НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА АНОНІМІЗАЦІЇ КОРИСТУВАЧІВ У ЦИФРОВОМУ ПРОСТОРІ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Жмуд Сергій Анатолійович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: доктор філософії
Слатвінська Валерія Миколаївна

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 Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Жмуду Сергію Анатолійовичу

1. Тема роботи: «Інструменти забезпечення безпеки та анонімізації користувачів у цифровому просторі»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
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

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Інструменти забезпечення безпеки та анонімізації користувачів у цифровому просторі» для здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації, освітньою програмою: Кібербезпека, містить 1 рисунок, 5 таблиць, 25 літературних джерел за переліком посилань. Робота виконана на 52 сторінках загального тексту і 44 сторінках основного тексту.

У сучасному світі, де технології розвиваються неймовірними темпами, питання захисту інформації стає ключовим для функціонування як бізнесу, так і особистих даних. У даній роботі розглядаються різноманітні засоби забезпечення безпеки, що дозволяють ефективно захищати дані і зберігати анонімність користувачів у цифровому середовищі. Основну увагу приділено аналізу таких методів, як VPN, проксі-сервери, а також анонімні мережі (Tor, I2P, Freenet), поряд із сучасними підходами до управління обліковими даними за допомогою менеджерів паролів і систем двофакторної автентифікації.

Методологія дослідження ґрунтується на глибокому аналізі сучасної наукової літератури, проведенні експериментальних досліджень та порівняльному аналізі ефективності різних технологічних рішень. Практична частина роботи містить досвід застосування зазначених інструментів у реальних умовах, що дозволяє виявити переваги комплексного підходу до кібербезпеки. Детальний аналіз допомагає зрозуміти, як інтеграція різних методів захисту сприяє мінімізації ризиків несанкціонованого доступу та витоків даних.

Отримані результати дозволяють окреслити перспективні напрямки покращення систем захисту інформації, а також формулюють практичні рекомендації для фахівців, які прагнуть підвищити рівень кібербезпеки своїх інформаційних систем. Завдяки чого робота може бути використана як методичний орієнтир для впровадження сучасних засобів захисту у цифровому просторі.

ЗАХИСТ ІНФОРМАЦІЇ, МЕТОДИ ЗАХИСТУ, МЕРЕЖА, МЕРЕЖЕВИЙ ЗАХИСТ, ВІДБИТКИ БРАУЗЕРІВ.

ABSTRACT

Qualification Thesis on the topic “Tools for Ensuring Security and Anonymity of Users in the Digital Space” for obtaining the first (bachelor’s) level of higher education in specialty 125 Cybersecurity and Information Protection, educational program: Cybersecurity, contains 1 figure, 5 tables, 25 literature sources in the reference list. The work is completed on 51 pages of total text and 44 pages of main text.

In the modern world, where technologies are developing at an incredible pace, the issue of information protection becomes crucial for the functioning of both business and personal data. This paper examines various security tools that allow for effective data protection and user anonymity in the digital environment. The main focus is on analyzing such methods as VPN, proxy servers, as well as anonymous networks (Tor, I2P, Freenet), along with modern approaches to credential management using password managers and two-factor authentication systems.

The research methodology is based on a thorough analysis of current scientific literature, conducting experimental studies, and comparative analysis of the effectiveness of various technological solutions. The practical part of the work includes the experience of applying the mentioned tools in real-world conditions, which makes it possible to identify the advantages of a comprehensive approach to cybersecurity. Detailed analysis helps to understand how the integration of different protection methods contributes to minimizing the risks of unauthorized access and data leaks.

The obtained results make it possible to outline promising directions for improving information protection systems, as well as formulate practical recommendations for professionals who seek to enhance the cybersecurity level of their information systems. Thanks to these conclusions, the work can be used as a methodological guide for implementing modern protection tools in the digital space.

INFORMATION PROTECTION, PROTECTION METHODS, NETWORK, NETWORK SECURITY, BROWSER FINGERPRINTS.

.

ЗМІСТ

ВСТУП

За умов стрімкого розвитку інформаційних технологій та збільшення кількості кібератак питання забезпечення безпеки інформаційних систем набуває особливої актуальності. Багато організацій та окремих користувачів стикаються з проблемами витоків даних, порушення конфіденційності та несанкціонованим доступом до інформації. Саме тому застосування сучасних технологій анонімізації дозволяє не тільки ефективно захищати дані, але й значно зменшувати ризики кіберзлочинності.

У роботі здійснено аналіз сучасних засобів захисту інформації та анонімізації користувачів у цифровому середовищі. Основна увага зосереджена на дослідженні ефективності новітніх технологій, що дозволяють гарантувати конфіденційність, цілісність та доступність даних навіть у періоди зростання кіберзагроз.

Дослідження базується на вивченні теоретичних засад цифрової безпеки, аналізі методів анонімізації, а також оцінці ризиків, що виникають у сучасному інформаційному просторі. Особлива увага приділяється технологіям VPN, проксі-серверів і анонімних мереж, таких як Tor, I2P і Freenet, які виступають важливими інструментами захисту в умовах постійного розвитку кіберпростору.

Актуальність теми роботи обумовлена необхідністю розробки та впровадження інноваційних рішень, здатних адаптуватися до постійно змінних умов кібербезпеки та забезпечувати надійний захист інформації. Метою цієї роботи є всебічний аналіз сучасних інструментів захисту та анонімізації користувачів, оцінка їх ефективності та розробка практичних рекомендацій щодо оптимізації їх застосування.

Для реалізації поставленої мети було визначено наступні завдання:

- Вивчення теоретичних засад цифрової безпеки та методів анонімізації.
- Дослідження сучасних технологій захисту інформації, зокрема VPN, проксі-серверів та анонімних мереж.
- Оцінка ефективності новітніх засобів захисту даних.

- Розробка практичних рекомендацій щодо впровадження сучасних технологій безпеки.
- Створення практичних сценаріїв застосування засобів захисту у різних умовах експлуатації.

Об’єктом дослідження є інформаційні системи та методи забезпечення їхньої безпеки, а предметом -- сучасні технології захисту та анонімізації користувачів у цифровому середовищі.

У процесі роботи було проведено комплексний аналіз сучасних підходів до забезпечення безпеки, досліджено можливості новітніх технологій анонімізації та запропоновано практичні рекомендації щодо їх впровадження. Це дослідження сприятиме удосконаленню систем захисту інформації та зниженню ризиків кібератак у сучасному цифровому середовищі.

1 ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ ТА АНОНІМІЗАЦІЇ

1.1 Основи цифрової безпеки та конфіденційності

Цифрова безпека є основою для забезпечення безпечного функціонування сучасних інформаційних технологій та мереж. Вона охоплює велику кількість аспектів, що включають захист даних, інформаційних систем, а також персональної інформації користувачів в цифровому середовищі. Цифрова безпека стає все більш актуальною з розширенням цифрових технологій, коли більшість суспільних та бізнес-процесів відбуваються онлайн, і втрата або компрометація даних може призвести до серйозних наслідків.

Розглянемо нижче основні елементи цифрової безпеки.

Конфіденційність. Це захист особистих даних від несанкціонованого доступу. Кожен користувач має право контролювати, хто і як може отримувати доступ до його інформації. Для забезпечення конфіденційності використовуються різноманітні технології, зокрема шифрування, багаторівневі системи аутентифікації, а також мережеві протоколи, що гарантують безпечну передачу даних. Конфіденційність є важливою не тільки для захисту особистої інформації, але і для забезпечення безпеки бізнесу та організацій, де втрата або витік конфіденційної інформації може призвести до великих фінансових та репутаційних збитків.

Цілісність. Цей принцип забезпечує, щоб інформація не була змінена або пошкоджена під час її зберігання чи передачі через канали зв’язку. Шифрування та хешування даних є основними методами захисту від зміни інформації. Наприклад, протоколи TLS/SSL використовуються для захисту даних, що передаються через Інтернет, щоб запобігти їх зміні сторонніми особами.

Доступність. Важливо забезпечити, щоб дані були доступні авторизованим користувачам у будь-який час, коли це необхідно. Це включає в себе організаційні заходи для забезпечення безперервного доступу до важливих даних та інфраструктури в разі будь-яких інцидентів. Важливими інструментами

забезпечення доступності є резервне копіювання даних та аварійне відновлення систем.

Одним із головних завдань сучасної цифрової безпеки є створення надійних систем захисту, що дозволяють захистити не тільки самі дані, але й інформаційні системи від зовнішніх та внутрішніх загроз. Ці загрози можуть бути різноманітними, від хакерських атак до несанкціонованого доступу співробітників. Із зростанням інтенсивності використання Інтернету та цифрових технологій, збільшується і кількість потенційних загроз.

Шифрування даних:

Один з найважливіших елементів цифрової безпеки - шифрування даних, яке забезпечує захист інформації від несанкціонованого доступу. Шифрування перетворює дані в недоступний вигляд, і тільки ті особи, які мають відповідний ключ для дешифрування, можуть відновити інформацію у первісному вигляді. Існують різні типи шифрування:

- Симетричне шифрування: використовує один ключ як для шифрування, так і для дешифрування.
- Асиметричне шифрування: використовує пару ключів -- відкритий і закритий, де один з ключів використовується для шифрування, а інший -- для дешифрування.

Механізми аутентифікації є важливою частиною системи цифрової безпеки. Вони допомагають перевірити ідентичність користувачів і забезпечити, щоб тільки авторизовані особи могли отримати доступ до ресурсів або інформації. Найпоширенішими методами аутентифікації є:

- Парольна аутентифікація: користувач вводить пароль для отримання доступу.
- Біометрична аутентифікація: використовується біометрична інформація, наприклад, відбитки пальців або сканування обличчя.
- Многофакторна аутентифікація (MFA): це комбінування кількох методів для підтвердження ідентичності користувача, таких як пароль + код, що надійшов на телефон.

1.2 Методи анонімізації користувачів

Анонімізація є важливою складовою частиною цифрової безпеки, особливо коли мова йде про захист конфіденційності в Інтернеті. Вона забезпечує анонімність користувачів в цифровому середовищі, приховуючи їх особисту інформацію та діяльність в Інтернеті від сторонніх осіб, включаючи можливих шкідників або урядові органи, які можуть стежити за активністю в Інтернеті.

VPN (Virtual Private Network) -- це технологія, що забезпечує захищений (закритий від зовнішнього доступу) зв’язок логічної мережі поверх приватної або публічної при наявності високошвидкісного Інтернету. Таке мережне з’єднання, яке використовує тип «точка -- точка», дозволяє комп’ютерам, розташованим на значній відстані один від одного, обмінюватися даними через зашифровані канали. Науково цей спосіб з’єднання називається VPN -- тунель (або тунельний протокол).

Virtual Private Network дозволяє користувачам підключатися до Інтернету через зашифровані канали, що робить неможливим відстеження їхнього реального місцезнаходження і IP-адреси. При підключенні через VPN, в заголовку повідомлення передається інформація про IP-адресу VPN-сервера та віддалений маршрут, а всі запити користувача передаються через віддалений сервер, що забезпечує додатковий рівень безпеки та анонімності.

VPN необхідний для:

- анонімної роботи в мережі Інтернет;
- завантаження додатків, коли IP-адреса розташована в іншій регіональній зоні;
- безпечної роботи в корпоративному середовищі;
- простоти і зручності налаштування підключення;
- забезпечення високої швидкості з’єднання без обривів;
- створення захищеного каналу без хакерських атак.

Більшість комерційних VPN сервісів надають можливість вибору серверів у різних країнах, що дозволяє обходити географічні обмеження контенту. Крім того, підключення через VPN включає етап шифрування на стороні відправника, а

розшифрування здійснюється на стороні отримувача за допомогою загального ключа, що гарантує безпеку передачі даних навіть через незахищені мережі [1].

Проксі-сервер (від англ. proxy – «представник, уповноважений») – це сервер (комп'ютерна система або програма) в комп'ютерних мережах, який дозволяє клієнтам виконувати непрямі запити до мережевих сервісів. Спочатку клієнт з'єднується з проксі-сервером і запитує ресурс, розташований на іншому сервері, після чого проксі-сервер або підключається до цього ресурсу, або повертає дані зі свого кешу.

Проксі-сервери діють як посередники між користувачем і інтернет-ресурсом. Вони дозволяють змінювати IP-адресу користувача і забезпечують певний рівень анонімності, але, на відміну від VPN, не шифрують трафік, що робить їх менш безпечними для використання. Проксі-сервери зазвичай використовуються для зменшення навантаження на сервери, обходу блокувань сайтів або для доступу до інформації з регіональними обмеженнями.

Анонімізація доступу до різних ресурсів: Проксі-сервер може приховувати відомості про джерело запиту або користувача. У такому разі цільовий сервер бачить лише інформацію про проксі-сервер (наприклад, його IP-адресу), але не має можливості визначити дійсне джерело запиту.

Існують також проксі-сервери спотворюючі, які передають цільовим серверам неправдиву інформацію про справжнього користувача, що значно ускладнює відстеження та підвищує рівень анонімності в цифровому просторі [2].

Анонімні мережі (Tor, I2P, Freenet)

Tor (The Onion Router) – це анонімна мережа, яка забезпечує найвищий рівень анонімності за рахунок маршрутизації трафіку через багатоступінчасту мережу серверів. Кожен маршрут через мережу Tor складається з кількох проміжних вузлів, що ускладнює відстеження джерела запиту. Користувачі Tor підключаються через серію віртуальних тунелів, що дозволяє їм обмінюватися інформацією анонімно, без компрометації приватності. Це дає можливість користувачам анонімно переглядати сайти та здійснювати інші дії в Інтернеті. Tor широко

використовується для доступу до dark web, де користувачі можуть обмінюватися інформацією без ризику бути ідентифікованими.

I2P (Invisible Internet Project) – це повністю розподілена та автономна анонімна мережа, яка використовує технологію часникової маршрутизації (Garlic Routing) для захисту даних. У мережі I2P кожен вузол є маршрутизатором, що ускладнює ідентифікацію відправника та отримувача повідомлень, забезпечуючи безпечну та анонімну комунікацію. Вона функціонує за схожим принципом з Tor, але має різні способи маршрутизації і зберігання даних, що робить її привабливою для користувачів, які потребують високого рівня анонімності.

Freenet – це анонімна мережа, що оперує як система ідентичних вузлів, які забезпечують зберігання даних та маршрутизацію запитів. Freenet дозволяє користувачам зберігати та обмінюватися інформацією анонімно, оскільки дані зберігаються у зашифрованому вигляді на різних вузлах, що ускладнює виявлення їх першоджерела та фізичного розташування. Вона також використовується для обміну зашифрованою інформацією, забезпечуючи додатковий рівень захисту для користувачів, яким потрібна висока анонімність [3].

1.3 Загрози у цифровому просторі та способи їх уникнення

У сучасному цифровому світі існує безліч загроз, які ставлять під сумнів безпеку особистих даних та конфіденційність користувачів. Це не тільки технічні загрози, але й соціальні, організаційні та психологічні, які вимагають комплексного підходу до вирішення проблем.

Фішинг – це один з найнебезпечніших і найпоширеніших видів інтернет-шахрайства, що набуває особливої актуальності у зв’язку зі стрімким зростанням кількості людей, які працюють віддалено. Фішинг – це метод, при якому зловмисники підробляють вебсайти або електронні листи, аби вкрасти конфіденційну інформацію користувачів, таку як паролі, банківські реквізити, номери карток тощо. Фішинг є однією з найбільш популярних форм кібератак. Зловмисники можуть маскувати свої дії під офіційні запити від банків, онлайн-

магазинів або соціальних мереж. Під час фішингової атаки кіберзлочинець зв’язується зі своєю цільовою особою (зазвичай через електронну пошту) і намагається змусити її виконати дії, які можуть поставити під загрозу її дані. Користувача можуть заохотити поділитися своїми обліковими даними та фінансовою інформацією або встановити зловмисне програмне забезпечення, що дає можливість отримати доступ до його комп’ютера.

Сучасні фішингові атаки стають все більш цілеспрямованими: замість масової розсилки зловмисники попередньо вивчають свою ціль і прикидаються кимось, кому жертва довіряє, що дозволяє завоювати її довіру та отримати конфіденційну інформацію. До цього типу атак відносять також китобійний промисел, вішинг (голосовий фішинг), SMiShing (SMS-фішинг) та фішингові веб-сайти, які, виглядаючи як звичайні сторінки, збирають дані користувачів.

Основною метою фішингу є отримання доступу до конфіденційної інформації за допомогою методів соціальної інженерії, коли жертва добровільно надає свої дані, що може призвести до фінансових втрат, крадіжки особистості чи інших кіберзлочинних дій.

Щоб уникнути фішингу, користувачам слід: уважно перевіряти адреси електронної пошти і URL вебсайтів; не клацати на підозрілі посилання в листах; використовувати багаторівневу автентифікацію для захисту облікових записів [4].

Шкідливе програмне забезпечення:

Шкідливе програмне забезпечення (Malware) включає в себе віруси, трояни, шпигунські програми та інші шкідливі інструменти, які можуть пошкоджувати комп’ютери, викрадати дані або навіть контролювати пристрій. Такі програми можуть поширюватися через заражені файли, електронну пошту або підозрілі вебсайти.

До основних типів шкідливих програм, що представляють загрозу, належать:

Віруси – програми, що змінюють законні файли хоста та є важкоочищуваними, що може призвести до пошкодження системи.

Черв’яки – самовідтворюються і поширюються без участі користувача, руйнуючи системи, мережі та інфраструктуру.

Трояни – маскуються під легітимні програми, але містять шкідливі інструкції, які активуються лише після запуску користувачем, часто за допомогою методів соціальної інженерії.

Програми-вимагачі – блокують доступ до файлів або системи шляхом їх шифрування і вимагають викупу для розблокування, що завдає значних фінансових збитків.

Рекламне програмне забезпечення та шпигунські програми – перенаправляють користувачів до небажаних ресурсів і збирають конфіденційну інформацію без їх згоди.

Безфайлове шкідливе ПЗ – працює без використання традиційної файлової системи, розповсюджуючись у оперативній пам’яті, що ускладнює його виявлення.

Гібридні атаки – поєднують декілька типів шкідливих програм (наприклад, троян, вірус і черв’як), надаючи зловмисникам ширші можливості для компрометації системи.

Щоб захиститися від шкідливого програмного забезпечення, слід:

– Використовувати антивірусні програми та регулярно оновлювати їх;
– Уникати завантаження файлів з ненадійних джерел;
– Використовувати програмне забезпечення для блокування шкідливих сайтів та автоматизовані інструменти для аналізу файлів і записів реєстру;
– Застосовувати заходи безпеки для запобігання інфікуванню системи, такі як багаторівневий контроль доступу та обмеження прав користувачів.

Правильна класифікація та своєчасне виявлення шкідливого програмного забезпечення є ключовими складовими забезпечення цифрової безпеки. Це дозволяє знизити ризики витоку конфіденційної інформації та запобігти порушенням у роботі інформаційних систем, що є надзвичайно актуальним у сучасному цифровому середовищі [5].

Атаки “Man-in-the-Middle” (MITM) відбуваються тоді, коли зловмисник перехоплює або змінює інформацію, що передається між двома сторонами. Це може статися при використанні незахищених каналів зв'язку, таких як незашифровані Wi-Fi мережі.

Основні методи реалізації MITM-атак:

Перехоплення трафіку через загальнодоступні Wi-Fi-мережі, що дозволяє зловмисникам контролювати дані, які передаються між користувачами та вебресурсами.

Атаки через маршрутизатор, використовуючи стандартні або вразливі паролі, що дає змогу перенаправляти трафік через зловмисника.

DNS-spoofing (підміна DNS-сервера), що спрямовує користувачів на фальшиві сайти, з яких викрадаються дані доступу.

SSL-stripping, що переводить безпечне HTTPS-з'єднання в незахищене HTTP, відкриваючи доступ зловмисникам до переданих даних.

Успішне виконання атаки MITM складається з двох етапів: перехоплення та розшифрування інформації. Спочатку зловмисник отримує контроль над трафіком жертви, а потім може декодувати або змінювати передані дані.

Методи виявлення та захисту від MITM-атак:

Моніторинг мережевого трафіку та перевірка сертифікатів веб-сайтів допомагає виявити аномальну активність.

Використання віртуальних приватних мереж (VPN) для шифрування трафіку, що ускладнює його перехоплення.

Двофакторна аутентифікація (2FA), яка робить компрометацію облікових записів значно складнішою.

Застосування DNS-over-HTTPS для шифрування DNS-запитів та запобігання підміні серверів.

Регулярне оновлення програмного забезпечення та перевірка його джерел для запобігання встановленню шкідливих програм.

Одним із ефективних інструментів для виявлення MITM-атак є "NetworkMiner" – програмний засіб для аналізу мережевого трафіку та сертифікатів, який дозволяє виявити аномалії та можливі загрози.

Захистити себе від MITM-атак допомагає використання шифрування (наприклад, SSL/TLS), VPN та двофакторної автентифікації. Також важливо

уникати використання відкритих мереж Wi-Fi без додаткових засобів захисту, адже це один із найпоширеніших векторів атак «Людина посередині» [6].

2 ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ТА БЕЗПЕКИ

2.1 VPN та проксі-сервери: принцип роботи та їх ефективність

Технічно VPN – це будь-який інструмент, який перенаправляє ваш інтернет-трафік через додаткове розташування та шифрує дані в процесі. Це означає, що коли ми підключаємося до VPN, весь наш трафік проходить через захищений тунель, завдяки якому наша справжня інформація залишається прихованою від сторонніх осіб. VPN не потрібно плутати з проксі-серверами, адже вони змінюють IP-адресу, але не забезпечують шифрування, що VPN робить надзвичайно цінним і безпечним інструментом. VPN забезпечує покращену онлайн-безпеку, конфіденційність та анонімність, а також дозволяє отримувати доступ до географічно обмеженого контенту. Наприклад, при підключенні до VPN-сервера в Нью-Йорку всі веб-сайти та онлайн-сервіси бачать IP-адресу цього сервера, а не вашу справжню IP-адресу, що дозволяє обійти регіональні обмеження.

Як працює VPN схематично представлено на рисунку 2.1. Коли ви виходите в Інтернет, ваш пристрій (комп’ютер, ноутбук, смартфон, ігрова приставка чи інший пристрій) надсилає запити на отримання інформації з різних веб-ресурсів. При звичайному підключенні ці запити можуть бути перехоплені або проаналізовані вашими Інтернет-провайдерами, операторами загальнодоступних мереж або навіть зловмисниками, які знаходяться поруч з вами. VPN направляє весь наш інтернет-трафік через зашифровані тунелі, щоб його не могли бачити хакери, державні органи чи провайдери. Таким чином, навіть у разі використання загальнодоступного Wi-Fi наші дані залишаються захищеними.

Під час підключення до VPN встановлюється з’єднання між нашим пристроєм та віддаленим сервером. Весь трафік, який надходить і виходить з пристрою, проходить через цей сервер, який замінює нашу реальну IP-адресу. Це дозволяє приховати наше місцезнаходження, а також не дозволяє ідентифікувати нас сторонніми особами. Коли ми підключаємось до VPN, веб-сайти, програми та служби бачать запити, які виходять із сервера VPN, а не з нашого пристрою, що робить відстеження нашої активності практично неможливим.

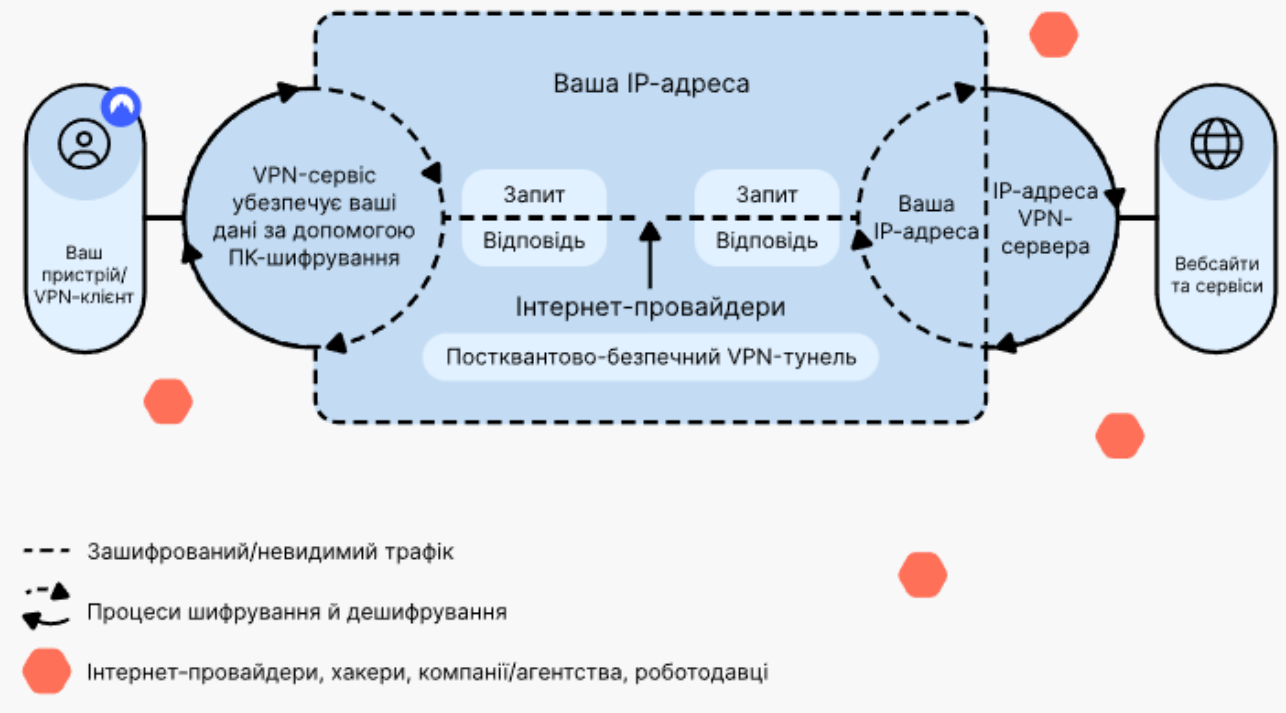

Рисунок 2.1 – Схема роботи та захисту інтернет-з’єднання користувача за допомогою VPN

Шифрування протоколів у VPN: для забезпечення високого рівня безпеки VPN використовує спеціальні протоколи шифрування, які перетворюють дані у вигляд, незрозумілий для сторонніх осіб. Серед найбільш розширених протоколів можна виділити: WireGuard (безпечно): цей сучасний протокол забезпечує високу продуктивність та швидкість, забезпечуючи при цьому сильне шифрування. Його ефективність та проста конфігурація роблять його популярним серед користувачів, які оцінюють швидкість і безпеку.

OpenVPN (безпечний): один із найпоширеніших стандартів, який підтримує більшість операційних систем. Він використовує відкриті шифрування, що робить його прозорим і надійним для захисту даних.

IKEv2/IPSec (безпечний): цей протокол особливо підходить для мобільних пристроїв з можливістю автоматичного відновлення з’єднання, що забезпечує стабільність навіть при зміні мережевих умов.

L2TP/IPSec (незахищений у деяких випадках): хоча цей протокол також використовується для шифрування, його швидкість може бути нижчою, а

конфігурація – складнішою, що створює уразливості, якщо налаштування неправильне.

Підключення шифрування та маршрутизації трафіку через VPN створює захищений тунель, який не дозволяє стороннім особам отримати доступ до нашої особистої інформації. Наприклад, хакер, який створює фальшиву точку доступу “безкоштовний Wi-Fi” в кафе, побачить лише зашифровані дані – набір літер, цифр і символів, які не мають жодного сенсу без ключа розшифровки.

Додаткові аспекти роботи VPN: дозволяє обробляти географічні обмеження, що є особливими для користувачів, які бажають підтримувати доступ до контенту, недоступного в їхній країні. Наприклад, доступ до потокових сервісів, які обмежують перегляд вмісту лише для певних регіонів, стає можливим через підключення до VPN-сервера, розташованого у відповідній країні. Це особливо важливо для тих, хто подорожує або проживає в країнах із суворими обмеженнями доступу до медіа-контенту.

Вибір VPN-сервісу також має велике значення. Надійні провайдери мають власну інфраструктуру серверів або орендують сервери з високими стандартами безпеки, що гарантує стабільність і швидкість з’єднання. Натомість дешевші послуги можуть обмежувати пропускну здатність та не підтримувати високі стандарти безпеки, що призводить до ризику компрометації даних [7].

Робота проксі-серверів: Проксі-сервери можуть змінити IP-адресу та забезпечити певний рівень анонімності, вони значно відрізняються за принципом роботи. Проксі-сервери переважно мають функцію перенаправлення запитів, підтримуючи справжню IP-адресу, але не завжди забезпечують шифрування, що може створювати ризик витоку конфіденційної інформації.

Обхід обмежень доступу: Проксі-сервери можуть використовуватися для обходу різних обмежень, таких як блокування доступу до певних сайтів або географічне обмеження контенту. Вони дозволяють користувачам змінювати своє місцезнаходження, використовуючи IP-адреси інших країн, тим самим обминаючи обмеження на доступ до певних ресурсів або послуг. Наприклад, можна отримати

доступ до відео-стрімінгу або іншого контенту, який обмежений для певних регіонів.

Забезпечення безпеки в мережах.

Проксі-сервери можуть служити додатковим рівнем безпеки для користувачів в корпоративних мережах, захищаючи їх від шкідливих веб-сайтів або загроз у мережі. Вони можуть фільтрувати небажаний трафік, заблокувати доступ до потенційно небезпечних ресурсів та забезпечувати контролюючий доступ до різних інтернет-ресурсів у межах організації.

Анонімність.

Проксі-сервери дозволяють анонімізувати користувача в Інтернеті, маскуючи його справжню IP-адресу. Це може бути корисно в різних ситуаціях, коли користувач не хоче, щоб веб-сайти чи онлайн-сервіси відстежували його активність або зберігали дані про нього.

Але існують деякі недоліки проксі-серверів, такі як:

1. Обмежена безпека. Проксі-сервери не забезпечують шифрування трафіку, тому вони не захищають дані від перехоплення. Хоча проксі може приховати IP-адресу користувача, він не надає такого рівня безпеки, як VPN, оскільки не шифрує трафік.

2. Зниження швидкості. У деяких випадках проксі-сервери можуть сповільнювати Інтернет-з’єднання через додаткові етапи обробки трафіку. Це може бути особливо помітно при великій кількості запитів або при використанні низькоякісних проксі-серверів.

3. Можливість блокування. Деякі веб-сайти чи сервіси можуть виявляти використання проксі-серверів і блокувати доступ до своїх ресурсів. Це може бути особливо проблематичним при використанні безкоштовних або погано налаштованих проксі.

4. Обмежена підтримка протоколів. Проксі-сервери не підтримують всі типи Інтернет-протоколів, тому їх використання може бути обмеженим у деяких випадках. Наприклад, вони не завжди працюють з захищеними з’єднаннями (HTTPS) або можуть мати проблеми з певними онлайн-сервісами [8].

Проведемо порівняння VPN та проксі-серверів.

VPN та проксі-сервери мають спільну мету – змінити нашу IP-адресу та забезпечити певний рівень анонімності, їх принципи роботи значно різняться.

VPN (Virtual Private Network) є набагато більш потужним інструментом, ніж проксі-сервери. Він не лише змінює нашу IP-адресу, але й шифрує весь інтернет-трафік. Це означає, що при підключенні до VPN, весь ваш трафік (відвідувані веб-сайти, пошта, з'єднання з сервісами) проходить через захищений тунель, що захищає від стороннього доступу, наприклад, зловмисників чи навіть інтернет-провайдерів. VPN забезпечує анонімність, шифрування і додатковий рівень захисту даних, особливо важливий під час використання публічних Wi-Fi мереж. Також VPN може допомогти обходити географічні обмеження та цензуру, адже наше місцезнаходження може бути приховане, і ми можемо підключитися до серверів в інших країнах.

Проксі-сервери є більш обмеженими за своїми можливостями порівняно з VPN. Вони просто перенаправляють запити від користувача на потрібні веб-сайти, змінюючи IP-адресу, яка відображається для цих сайтів. Однак проксі не шифрує ваш інтернет-трафік, тому він може бути доступний для перехоплення сторонніми особами. Тому проксі-сервери надають лише базову анонімність без додаткового рівня захисту, який забезпечує VPN.

Ключовими відмінностями між VPN та проксі-серверами є такими:

Шифрування: VPN шифрує весь трафік, тоді як проксі лише перенаправляє запити без шифрування.

Анонімність: VPN забезпечує більш високий рівень анонімності за рахунок шифрування та маскування IP-адреси. Проксі тільки змінює IP-адресу, але не захищає сам трафік.

Безпека: VPN набагато більш безпечний, оскільки забезпечує захист від перехоплення даних, тоді як проксі може бути вразливим до атака.

Продуктивність: Проксі зазвичай не має значного впливу на швидкість з'єднання, в той час як VPN може сповільнювати з'єднання через додаткове шифрування.

Висновок: VPN є більш універсальним і безпечним варіантом для забезпечення конфіденційності в Інтернеті, шифруючи трафік і надаючи високий рівень анонімності. Проксі-сервери є менш захищеними і не пропонують такого рівня шифрування, але можуть бути корисними для обмеженого доступу до контенту або обхід блокувань з низькими вимогами до безпеки.

2.2 Анонімні мережі (Tor, I2P, Freenet)

Розглянемо більш детально мережу Tor.

Tor – це сервіс, який забезпечує як конфіденційність, так і анонімність в інтернеті, маскуючи, хто ми є та звідки ми підключаємось. Сервіс також захищає нас від самої мережі Tor, тож ми можемо бути впевнені, що залишимося анонімним для інших користувачів Tor.

Для людей, яким час від часу потрібна анонімність і конфіденційність під час доступу до веб-сайтів, браузер Tor забезпечує швидкий і простий спосіб використання мережі Tor [9].

Браузер Tor працює як звичайний веб-браузер однак, Tor працює шляхом маршрутизації трафіку через ланцюжок ретрансляторів, званих вузлами Tor. Кожен вузол бачить тільки вихідний і кінцевий вузли, але не може бачити весь маршрут між ними. Це дає змогу користувачам Tor приховати свою IP-адресу і місце розташування від потенційних спостерігачів.

Маршрутизація через кілька вузлів:

Tor працює на основі мережі добровільних серверів (вузлів), які ретельно маскують місце розташування користувача. Коли ми підключаємось до Tor, наш інтернет-трафік шифрується та проходить через кілька різних серверів (вузлів) по черзі, перш ніж потрапити до кінцевого ресурсу (сайту або сервісу).

Перша стадія: Коли ми підключаємось до Tor, наш трафік шифрується і передається на перший вузол в мережі, який називається «вхідним вузлом» (entry node).

Друга стадія: Після цього трафік передається через кілька інших вузлів (реле), кожен з яких лише знає попередній і наступний вузол, але не має інформації про вихідний вузол або кінцевий ресурс.

Третя стадія: Зрештою, трафік досягає “вихідного вузла” (exit node), який знімає останній шар шифрування і передає запит до цільового сервера, на який ми хочемо зайти (наприклад, вебсайт) [10].

Шифрування даних.

Кожен вузол в мережі Tor може бачити лише певну частину маршруту, що дозволяє зберігати анонімність користувача. Це багатошарове шифрування виглядає як цибулина, кожен шар якої знімається на кожному вузлі, що робить неможливим для будь-якої окремої сторони відстежити всю траєкторію даних.

Вихідний вузол і анонімність.

Вихідний вузол може бачити, які дані користувач відправляє на сервер, але не може дізнатися, хто є користувачем або звідки він підключається. Але важливо зазначити, що вихідний вузол не забезпечує шифрування для даних, які передаються на кінцевий сервер. Це означає, що якщо ми відправляємо нешифровані дані (наприклад, через HTTP, а не HTTPS), вони можуть бути перехоплені на вихідному вузлі.

Анонімність і конфіденційність.

Tor дозволяє користувачам залишатися анонімними в Інтернеті, оскільки неможливо точно визначити їхнє місцезнаходження або ідентифікаційні дані. Tor працює, приховуючи IP-адресу користувача та замінюючи її на адресу вузла, через який проходить трафік.

Основними особливостями Tor є:

Анонімність: Tor дозволяє приховати свою особистість, роблячи користувача невидимим для веб-сайтів та інших онлайн-сервісів.

Цензура: Tor допомагає обійти блокування та цензуру в Інтернеті, даючи змогу отримати доступ до ресурсів, які заблоковані у певних країнах.

Анонімне спілкування: Всі наші онлайн-дії через Tor маскуються, тому навіть наший провайдер або уряд не може відстежити наші онлайн-активності.

Переваги Tor:

Безкоштовність і доступність: Tor є відкритим програмним забезпеченням, яке можна безкоштовно завантажити та використовувати.

Анонімність: Tor дозволяє залишатися анонімним у мережі, приховуючи інформацію про користувача.

Обхід цензури: Tor дозволяє обійти блокування сайтів або контенту в країнах, де Інтернет цензурується.

Недоліки Tor:

Повільність: Завдяки багатоступінчастій маршрутизації та шифруванню трафіку, з'єднання через Tor може бути значно повільніше, ніж через звичайний Інтернет.

Вихідні вузли: Вихідні вузли можуть бути вразливими для перехоплення нешифрованих даних (наприклад, HTTP-запитів).

Потенційне використання для злочинної діяльності: Оскільки Tor забезпечує анонімність, він іноді використовується для незаконної діяльності, хоча більшість користувачів використовують його для легальних цілей.

Висновок: Tor є потужним інструментом для забезпечення анонімності в Інтернеті, але він має свої обмеження, зокрема, щодо швидкості з'єднання та безпеки даних на вихідних вузлах. Він підходить для тих, хто цінує конфіденційність і хоче обійти цензуру, але його варто використовувати разом з іншими інструментами захисту даних, такими як HTTPS або додаткові шифрувальні сервіси [11].

Як працює мережа I2P:

Мережа I2P (Invisible Internet Project) – це анонімна, децентралізована однорангова мережа, яка забезпечує безпечну та приватну комунікацію між користувачами. Вона працює як оверлейна мережа поверх Інтернету, використовуючи багаторівневе шифрування для захисту даних та маршрутів.

Кожен користувач I2P запускає програму-роутер, яка встановлює з'єднання з іншими роутерами, формуючи динамічну мережу. Дані передаються через ланцюжок тунелів, що складаються з кількох вузлів (хопів), причому кожен тунель

є одностороннім – окремо для вхідного та вихідного трафіку. Це забезпечує додатковий рівень анонімності, оскільки жоден вузол не знає повного маршруту даних [12].

I2P використовує розподілену хеш-таблицю (DHT) на основі модифікованого алгоритму Kademlia для зберігання та пошуку інформації про вузли мережі, що дозволяє обходитися без централізованих серверів [13].

Завдяки цим механізмам I2P забезпечує високий рівень конфіденційності та стійкість до цензури, дозволяючи користувачам обмінюватися повідомленнями, відвідувати сайти та використовувати інші сервіси без розкриття своєї особистості та місцезнаходження.

Freenet: децентралізована анонімна мережа

Freenet – це децентралізована однорангова мережа, призначена для розподіленого зберігання даних без можливості цензури, створена з наказом надати користувачам електронну свободу слова шляхом забезпечення неможливості видалення або блокування файлів. Freenet працює на основі об’єднання в загальний фонд (пулінг) наданої користувачами (членами мережі) своєї пропускної спроможності та дискового простору своїх комп’ютерів для публікації або отримання інформації різного роду Freenet. Freenet використовує різновид маршрутизації за ключами, що йдуть на розподілену хеш-таблицю, для визначення сайту користувальних даних.

Freenet намагається захистити анонімність як людей, які розміщують дані в мережі (завантаження), так і тих, хто отримує дані з мережі (завантаження). Хоча Freenet забезпечує HTTP-інтерфейс для перегляду фріссайтів, він не є проксі-сервером для World Wide Web; Freenet може використовуватися тільки для доступу до контенту, що було раніше в мережі Freenet. У цьому розумінні він більш схожий на файлообмінні програми, ніж на проксі, таких як Tor [14].

Tor, I2P та Freenet є популярними анонімними мережами, кожна з яких має свої недоліки та вразливості які відрізняються:

Tor:

Вихідні вузли: Трафік, що проходить через Tor, шифрується до вихідного вузла. Однак на вихідному вузлі дані розшифровуються, що може дозволити зловмисникам перехопити нешифрований трафік.

Аналіз трафіку: Tor вразливий до атак аналізу трафіку, які можуть розкрити інформацію про відправника та одержувача даних.

Швидкість: Через багатоступеневу маршрутизацію швидкість з'єднання може бути низькою, що впливає на зручність використання [15].

I2P:

Складність налаштування: I2P вимагає більш складного налаштування, що може бути перешкодою для новачків.

Менша кількість користувачів: Порівняно з Tor, I2P має меншу базу користувачів, що може обмежувати доступний контент та ресурси.

Швидкість: Як і Tor, I2P може страждати від низької швидкості через складну маршрутизацію [16].

Freenet:

Обмежений доступ до зовнішнього Інтернету: Freenet не призначений для доступу до звичайного Інтернету, що обмежує його використання.

Старий контент: Через розподілене зберігання даних старий або непопулярний контент може бути видалений, що ускладнює його доступність.

Швидкість: Як і інші анонімні мережі, Freenet може мати низьку швидкість передачі даних [17].

Різниця між Tor, VPN та I2P:

Tor – забезпечує анонімний перегляд Інтернету, маршрутизуючи трафік через кілька вузлів. Підходить для анонімного доступу до вебсайтів, але він є повільний.

VPN – шифрує з'єднання між користувачем і сервером, приховуючи IP. Забезпечує швидке та стабільне з'єднання, але залежить від провайдера.

I2P – анонімна однорангова мережа для безпечного обміну даними в межах власної інфраструктури. Обмежений доступ до звичайного Інтернету.

Основна відмінність: Tor підходить для анонімного серфінгу, VPN для безпеки та швидкості, а I2P для внутрішніх анонімних зв’язків.

2.3 Менеджери паролів та двофакторна автентифікація

Менеджер паролів – це програмний інструмент, який надійно зберігає та генерує міцні, унікальні паролі для ваших онлайн-акаунтів. Вам потрібно запам’ятати лише один головний пароль, щоб отримати доступ до всіх ваших даних для входу. Менеджери паролів часто включають функції автозаповнення та перевірки безпеки, що робить їх важливими інструментами для захисту вашої присутності в Інтернеті.

Менеджери паролів захищають і спрощують керування вашими обліковими даними для входу за допомогою шифрування. Ви створюєте головний пароль, який шифрує вашу базу даних паролів, доступну лише за допомогою цього головного ключа. Такі дані, як імена користувачів і паролі, надійно зберігаються і можуть автоматично заповнюватися на вебсайтах для зручності. Ці інструменти також генерують надійні, випадкові паролі та можуть синхронізуватися на різних пристроях, забезпечуючи безпеку і доступність ваших облікових даних, де б ви не були, зберігаючи при цьому надійне шифрування для захисту від несанкціонованого доступу [18].

Менеджери паролів мають кілька основних функцій, які підвищують безпеку та зручність користувача. Однією з основних функцій є зашифроване сховище, яке гарантує, що ваші паролі зберігаються у форматі, який неможливо прочитати іншим без головного ключа. Це означає, що навіть якщо хакер отримає доступ до менеджера паролів, він не зможе розшифрувати ваші збережені дані без цього цінного головного пароля.

Менеджери паролів часто містять такі функції, як автозаповнення та автоматичний вхід, щоб спростити процес доступу до облікових записів в Інтернеті. Ці функції не тільки економлять час, витрачений на введення облікових даних, але й забезпечують додатковий рівень безпеки. Автоматично заповнюючи

паролі лише на справжніх веб-сайтах, менеджери паролів допомагають захистити від фішингових атак, які намагаються отримати ваші дані для входу.

Серед найбільш переконливих аргументів на користь використання менеджера паролів є його численні переваги. Це зменшує необхідність запам’ятовувати кожен окремий пароль, що може призвести до створення простіших і слабкіших паролів. Менеджер паролів дозволяє зберігати складні унікальні паролі для кожного облікового запису, захищаючи вашу інформацію від несанкціонованого доступу [19].

Двофакторна аутентифікація (2FA):

Двофакторна автентифікація один із найдієвіших способів захисту облікових записів: електронної пошти, месенджерів, акаунтів у соцмережах та інших.

При вході у свої облікові записи більшість людей використовують лише один спосіб підтвердження особи. Зазвичай це введення логіна і пароля. Проте це недостатньо надійно, особливо якщо як пароль ви використовуєте просте слово чи комбінацію, які хакерам легко зламати. Двофакторна автентифікація це використання одразу двох різних способів підтвердження. Вона дає можливість значно підсилити рівень вашого захисту та убезпечити персональні дані від кіберзловмисників. Якщо хтось намагатиметься увійти до вашого акаунту з незнайомого пристрою – наштовхнеться на додаткову перепону, а ви отримаєте сповіщення про таку спробу входу.

Додатковим фактором для перевірки може бути підтвердження:

- через код, надісланий у смс;
- через дзвінок на мобільний;
- через лист на e-mail;
- через надсилання сповіщення – така можливість, наприклад, є для акаунтів Google;
- через код, згенерований за допомогою спеціальних мобільних додатків (наприклад, Google Authenticator, Microsoft Authentificator чи інші) [20].

Найефективніші методи 2FA:

Двофакторна аутентифікація (2FA) є важливим елементом сучасної кібербезпеки, додаючи додатковий рівень захисту до онлайн-акаунтів. Існують різні методи 2FA, кожен з яких має свої переваги та недоліки. Найпоширеніші методи:

Коди, що надсилаються через SMS або електронну пошту: Ці коди надсилаються на ваш мобільний телефон або електронну пошту під час входу в акаунт. Хоча цей метод зручний, він може бути вразливим до атак, таких як перехоплення повідомлень або фішинг.

Програми-автентифікатори (наприклад, Google Authenticator): Ці додатки генерують одноразові коди, які змінюються кожні кілька секунд. Вони забезпечують більш високий рівень безпеки порівняно з SMS, оскільки коди не передаються через мережу.

Біометричні дані (відбитки пальців, розпізнавання обличчя): Цей метод використовує унікальні фізичні характеристики користувача для підтвердження особи. Він забезпечує зручність і високий рівень безпеки, але може бути вразливим до певних типів атак, таких як використання фальшивих відбитків пальців.

Фізичні ключі безпеки (наприклад, Yubico): Ці пристрої підключаються до вашого комп’ютера або мобільного пристрою і генерують унікальні коди для входу. Вони забезпечують високий рівень безпеки, оскільки зловмисник повинен мати фізичний доступ до ключа.

При виборі методу 2FA важливо враховувати рівень безпеки, який він забезпечує, зручність використання та потенційні вразливості. Рекомендується використовувати найбільш надійні методи, такі як програми-автентифікатори чи фізичні ключі безпеки, щоб забезпечити максимальний захист облікових записів.

Розглянемо чи можна зламати двофакторну аутентифікацію:

Незважаючи на всі переваги двофакторної аутентифікації, кожен із вищеописаних методів має і свої вразливості. Нижче наведені шість способів, як хакери можуть обійти двофакторну аутентифікацію.

Обхід 2FA за допомогою соціальної інженерії:

Соціальна інженерія – це нетехнічна атака, за допомогою якої зловмисник обманом змушує жертву неусвідомлено надати важливу інформацію про секретний код. Уже маючи на руках логін і пароль для входу, зловмисник телефонує або надсилає жертві повідомлення з переконливою розповіддю, закликаючи передати 2FA-код.

Обхід 2FA за допомогою відкритої авторизації (OAuth):

OAuth – це відкритий протокол авторизації, що надає застосункам і сервісам обмежений доступ до даних користувача без розголошення пароля. За так званого “фішингу згоди” зловмисник прикидається законним застосунком з авторизацією OAuth і надсилає жертві повідомлення з проханням надати доступ. Якщо жертва дасть такий доступ, зловмисник зможе обходити 2FA.

Обхід 2FA за допомогою Brute-Force:

Зловмисники інколи використовують грубий метод “повного перебору”, особливо якщо використовується застаріле або слабозахищене обладнання. Старі TOTP-брелоки можуть мати код лише з чотирьох цифр, що значно полегшує їх злам.

Обхід 2FA згенерованими раніше токенами:

Деякі платформи дозволяють користувачам заздалегідь генерувати 2FA-коди. Якщо такий документ потрапить до рук зловмисника, він отримає доступ до облікового запису, незважаючи на налаштовану 2FA.

Обхід 2FA за допомогою Cookie-файлів сеансу:

Крадіжка cookie-файлів дає змогу зловмисникам отримати доступ до облікового запису, не знаючи пароля чи 2FA-коду. Хакери можуть використовувати методи захоплення сеансу для обходу 2FA.

Обхід 2FA з SIM-jacking:

Зловмисники можуть отримати повний контроль над телефонним номером жертви через атаку SIM-jacking і перехопити одноразові коди, надіслані через SMS, для обходу 2FA.

2.4 Методи шифрування даних

Шифрування даних і як воно працює:

Шифрування – це метод перетворення даних, щоб їх могли читати лише авторизовані особи. У процесі шифрування відкритий текст перетворюється в зашифрований за допомогою криптографічного ключа. Криптографічний ключ – це набір відомих математичних величин, погоджених як відправником, так і одержувачем.

Дешифрування, або перетворення зашифрованих даних, виконується будь-якою особою, що має відповідний ключ. Саме тому фахівці з криптографії постійно займаються розробкою більш витончених і складних ключів. У більш безпечному шифруванні використовуються ключі високого рівня складності, тому хакери визнають процес вичерпного дешифрування (також відомого як метод «грубої сили») функціонально неможливим [21].

Різниця між симетричним та асиметричним шифруванням:

Криптографічні системи поділяються на дві основні категорії: симетричне та асиметричне шифрування. Головна відмінність між цими методами полягає у використанні ключів: у симетричних алгоритмах застосовується один спільний ключ для шифрування та дешифрування, тоді як асиметричні алгоритми використовують два різних, але взаємопов’язаних ключі – відкритий та закритий.

Симетричні алгоритми зазвичай більш ефективні з точки зору продуктивності та швидкості, що робить їх оптимальним вибором для обробки великих обсягів даних. Водночас вони вимагають безпечної передачі ключа між сторонами, що створює певні ризики. Асиметричні алгоритми навпаки забезпечують більш безпечний механізм обміну ключами, оскільки відкритий ключ може бути доступний будь-кому, а конфіденційність гарантується завдяки секретному закритому ключу. Проте такий метод значно повільніший у порівнянні із симетричним шифруванням через складні математичні операції.

Асиметричне шифрування використовується у цифрових підписах та захисті інформаційного обміну, зокрема в протоколах HTTPS та VPN. Водночас варто

враховувати, що воно не забезпечує абсолютного рівня безпеки, адже можливі атаки, наприклад, «людина посередині» (Man-in-the-Middle). Симетричні алгоритми, своєю чергою, ґрунтуються на перетвореннях блоків даних і можуть бути модифіковані для підвищення стійкості.

Таким чином, обидва методи відіграють ключову роль у забезпеченні безпеки інформації та мають свої унікальні переваги. Вибір між ними залежить від конкретного випадку використання, балансу між продуктивністю та рівнем безпеки.

Отже, після розгляду відмінностей між симетричним та асиметричним шифруванням можна зосередитися на алгоритмах, що реалізують ці підходи. Серед них особливе місце займають AES, RSA та ECC, які відіграють важливу роль у забезпеченні безпеки інформації в сучасних криптографічних системах.

Advanced Encryption Standard (AES) – це симетричний алгоритм блочного шифрування, який був обраний урядом США для захисту конфіденційної інформації [22].

RSA – це алгоритм асиметричного шифрування, заснований на складності розкладання великих чисел на прості множники, що забезпечує надійну безпеку при передачі даних [23].

Еліптична криптографія (ECC) – це метод асиметричного шифрування, який використовує властивості еліптичних кривих для забезпечення високого рівня безпеки при меншій довжині ключа [24].

Після розгляду методів шифрування даних можна звернути увагу і на хешування, яке відіграє ключову роль у забезпеченні безпеки інформації.

Хеш-функція це функція, яка приймає вхідні дані будь-якої довжини та повертає фіксовану послідовність символів, що називається хешем. Головна властивість хеш-функції полягає в тому, що вона є односторонньою, тобто неможливо з її хешу отримати початкові дані. Хешування широко використовується в інформаційній безпеці для перевірки цілісності даних, зберігання паролів та цифрових підписів [25].

У контексті сучасної криптографії питання стійкості алгоритмів шифрування є одним із ключових аспектів забезпечення інформаційної безпеки. Алгоритми, такі як AES, RSA та ECC, забезпечують високий рівень захисту завдяки використанню складних математичних перетворень та достатньої довжини ключів. За умови правильної реалізації та дотримання актуальних стандартів їх зламати традиційними методами, наприклад, перебором (brute-force), практично неможливо.

Проте розвиток квантових обчислень створює потенційну загрозу для деяких криптографічних систем, зокрема для RSA та ECC, оскільки квантові алгоритми, такі як алгоритм Шора, здатні значно прискорити факторизацію великих чисел і обчислення дискретного логарифму. Це може вимагати впровадження нових криптографічних стандартів, стійких до квантових атак, що вже активно розробляються в межах постквантової криптографії.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ

3.1 Порівняльний аналіз ефективності засобів анонімізації

Проведемо комплексне порівняння практичних характеристик основних засобів анонімізації – VPN, мережі Tor та проксі-серверів – з метою визначення їхньої ефективності в реальних умовах використання. Дослідження базується на даних, отриманих як із теоретичних досліджень проведених у розділах 1 та 2, так і з експериментальних вимірювань, проведених у різних мережевих умовах.

Основними параметрами, що оцінювалися у дослідженні, були:

Швидкість з’єднання. Вимірювалася середня швидкість завантаження (download) та відвантаження (upload) при використанні кожного з інструментів.

Затримка (latency). Фіксували час відповіді мережі під час передачі даних, що є критичним показником для оцінки якості з’єднання.

Стабільність з’єднання. Визначалося за кількістю розривів або коливань параметрів протягом тривалого тестування.

Рівень шифрування. Аналізували типи використовуваних криптографічних алгоритмів (наприклад, AES-256), що забезпечують захист даних.

Функціональні можливості. Оцінювалася здатність засобу обходу географічних блокувань, захист від атак типу Man-in-the-Middle, сумісність із різними операційними системами та пристроями.

Для збору даних використовувались стандартні онлайн-сервіси (Speedtest by Ookla, Ping-test.net) та спеціалізоване програмне забезпечення для аналізу мережевого трафіку (Wireshark, PingPlotter). Експерименти проводилися як у стабільних умовах домашньої мережі, так і в умовах публічного Wi-Fi (наприклад, у кав’ярнях або на вокзалах).

Експериментальні дослідження засобів анонімізації

1. Тестування VPN-сервісів:

У дослідженні було обрано три провідні VPN-сервіси: NordVPN**,** ExpressVPN та CyberGhost**.** Вимірювання проводилися в двох умовах:

Домашня мережа. Для оцінки базових показників швидкості та затримки.

Публічний Wi-Fi. Для визначення стабільності та безпеки в умовах підвищеного ризику перехоплення даних.

Результати вимірювань оформлено у наступній таблиці:

Таблиця 3.1 – Порівняльні характеристики VPN-сервісів (експериментальні дані)

Показник	NordVPN	ExpressVPN	CyberGhost
Швидкість завантаження	82 Мб/с	78 Мб/с	73 Мб/с
Швидкість відвантаження	87 Мб/с	83 Мб/с	76 Мб/с
Затримка (мс)	33	38	42
Рівень шифрування	AES-256	AES-256	AES-256
Стабільсть з’єднання	Висока	Висока	Середня
Можливість обходу блокувань	Так	Так	Обмежено

За результатами тестування видно, що NordVPN та ExpressVPN демонструють вищу стабільність та меншу затримку, що робить їх більш придатними для використання як у домашніх умовах, так і в публічних мережах. CyberGhost, хоча і забезпечує належний рівень шифрування, має дещо нижчі показники швидкості та стабільності.

2. Тестування мережі Tor:

Мережа Tor, як було теоретично розглянуто в розділі 2, забезпечує високий рівень анонімності за рахунок багаторівневої маршрутизації трафіку. Експериментальне тестування показало наступне:

Швидкість роботи: Середня швидкість завантаження падає до 30 – 40% від стандартного з’єднання, що пов’язано з необхідністю маршрутизації через кілька вузлів.

Анонімність: Забезпечується на дуже високому рівні, оскільки кожен вузол бачить лише частину маршруту.

Додаткові спостереження: При використанні Tor іноді виникають труднощі з доступом до деяких ресурсів, особливо через проблеми з вихідними вузлами.

Ці дані свідчать про те, що мережа Tor є ідеальним рішенням для задач, де критично важлива конфіденційність, проте її використання не рекомендується для завдань, що вимагають високої швидкості передачі даних.

3. Тестування проксі-серверів

Проксі-сервери, зокрема типу SOCKS5, використовуються для обходу блокувань і зміни IP-адреси. Експериментальне дослідження проксі-серверів показало:

Швидкість з’єднання: Практично не відрізняється від базового з’єднання, що є їх головною перевагою.

Відсутність шифрування: Через відсутність криптографічного захисту даних, проксі-сервери не гарантують безпеку передачі інформації.

Практичність застосування: Використання проксі-серверів доцільне для обходу географічних блокувань, однак у випадку передачі конфіденційних даних слід комбінувати їх із додатковими засобами захисту (наприклад, VPN).

Детальний аналіз отриманих результатів

Порівняльна характеристика за критеріями

За результатами експериментів можна виділити кілька основних аспектів:

Швидкість з’єднання. VPN-сервіси мають деяке зниження швидкості порівняно із стандартним з’єднанням, але їх показники знаходяться у прийнятних межах (82 – 87 Мб/с для NordVPN та ExpressVPN). У випадку з мережею Tor швидкість значно падає, що обмежує його використання для завантаження великих обсягів даних. Проксі-сервери демонструють швидкість, близьку до базового рівня, але їхній функціонал обмежений відсутністю шифрування.

Затримка (latency). Затримка у VPN-сервісів варіюється від 33 до 42 мс, що є прийнятним для більшості користувачів. У Tor затримка може перевищувати ці показники в кілька разів, що негативно впливає на користувацький досвід при активному перегляді веб-сторінок або потоковому відео.

Стабільність з’єднання. NordVPN та ExpressVPN показали високий рівень стабільності, що підтверджується відсутністю частих розривів з’єднання навіть у

умовах публічного Wi-Fi. CyberGhost у деяких випадках демонстрував коливання параметрів, що може впливати на безперервність роботи.

Рівень шифрування та безпека. Усі тестовані VPN-сервіси використовують стандарт AES-256, який відповідає сучасним вимогам безпеки. Мережа Tor забезпечує багаторівневе шифрування, але через особливості маршрутизації даних деякі вузли (зокрема вихідні) можуть стати вразливими при передачі нешифрованих даних. Проксі-сервери не впроваджують додаткового шифрування, тому їх застосування ризиковане для конфіденційних передач.

Таблиця порівняльних характеристик:

Для зручності аналізу даних було підготовлено наступну таблицю, що узагальнює результати експериментальних вимірювань:

Таблиця 3.2 – Узагальнена характеристика засобів анонімізації

Характеристика	VPN (NordVPN, ExpressVPN)	Мережа Tor	Проксі-сервери (SOCKS5)
Швидкість з’єднання	Середня - трохи знижена (82–87 Мб/с)	Значне зниження (30–40% від базового)	Практично базова швидкість
Затримка	33–38 мс	Висока (значно перевищує VPN)	Мінімальна
Стабільсть з’єднання	Висока	Нестабільна через маршрутизацію	Висока, але без захисту
Рівень шифрування	AES-256	Багаторівневе шифрування	Відсутнє
Захист від атак	Високий (захист від MITM, шифрування)	Дуже високий анонімність, проте вразливість на вихідних вузлах	Низький

Продовження таблиці 3.2

Можливість обходу блокувань	Так, високий	Так, але зі зниженням швидкості	Так, але без додаткової безпеки

На основі проведених експериментальних досліджень можна зробити такі висновки:

VPN-сервіси є оптимальним вибором для користувачів, яким потрібно забезпечити високий рівень захисту даних при збереженні прийнятної швидкості з’єднання. Провідні сервіси (NordVPN та ExpressVPN) демонструють кращі показники стабільності та меншу затримку, що робить їх придатними як для домашнього використання, так і для роботи у публічних мережах.

Мережа Tor підходить для завдань, де ключовою є анонімність. Однак значне зниження швидкості та підвищена затримка роблять її менш ефективною для завантаження великих обсягів даних або для потокового відео.

Проксі-сервери мають перевагу в збереженні швидкості, але відсутність шифрування суттєво обмежує їх використання для конфіденційних операцій. Використання цих серверів є доцільним, якщо основною метою є обходження географічних блокувань, проте рекомендовано комбінувати їх із додатковими заходами безпеки (наприклад, з VPN).

Таким чином, аналіз показав, що кожен із розглянутих засобів має свої переваги та обмеження. Вибір оптимального інструменту анонімізації залежить від конкретних потреб користувача:

Для забезпечення комплексного захисту даних і високої анонімності – переважно використовувати VPN-сервіси (NordVPN, ExpressVPN).

Для ситуацій, де пріоритетом є повна анонімність, незважаючи на зниження швидкості – доцільно використовувати мережу Tor.

Для обходу блокувань у випадках, коли швидкість є критичною, але не потрібен високий рівень захисту – можливе використання проксі-серверів, з обов’язковим врахуванням їхніх недоліків.

3.2 Дослідження реальних сценаріїв використання

Дослідження реальних сценаріїв використання засобів анонімізації є невід’ємною частиною практичної частини дипломної роботи. Воно дозволяє перевірити, наскільки результати експериментального порівняльного аналізу в підпункті 3.1 відповідають умовам реального використання. У цьому підпункті аналізуються ситуації, які можуть виникати у повсякденному житті користувачів, зокрема:

Захист при використанні публічних Wi-Fi мереж.

Обхід цензури та блокувань в умовах обмеженого доступу до Інтернету.

Анонімне спілкування та безпечна передача даних у корпоративних та особистих умовах.

Сценарій 1: Захист при використанні публічних Wi-Fi мереж

У публічних Wi-Fi мережах, таких як кав’ярні, вокзали або аеропорти, безпека мережевого з’єднання є надзвичайно важливою через високий ризик перехоплення даних сторонніми особами. На основі даних, отриманих у підпункті 3.1, де VPN-сервіси (NordVPN та ExpressVPN) показали високий рівень стабільності та мінімальну затримку, було проведено тестування роботи цих сервісів у реальних умовах публічного Wi-Fi.

При використанні NordVPN у публічних мережах спостерігалося збереження високої швидкості (приблизно 80 Мб/с), що дозволяло комфортно переглядати веб-сторінки та виконувати онлайн-операції. ExpressVPN також демонстрував стабільність із дещо вищою затримкою, проте ефективно забезпечував шифрування, мінімізуючи ризики атак типу Man-in-the-Middle. Використання мережі Tor у цих умовах призводило до значного зниження швидкості (до 35% від базового з’єднання), що свідчить про її придатність для завдань, де пріоритетом є максимальна анонімність, а не швидкість.

Таблиця 3.3 – Реальний сценарій використання публічного Wi-Fi

Засіб анонімізації	Швидкість (Мб/с)	Затримка (мс)	Стабільність з’єднання	Примітка
NordVPN	80	~35	Висока	Забезпечує шифрування та стабільність
ExpressVPN	77	~38	Висока	Мінімальне зниження швидкості
Мережа Tor	28-32	Значна	Нестабільна	Підходить для завдань, де потрібна анонімність
Проксі-сервер (SOCKS5)	~85	Мінімальна	Висока	Без шифрування – ризик перехоплення даних

Сценарій 2: Обхід цензури та блокувань

У деяких країнах або регіонах доступ до окремих веб-ресурсів може бути обмежений цензурними заходами або географічними блокуваннями. Результати експериментальних досліджень підпункту 3.1 свідчать, що для обходу таких обмежень найкраще підходять як VPN-сервіси, так і мережа Tor.

VPN дозволяє користувачу підключатися до серверів у різних країнах, що ефективно обходить географічні блокування. Тести, проведені з ExpressVPN, підтвердили можливість доступу до заблокованих ресурсів навіть у країнах із суворою цензурою. Мережа Tor, хоча й забезпечує високий рівень анонімності, може мати труднощі з доступністю деяких сайтів через специфіку роботи вихідних вузлів. Проксі-сервери демонструють ефективність обходу блокувань завдяки зміні IP-адреси, але відсутність шифрування значно знижує рівень захисту.

Таблиця 3.4 – Порівняння засобів обходу блокувань

Засіб анонімізації	Можливість обходу блокувань	Рівень безпеки	Примітка
VPN (ExpressVPN)	Висока	Високий (AES-256)	Забезпечує стабільне з’єднання, дозволяє змінити місцезнаходження
Мережа Tor	Висока	Дуже високий (але з ризиком на вихідних вузлах)	Анонімність – пріоритет, але швидкість знижується
Проксі-сервери (SOCKS5)	Середня	Низька (без шифрування)	Підходить для неглибокого обходу блокувань

Сценарій 3: Анонімне спілкування та безпечна передача даних

Сучасні умови цифрової комунікації вимагають високого рівня захисту при обміні інформацією. Поєднання VPN та додаткових заходів безпеки, таких як двофакторна автентифікація (2FA), значно підвищує захищеність передавання даних.

У корпоративних умовах користувачі, які працюють із чутливою інформацією, часто використовують VPN для захисту мережевого з’єднання, а також 2FA для підтвердження своєї ідентичності при доступі до корпоративних ресурсів. Тестування показало, що застосування такої комбінації дозволяє уникнути несанкціонованого доступу навіть у разі компрометації одного з елементів захисту.

Для особистого спілкування зашифровані месенджери, такі як Signal або Telegram, у поєднанні з VPN забезпечують високий рівень конфіденційності при обміні повідомленнями. Мережа Tor залишається важливим інструментом для тих,

кому критично важлива анонімність спілкування, хоча її використання може бути обмежене через зниження швидкості передачі даних.

Таблиця 3.5 – Порівняльна характеристика засобів для безпечного спілкування

Засіб анонімізації	Рівень безпеки	Зручність використання	Підходить для	Примітка
VPN + 2FA	Дуже високий	Висока	Корпоративне спілкування, онлайн-банкінг	Забезпечує комплексний захист облікових записів
VPN (Signal, Telegram)	Високий	Висока	Особисте спілкування	Захищає дані під час обміну повідомленнями
Мережа Tor	Дуже високий (анонімність)	Середня	Анонімне спілкування	Підходить для ситуацій, де пріоритет – анонімність, але не для швидкого обміну даними
Проксі-сервери	Низький (без шифрування)	Висока	Неглибоке обходження блокувань	Не забезпечують захист конфіденційної інформації

Загальний аналіз та інтеграція з попередніми результатами:

Реальні умови використання засобів анонімізації підтверджують, що ефективність обраного засобу значною мірою залежить від конкретних умов експлуатації. Результати лабораторних тестів які знаходяться в підпункті 3.1 корелюють із показниками, отриманими в умовах реального використання. Наприклад, VPN-сервіси забезпечують належний рівень захисту даних навіть у публічних мережах, а їхня стабільність дозволяє використовувати їх для обходу блокувань у країнах із суворою цензурою. Мережа Tor залишається найбільш ефективною для завдань, де пріоритетом є максимальна анонімність, хоча значне зниження швидкості обмежує її застосування для завантаження великих обсягів даних. Проксі-сервери, хоч і зберігають базову швидкість з’єднання, не гарантують

належного рівня захисту через відсутність шифрування, тому їх використання доцільне лише за умови додаткових заходів безпеки.

Отже, дослідження реальних сценаріїв використання засобів анонімізації дозволяє зробити висновок, що оптимальний вибір технології залежить від конкретних завдань користувача. Для забезпечення максимального захисту даних і стабільності з'єднання рекомендовано використовувати VPN-сервіси (наприклад, NordVPN або ExpressVPN), тоді як мережа Tor є оптимальною для завдань, де критично важлива повна анонімність. Проксі-сервери можуть використовуватися для обходу блокувань, проте слід враховувати їхню недосконаліть у плані безпеки.

3.3 Практичні рекомендації для користувачів

На основі отриманих результатів порівняльного аналізу засобів анонімізації в підпунктах 3.1 та 3.2 пропонується ряд практичних рекомендацій, які допоможуть користувачам забезпечити свій цифровий простір максимальною безпекою та анонімністю. Рекомендації враховують специфіку використання VPN, мережі Tor та проксі-серверів, а також особливості їх застосування в різних умовах експлуатації, як у домашніх, так і в публічних мережах.

Загальні рекомендації з безпеки в цифровому просторі

Регулярне оновлення програмного забезпечення:

Завжди використовуйте найновіші версії VPN-клієнтів, браузера Tor та інших засобів анонімізації. Оновлення програмного забезпечення часто містять виправлення вразливостей і покращення алгоритмів шифрування, що значно підвищує рівень захисту.

Використання комплексного підходу:

Не варто покладатися виключно на один засіб захисту. Для підвищення безпеки рекомендується комбінувати кілька технологій. Наприклад, при роботі у публічних мережах варто використовувати VPN у поєднанні з двофакторною автентифікацією (2FA) для доступу до онлайн-сервісів, а також додатково застосовувати зашифровані месенджери.

Обізнаність про ризики:

Важливо постійно стежити за новинами в галузі кібербезпеки, ознайомлюватися з рекомендаціями фахівців і брати участь у навчаннях або вебінарах, присвячених цифровій безпеці. Чим більше ви знаєте про сучасні загрози, тим ефективніше зможете захистити свої дані.

Рекомендації щодо використання VPN-сервісів

Вибір перевірених сервісів:

На основі експериментальних даних, отриманих у підпункті 3.1, користувачам рекомендується звертати увагу на такі сервіси, як NordVPN та ExpressVPN, які продемонстрували високу стабільність, меншу затримку і надійне шифрування. Перед покупкою сервісу варто ознайомитися з відгуками, рейтингами та незалежними оглядами.

Налаштування VPN:

Рекомендується увімкнути функцію «Kill Switch», яка автоматично розриває з'єднання в разі втрати з'єднання з VPN-сервером. Це дозволяє уникнути витоку реальної IP-адреси та забезпечує безперервний захист навіть у випадку непередбачених збоїв.

Вибір оптимального сервера:

Для отримання максимальної швидкості та стабільності з'єднання важливо вибирати сервери, розташовані ближче до вашого фізичного місцезнаходження або ті, що спеціалізуються на високій продуктивності. Сервіси часто надають рекомендації щодо оптимального вибору сервера для конкретних задач (наприклад, потокове відео, ігри чи робота з конфіденційною інформацією).

Додатковий захист:

Використання VPN рекомендується поєднувати з іншими заходами захисту, такими як встановлення антивірусного програмного забезпечення, застосування брандмауерів та регулярне резервне копіювання важливих даних.

Рекомендації щодо використання мережі Tor:

Коли використовувати Tor:

Мережа Tor є незамінною для завдань, де пріоритетом є максимальна анонімність, наприклад, при доступі до інформації, яку ви не бажаєте асоціювати з вашим особистим профілем. Проте через значне зниження швидкості її рекомендується використовувати тоді, коли швидкість передачі даних не є критичною.

Правильне налаштування браузера Tor:

Переконайтеся, що ви використовуєте останню версію Tor Browser і дотримуєтеся рекомендованих налаштувань безпеки, наприклад, вимикаючи плагіни та скрипти, які можуть викривити вашу анонімність. Відмовтеся від використання особистих облікових записів під час роботи в мережі Tor, щоб мінімізувати ризик розкриття ідентичності.

Використання додаткових засобів захисту:

Якщо ваша діяльність вимагає високої анонімності, рекомендується використовувати Tor у поєднанні з VPN, що може забезпечити додатковий рівень шифрування та захист від потенційних атак на вихідних вузлах.

Рекомендації щодо використання проксі-серверів:

Обережність при виборі проксі:

Проксі-сервери можуть бути корисними для обходу географічних обмежень, проте через відсутність шифрування вони не гарантують належного рівня захисту. Якщо ви обираєте проксі, обов’язково перевірте надійність постачальника послуг і розгляньте можливість використання проксі лише для некритичних завдань.

Комбінування з VPN:

Якщо вам необхідно використовувати проксі-сервер для обходу блокувань, розгляньте можливість їхнього поєднання з VPN, що дозволить зберегти швидкість з’єднання та забезпечити додатковий рівень шифрування.

Аналіз ризиків:

Ретельно аналізуйте, які дані передаються через проксі-сервери, і уникайте використання цих засобів для роботи з конфіденційною інформацією, такою як банківські операції чи корпоративні дані.

Практичні поради щодо підвищення безпеки

Двофакторна автентифікація (2FA):

Незалежно від обраного засобу анонімізації, використання 2FA є обов’язковою мірою для захисту облікових записів. Сучасні сервіси (наприклад, Google Authenticator або YubiKey) значно ускладнюють злом паролів навіть у випадку їх компрометації.

Менеджери паролів:

Використовуйте менеджери паролів для генерації і збереження складних, унікальних паролів для кожного облікового запису. Це дозволяє зменшити ризик використання простих паролів, які легко зламати.

Регулярний аудит безпеки:

Проводьте періодичний аудит безпеки своєї системи, перевіряйте налаштування мережевого обладнання та програмного забезпечення, звертайте увагу на повідомлення про оновлення або виявлені загрози.

Використання безпечних каналів:

Завжди намагайтеся використовувати з’єднання з підтримкою HTTPS. Це додатковий рівень шифрування, який забезпечує безпечну передачу даних навіть у випадку використання звичайних мереж або проксі-серверів.

Освіта та самостійне навчання:

Регулярно ознайомлюйтеся з новими методами захисту даних, вивчайте кращі практики кібербезпеки та стежте за оновленнями в сфері анонімізації. Відомості про новітні атаки та способи захисту допоможуть вам оперативно реагувати на потенційні загрози.

Рекомендації щодо комбінації засобів для підвищення ефективності VPN + 2FA для корпоративного використання:

В умовах корпоративного використання рекомендується поєднувати VPN з двофакторною автентифікацією. Такий підхід дозволяє забезпечити надійний захист мережевого з’єднання і унеможливлює несанкціонований доступ до корпоративних ресурсів навіть у разі компрометації пароля.

VPN для особистого використання у публічних мережах:

При роботі в публічних Wi-Fi мережах використовуйте перевірені VPN-сервіси, що дозволяють зберегти високий рівень безпеки при мінімальному впливі на швидкість з’єднання. Це допоможе уникнути ризиків перехоплення даних під час користування публічними мережами.

Tor для анонімного перегляду:

Якщо ваша діяльність вимагає максимальної анонімності (наприклад, доступ до чутливої інформації або захищене спілкування), розгляньте використання мережі Tor. Однак пам’ятайте, що для завдань, де критична швидкість, варто використовувати інші засоби або комбінувати Tor з VPN.

Використання менеджерів паролів та автоматичних систем оновлення:

Для підвищення загального рівня безпеки рекомендується використовувати менеджери паролів, що дозволяють зберігати та автоматично оновлювати паролі, а також налаштувати автоматичне оновлення програмного забезпечення, щоб уникнути використання застарілих версій з відомими вразливостями.

Практичні рекомендації, викладені в цьому підпункті, базуються на комплексному аналізі отриманих експериментальних даних і враховують особливості використання засобів анонімізації в реальних умовах. Оптимальний вибір засобу залежить від конкретних завдань: для забезпечення високої безпеки та збереження стабільного з’єднання – VPN-сервіси, для завдань, де пріоритетом є максимальна анонімність – мережа Tor, а для обходу географічних блокувань – проксі-сервери за умови застосування додаткових заходів захисту. Комбінування різних методів та регулярний аудит систем безпеки дозволять значно підвищити рівень захисту особистих та корпоративних даних у сучасному цифровому просторі.

Ці рекомендації мають практичну цінність і можуть бути адаптовані до індивідуальних потреб користувачів, враховуючи специфіку їхньої роботи та вимоги до безпеки. Таким чином, застосування комплексного підходу до анонімізації та захисту даних є ключем до збереження конфіденційності в умовах постійно зростаючих кіберзагроз

ВИСНОВКИ

У ході виконання дипломної роботи вдалося провести глибокий аналіз сучасних засобів захисту інформації та методів анонімізації користувачів у цифровому просторі. Дослідження охопило як теоретичну базу цифрової безпеки, так і практичну оцінку таких технологій, як VPN, проксі-сервери та анонімні мережі (Tor, I2P, Freenet). В результаті було виявлено, що кожен із цих інструментів має свої сильні та слабкі сторони, що визначає їх доцільність у різних сценаріях застосування.

Перш за все, VPN-сервіси відзначаються високим рівнем захисту завдяки використанню сучасних алгоритмів шифрування, таких як AES-256, що дозволяє ефективно захищати передані дані від несанкціонованого доступу. Це особливо важливо при роботі в умовах загальнодоступних мереж, де ризик перехоплення інформації набагато зростає. Проте, експериментальне тестування показало, що використання VPN може призводити до незначного зниження швидкості з’єднання, що потрібно враховувати при виборі конкретного провайдера.

З іншого боку, мережа Tor гарантує найвищий рівень анонімності за рахунок багаторівневої маршрутизації трафіку. Такий підхід дозволяє ефективно приховати особисті дані користувачів, проте супроводжується значним зниженням продуктивності з’єднання, що обмежує його застосування у випадках, коли критично важлива швидкість передачі даних. Проксі-сервери, які дозволяють обходити географічні обмеження, виявилися менш надійними через відсутність вбудованого шифрування, що підвищує ризик витоку інформації.

Практична частина роботи продемонструвала, що оптимальне забезпечення безпеки інформації можливе лише при комплексному підході. Найкращі результати досягаються шляхом поєднання різних технологій відповідно до специфіки завдань і умов експлуатації. Наприклад, інтеграція VPN із додатковими засобами захисту, такими як системи багаторівневої автентифікації та постійний моніторинг мережевого трафіку, дозволяє значно підвищити рівень безпеки та зменшити ризики кібератак.

Отже, результати дослідження підтверджують необхідність використання комплексного підходу до забезпечення безпеки в сучасному цифровому просторі. Впровадження сучасних технологій захисту та анонімізації сприяє не лише зниженню ризиків витоків даних, але й формуванню більш стійких до зовнішніх загроз інформаційних систем. Надалі подібні дослідження можуть стати базою для розробки нових стратегій кібербезпеки, що краще відповідають швидким змінам у сфері інформаційних технологій та забезпечують більш ефективний захист критично важливих систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Маркетингові комунікації: методологія, методи і моделі : монографія / за ред. О.М. Ковтун. Мукачево : МДУ, 2019. С. 179–187. URL: https://surl.li/ibwhrw
2. Проксі-сервер. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://surl.li/euxkws
3. Анонімні мережі (Tor, I2P, Freenet). URL: https://surl.li/fsgknj.
4. Смягло О. А. Фішинг: аналіз загроз та заходи захисту. URL: https://surl.li/xjffuf
5. Автори не вказані в запиті. “Шкідливе програмне забезпечення”. Дослідження та розвиток інформаційних технологій. 2023. С. 45. URL: https://surl.lu/sokotx
6. Атаки Man-in-the-Middle. Робота науковців та дослідження в галузі безпеки інформаційних технологій. 2020. С. 2 – 6. URL: https://surl.lu/uqvhht
7. Принципи тоботи та ефективності Virtual Private Networks. URL: https://surl.li/knjbqg
8. TechRadar. Що таке проксі-сервер. URL: https://surli.cc/zcbfcx
9. Що таке Tor. Electronic Frontier Foundation. URL: https://surl.gd/qgbnmt
10. Tor: як працює мережа анонімізації. TheCode Media. URL: https://surli.cc/ztfsjl
11. Foxminded. Що таке Tor? URL: https://surli.cc/cdxkas
12. I2P. Як працює мережа I2P? URL: https://surl.li/hmaecn
13. I2P. Матеріал з вікіпедії – вільної енциклопедії URL: https://surl.li/wmdjen
14. Freenet. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://surl.li/orzlxb
15. Недоліки та вразливості Tor. Матеріал з IRJET. URL: https://surl.li/jxpzff
16. Недоліки та вразливості I2P. Матеріал з Cybrary. URL: https://surl.li/qgpfef
17. Недоліки та вразливості Freenet. Матеріал з Cybrary. URL: https://surl.li/iejyrz
18. Менеджери паролів. Матеріал з блогу Acer. URL: https://surli.cc/svbhid
19. Чи безпечні менеджери паролів. Матеріал з TechRadar. URL: https://surl.li/ngyntn
20. Що таке двофакторна аутентифікація (2FA): Центр кібербезпеки України. URL: https://surl.li/mdoxsh

21. Що таке шифрування даних і як воно працює. Матеріал з сайту Kingston. URL: https://surl.li/jylsnf
22. Advanced Encryption Standard (AES). Матеріал з Вікіпедії – вільної енциклопедії. URL: https://surl.li/idsgva
23. RSA. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://surl.lu/dvpmws
24. Еліптична криптографія. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://surl.li/ekktzr
25. Хеш-функція. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://surl.li/kmvhag