вимірювання без використання будь-яких засобів анонімізації для встановлення базових показників продуктивності інтернет-з’єднання клієнтської машини та її взаємодії з тестовим веб-ресурсом. Далі, послідовно для кожного засобу анонімізації – OpenVPN, SOCKS5 проксі, HTTP/HTTPS проксі та SSH-тунелю – активувалося відповідне з’єднання або налаштовувався проксі-сервер на клієнтській машині. Після кожної активації

проводився повний цикл тестів, що включав:

1. Перевірку маскування IP-адреси та наявність DNS-витоків за допомогою онлайн-сервісів.
2. Вимірювання швидкості завантаження, віддачі та пінгу за допомогою speedtest-cli.
3. Тестування максимальної пропускної здатності каналу за допомогою iperf3.
4. Оцінку продуктивності веб-доступу до тестової сторінки за допомогою ab та інструментів розробника веб-браузера.
5. Моніторинг навантаження на ресурси VPS під час проведення інтенсивних тестів.

Усі вихідні дані інструментів тестування, а також скріншоти, що підтверджують результати перевірки IP-адреси, DNS-витоків та навантаження на сервер, ретельно зберігалися для подальшого включення до додатків кваліфікаційної роботи. Процес збору даних був максимально формалізований для уникнення помилок та забезпечення повноти експериментальної інформації.

3.3 Представлення та аналіз отриманих результатів тестування

Після проведення експериментальних вимірювань згідно з розробленою методикою, було отримано масив даних, що характеризують ефективність досліджуваних засобів анонімізації трафіку за різними критеріями. У даному підрозділі наведено систематизовані результати тестування та проведено їх порівняльний аналіз. Для наочності дані представлені у вигляді таблиць та графіків.

1. Порівняння швидкості передачі даних та затримки:

Одними з ключових показників, що визначають комфорт роботи в мережі при використанні засобів анонімізації, є швидкість завантаження (Download), швидкість віддачі (Upload) та мережева затримка (Ping). Вимірювання цих параметрів проводилися за допомогою утиліти speedtest-cli та iperf3. Усереднені результати для

кожного досліджуваного засобу, а також для контрольного вимірювання (без анонімізації), представлені нижче (таблиця 3.1).

Таблиця 3.1 – Порівняльні показники швидкості передачі даних та затримки

Засіб анонімізації	Швидкість завантаження (Mpbs)	Швидкість вивантаження (Mbps)	Затримка (ms)	Пропускна здатність (Mbps)
Контрольний тест	37,15	29,33	39,91	37,07
OpenVPN	20,47	20,61	48,9	25,0
SOCKS5	34,12	28,01	41,02	33,2
HTTP/S	33,21	26,71	45,10	36,7
SSH тунель	28,85	25,93	42,18	32,1

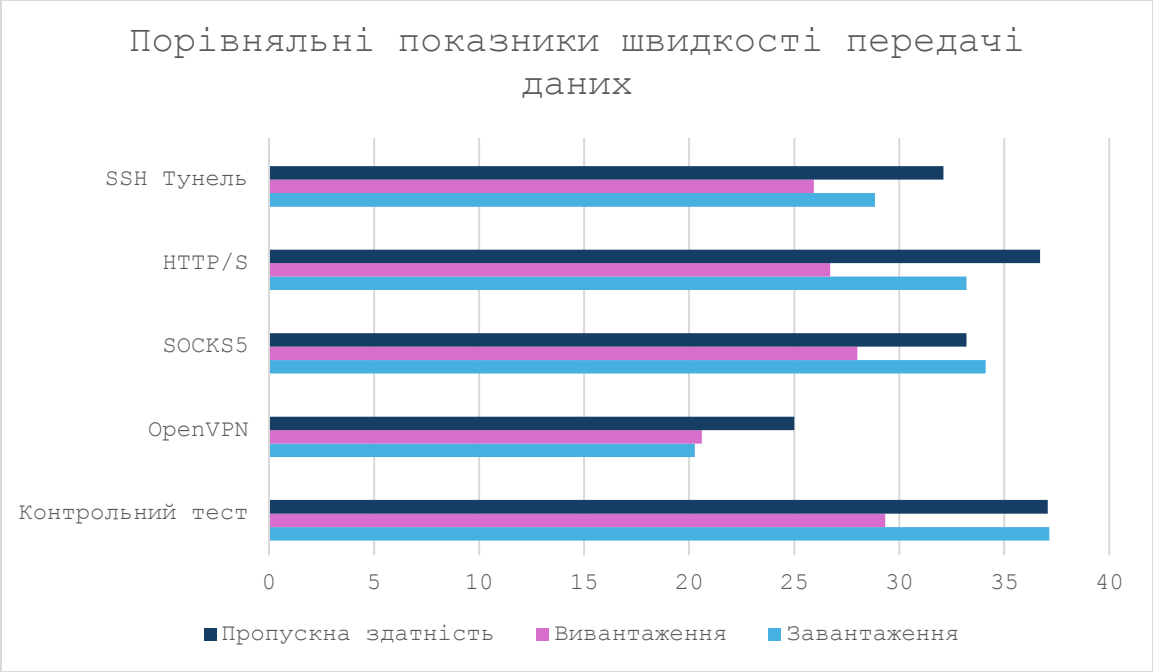

Рисунок 3.1 - Порівняльні показники швидкості передачі даних

Аналіз даних, представлених у вище, дозволяє зробити наступні висновки щодо

впливу засобів анонімізації на швидкісні характеристики інтернет-з’єднання.

Як і очікувалося, контрольний тест без використання засобів анонімізації демонструє найвищі показники швидкості завантаження 37,15 Mbps) та віддачі 29,33 Mbps), а також найнижчу затримку (39,91 ms). Ці значення слугують еталоном для оцінки накладних витрат, що вносяться кожною з досліджуваних технологій.

При використанні OpenVPN, спостерігається помітне зниження швидкості передачі даних, Швидкість завантаження склала 20,47 Mbps, що на 44% нижче контрольного показника, а швидкість віддачі – 20,61 Mbps (зниження на 8,72 Mbps). Затримка при цьому зросла до 48,9 ms.

SOCKS5 проксі продемонстрував відносно високі швидкісні показники. Швидкість завантаження склала 34,12 Mbps (приблизно 91,8% від контрольного значення), а віддачі – 28,01 Mbps (приблизно 95,5% від контрольного значення). Затримка при використанні SOCKS5 проксі була на рівні 41,02 ms, що лише незначно вище контрольного показника. Тест iperf3 показав пропускну здатність 33,2 Mbps. Такі результати можна пояснити тим, що протокол SOCKS5 сам по собі не здійснює шифрування трафіку, тому накладні витрати є мінімальними

Для HTTP/HTTPS проксі швидкість завантаження становила 33,21 Mbps, швидкість віддачі – 26,71 Mbps, а затримка – 45,10 ms. Пропускна здатність за даними iperf3 склала 36,7 Mbps. Ці показники є дещо гіршими за SOCKS5 за швидкістю віддачі та затримкою, але демонструють високу пропускну здатність за iperf3, навіть вищу, ніж у SOCKS5, що може свідчити про ефективність реалізації проксі-сервера Squid для певних типів TCP-трафіку або менші накладні витрати самого proxychains при тестуванні iperf3 через HTTP проксі.

Використання SSH-тунелю в режимі SOCKS-проксі (створеного командою ssh -D) призвело до швидкості завантаження 28,85 Mbps та віддачі 25,93 Mbps. Затримка при цьому склала 42,18 ms. Тест iperf3 показав пропускну здатність на рівні 32,1 Mbps. Порівняно з "чистим" SOCKS5 проксі, SSH-тунель вносить додаткові накладні витрати на SSH-шифрування, що пояснює нижчі швидкісні показники (швидкість

завантаження приблизно на 15,4% нижча, ніж у SOCKS5, а швидкість віддачі – приблизно на 7,4% нижча). Однак, ці показники все ще можуть бути прийнятними для багатьох завдань, враховуючи високий рівень безпеки, що забезпечується SSH, і вони значно кращі, ніж у OpenVPN.

Отже, за критеріями швидкості передачі даних та мінімальної затримки, найменший вплив на з'єднання має SOCKS5 проксі (за умови відсутності додаткового шифрування), зберігаючи понад 90% вихідної швидкості. HTTP/HTTPS проксі також демонструє хороші показники, особливо за пропускною здатністю iperf3. Технології, що передбачають шифрування (OpenVPN, SSH-тунель), очікувано вносять більші накладні витрати, причому OpenVPN демонструє найбільше зниження продуктивності за швидкістю speedtest-cli. SSH-тунель, забезпечуючи шифрування, пропонує компромісний варіант між швидкістю SOCKS5 та безпекою OpenVPN.

2. Порівняння продуктивності веб-доступу:

Окрім загальної швидкості інтернет-каналу, важливим аспектом для користувачів є реальна продуктивність при доступі до веб-ресурсів. Цей параметр оцінювався за допомогою двох показників: часу повного завантаження стандартизованої тестової веб-сторінки та продуктивності веб-сервера при доступі через засоби анонімізації, виміряної утилітою ab (Apache Benchmark). Усереднені результати тестування представлені нижче (таблиця 3.2).

Таблиця 3.2 – Результати порівняння веб-доступу

Засіб анонімізації	Час завантаження сторінки (мс)	Кількість запитів на секунду (req/s)	Середній час на запит (ms/req)
Контрольний тест	19	114,49	8,734
OpenVPN	27	109,23	9,155
SOCKS5	20	122,29	8,138
HTTP/S	21	123,13	8,155
SSH тунель	24	117,24	8,891

Рисунок 3.2 – Діаграма часу завантаження сторінки

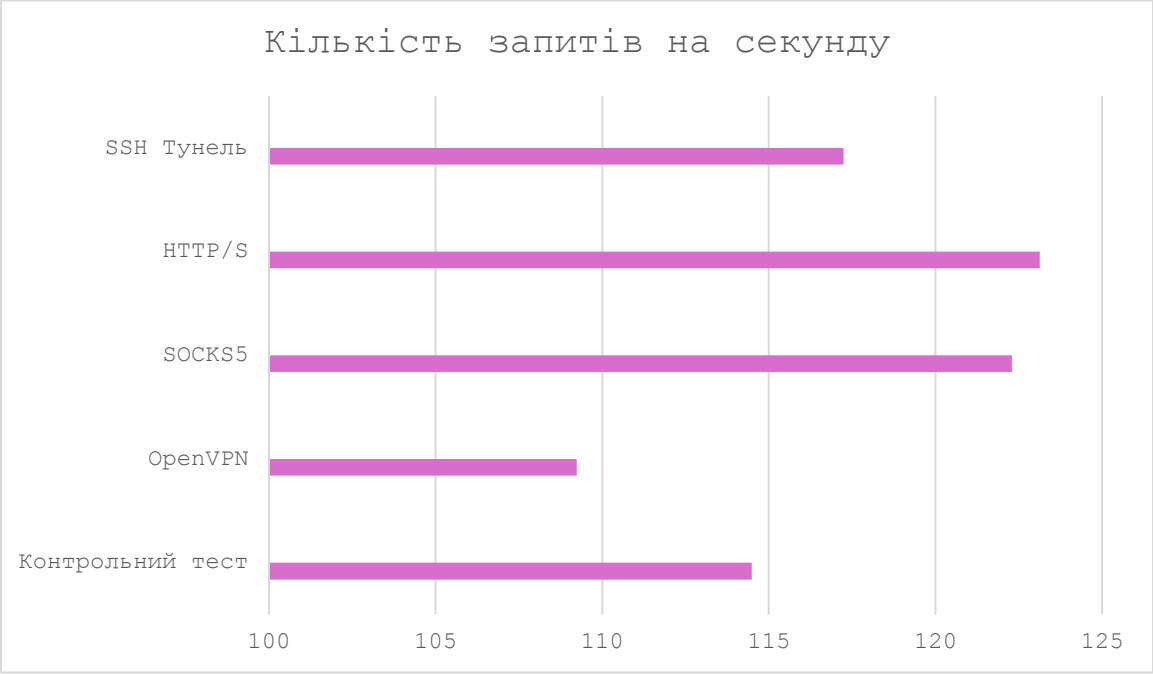

Рисунок 3.3 – Діаграма кількості запитів на секунду

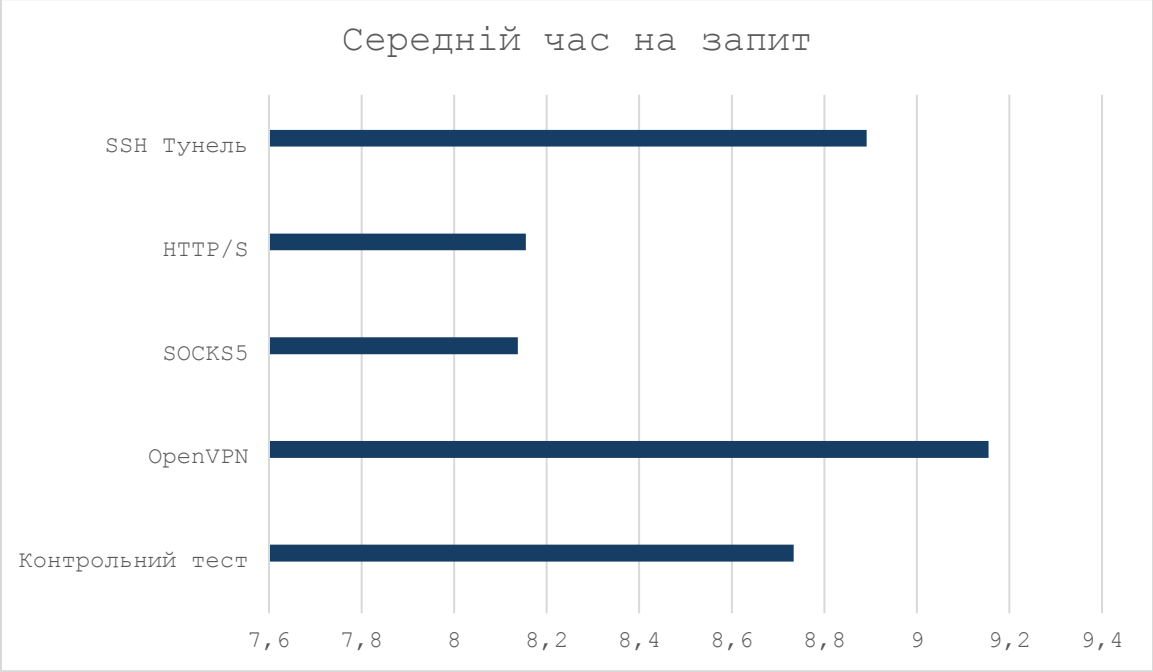

Рисунок 3.4 – Діаграма середнього часу запиту

Аналіз показників продуктивності веб-доступу, наведених вище (таблиця 3.2) та на візуалізованих вище Рисунках (рисунок 3.2, рисунок 3.3, рисунок 3,4), дозволяє оцінити вплив досліджуваних засобів анонімізації на швидкість взаємодії з веб-сервісами.

Контрольний тест, проведений без використання засобів анонімізації, очікувано показав найкращі результати: час завантаження тестової веб-сторінки склав 19 мс, а утиліта ab зафіксувала 114,49 запитів на секунду при середньому часі на запит 8,734 мс. Ці значення слугують базовими для порівняння.

При використанні OpenVPN, час завантаження тестової сторінки збільшився до 27 мс, що на 42,1% більше порівняно з контрольним тестом. Це свідчить про помітний вплив на швидкість рендерингу веб-контенту. Продуктивність, виміряна ab, знизилася до 109,23 запитів/с (на 4,6% менше), а середній час на запит зріс до 9,155 мс (на 4,8% більше). Це узгоджується з результатами тестів швидкості з попереднього підрозділу і підтверджує, що накладні витрати OpenVPN, пов’язані з шифруванням та тунелюванням, суттєво впливають на швидкість обробки веб-запитів.

SOCKS5 проксі продемонстрував результати, найбільш наближені до контрольного тесту, а за показниками ab навіть дещо його перевершив. Час завантаження сторінки склав 20 мс (збільшення на 5,3%). Утиліта ab зафіксувала 122,29 запитів/с (збільшення на 6,8% порівняно з контролем) при середньому часі на запит 8,138 мс (зменшення на 6,8%). Такі високі показники пояснюються мінімальними накладними витратами самого протоколу SOCKS5, який не виконує шифрування трафіку за замовчуванням. Незначне перевищення показників ab над контрольним тестом може бути пов’язане з особливостями мережевої взаємодії або незначними флуктуаціями умов тестування, однак загалом свідчить про дуже низький вплив SOCKS5 на продуктивність.

Результати для HTTP/HTTPS проксі також виявилися дуже близькими до контрольних та SOCKS5. Час завантаження сторінки становив 21 мс (збільшення на 10,5% відносно контролю). Кількість запитів на секунду за даними ab склала 123,13 (збільшення на 7,5%), а середній час на запит – 8,155 мс (зменшення на 6,6%). Це свідчить про високу ефективність HTTP/HTTPS проксі для веб-доступу, особливо якщо враховувати потенційні можливості кешування, хоча в даному тесті з простою статичною сторінкою цей фактор міг не відіграти значної ролі.

SSH-тунель, що функціонував як SOCKS-проксі, продемонстрував час завантаження сторінки 24 мс (збільшення на 26,3% відносно контролю). Продуктивність за тестами ab склала 117,24 запитів/с (збільшення на 2,4%), при середньому часі на запит 8,891 мс (збільшення на 1,8%). Ці показники є кращими за OpenVPN, але дещо поступаються "чистим" SOCKS5 та HTTP/HTTPS проксі. Це відображає вплив шифрування, яке забезпечується SSH-протоколом, на загальну продуктивність, хоча цей вплив виявився менш значним, ніж у випадку OpenVPN для даного типу навантаження.

Загалом, за критерієм продуктивності веб-доступу, найменший негативний вплив демонструють SOCKS5 проксі та HTTP/HTTPS проксі, які за деякими показниками навіть незначно перевершили контрольний тест. OpenVPN, як

технологія з більш інтенсивним шифруванням та тунелюванням, суттєвіше знижує швидкість завантаження сторінок та обробки запитів. SSH-тунель займає проміжне положення, забезпечуючи надійне шифрування при помірному впливі на продуктивність веб-доступу.

3. Оцінка рівня анонімності та безпеки:

Ключовим призначенням засобів анонімізації є захист приватності користувача шляхом приховування його реальної ідентифікаційної інформації та шифрування трафіку. Оцінка рівня анонімності та безпеки досліджуваних засобів проводилася за трьома основними аспектами: здатність маскувати реальну IP-адресу клієнта, наявність або відсутність DNS-витоків, а також характер використовуваного шифрування трафіку. Результати перевірок систематизовано (таблиця 3.3).

Таблиця 3.3 – результати оцінки рівня анонімності

Засіб анонімізації	Маскування IP	DNS-витоки	Тип шифрування
Контрольний тест	Ні	Так	Відсутнє
OpenVPN	Так	Ні	AES-256-GCM
SOCKS5	Так	Ні	Ні
HTTP/S	Так	Так	HTTPS
SSH тунель	Так	Ні	Шифрування SSH

Усі протестовані засоби анонімізації – OpenVPN, SOCKS5 проксі, HTTP/HTTPS проксі та SSH-тунель – успішно впоралися із завданням маскування реальної IP-адреси клієнта. При перевірці на спеціалізованому онлайн-сервісі (ipleak.net) у всіх випадках відображалася IP-адреса віртуального приватного сервера, на якому були розгорнуті відповідні сервіси, а не реальна IP-адреса клієнтської машини. Це підтверджує базову функціональність усіх обраних технологій щодо приховування основного ідентифікатора користувача в мережі.

Щодо наявності DNS-витоків, результати виявилися різними для досліджуваних засобів. OpenVPN продемонстрував відсутність DNS-витоків. Це свідчить про те, що при коректному налаштуванні клієнта OpenVPN усі DNS-запити спрямовуються через зашифрований VPN-тунель, використовуючи DNS-сервери, визначені конфігурацією VPN-сервера. Аналогічно, SOCKS5 проксі та SSH-тунель (SOCKS) у ході тестування також не показали DNS-витоків. Це вказує на те, що використані клієнтські програми (зокрема, веб-браузер) були належним чином налаштовані на передачу DNS-запитів через відповідний SOCKS-проксі. На відміну від них, при використанні HTTP/S проксі було зафіксовано DNS-витоки. Це означає, що DNS-запити відправлялися до DNS-серверів локального інтернет-провайдера клієнта, оминаючи проксі-сервер, що може розкривати інформацію про відвідувані користувачем ресурси, незважаючи на маскування IP-адреси для HTTP/S трафіку.

Щодо типу шифрування трафіку, тут також спостерігаються суттєві відмінності. OpenVPN забезпечує надійне наскрізне шифрування всього трафіку між клієнтом та VPN-сервером, використовуючи сучасний симетричний шифр AES-256-GCM в рамках протоколу SSL/TLS. Це захищає дані як від прослуховування на шляху до VPN-сервера, так і від інтернет-провайдера.

SSH-тунель також гарантує високий рівень безпеки, оскільки весь трафік, що проходить через тунель (включаючи трафік SOCKS-проксі), шифрується за допомогою стійких алгоритмів, властивих протоколу SSH.

SOCKS5 проксі, як і очікувалося, за замовчуванням не забезпечує шифрування трафіку. Безпека переданих даних повністю залежить від того, чи використовує шифрування сам прикладний протокол. Якщо через SOCKS5 передається незашифрований трафік, він залишається вразливим.

Для HTTP/S проксі шифрування застосовується лише для HTTPS-трафіку. При доступі до HTTPS-сайтів через HTTP-проксі з використанням методу CONNECT (або при використанні HTTPS-проксі), встановлюється зашифрований SSL/TLS тунель між клієнтом та кінцевим веб-сервером. Однак, якщо доступ здійснюється до

звичайного HTTP-сайту, трафік не шифрується. Також варто зазначити, що початковий запит CONNECT до проксі-сервера може містити ім’я хоста цільового HTTPS-сайту у відкритому вигляді.

Таким чином, за критеріями комплексного забезпечення анонімності та безпеки (маскування IP, відсутність DNS-витоків за умови правильного налаштування, надійне шифрування всього трафіку) найкращі результати демонструють OpenVPN та SSH-тунель. SOCKS5 проксі, хоча й показав відсутність DNS-витоків у даному експерименті (завдяки налаштуванням клієнта), не забезпечує шифрування трафіку самостійно. HTTP/HTTPS проксі шифрує лише HTTPS-трафік і був схильний до DNS-витоків.

4. Суб’єктивна оцінка складності налаштування та використання:

Окрім об’єктивних технічних показників, важливим фактором, що впливає на вибір засобу анонімізації, є простота його налаштування та зручність повсякденного використання, особливо для користувачів без глибоких технічних знань. У ході проведення експерименту було проведено суб’єктивну оцінку цих аспектів для кожного досліджуваного засобу за 5-бальною шкалою, де 1 бал відповідає дуже високій складності, а 5 балів – дуже високій простоті та зручності. Результати оцінки представлено (Таблиця 3.4).

Таблиця 3.4 – Результати суб’єктивної оцінки складності налаштування

Засіб анонімізації	Складність налаштування сервера	Складність налаштування клієнта	Зручність повсякденного використання	Коментар
OpenVPN	3	4	4	Налаштування сервера за допомогою скрипта значно спрощує процес.

Продовження таблиці 3.4

SOCKS5	3	4	4	Налаштування Dante вимагає редагування конфігураційного файлу
HTTP/S	2	4	4	Конфігурація Squid може бути досить складною через велику кількість опцій та необхідність розуміння ACL для безпечного налаштування. Налаштування клієнта просте.
SSH тунель	5	3	3	Сервер SSH зазвичай вже налаштований на VPS. Створення тунелю на клієнті – одна команда, але потребує розуміння роботи з терміналом та SSH.

Аналіз суб’єктивних оцінок складності налаштування та зручності використання дозволяє зробити висновки щодо доступності досліджуваних технологій для різних категорій користувачів.

Отримані в ході експериментального дослідження результати є достатньою

емпіричною базою для проведення їх глибокого порівняльного аналізу, формулювання обґрунтованих загальних висновків щодо переваг та недоліків кожного із засобів, а також для розробки практичних рекомендацій щодо їх вибору залежно від потреб користувача, що буде представлено у заключній частині кваліфікаційної роботи.

ВИСНОВОК

У кваліфікаційній роботі було розглянуто актуальне завдання порівняння ефективності поширених засобів анонімізації трафіку користувача з метою надання обґрунтованих рекомендацій щодо їх вибору.

У процесі досягнення поставленої мети дослідження було виконано наступні завдання:

1. Проведено аналіз предметної галузі, в рамках якого розглянуто сучасні загрози приватності в мережі Інтернет, основні методи збору даних та принципи роботи популярних засобів анонімізації, таких як OpenVPN, SOCKS5 проксі, HTTP/HTTPS проксі та SSH-тунелі. Це дозволило визначити ключові аспекти, що впливають на їхню ефективність
2. Розроблено та обґрунтовано методику дослідження, що включає визначення критеріїв оцінки ефективності (швидкість передачі даних, затримка, продуктивність веб-доступу, рівень анонімності та безпеки, складність налаштування та використання) та вибір відповідного інструментарію для проведення експериментальних вимірювань.
3. Налаштовано тестове середовище та розгорнуто досліджувані засоби анонімізації, що забезпечило контрольовані умови для проведення експериментів.
4. Проведено експериментальне тестування обраних засобів анонімізації за визначеними критеріями, в результаті чого отримано масив емпіричних даних.

На основі проведеного експериментального дослідження та аналізу отриманих результатів встановлено суттєві відмінності в ефективності досліджуваних засобів анонімізації. Щодо швидкості передачі даних та продуктивності веб-доступу, найменший негативний вплив продемонстрували SOCKS5 проксі та HTTP/HTTPS проксі, показники яких були найбільш наближені до контрольних. Натомість,

OpenVPN, особливо при використанні протоколу TCP, вносив найбільші накладні витрати. SSH-тунель показав компромісну продуктивність, поєднуючи шифрування з помірними втратами швидкості.

У контексті рівня анонімності та безпеки, всі досліджувані засоби успішно маскували реальну IP-адресу клієнта. Однак за критеріями комплексного забезпечення безпеки, включаючи запобігання DNS-витокам та надійне шифрування всього трафіку, найкращі результати показали OpenVPN та SSH-тунель. SOCKS5 проксі не забезпечує шифрування за замовчуванням, а HTTP/HTTPS проксі шифрує лише HTTPS-трафік і продемонстрував схильність до DNS-витоків. Щодо складності налаштування та використання, найпростішим у розгортанні серверної частини виявився SSH-тунель, тоді як конфігурація HTTP/HTTPS проксі (Squid) вимагала найбільшої технічної підготовленості.

Таким чином, мета дипломної роботи – здійснити порівняльний аналіз ефективності обраних засобів анонімізації трафіку користувача та розробити рекомендації щодо їх вибору – досягнута.

На основі отриманих результатів сформульовано практичні рекомендації. Користувачам, для яких пріоритетом є максимальний рівень безпеки, рекомендується використовувати OpenVPN або SSH-тунель. Якщо ж критично важливою є висока швидкість передачі даних при менш жорстких вимогах до шифрування, прийнятними варіантами можуть бути SOCKS5 проксі (бажано в поєднанні з SSH для шифрування) або HTTP/HTTPS проксі. Підкреслено, що вибір конкретного засобу анонімізації завжди повинен базуватися на індивідуальному аналізі потреб користувача, моделі загроз та готовності йти на компроміс між безпекою, швидкістю та зручністю.

Результати даної кваліфікаційної роботи можуть бути корисними для широкого кола користувачів при виборі засобів захисту своєї приватності в мережі Інтернет, а також для системних адміністраторів та фахівців з кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cadwalladr, C., Graham-Harrison, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
2. Confessore, N. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. URL: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
3. Freedom House. Freedom on the Net Report (2025) URL: https://freedomhouse.org/report/freedom-net
4. Solove, D. J. Understanding Privacy. Harvard University Press.
5. Al-Fuqaha, A., Guibene, W., Ayyash, M., & Mohammed, A. Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials URL: https://www.researchgate.net/publication/279177017_Internet_of_Things_A_Survey_on_Enabling_Technologies_Protocols_and_Applications
6. OWASP. Man-in-the-Middle Attack (MitM). URL: https://owasp.org/www-community/attacks/Man-in-the-middle_attack
7. Pfitzmann, A., Hansen, M. Anonymity, unobservability, and pseudonymity-A proposal for terminology. In Designing privacy enhancing technologies URL: https://www.researchgate.net/publication/221331797_Anonymity_Unobservability_and_Pseudonymity_-_A_Proposal_for_Terminology
8. Diwen Xue, Reethika Ramesh, Arham Jain. OpenVPN is Open to VPN Fingerprinting URL: https://dl.acm.org/doi/full/10.1145/3618117
9. Egelman, S., & Schechter, S. (2013). The prices of anominity: an Top and I2P estimate. In Proceedings of the 22nd USENIX Security Symposium URL:

https://www.researchgate.net/publication/327445307_An_Empirical_Study_of_the_I2P_Anonymity_Network_and_its_Censorship_Resistance

10. Peter Membrey Shedding Light on Hidden Dangers: A New Perspective on DNS Leaks URL: https://www.researchgate.net/publication/379592272_Shedding_Light_on_Hidden_Dangers_A_New_Perspective_on_DNS_Leaks

Додаток А. Вміст конфігураційних файлів

Файл Danted.conf

```
logoutput: /var/log/danted.log
internal: eth0 port = 1080
external: eth0

method: none

client pass {
        from: 0.0.0.0/0 to: 0.0.0.0/0
        log: connect error
}
pass {
        from: 0.0.0.0/0 to: 0.0.0.0/0
        protocol: tcp udp
        log: connect error
```

Файл squid.conf

```
# /etc/squid/squid.conf

# Порт, на якому Squid буде приймати з’єднання
http_port 3128

# === Access Controls (ACLs) ===
# Стандартні ACL для визначення безпечних портів та методу CONNECT
acl SSL_ports port 443
acl Safe_ports port 80

acl CONNECT method CONNECT

# Дозволяємо доступ з localhost
acl localhost src 127.0.0.1/32 ::1
http_access allow localhost

# === ДОЗВІЛ ДОСТУПУ ДЛЯ ТЕСТУВАННЯ ===
acl all_sources src 0.0.0.0/0
http_access allow all_sources


# === Налаштування кешу ===
```

```
sudo mkdir -p /var/spool/squid; sudo chown proxy:proxy
/var/spool/squid; sudo squid -z
cache_dir ufs /var/spool/squid 100 16 256

# Розмір об’єктів, що зберігаються в оперативній пам’яті (RAM)
cache_mem 64 MB

# === Налаштування логування ===
access_log daemon:/var/log/squid/access.log squid

cache_effective_user proxy
cache_effective_group proxy
```