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

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ПРОГНОЗУВАННЯ КІБЕРАТАК ІЗ ЗАСТОСУВАННЯМ OPEN-SOURCE INTELLIGENCE (OSINT)»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека та захист інформації»
Орел Артем Олександрович

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

Рецензент: к.фіз.-мат.н., доцент
Чепурна Олена Євгенівна

Одеса – -2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 «Інформаційні технології»**
Спеціальність: **125 «Кібербезпека та захист інформації»**
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 Орлу Артему Олександровичу

1. Тема роботи: «Прогнозування кібератак із застосуванням Open-source intelligence (OSINT)»
Керівник роботи: ~~д~~к.т.н, професор Соколов Артем 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
1	Аналіз вимог до проекту	10.02.2025 – 20.02.2025	
2	Огляд та аналіз ключових джерел OSINT	21.03.2025 – 30.03.2025	
3	Аналіз інструментів для виконання проекту	01.04.2025 – 06.04.2025	
4	Дослідження інструментарію	07.04.2025 – 10.04.2025	
5	Практичний збір OSINT-даних	16.04.2025 – 20.04.2025	
6	Виявлення індикаторів та прогнозування кібератак	21.04.2025 – 23.04.2025	
7	Аналіз результатів та висновки	24.04.2025 – 30.04.2025	
8	Оформлення пояснювальної записки	01.05.2025 – 10.05.2025	

Здобувач _____
(підпис) (прізвище та ініціали)
Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Отформатировано: Обычный, По центру, междустрочный, 1,5 строки

Кваліфікаційна робота на тему «Розгортання засобів анонімізації на прикладі OpenVPN» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації», освітньою програмою: «Кібербезпека», містить 13 рисунків, 6 таблиць та 10 літературних джерел за переліком посилань. Робота виконана на 59 сторінок загального тексту і 42 сторінки основного тексту.

У роботі досліджено теоретичні аспекти анонімізації в Інтернеті та особливості технології OpenVPN, проаналізовано її застосування для забезпечення приватності та захисту даних. Окремо розглянуті інші методи анонімізації, такі як Tor та проксі-сервери, а також їх порівняння з OpenVPN за різними параметрами. Проведено тестування ефективності OpenVPN, зокрема щодо швидкості з'єднання, затримки та захисту від витоків DNS і WebRTC.

Робота є актуальною для фахівців з кібербезпеки, аналітиків з захисту даних, а також для всіх, хто прагне забезпечити приватність під час використання Інтернету. Висновки та рекомендації, представлені в роботі, можуть бути використані для розробки методик підвищення ефективності інструментів анонімізації, вдосконалення систем кіберзахисту та підготовки спеціалістів у сфері захисту приватності та кібербезпеки.

OPENVPN, АНОНІМІЗАЦІЯ, КІБЕРБЕЗПЕКА, ПРИВАТНІСТЬ, ЗАХИСТ ДАНИХ, DNS-ВИТОКИ, WEBRTC-ВИТОКИ.

ABSTRACT

Отформатировано: Обычный, По центру, междустрочный, 1,5 строки

The qualification thesis on the topic "Anonymization Tools Deployment using OpenVPN" for obtaining the first (bachelor's) level of higher education in the specialty 125 "Cybersecurity and information protection", educational program "Cybersecurity", contains 18 figures, 13 tables, and 19 references. The work is executed on 40 pages of general text and 32 pages of the main text.

The thesis explores the theoretical aspects of anonymization on the Internet and the features of the OpenVPN technology, analyzing its application for ensuring privacy and data protection. Other anonymization methods, such as Tor and proxy servers, are also reviewed, along with a comparison to OpenVPN across various parameters. Efficiency tests of OpenVPN were conducted, focusing on connection speed, latency, and protection against DNS and WebRTC leaks.

The work is relevant for cybersecurity specialists, data protection analysts, and anyone who seeks to ensure privacy while using the Internet. The conclusions and recommendations presented in the thesis can be used to develop methods for improving anonymization tools, enhancing cybersecurity systems, and training specialists in privacy and cybersecurity protection.

OPENVPN, ANONYMIZATION, CYBERSECURITY, PRIVACY, DATA PROTECTION, DNS LEAKS, WEBRTC LEAKS.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний світ цифрових технологій характеризується стрімким зростанням обсягів інформації, що передається через мережу Інтернет. З одного боку, це відкриває нові можливості для комунікації, бізнесу та доступу до знань, але з іншого – створює серйозні виклики для забезпечення конфіденційності та безпеки даних. У контексті глобалізації та розвитку інформаційного суспільства питання анонімності користувачів набуває особливої актуальності. Використання технологій віртуальних приватних мереж (VPN), зокрема OpenVPN, стало одним із ключових інструментів для захисту персональних даних, обходу цензури та забезпечення приватності в Інтернеті.

Актуальність теми дослідження зумовлена зростаючою потребою в ефективних і доступних засобах анонімності, які можуть бути застосовані як окремими користувачами, так і організаціями. У той же час, незважаючи на популярність OpenVPN як одного з найнадійніших рішень, багато користувачів стикаються з труднощами в його налаштуванні, оптимізації та оцінці ефективності. Це підкреслює необхідність детального аналізу теоретичних і практичних аспектів використання OpenVPN, що й стало основою для цієї дипломної роботи.

Метою дипломної полягає в дослідженні теоретичних основ анонімності в Інтернеті та практичного застосування OpenVPN як інструменту забезпечення конфіденційності, а також у розробці рекомендацій щодо його ефективного використання.

Завдання дослідження:

1) Проаналізувати теоретичні аспекти анонімності, включаючи структуру Інтернету та еволюцію VPN-технологій.

2) Вивчити принципи роботи OpenVPN і порівняти його з іншими засобами анонімності.

3) Розглянути практичні аспекти налаштування OpenVPN-клієнта на операційній системі Windows.

4) Провести тести ефективності OpenVPN та проаналізувати отримані результати.

5) Надати практичні рекомендації щодо використання OpenVPN для забезпечення анонімності та безпеки.

Об’єктом дослідження є технології забезпечення анонімності в Інтернеті.

Предметом дослідження є особливості функціонування та практичного використання OpenVPN як засобу анонімності.

Практичне значення результатів. Методи дослідження включають аналіз літературних джерел, порівняльний аналіз різних інструментів анонімності, експериментальні тести продуктивності OpenVPN, а також узагальнення отриманих даних.

Структура роботи складається з трьох основних розділів. У першому розділі розглядаються теоретичні аспекти анонімності, включаючи історію розвитку VPN-технологій та принципи роботи OpenVPN. Другий розділ присвячено практичному використанню OpenVPN, зокрема налаштуванню клієнта на Windows, проведенню тестів ефективності та аналізу їх результатів. У висновках підсумовуються основні результати дослідження та надаються рекомендації щодо оптимізації використання OpenVPN. Робота завершується переліком використаних джерел.

Таким чином, дана дипломна робота спрямована на поглиблення розуміння технологій анонімності та практичне вдосконалення використання OpenVPN, що має як теоретичне, так і прикладне значення в умовах сучасного цифрового середовища.

1 ТЕОРЕТИЧНІ АСПЕКТИ АНОНІМІЗАЦІЇ

1.1 Структура інтернету та анонімізація

Інтернет є надзвичайно складною, глобальною системою, що поєднує в собі мільйони комп'ютерних пристроїв, мереж і серверів у всьому світі. Він виконує роль основного комунікаційного середовища, завдяки якому мільярди користувачів можуть отримувати, обмінюватися та передавати інформацію в будь-якому куточку планети практично миттєво. Структура Інтернету має багатошарову архітектуру, яка включає різні компоненти, що взаємодіють між собою для забезпечення безперервного і швидкого обміну даними.

Основними елементами цієї мережі є:

1) Кінцеві користувацькі пристрої, такі як комп'ютери, смартфони, планшети, які виконують роль клієнтів, ініціюючи запити на отримання інформації чи послуг;
2) Сервери, що обробляють ці запити, зберігають дані і надають доступ до ресурсів, включаючи вебсайти, хмарні сервіси, бази даних та інше;
3) Провайдери інтернет-послуг (ISP), які забезпечують підключення клієнтів до глобальної мережі, надаючи фізичні та логічні канали зв'язку;
4) Магістральні мережі та маршрутизатори, що відповідають за передачу інформації між різними сегментами Інтернету та оптимальний маршрут трафіку.

Взаємодія цих компонентів відбувається на основі міжнародних стандартів і протоколів, найважливішим серед яких є протокол TCP/IP. Цей набір протоколів визначає правила адресації, маршрутизації та передачі даних у вигляді пакетів.

Кожен пристрій, підключений до Інтернету, має унікальну IP-адресу – цифровий ідентифікатор, який служить для маршрутизації пакетів і вказує на його місце у глобальній мережі. Ці адреси бувають статичними (постійними) або динамічними (тимчасовими). Відкритість IP-адрес у мережі є одночасно її перевагою і слабкістю, адже вони можуть розкривати інформацію про місцезнаходження користувача.

Для зручності користувачів та автоматизації процесу адресації в Інтернеті існує система доменних імен (DNS), яка переводить числові IP-адреси у легкозапам’ятовувані імена. DNS-система є ієрархічною та складається з кореневих серверів, доменів верхнього рівня і локальних DNS-серверів, що відповідають за конкретні ділянки мережі.

Структурна схема Інтернету, що показує взаємодію користувачів, провайдерів і серверів зображена на рисунку 1.1.

Рисунок 1.1 – Структурна схема Інтернету

Проте з розширенням використання Інтернету виникають питання безпеки і приватності. Кожен користувач залишає цифровий слід — IP-адресу, час і місце підключення, історію відвідувань, що може бути використано для відстеження, збору особистих даних, а інколи і для обмежень доступу чи цензури.

Сучасні веб-технології, такі як WebRTC, можуть навіть безпосередньо розкривати реальну IP-адресу користувача, ігноруючи налаштування проксі чи VPN, що ставить під загрозу анонімність.

Зважаючи на ці виклики, важливим стає використання технологій анонімізації, які дозволяють захистити персональні дані і зберегти конфіденційність. Основні методи анонімізації в Інтернеті:

Віртуальні приватні мережі (VPN)

1) VPN – створюють захищений тунель між пристроєм користувача і VPN-сервером, шифруючи весь трафік і змінюючи його видиму IP-адресу. Це забезпечує користувачеві можливість обходити географічні обмеження, уникати стеження і захищати дані від перехоплення.

2) Tor (The Onion Router) – це мережа, яка маршрутизує інтернет-трафік через декілька випадково обраних вузлів, кожен з яких шифрує дані додатковим шаром (аналогія з шарами цибулі). Це значно ускладнює відстеження реального джерела трафіку.
3) Проксі-сервери – виступають безпосередньо істинними посередниками між користувачем і Інтернетом, приховуючи справжню IP-адресу. Проте проксі не шифрують трафік і не забезпечують повну анонімність.

Деякі браузери мають вбудовані функції анонімності, блокують відстеження, а також можуть автоматично працювати через проксі або VPN.

Таблиця 1.1 – Порівняння основних методів анонімізації за параметрами безпеки, швидкості та зручності.

Метод анонімізації	Безпека	Швидкість	Зручність використання
VPN (Virtual Private Network)	Висока (шифрування всього трафіку)	Висока (залежить від сервера і шифру)	Висока (проста настройка, сумісність з різними пристроями)
Tor (The Onion Router)	Дуже висока (багатошарове шифрування)	Низька (через багато вузлів і шифрування)	Середня (потрібен спеціальний браузер)
Проксі-сервери	Низька (без шифрування, лише приховування IP)	Висока (залежить від сервера)	Висока (легко використовувати)
Анонімні браузери / розширення	Середня (залежить від функціоналу)	Висока	Висока (зручні для повсякденного користування)

Попри наявність широкого спектру інструментів анонімізації, користувачі стикаються з низкою сучасних викликів, які ставлять під загрозу конфіденційність в Інтернеті. Наприклад, навіть при використанні VPN, браузери можуть розкривати реальну IP-адресу через протокол WebRTC. Цей протокол, що забезпечує голосовий і відеозв'язок у реальному часі, використовує локальні IP-адреси для прямого з'єднання між пристроями. Це призводить до так званих WebRTC-витоків, коли реальна IP-адреса стає доступною навіть через захищене іентернет з'єднання.

Крім того, існує ще один небезпечний інструмент - браузерний відбиток (browser fingerprinting) (див. рисунок 1.2). Цей метод дозволяє ідентифікувати пристрій користувача на основі сукупності параметрів: тип операційної системи, версія браузера, встановлені шрифти, розширення, часова зона, роздільна здатність екрану тощо. Навіть якщо змінити IP-адресу, користувач може бути впізнаний саме за унікальним поєднанням технічних характеристик.

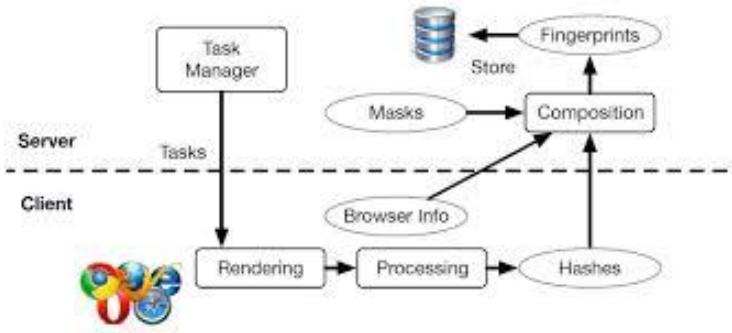

Рисунок 1.2 – Візуалізація того, як формується browser fingerprint з різних параметрів пристрою.

Ще одним інструментом деанонімізації є cookies (куки) - невеликі файли, які зберігаються в браузері для запам'ятовування сесій. Хоча вони потрібні для авторизації і зручності користування сайтом, багато рекламних мереж використовують куки для персоналізованого відстеження, формуючи профілі поведінки користувачів.

Не менш важливою є геолокація, яка використовується не тільки на мобільних пристроях через GPS, але і на десктопах - через IP-адресу, Wi-Fi точки доступу та навіть Bluetooth-маяки. Сайти можуть отримувати дані про ваше місцезнаходження з точністю до кількох метрів.

Наприклад, у 2018 році компанія Google потрапила в скандал, коли стало відомо, що вона відстежувала місцезнаходження користувачів Android навіть при вимкненому GPS. Це викликало хвилю критики з боку правозахисників і стало ще одним доказом того, що повної приватності в Інтернеті досягти надзвичайно складно без ретельного контролю над усіма каналами витоку даних.

Також важливо згадати про використання анонімізаторів у країнах з обмеженим доступом до Інтернету. Наприклад, у Китаї, Ірані чи Північній Кореї державна політика передбачає жорстку фільтрацію і цензуру Інтернету. Для обходу таких обмежень VPN і Tor стали життєво необхідними інструментами для журналістів, активістів і дослідників.

У контексті кібербезпеки стає очевидним, що сама структура Інтернету є відкритою і потенційно вразливою. Лише поєднання декількох рівнів захисту – VPN + анонімний браузер + блокування WebRTC + відключення скриптів – може забезпечити порівняно високий рівень анонімності.

Однак навіть це не гарантує повної безпеки. Як правило, помилки самого користувача, наприклад, вхід у свій акаунт Google під час роботи через VPN, повністю нівелюють усі заходи анонімізації. Саме тому важливо не тільки використовувати технічні інструменти, але й дотримуватися грамотної поведінки в Інтернеті.

Питання анонімності в мережі тісно пов’язане не лише з технічними, але й з етичними та юридичними аспектами. З одного боку, право на приватність є фундаментальним елементом прав людини, закріпленим у міжнародних документах, зокрема в Загальній декларації прав людини та Європейській конвенції про захист прав людини. З іншого – анонімність нерідко використовується для приховування протиправної діяльності: кіберзлочинності, нелегальної торгівлі, хакерських атак тощо.

Законодавства багатьох країн мають суперечливе ставлення до анонімізаторів. Наприклад, у деяких державах використання VPN не заборонене, але обмежується на рівні провайдерів і урядового моніторингу. Водночас, у країнах із жорсткою цензурою, таких як Китай чи Росія, існують заборони на використання Tor та комерційних VPN-сервісів без реєстрації.

Суспільне значення анонімності також неоднозначне. Для звичайного громадянина – це інструмент захисту особистих даних, для журналіста – гарантія безпеки джерел, а для опозиційного активіста – єдиний спосіб висловити думку. У той же час, зловмисники використовують ті самі технології для приховування слідів злочинів.

Таким чином, важливо розглядати анонімність не лише як технічну можливість, а як соціальне явище, що вимагає балансу між індивідуальними правами та суспільною безпекою. Саме цей баланс має визначати політику держав, підхід розробників програмного забезпечення та поведінку самих звичайних користувачів.

1.2 Історія та розвиток VPN-технологій

Віртуальні приватні мережі (VPN) з’явилися як відповідь на необхідність безпечного передавання даних через загальнодоступні мережі, насамперед через Інтернет. Попри відносну новизну технології для широкого загалу, її коріння сягає ще 1990-х років, коли компанії почали шукати способи організувати захищений зв’язок між віддаленими офісами.

Перші кроки у розвитку VPN-технологій були зроблені корпорацією Microsoft, яка в 1996 році представила протокол PPTP (Point-to-Point Tunneling Protocol). Цей протокол дозволяв створювати зашифровані тунелі через публічний Інтернет, і саме він започаткував еру масового використання віртуальних приватних мереж.

PPTP мав низку переваг – простота налаштування, підтримка більшістю операційних систем. Проте з часом виявилися його серйозні недоліки – слабкі алгоритми шифрування та вразливість до атак типу «man-in-the-middle». Це зумовило появу нових, безпечніших протоколів:

1. L2TP/IPsec (Layer 2 Tunneling Protocol) – поєднання двох технологій: тунелювання та шифрування. Відзначається вищою безпекою, але іноді має проблеми з фаєрволами через використання нестандартних портів.

2. OpenVPN – з'явився на початку 2000-х як відкрите рішення з підтримкою TLS/SSL-шифрування. Гнучкий, кросплатформний та підтримується спільнотою. Зараз це один із найпопулярніших і надійніших VPN-протоколів.

3. IKEv2/IPsec – протокол, що використовується особливо активно на мобільних пристроях. Має високу стабільність при зміні мереж (наприклад, при переході з Wi-Fi на LTE) і хорошу продуктивність.

4. WireGuard – найсучасніший із основних VPN-протоколів. Розроблений у 2019 році, вирізняється мінімалістичним кодом, високою швидкістю і високим рівнем безпеки. Дуже швидко набирає популярності безпосередньо серед звичайних користувачів.

Таблиця 1.2 – Основні безпосередні етапи розвитку VPN-технологій

Протокол	Безпека	Швидкість	Зручність використання
PPTP	Низька (вразливий до атак)	Висока	Висока (простий у налаштуванні)
L2TP/IPsec	Висока (AES-шифрування)	Середня (затримки через подвійне шифрування)	Середня (може блокуватись фаєрволами)
OpenVPN	Дуже висока (TLS, AES)	Висока (залежить від конфігурації)	Висока (гнучкий, кросплатформенний)
IKEv2/IPsec	Висока (автоматичне повторне з'єднання)	Висока	Висока (підтримка мобільних пристроїв)
WireGuard	Дуже висока	Дуже висока	Висока

VPN-технології еволюціонували з вузькоспеціалізованих корпоративних рішень у важливий елемент цифрової безпеки для приватних користувачів, еволюція зображена на рисунку 1.3. Якщо спочатку VPN використовувалися для захисту внутрішньої мережі компанії, то з часом вони стали інструментом для:

1. Обходу цензури;

2. Захисту конфіденційності;

3. Доступу до геозаблокованих ресурсів (наприклад, Netflix, BBC iPlayer);

4. Безпечного використання публічних Wi-Fi-мереж.

Особливо різко зріс попит на VPN після скандалу з Едвардом Сноуденом у 2013 році, коли стало відомо про масштабне стеження за користувачами з боку спецслужб. З того часу багато людей стали усвідомлено підходити до безпеки в мережі.

У 2020-х роках розвиток VPN продовжує набирати обертів. З'являються мобільні VPN-додатки, браузерні розширення, корпоративні рішення з багаторівневою автентифікацією, а також інтеграція VPN із хмарними сервісами.

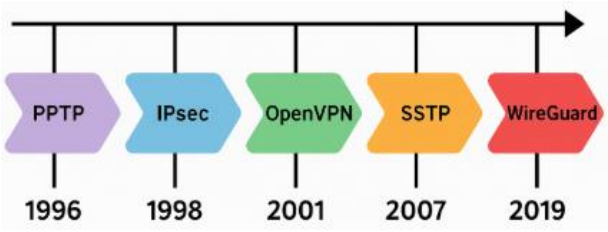

Рисунок 1.3 – Еволюція VPN-технологій від PPTP до WireGuard

Таким чином, VPN-технології пройшли шлях від експериментального інструменту до масового сервісу, що сьогодні використовується мільйонами людей по всьому світу. Їхній розвиток є відповіддю на постійні виклики цифрової епохи – стеження, витоки даних, цензура та кіберзлочинність.

Однією з найбільш актуальних сфер застосування VPN-технологій є політична і соціальна реальність сучасного світу. У країнах з авторитарними

режимами VPN часто виступає єдиним способом отримати доступ до об’єктивної інформації. Наприклад, у Китаї, де заблоковані Google, YouTube, Wikipedia та багато інших ресурсів, мільйони людей щодня використовують VPN для вільного доступу до знань та міжнародних новин.

Схожа ситуація спостерігалася в Ірані під час протестів, у Росії в періоди блокування месенджерів, у Туреччині під час політичних заворушень. Усі ці випадки демонструють, що VPN є не просто технічним інструментом, а інструментом свободи слова та самовираження.

Комерційне використання VPN також є дуже важливим. Багато компаній використовують VPN для організації безпечного доступу працівників до корпоративної мережі з будь-якої точки світу. У період пандемії COVID-19 ця потреба зросла в рази – мільйони співробітників по всьому світу працювали з дому, підключаючись до внутрішніх ресурсів компаній через корпоративні VPN-мережі.

Крім того, VPN-технології дозволяють бізнесам здійснювати моніторинг і аналітику з різних країн (наприклад, перевіряти локальну видачу Google або доступність сайту в певному регіоні), що є важливим для SEO-агенцій, маркетологів і контент-менеджерів.

В освітньому середовищі VPN використовується для доступу до університетських бібліотек, наукових журналів, баз даних (наприклад, JSTOR, Scopus, Web of Science), які іноді доступні лише в певних мережах. VPN дозволяє студентам і викладачам користуватись ресурсами з будь-якої точки світу.

Не можна оминути увагою також використання VPN звичайними користувачами – для обхід геозаблокувань (наприклад, перегляд Netflix або Spotify, недоступних у певному регіоні), для безпечного підключення до публічного Wi-Fi у кафе, аеропортах або готелях, для уникнення трекінгу з боку рекламних мереж і навіть для зменшення цін на авіаквитки (зміна країни дає інші тарифи).

Популярні комерційні сервіси VPN – NordVPN, Surfshark, ExpressVPN, ProtonVPN – пропонують зручні інтерфейси, мобільні додатки, вибір серверів у понад 50 країнах, підтримку WireGuard і політику відсутності журналів (no-logs

policy). Деякі з них інтегрують в себе блокувальники реклами, kill-switch і навіть сканери витоків.

Окремої уваги заслуговує тенденція інтеграції VPN у браузери – наприклад, Opera має вбудований безкоштовний VPN. Також компанії-гіганти, як Google і Apple, експериментують із створенням власних приватних проксі-сервісів і DNS-обфускації.

Сучасні тенденції свідчать, що VPN буде і надалі розвиватись:

1. Зростає попит на мультиплатформенність і інтеграцію в мобільні ОС; з’являються гібридні рішення з Zero Trust архітектурою;

2. Розвивається квантова криптографія, яка потенційно змінить різноманітні протоколи шифрування.

Крім того, політична ситуація, кібервійни, боротьба за приватність, розширення 5G і супутникового Інтернету (Starlink, OneWeb) стимулюють розробку все більш швидких, захищених і невидимих тунелів.

У різних країнах ставлення до використання VPN-технологій суттєво відрізняється. У більшості демократичних держав VPN дозволений і розглядається як інструмент підвищення безпеки користувача. Проте в деяких країнах, таких як Китай, Іран, Росія або ОАЕ, VPN-сервіси підлягають суворому контролю або повній забороні, а користувачам загрожують штрафи за несанкціоноване використання.

Такі обмеження зазвичай мотивуються необхідністю забезпечення національної безпеки або боротьбою з "інформаційною війною", але на практиці часто перешкоджають реалізації базових прав людини – свободи слова, доступу до інформації та приватного життя. Саме тому VPN-технології часто опиняються в центрі дискусій про баланс між безпекою держави та правами громадян.

З технічного боку, VPN дозволяє уникнути масового збору даних про поведінку користувачів, що активно використовують рекламні та аналітичні компанії. Це дає людині змогу самостійно контролювати власну цифрову ідентичність. Проте водночас VPN може бути використаний і для недоброчесної

діяльності – приховування злочинної активності, зламу систем, розповсюдження забороненого контенту.

Таким чином, виникає етична дилема: наскільки виправданим є повне шифрування та анонімність, якщо це може слугувати як добру, так і злу. З огляду на це, провайдери VPN часто публікують так звані transparency reports – звіти про співпрацю з правоохоронними органами та свою політику щодо збереження або знищення журналів активності.

Законодавство ЄС (зокрема, GDPR) підтримує право особи на приватність в Інтернеті, що непрямо сприяє використанню VPN-технологій. Проте існує загроза майбутнього тиску на постачальників таких послуг, особливо в умовах глобальної цифрової регуляції, боротьби з тероризмом і фейковими новинами.

1.3 Принципи роботи OpenVPN

OpenVPN – це один із найпопулярніших VPN‑протоколів з відкритим вихідним кодом, який забезпечує безпечну та зашифровану передачу даних між клієнтом і сервером. Він розроблений як гнучкий і масштабований інструмент, що дозволяє налаштування практично під будь‑які потреби користувача – від особистого використання до корпоративних мереж.

Основою архітектури OpenVPN є модель “клієнт-сервер” (див. рисунок 1.4), у якій клієнтський пристрій встановлює з’єднання з віддаленим VPN‑сервером. Сервер обробляє запити, створює захищене з’єднання та шифрує весь переданий трафік. При цьому між клієнтом і сервером встановлюється віртуальний тунель, через який проходять усі пакети даних.

Однією з ключових переваг OpenVPN є використання бібліотеки OpenSSL, яка забезпечує підтримку сучасних алгоритмів шифрування, таких як AES‑128, AES‑256, Blowfish, ChaCha20. Крім того, OpenVPN використовує протокол TLS (Transport Layer Security) для обміну ключами і встановлення надійного зашифрованого каналу.

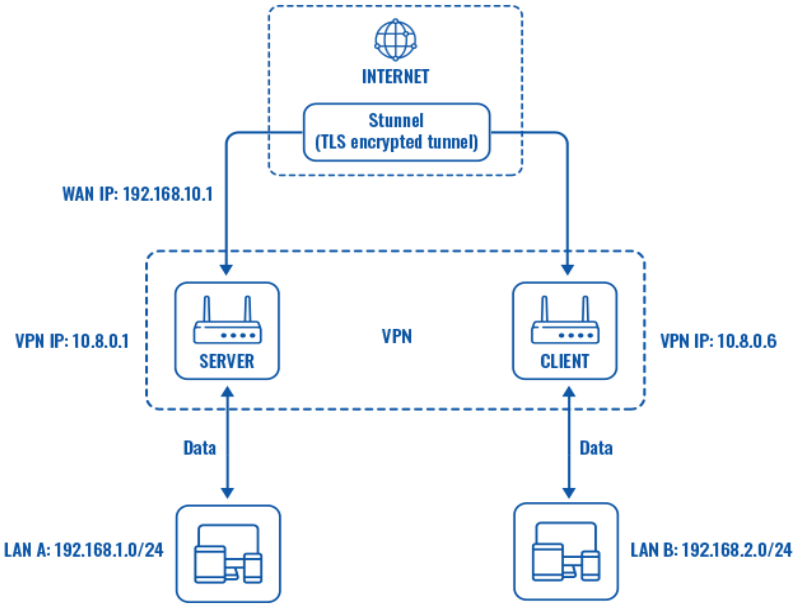

Рисунок 1.4 – Типова архітектура OpenVPN: клієнт – тунель – сервер

OpenVPN може працювати як через протокол TCP, так і через UDP. TCP забезпечує надійність, але може бути повільнішим через підтвердження кожного пакета. UDP, навпаки, швидший, але менш надійний. Зазвичай для VPN-трафіку рекомендується UDP, оскільки важливіше забезпечити мінімальні затримки.

Важливим елементом є також режими роботи мережевого інтерфейсу:

TUN (network TUNnel) – створює точку-точку IP-тунель, який працює на рівні 3 (мережевий рівень моделі OSI), ідеально підходить для передачі IP-пакетів;

TAP (network tap) – імітує Ethernet-пристрій, передає пакети 2 рівня (канального), дозволяє створювати повноцінні віртуальні мережі (наприклад, віртуальний міст між офісами).

Користувач, який хоче підключитися до VPN‑мережі за допомогою OpenVPN, повинен мати конфігураційний файл (файл з розширенням .ovpn), у якому вказуються:

1. Адреса VPN‑сервера (remote);
2. Тип протоколу (proto);
3. Порт (часто 1194 або 443);
4. Тип шифрування (cipher);
5. Сертифікати безпеки (<ca>, <cert>, <key>);
6. Параметри маршрутизації (redirect-gateway def1, route, dhcp-option).

Ці параметри можуть бути змінені залежно від вимог провайдера VPN або корпоративної політики. Важливо розуміти, що OpenVPN може використовувати як аутентифікацію за логіном і паролем, так і сертифікатну авторизацію, або ж комбіновану схему.

Процес встановлення захищеного з’єднання в OpenVPN відбувається за допомогою TLS‑рукостискання (TLS Handshake). На цьому етапі клієнт і сервер обмінюються сертифікатами, перевіряють їхню справжність та узгоджують параметри шифрування. Якщо обидві сторони успішно пройшли автентифікацію, створюється сеансовий ключ, який використовується для симетричного шифрування всіх наступних даних.

Після цього починається тунелювання – передача трафіку через віртуальний адаптер (TUN або TAP), який обробляє пакети так, ніби вони проходять через фізичну мережу (рис. 1.5). Завдяки цьому користувач може виглядати для зовнішніх ресурсів так, ніби він фізично знаходиться в іншій країні.

OpenVPN також підтримує механізми захисту від витоків DNS, що часто виникають при переході між мережами або при нестабільному з’єднанні. Витоки DNS можуть видати реальну IP‑адресу користувача навіть при активному VPN.

Щоб цього уникнути, у конфігураційний файл додаються директиви:

```
scss
block-outside-dns
dhcp-option DNS 8.8.8.8
```

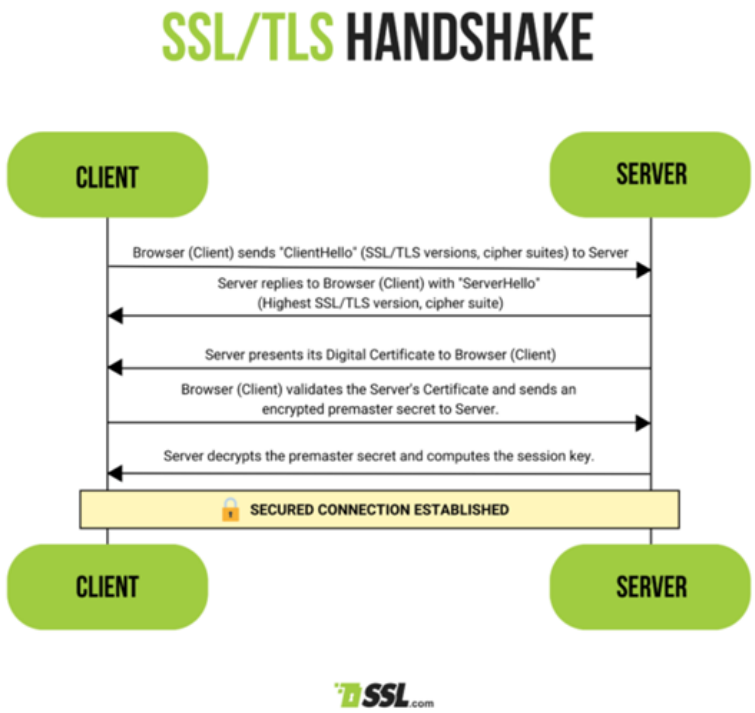

Рисунок 1.5 – TLS‑рукостискання з обміном сертифікатами й ключами

Це дозволяє примусово направити всі DNS‑запити через VPN‑тунель, а не безпосередньо через локального провайдера.

Аналогічно WebRTC‑витоки, які можуть виникати в браузерах (особливо в Chrome/Edge), потребують додаткових налаштувань. Зазвичай проблему вирішують плагіни або конфігурація браузера.

Серед можливостей, які забезпечують гнучкість і надійність роботи програми OpenVPN:

1. Kill Switch – функція, яка миттєво розриває Інтернет-з’єднання у випадку втрати VPN‑тунелю, запобігаючи випадковому витоку даних;

2. Reconnection – автоматичне відновлення з'єднання після розриву або переходу мережі (наприклад, Wi‑Fi → мобільна мережа);

3. Compression (компресія трафіку) – можливість стискати дані перед передачею (хоча у нових версіях вона часто вимкнена через ризик атак);

Обфускація трафіку – функції, які дозволяють маскувати VPN‑трафік під звичайний HTTPS, що важливо в країнах, де VPN‑трафік безспосередньо блокується методами DPI‑фільтрів.

OpenVPN доступний на багатьох платформах: Windows, macOS, Linux, Android, iOS. Існують офіційні клієнти, а також альтернативи, такі як OpenVPN GUI, Tunnelblick (для macOS), OpenVPN Connect (для мобільних ОС). Деякі маршрутизатори також підтримують OpenVPN на рівні прошивки (наприклад, ASUS, MikroTik, DD‑WRT).

Для автоматизації підключення використовуються скрипти, або ж VPN інтегрується в системний менеджер мережі (наприклад, NetworkManager на Linux).

У корпоративних мережах OpenVPN часто використовується для створення віртуальних приватних корпоративних мереж (Intranet), які з'єднують офіси в різних містах або країнах. Кожен офіс підключається до загального сервера, і трафік передається в зашифрованому вигляді.

Для приватних осіб OpenVPN – це інструмент цифрової безпеки, який безпосередньо дозволяє:

1. Переглядати заблоковані сайти,

2. Уникати стеження,

3. Безпечно підключатись у публічних Wi‑Fi мережах,

4. Приховувати IP та місцезнаходження.

OpenVPN є золотою серединою між надійністю, гнучкістю та безпекою. Хоча WireGuard сьогодні вважається перспективнішою альтернативою, OpenVPN продовжує домінувати завдяки довгій історії, активній спільноті та підтримці майже на всіх платформах. OpenVPN широко застосовується в наступних сферах:

1. Віддалена робота: після пандемії COVID-19 зросла потреба у безпечному підключенні працівників до внутрішніх ресурсів компаній. OpenVPN використовується для забезпечення шифрованого доступу до локальних серверів.

2. Хмарні рішення: підключення до Amazon AWS, Microsoft Azure або Google Cloud часто налаштовується через OpenVPN для захисту адміністративного доступу та синхронізації внутрішніх сервісів.

3. IoT та домашні мережі: користувачі можуть підключитися до своєї домашньої мережі (роутерів, NAS, камер) через VPN, забезпечуючи контроль і безпеку з будь-якої точки світу.

4. Школи та університети: освітні заклади надають студентам доступ до навчальних ресурсів через VPN, особливо під час дистанційного навчання.

Попри появу нових технологій, таких як WireGuard, OpenVPN активно розвивається. Зокрема, у версіях 2.5 і вище з’явилися:

1. Покращене керування шифруванням – підтримка data-ciphers зі зворотною безспосередньою сумісністю;

2. Модуль DCO (Data Channel Offload) – для зменшення навантаження на центральний процесор;

3. Краща інтеграція з мобільними ОС – офіційні клієнти для Android та iOS постійно оновлюються.

Оскільки протокол має відкритий код, він адаптується до змін у безпеці, відповідає вимогам часу та очікуванням користувачів. Це робить OpenVPN живою технологією, а не статичним стандартом.

2. ПОРІВНЯННЯ РІЗНИХ ЗАСОБІВ АНОНІМНОСТІ

2.1 Основні характеристики TOR порівняно з OpenVPN

Tor (The Onion Router) – це мережева система, яка забезпечує анонімний доступ до Інтернету шляхом багаторівневої маршрутизації трафіку через добровільні вузли по всьому світу. Трафік зашифровується шарами (як цибуля – звідси й назва), що унеможливлює визначення джерела або кінцевого пункту пакету. Основні елементи Tor:

1. Вхідний вузол (entry node) – перша точка, яка отримує ваш запит.
2. Проміжні вузли (relay nodes) – переправляють трафік.
3. Вихідний вузол (exit node) – передає запит до кінцевого сайту.

Таблиця 2.1 – Порівняльна характеристика Tor та OpenVPN

Параметр	Tor	OpenVPN
Рівень анонімності	Дуже високий (багаторівнева маршрутизація)	Середній (IP змінено, але шляхи відомі)
Швидкість з’єднання	Низька	Висока/середня залежно від сервера
Шифрування	TLS + власне багаторівневе шифрування	AES, Blowfish, TLS
Сумісність	Обмежена (Tor Browser або bridge)	Універсальна (усі ОС, вбудована підтримка)
Стабільність	Схильна до обривів	Стабільна
Масштабування	Добровольна мережа (обмежена керованість)	Керується адміністратором VPN

Tor не призначений для передачі великих обсягів даних або потокового відео – його завдання в першу чергу анонімність, а не продуктивність. До того ж, вихідний вузол у Tor може бачити незашифровані запити, тому додаткове шифрування (наприклад, HTTPS) критично важливе.

OpenVPN, навпаки, гарантує шифрування на весь маршрут, але сервер знає IP клієнта. Тобто OpenVPN не є повністю анонімним, якщо не використовуються додаткові засоби (наприклад, плаваючі IP, proxy, мульти-VPN).

У той час як OpenVPN ідеальний для довготривалого з'єднання, роботи з корпоративними ресурсами та трансляції медіа, Tor залишається найкращим вибором для тих, хто хоче приховати сам факт перебування в Інтернеті.

Tor найчастіше використовується активістами, журналістами, правозахисниками та громадянами країн з обмеженим доступом до інформації. З його допомогою можна:

1. Отримувати доступ до заблокованих новинних ресурсів, соціальних мереж або месенджерів.

2. Анонімно публікувати матеріали.

3. Спілкуватися без стеження з боку урядів або інтернет-провайдерів.

4. Відвідувати сайти в мережі .onion, що доступні тільки через Tor.

Наприклад, у 2022 році під час обмежень доступу до Twitter в Ірані, користувачі переходили на Tor Browser, щоб зберегти зв'язок із зовнішнім світом. Завдяки Tor їм вдалось передавати відео протестів і комунікувати з міжнародними та локальними ЗМІ.

OpenVPN, у свою чергу, є універсальним рішенням, яке застосовується як у побуті, так і на підприємствах. Його використовують для:

1. Захищеного віддаленого підключення до внутрішніх серверів компанії.

2. Обходу географічних блокувань стримінг-сервісів (Netflix, HBO, Spotify) .

3. Безпечного користування публічним Wi-Fi.

4. Онлайн-банкінгу та здійснення фінансових операцій у мережі.

Наприклад, підприємство з кількома філіями у різних містах України може з’єднати офіси через VPN-сервер. Співробітники отримують доступ до спільної бази даних через OpenVPN, навіть працюючи з дому.

Існують схеми, за якими Tor і OpenVPN можуть використовуватись одночасно для досягнення максимальної приватності:

VPN over Tor – спочатку користувач підключається до мережі Tor, а потім через неї – до VPN. Це підвищує анонімність, але вимагає складної конфігурації.

Tor over VPN – спочатку підключення до VPN, а вже потім — запуск Tor Browser. Такий варіант популярніший і простіший, адже дозволяє приховати факт використання Tor від провайдера.

Таблиця 2.2 – Варіанти використання Tor та OpenVPN

Сценарій використання	Tor	OpenVPN
Доступ до заблокованих сайтів	Так	Так
Високий рівень анонімності	Так	Ні
Стрімінг і медіа	Ні	Так
Використання публічного Wi-Fi	Обмежено	Так
Підключення до корпоративної мережі	Ні	Так
Робота з .onion сайтами	Так	Ні
Швидкість з’єднання	Низька	Висока

Tor та OpenVPN відіграють особливу роль у країнах з авторитарними урядами, де обмежено свободу слова та доступ до ресурсів. Наприклад, у Китаї “Великий фаєрвол” блокує VPN-з’єднання на рівні глибокої інспекції пакетів (DPI),

а Tor часто повністю заборонений. У таких умовах користувачі змушені шукати обфускуючі плагіни та нестандартні порти, щоб забезпечити обхід блокувань.

OpenVPN дозволяє приховати факт використання VPN за допомогою TCP‑порту 443, який використовується для HTTPS, таким чином роблячи трафік схожим на звичайне веб-з’єднання. Tor, зі свого боку, використовує "мости" (bridges) – спеціальні вузли, які не публікуються в загальному реєстрі, і їх важко заблокувати.

Незважаючи на високий рівень захисту, як Tor, так і OpenVPN мають уразливості, які можуть бути використані зловмисниками або урядами.

У Tor найслабшою ланкою залишається вихідний вузол, оскільки трафік у цьому пункті може бути незашифрованим. Якщо користувач не використовує HTTPS, його дані можуть бути перехоплені.

OpenVPN покладається на довіру до сервера, тому VPN-провайдер, який зберігає журнали, може передати їх за запитом державних органів. Деякі VPN-провайдери декларують політику "no logs", однак її важко перевірити.

Також існують атаки типу “аналітики трафіку”, які дозволяють корелювати вхідні та вихідні запити навіть при наявності шифрування, особливо якщо використовується нестійке з’єднання.

Важливо підкреслити, що жодна з технологій не є панацеєю. Анонімність в Інтернеті – це не тільки технічні інструменти, але й поведінка користувача. Якщо людина заходить на акаунт зі справжнім ім’ям через Tor, або використовує незахищений браузер із VPN, – це зводить нанівець усі заходи безпеки.

Більш ефективно використовувати комбіновані підходи, коли OpenVPN шифрує з’єднання, а Tor забезпечує багаторівневу маршрутизацію. Також важливими залишаються використання HTTPS, блокувальників скриптів, анонімних пошуковиків (StartPage, DuckDuckGo), і оновленого ПЗ.

У багатьох країнах використання Tor або OpenVPN є небажаним або навіть забороненим. Китай активно бореться з VPN-сервісами. Доступ до більшості публічних серверів заблоковано, а використання VPN без державного дозволу карається законом. Tor також майже повністю заблоковано.

Росія внесла Tor до списку заборонених ресурсів, і постійно відбуваються спроби обмежити безспосередню роботу VPN.

Іран і Туреччина обмежують або сповільнюють доступ до захищених протоколів, зокрема TLS, використовуваних VPN та Tor.

Попри це, в демократичних країнах використання цих інструментів залишається законним, особливо в контексті захисту персональних даних та цифрової безпеки. Наприклад, в ЄС Tor і VPN вважаються інструментами реалізації права на приватність, гарантованого законодавством (зокрема GDPR).

Технології анонімності стрімко еволюціонують. З кожним роком з'являються:

1. Нові VPN-протоколи з фокусом на швидкість і простоту (WireGuard).

2. Мобільні додатки, що приховують активність з мінімальними знаннями з боку користувача (ProtonVPN, Mullvad, iVPN);

3. Захищені операційні системи, як Tails OS, які працюють виключно через Tor та не залишають слідів на пристрої.

4. Також все більшої популярності набуває ідея "децентралізованих VPN" , які використовують блокчейн та peer-to-peer з'єднання, дозволяючи обійти навіть глибоке сканування DPI.

У майбутньому важливим буде не лише захист від зовнішнього стеження, але й власна цифрова грамотність користувачів – розуміння ризиків, поведінкових патернів, правильна конфігурація ПЗ і поєднання технологій.

2.2 Переваги та обмеження комерційних VPN

У сучасному світі, де цифрова безпека та конфіденційність стають все більш актуальними, комерційні VPN‑сервіси займають ключову позицію на ринку інструментів анонімізації. На відміну від самостійного розгортання OpenVPN або використання Tor, комерційні сервіси орієнтовані на звичайного користувача: вони пропонують прості застосунки, швидке підключення і мінімальні технічні вимоги.

За оцінками дослідницьких агентств, до 2025 року більше 30% інтернет-користувачів регулярно використовуватимуть VPN, і велика частина з них – через платні сервіси, такі як NordVPN, Surfshark, ExpressVPN, ProtonVPN, тощо. Переваги комерційних VPN:

1. Простота використання – платні VPN мають безспосередньо інтуїтивно зрозумілі застосунки для всіх платформ: Windows, Android, iOS, macOS. Користувачеві не потрібно конфігурувати маршрути чи шифрування вручну – достатньо натиснути одну кнопку.

2. Висока швидкість з'єднання – завдяки оптимізації серверів, сучасні VPN надають мінімальну затримку, швидке завантаження та стабільне з'єднання, навіть під час потокового відео у Full HD чи 4K.

3. Розширений функціонал – комерційні сервіси зазвичай надають:

3.1 Kill Switch (автоматичне блокування трафіку при обриві VPN);

3.2 Multi-Hop VPN (ланцюг серверів для підвищеної анонімності);

3.3 Obfuscation (приховування факту використання VPN);

3.4 Split Tunneling (вибір програм, які йдуть через VPN).

4. Стабільність і підтримка – комерційні сервіси гарантують цілодобову технічну підтримку, часті оновлення, доступ до тисяч серверів у різних країнах, що забезпечує стабільну роботу з будь-якої точки світу.

У сучасному світі, де питання цифрової безпеки та конфіденційності набувають особливої важливості, комерційні VPN-сервіси відіграють ключову роль на ринку інструментів для анонімізації. У порівнянні з такими рішеннями, як самостійне налаштування OpenVPN або використання Tor, комерційні VPN-сервіси націлені насамперед на користувачів, які шукають зручність і ефективність. Вони забезпечують простоту використання завдяки інтуїтивно зрозумілим додаткам, швидкому підключенню та мінімальним технічним вимогам. Таким чином, навіть користувач без глибоких технічних знань може забезпечити себе надійним захистом від витоків даних та зберегти свою анонімність в Інтернеті. Сервіси надають не лише високий рівень безпеки, але й гарантують швидкість з'єднання, що робить їх популярними серед широкого кола користувачів, від

звичайних людей до підприємств, що потребують надійного захисту своїх комунікацій.

Таблиця 2.3 – Порівняння комерційного та безкоштовного VPN

Параметр	Комерційний VPN	Безкоштовний VPN / самостійний
Швидкість	Висока	Середня або низька
Локації серверів	Багато країн, оптимізація	Обмежена кількість
Приватність	Декларується (no-logs)	Часто сумнівна або відсутня
Техпідтримка	24/7	Відсутня
Додаткові функції	Kill Switch, Multi-Hop, Obfuscation	Потребує ручного налаштування
Ціна	$2–10/міс.	Безкоштовно або витрати на власний сервер

Незважаючи на численні переваги, комерційні VPN-сервіси мають певні обмеження і потенційні ризики, про які користувачам слід знати. Найбільшими проблемами є:

1. Надійність і довіра до провайдера – хоча багато VPN-сервісів заявляють про свою політику "no-logs", що означає відсутність збереження журналів активності користувачів, існує ризик, що ці дані все ж можуть бути збережені або передані за запитом правоохоронних органів. Користувачі повинні довіряти провайдеру, адже навіть без жодних правових зобов’язань, компанія може бути змушена передавати інформацію за запитом державних структур. Наприклад, у 2016 році компанія PureVPN допомогла FBI виявити людину, що займалася кіберзлочинною діяльністю, на основі наданих даних з логів.

2. Швидкість і продуктивність – підключення безпосередньо через VPN завжди супроводжується деяким зниженням швидкості з’єднання. Це відбувається через шифрування та маршрутизацію трафіку через віддалені сервери. Звісно, VPN-

провайдери роблять все можливе для оптимізації серверних ресурсів, але безліч користувачів може відчувати зниження швидкості при перегляді відео, геймінгу чи інших завданнях, що потребують великого обсягу даних.

3. Обмеження доступу до деяких сайтів та сервісів – деякі популярні вебсайти і стримінгові сервіси, зокрема Netflix, Hulu, BBC iPlayer, активно блокують IP-адреси відомих VPN-провайдерів. Це означає, що навіть якщо ви підключитеся до VPN, можливо, не зможете отримати доступ до певного контенту. Наприклад, Netflix застосовує активні фільтри для виявлення та блокування IP-адрес VPN-сервісів, що обмежує користувачів у доступі до контенту, доступного в інших країнах.

4. Безпека в публічних мережах Wi-Fi – Публічні мережі Wi-Fi, які є звичними в аеропортах, кафе чи готелях, можуть бути небезпечними, оскільки часто не мають належного шифрування. VPN забезпечує захист від атак "Man in the Middle" (MITM) (див. рисунок 2.1), коли зловмисники можуть перехоплювати трафік користувачів. Але існують певні вразливості, наприклад, у старих протоколах шифрування.

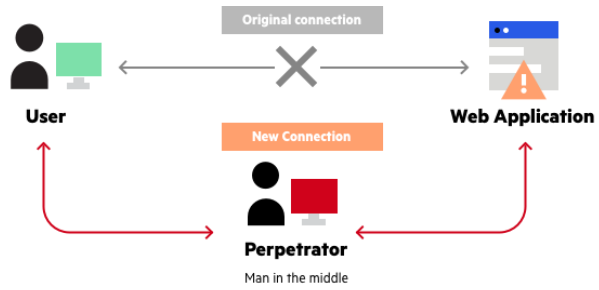

Рисунок 2.1 – Концепція "Man in the Middle" (MITM)

При виборі VPN-провайдера необхідно звернути увагу на кілька важливих факторів. Важливо вибрати провайдера, який дійсно дотримується політики "no-logs". Враховуючи, що VPN-провайдери можуть бути змушені співпрацювати з

державними органами в межах юрисдикції, важливо ознайомитись з їхнім місцезнаходженням і політикою.

Важливе значення має рівень шифрування, який використовує VPN. Сучасні сервіси використовують AES-256 або ChaCha20 для шифрування трафіку, а також OpenVPN або WireGuard як протоколи, що забезпечують високу безпеку і швидкість з'єднання.

Чим більше серверів у різних країнах, тим більший вибір і менше навантаження на конкретні вузли. Важливо перевірити, чи має провайдер сервери в потрібних регіонах і забезпечує ли він достатній рівень швидкості для ваших потреб (наприклад, для стрімінгу).

Більшість комерційних VPN-сервісів підтримують найпопулярніші операційні системи: Windows, macOS, Android, iOS. Також важливо перевірити наявність додатків для рутованих або неофіційних платформ, якщо це необхідно для специфічних налаштувань.

Комерційні VPN-сервіси є важливим інструментом для забезпечення безпеки та приватності в Інтернеті. Однак користувачам важливо усвідомлювати їхні обмеження і потенційні ризики, а також ретельно вибирати провайдерів на основі критеріїв безпеки, швидкості, підтримки та політики конфіденційності. Необхідно пам'ятати, що VPN – це інструмент захисту, але не єдиний засіб забезпечення анонімності в мережі.

Попри велику популярність і заявлені рівні безпеки, комерційні VPN-провайдери не застраховані від інцидентів безпеки. У минулому кілька великих VPN-сервісів потрапили в скандали через витоки даних користувачів:

1. PureVPN і FBI – у 2016 році VPN-сервіс PureVPN співпрацював з Федеральним бюро розслідувань (FBI) для надання інформації про користувача, який скоїв кіберзлочин. Незважаючи на те, що PureVPN заявляє, що не зберігає журнали користувачів, цей випадок продемонстрував важливість довіри до провайдерів. Компанія після інциденту змінила свою політику, але репутаційний шкода вже була завдана.

2. Hola VPN – Hola VPN, безкоштовний VPN-сервіс, був причетний до скандалу, коли було виявлено, що він використовував користувачів як вихідні вузли для ботнетів. Це означає, що користувачі стали частиною великої мережі, що використовувалася для здійснення атак. Цей випадок привернув увагу до проблеми безпеки безкоштовних VPN.

3. NordVPN – відомий сервіс NordVPN у 2018 році зазнав хакерської атаки на один із своїх серверів. Компанія стверджує, що дані користувачів не були скомпрометовані, оскільки сервер не містив журналів. Проте цей інцидент викликав занепокоєння серед користувачів про можливі вразливості навіть у відомих платних VPN-провайдерів.

Ці інциденти показують, що навіть найкращі VPN-послуги можуть стати мішенню для атак і не гарантують абсолютну безпеку. Тому важливо обирати провайдерів з надійною політикою щодо збереження даних і їхнього захисту.

Анонімність, яку забезпечують VPN, іноді використовують не тільки для захисту приватності, а й для приховування незаконної діяльності. Це ставить перед суспільством питання про етичне використання таких технологій.

Використання VPN для захисту особистої інформації, а також для обходу цензури – це безумовно позитивний аспект. Однак існує й інший бік медалі: VPN часто використовуються для приховування злочинної діяльності, такої як незаконна торгівля наркотиками, порнографією, хакерські атаки або онлайн-шахрайство.

Мережа Tor і анонімні VPN використовуються для доступу до DarkNet – частини Інтернету, де відбуваються несанкціоновані операції, в тому числі торгівля нелегальними товарами. Відомо, що багато злочинних угрупувань використовують анонімізатори для приховування своїх слідів. Однак це не означає, що анонімність сама по собі є поганою: вона є важливою для правозахисників і журналістів, які працюють у країнах з репресивними режимами.

Важливо розуміти, що хоча захист конфіденційності користувачів є ключовим аспектом VPN, деякі зловмисники також можуть зловживати цією

технологією. Користувачі повинні усвідомлювати, як і чому вони використовують VPN, адже зловживання може призвести до порушення закону і етичних норм.

VPN є ефективним інструментом для забезпечення безпеки та анонімності в Інтернеті, але з їх використанням пов'язані певні ризики і етичні питання. Користувачі повинні бути обізнані щодо потенційних небезпек, таких як витоки даних, зловживання анонімністю для протиправних цілей та можливі правові обмеження у різних країнах. Однак при правильному використанні, VPN забезпечують високий рівень захисту приватної інформації, а також можливість обходу географічних обмежень та цензури.

2.3 Практичні рекомендації щодо вибору інструменту

З огляду на широкий вибір інструментів для анонімізації в Інтернеті, користувачам необхідно ретельно обирати відповідний інструмент в залежності від своїх потреб і ситуації. У цьому розділі надаються практичні рекомендації, що допоможуть вибрати найкращий інструмент для забезпечення анонімності та захисту персональних даних.

VPN є одним із найпопулярніших інструментів для забезпечення приватності і безпеки в Інтернеті. Ось кілька факторів, які варто враховувати при виборі VPN‑провайдера:

1. Безпека та шифрування – одним із основних критеріїв вибору VPN є рівень безпеки. VPN повинен підтримувати сучасні криптографічні алгоритми, такі як AES-256 для шифрування, RSA для обміну ключами та SHA-256 для перевірки цілісності. Якщо безпека є пріоритетом, важливо, щоб VPN-провайдер використовував сильні алгоритми шифрування і пропонував політику no-logs (відсутність журналів активності).

2. Локація серверів і швидкість – чим більше серверів VPN має в різних країнах, тим більше можливостей для обходу географічних обмежень і зменшення затримок. Звертайте увагу на якість серверів (зокрема на швидкість), яка може змінюватись в залежності від місцезнаходження сервера. Якщо ви плануєте

використовувати VPN для стрімінгу або ігрових платформ, швидкість стане важливим критерієм.

3. Легкість налаштування та сумісність – хороший VPN-сервіс повинен бути простим у налаштуванні і підтримувати всі основні операційні системи – Windows, macOS, iOS, Android, Linux. Важливо, щоб він мав зрозумілий інтерфейс і можливість підключення без додаткових налаштувань.

4. Ціна – більшість платних VPN вимагають підписки, але ціни можуть варіюватися від $2 до $10 на місяць залежно від провайдера і набору функцій. Варто звернути увагу на акції і знижки для довгострокових підписок (1-2 роки). Багато провайдерів також пропонують гарантії повернення коштів протягом певного періоду.

Tor є найкращим вибором, коли необхідно забезпечити вищий рівень анонімності. Однак є кілька нюансів, які варто враховувати:

1. Анонімність – Tor забезпечує багаторівневу маршрутизацію через випадково обрані вузли, що робить його однією з найбезпечніших технологій для анонімного серфінгу. Tor ідеально підходить для обходу цензури та приховування реальної IP-адреси.

2. Швидкість – одним з основних обмежень Tor є його низька швидкість. Кількість вузлів і додаткове шифрування значно знижують пропускну здатність. Top не підходить для стрімінгу або інтенсивного завантаження файлів, але є чудовим вибором для анонімного перегляду веб-сайтів.

3. Сумісність – для використання Tor необхідно завантажити спеціальний браузер Tor Browser, який базується на Mozilla Firefox. Це означає, що Tor не може використовуватися для всіх додатків, і його підтримка обмежена лише браузером.

4. Вартість – Tor є безкоштовним, що робить його привабливим для користувачів, які шукають анонімність без фінансових витрат.

Вибір між Tor і OpenVPN залежить від цілей, які ви ставите перед собою. Tor забезпечує найвищий рівень анонімності, але знизить швидкість і обмежить можливості для потокового відео та завантажень. OpenVPN, з іншого боку, є

гнучким і швидким інструментом для захисту даних та зручності використання, особливо у роботі з корпоративними мережами та для обходу геоблокувань.

Таблиця 2.4 – Порівняння OpenVPN та Tor

Параметр	Tor	OpenVPN
Анонімність	Дуже висока (багаторівнева маршрутизація)	Середня (IP змінено, але шляхи відомі)
Швидкість	Низька	Висока (залежить від сервера і шифру)
Шифрування	Шифрування на кожному етапі (TLS + Onion)	AES-256, TLS, RSA
Сумісність	Потрібен Tor Browser	Універсальна (Windows, macOS, Android)
Використання	Анонімний серфінг, DarkNet	Віддалена робота, стрімінг, безпечний Wi-Fi
Вартість	Безкоштовно	Від $2/місяць

Завжди треба пам’ятати, що ні один із інструментів не є абсолютним, і найкращим варіантом може бути комбіноване використання VPN і Tor. Це дозволяє поєднати сильні сторони кожної технології, забезпечивши як анонімність, так і швидкість, що робить їх найбільш потужним інструментом для безпечного серфінгу в Інтернеті.

Вибір між різними засобами анонімізації – таким як VPN, Tor, або проксі-сервери – є важливим кроком, що залежить від конкретних завдань користувача. Важливо враховувати багато аспектів, серед яких рівень безпеки, швидкість

з’єднання, зручність використання і типи даних, які планується обробляти через мережу.

Для забезпечення приватності та безпеки в Інтернеті VPN є одним із найпопулярніших інструментів. VPN зазвичай використовується для шифрування трафіку і маскування реальної IP-адреси. Вибір VPN зазвичай залежить від потреби у забезпеченні швидкості з’єднання, а також від стабільності роботи. Користувачі повинні звертати увагу на кількість серверів у різних країнах, що дозволяє отримати доступ до контенту з інших регіонів. Комерційні VPN, як правило, мають високу швидкість і підтримку сучасних протоколів, таких як AES-256 для шифрування і OpenVPN для забезпечення безпечного з’єднання.

Однією з найбільших переваг VPN є проста настройка. Всі основні операційні системи (Windows, macOS, Linux, iOS, Android) підтримують роботу з VPN без необхідності в глибоких технічних знаннях. Користувачам достатньо встановити додаток VPN, підключитися до сервера і вибрати країну для зміни IP-адреси. Однак одним з обмежень використання VPN є те, що не всі сервіси забезпечують максимальну анонімність. І хоча більшість VPN-сервісів заявляють про політику "no-logs" (відсутність збереження даних), є ризик, що ці дані можуть бути передані у разі запиту від правоохоронних органів.

Tor, на відміну від VPN, гарантує дуже високий рівень анонімності. Він працює шляхом багаторівневої маршрутизації, коли трафік передається через кілька випадково обраних серверів, що робить неможливим відстеження джерела запиту. Ця технологія є ідеальним рішенням для обходу цензури в країнах з обмеженням доступу до Інтернету, таких як Китай або Іран, а також для доступу до ресурсів в DarkNet. Однак, важливо розуміти, що Tor має значні обмеження по швидкості. Шифрування на кожному етапі та багаторівнева маршрутизація значно знижують пропускну здатність, що робить Tor не найкращим вибором для стрімінгу відео чи завантаження великих файлів.

У той же час, публічні проксі-сервери є менш надійними для забезпечення анонімності, оскільки не шифрують дані, а лише приховують реальну IP-адресу користувача. Використання проксі доцільне у випадках, коли потрібно обійти

географічні блокування або доступ до сервісів без високих вимог до безпеки. Проте безпосередньо на проксі не можна покладатися для захисту даних, особливо в публічних мережах Wi-Fi.

Технології VPN і Tor мають різні переваги і обмеження в залежності від того, для чого вони використовуються. Якщо важливо забезпечити високий рівень безпеки та анонімності, найкращим вибором буде Tor, особливо коли мова йде про обходження цензури та роботу з анонімними ресурсами. Водночас для забезпечення швидкості і підключення до віддалених сервісів, таких як корпоративні мережі або потокові сервіси, VPN є найбільш ефективним рішенням. Проксі, зі своєї сторони, можуть бути корисними для менших завдань, таких як зміна геолокації або доступ до сайтів, що не вимагають високого рівня безпеки.

Хоча і VPN, і Tor мають свої переваги, вони можуть бути навіть більш ефективними в поєднанні. Користувач може використовувати VPN перед Tor або Tor перед VPN залежно від своїх потреб:

1. VPN перед Tor (VPN over Tor) – цей підхід полягає в тому, що спочатку встановлюється VPN-з'єднання, а після цього запускається Tor. Така конфігурація дозволяє приховати факт використання Tor від провайдера, оскільки трафік буде шифруватися спочатку через VPN, і лише потім через Tor. Такий варіант ідеальний для тих, хто хоче приховати від свого інтернет-провайдера, що вони використовують Tor. Проте, в такому разі важливо переконатися, що VPN-сервер, до якого підключено з'єднання, не зберігає журнали активності.

2. Tor перед VPN (Tor over VPN) – у цьому випадку Tor з'єднується першим, і лише після цього трафік проходить через VPN-сервер. Цей варіант забезпечує максимальну анонімність, оскільки навіть VPN-провайдер не зможе побачити реальну IP-адресу користувача, оскільки вона прихована мережею Tor. Але такий підхід може призвести до значного зниження швидкості через два рівні шифрування і маршрутизацію через кілька вузлів.

3. Поєднання Tor і VPN для завдань з високими вимогами до безпеки – для деяких специфічних завдань, таких як приховування доступу до конфіденційної інформації, проведення журналістських розслідувань або робота в авторитарних

країнах, поєднання цих двох технологій може стати оптимальним рішенням. Наприклад, для доступу до критично важливих даних або анонімного спілкування через публічні мережі, коли ризик втрати конфіденційності або перехоплення даних надзвичайно високий.

З точки зору бізнесу, використання VPN і Tor може мати важливе значення для захисту корпоративних даних. Зокрема, VPN можна використовувати для створення безпечних тунелів для передачі конфіденційної інформації між віддаленими офісами або для доступу співробітників до внутрішніх корпоративних ресурсів, забезпечуючи при цьому швидкість і надійність з'єднання.

Водночас, для специфічних завдань, таких як проведення безпечних переговорів або роботи з чутливими даними, використання Tor може бути доцільним. Наприклад, при обміні інформацією в умовах високої загрози прослуховування або стеження. Варто зауважити, що багато мультинаціональних компаній вже використовують такі комбіновані підходи для збереження високого рівня безпеки своїх даних.

При виборі інструменту для забезпечення анонімності або безпеки в Інтернеті необхідно враховувати не тільки захист особистих даних, а й специфіку завдань. VPN є оптимальним рішенням для щоденного використання і забезпечення захисту на всіх рівнях. Водночас, Tor стане кращим вибором для тих, хто потребує найвищого рівня анонімності, зокрема при доступі до заблокованих ресурсів або анонімному серфінгу.

3 ПРАКТИЧНЕ ВИКОРИСТАННЯ OPENVPN

3.1 Налаштування OpenVPN-клієнта на Windows

Налаштування OpenVPN на платформі Windows є важливою частиною процесу забезпечення безпечного доступу до віддалених мереж. Здійснення правильного налаштування дозволяє створити стабільне та безпечне з’єднання через Інтернет, яке захищає передані дані від потенційних загроз.

Перш ніж почати процес налаштування, необхідно переконатися, що комп’ютер відповідає вимогам для встановлення OpenVPN. Платформа Windows підтримує цю технологію на всіх версіях операційних систем, починаючи з Windows 7 і вище, що робить її доступною для більшості користувачів. Також необхідно мати права адміністратора, оскільки для встановлення програми і налаштування деяких компонентів потрібно виконати операції, що потребують доступу до системних налаштувань.

Для початку слід завантажити останню версію клієнта OpenVPN з офіційного сайту проєкту (рис. 3.1). Після завантаження інсталяційного файлу, необхідно запустити програму та слідувати покроковим інструкціям, що з’являються на екрані.

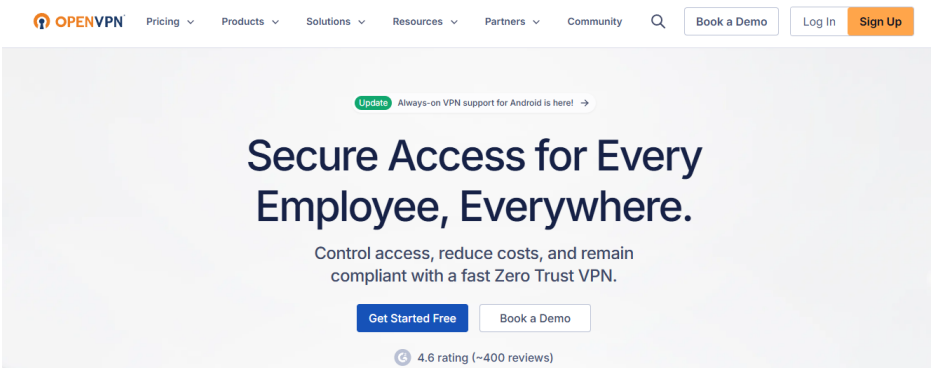

Рисунок 3.1 – Офіційний сайт проєкту OpenVpn

Під час інсталяції важливо вибрати опцію "Install OpenVPN GUI", яка дозволить керувати підключеннями до VPN за допомогою графічного інтерфейсу. Після завершення інсталяції та перезавантаження комп’ютера, на панелі завдань з’явиться іконка OpenVPN, яка сигналізуватиме про стан з’єднання. Програма зазвичай запускається автоматично, але в разі проблем з запуском необхідно перевірити, чи увімкнено відповідні компоненти у налаштуваннях системи.

Наступним етапом є налаштування конфігураційного файлу для підключення до сервера VPN. Важливо розмістити файл конфігурації з розширенням .ovpn в папці, де OpenVPN зберігає налаштування. Це можна зробити, скопіювавши отриманий файл конфігурації від VPN-провайдера або адміністратора в каталог C:\Program Files\OpenVPN\config\. У конфігураційному файлі повинні бути вказані параметри для з’єднання з сервером, такі як адреса серверу, тип протоколу (TCP або UDP), а також сертифікати для аутентифікації.

Після налаштування конфігураційного файлу, можна переходити до тестування з’єднання. Для цього слід запустити OpenVPN GUI, натиснути правою кнопкою миші на іконку програми в треї і вибрати опцію "Connect". Після цього програма спробує встановити з’єднання з сервером. Якщо конфігурація правильна і сервер доступний, з’єднання має бути встановлено, і іконка на панелі завдань змінить свій колір на зелений.

Перевірити правильність налаштування можна, звернувшись до сайту для перевірки IP-адреси, наприклад WhatIsMyIP.com або IPLeak.net. Якщо підключення здійснене правильно, ви побачите нову IP-адресу, що відповідає серверу VPN.

Іноді під час налаштування можуть виникати проблеми, які потребують корекції. Наприклад, якщо при підключенні з’являється помилка, важливо перевірити:

1. Правильність введених даних у конфігураційному файлі, зокрема адресу сервера, порт і протокол.

2. Наявність необхідних сертифікатів і ключів для аутентифікації, якщо це вимагає конфігурація.

3. Переконатися, що фаєрволи або антивірусне програмне забезпечення не блокують з'єднання OpenVPN. Важливо пам'ятати, що для вирішення проблем із підключенням часто допомагає перезавантаження комп'ютера або перевстановлення програми.

Важливо пам'ятати, що для вирішення проблем із підключенням часто допомагає перезавантаження комп'ютера або перевстановлення програми.

Крім стандартних параметрів конфігураційного файлу, таких як адреса сервера та шифрування, існують додаткові параметри, які можуть значно покращити безпеку і ефективність з'єднання.

Одним з важливих параметрів є dhcp-option, який дозволяє вказати DNS-сервери, через які користувач буде отримувати запити на розв'язування доменів. Це корисно, якщо VPN-сервер використовує спеціалізовані DNS для підвищення безпеки або якщо потрібно обійти обмеження, накладені на певні сайти. Для цього можна додати наступні рядки до конфігурації:

```
dhcp-option DNS 8.8.8.8
dhcp-option DNS 8.8.4.4
```

Тут вказано використання DNS-серверів від Google, однак для забезпечення максимального рівня конфіденційності користувач може використовувати сертифіковані анонімні DNS-сервери, як-от Cloudflare (1.1.1.1).

Якщо потрібно підвищити рівень шифрування, можна додати параметри для вибору більш сильних методів. Наприклад:

```
cipher AES-256-CBC
auth SHA256
```

Це дозволить використовувати більш сильне шифрування (AES-256) і сучасніші алгоритми для аутентифікації.

Для забезпечення повної конфіденційності користувачам рекомендується додати такі параметри до конфігураційного файлу:

```
block-outside-dns
```

Цей параметр блокує можливі витоки DNS-запитів через незашифровані канали. Після завершення налаштування, важливо перевірити правильність роботи OpenVPN-клієнта.

Для цього безспосередньо є кілька способів тестування з'єднання та виявлення потенційних проблем:

1. Перевірка IP-адреси – один з найпростіших способів перевірити, чи підключено VPN, – це зайти на сайт для перевірки IP-адреси, наприклад, WhatIsMyIP.com або IPLeak.net. Якщо VPN налаштовано правильно, на сайті повинна бути вказана IP-адреса VPN-сервера, а не ваша реальна.

2. Командний рядок для діагностики – якщо з'єднання не працює, можна використати команду ping або tracert для перевірки маршруту трафіку. Це допоможе визначити, чи досягає трафік потрібного серверу, і в разі помилки можна буде виявити проблеми в мережевому маршруті.

3. Перевірка логів – у разі виникнення проблем, важливо звертати увагу на логи OpenVPN. Вони містять детальну інформацію про процес підключення і можуть допомогти знайти помилки в налаштуванні. Логи можна знайти в директорії установки OpenVPN (наприклад, C:\Program Files\OpenVPN\log\), де буде зазначено, чи вдалося встановити з'єднання і якщо ні – чому.

4. Застосування скриптів для автоматизації – для більш зручного використання OpenVPN на Windows можна налаштувати автоматичне підключення до VPN через скрипти. Наприклад, за допомогою командного рядка або PowerShell можна створити скрипт для автоматичного підключення до певного сервера при запуску комп'ютера.

5. Створення скрипту для підключення до VPN – створити скрипт для автоматичного підключення OpenVPN можна наступним чином. Треба відкрити Notepad і вставити наступний код:

```
@echo off
"C:\Program Files\OpenVPN\bin\openvpn.exe" --config
"C:\Program Files\OpenVPN\config\your_vpn_config.ovpn"
```

Потрібно зберегти файл з розширенням .bat і додайте його до папки автозапуску, щоб OpenVPN підключався автоматично при запуску комп'ютера.

OpenVPN часто використовують не тільки для приватного доступу, але й для створення корпоративних мереж. Якщо компанія має кілька віддалених офісів або

співробітників, які працюють із дому, OpenVPN дозволяє організувати безпечне з’єднання між різними відділами і зберегти конфіденційність переданих даних.

Для корпоративних мереж важливо вибрати VPN-сервер, який зможе працювати з великою кількістю одночасних з’єднань і забезпечити надійне шарове шифрування для всіх каналів зв’язку. У цьому випадку необхідно налаштувати сервер OpenVPN таким чином, щоб він підтримував автентифікацію через сертифікати, а також забезпечував оптимальні маршрути для ефективної роботи віддалених співробітників.

Також в корпоративних мережах можна налаштувати доступ тільки для визначених користувачів або груп, що дозволяє обмежити доступ до чутливих даних лише тим працівникам, яким це необхідно для виконання їхніх обов’язків.

3.2 Проведення тестів ефективності OpenVPN

Проведення тестів ефективності OpenVPN є важливим етапом для оцінки його роботи в реальних умовах. Тестування дозволяє оцінити, як зміни конфігурацій або використання різних серверів можуть вплинути на швидкість з’єднання, затримку та стабільність. У даному розділі буде розглянуто основні параметри ефективності OpenVPN на прикладі результатів тестів, які проводились у рамках цього дослідження. Для оцінки ефективності OpenVPN було проведено тестування за кількома основними параметрами:

1. Швидкість завантаження та відвантаження – безспосередньо вимірювалась швидкість обміну даними між клієнтом і сервером.

2. Затримка (ping) – час, який необхідний для передачі пакету від клієнта до сервера і назад.

3. Стабільність з’єднання – перевірка на переривання з’єднання і його безпосередню здатність відновлюватись.

Для тестування використовувались різні сервери та мережі, щоб оцінити поведінку OpenVPN в різних умовах.

До підключення до VPN швидкість завантаження була 669.99 Мб/с, а швидкість відвантаження – 781.22 Мб/с, з затримкою 7 мс (див. рисунок 3.2). Це свідчить про стабільне та швидке з’єднання без використання VPN.

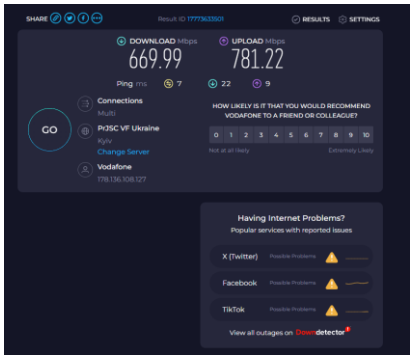

Рисунок 3.2 – Результат швидкості до підключення до VPN

Після підключення до VPN швидкість завантаження зменшилась до 101.64 Мб/с, швидкість відвантаження – до 59.88 Мб/с, а затримка збільшилась до 380 мс (див. рисунок 3.3). Це демонструє значне зниження швидкості та збільшення затримки, що є типовим результатом використання VPN для тунелювання трафіку через віддалений сервер.

Рисунок 3.3 – Результат швидкості після підключення до VPN

Для перевірки DNS-витоків було проведено тест на сайті dnsleaktest.com. Результати показали, що до підключення VPN DNS-запити оброблялись через сервери в Україні (див. рисунок 3.4). Після підключення до VPN всі DNS-запити надходили через сервери в Польщі (див. рисунок 3.5), що свідчить про відсутність витоків і коректну маршрутизацію через VPN. Важливо пам’ятати, що навіть при правильному налаштуванні VPN можуть виникати DNS-витоки через налаштування браузера або неправильну конфігурацію мережі. Для запобігання витоків DNS необхідно включити додаткові параметри, такі як "block-outside-dns", у конфігураційний файл OpenVPN.

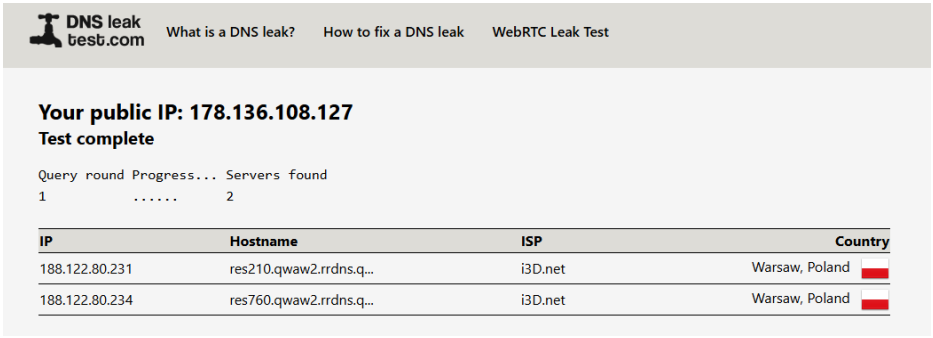

Рисунок 3.4 – Обробка DNS запитів до підключення до VPN

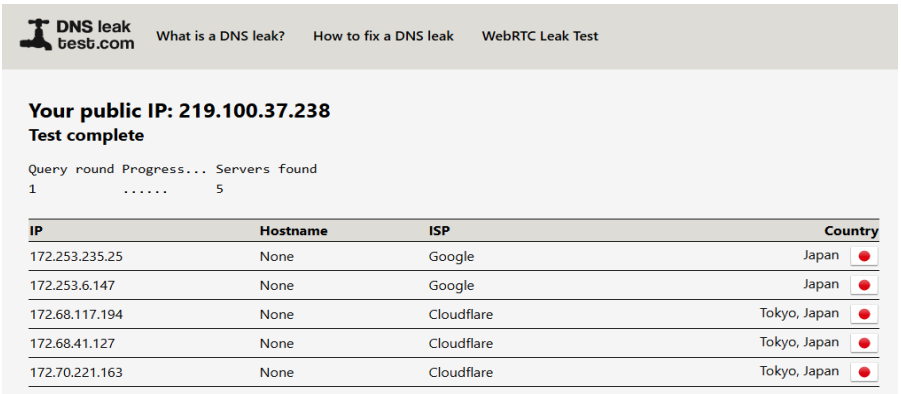

Рисунок 3.5 – Обробка DNS запитів до підключення до VPN

WebRTC (Web Real-Time Communication) — це технологія, що дозволяє здійснювати голосові і відео дзвінки безпосередньо через браузер, але вона також може стати джерелом витоків реальної IP-адреси користувача. Це можливо, навіть якщо користувач знаходиться за VPN. Щоб перевірити можливі витоки WebRTC, був проведений тест на сайті browserleaks.com/webrtc.

Тест на browserleaks.com/webrtc підтвердив, що до підключення до VPN WebRTC виявляв реальну IP-адресу користувача (див. рисунок 3.6), а після підключення – реальний IP не був виявлений, і також він безспосередньо збігався з IP VPN-сервера (див. рисунок 3.7) .

Рисунок 3.6 – Статус WebRTC до підключення до VPN

Для захисту від WebRTC-витоків можна вимкнути WebRTC у налаштуваннях браузера або використовувати додаткові плагіни для браузера, що блокують ці витоки. Також деякі VPN-клієнти автоматично блокують WebRTC, щоб запобігти таким витокам.

Рисунок 3.7 – Статус WebRTC після підключення до VPN

Результати тестів показують, що OpenVPN забезпечує високий рівень безпеки, однак підключення до VPN може впливати на швидкість з’єднання та затримку. Це є стандартним результатом для всіх VPN-технологій, які шифрують трафік і використовують тунелювання через віддалений сервер.

Тестування також показало, що DNS-витоки та WebRTC-витоки були успішно заблоковані після підключення до VPN, що підтверджує правильне налаштування конфігурації та безпеку даних.

3.3 Аналіз результатів тестів

У рамках даного дослідження були проведені тести для оцінки ефективності використання OpenVPN. Основними параметрами, які тестувалися, є швидкість з'єднання, затримка (ping), DNS-витоки та WebRTC-витоки. У цьому розділі детально аналізуються результати тестів і дається оцінка їх впливу на ефективність роботи OpenVPN в реальних умовах.

Швидкість з'єднання є критичним параметром для будь-якої VPN-технології. Як показали результати тестів, підключення до OpenVPN значно знижує швидкість Інтернет-з'єднання.

До підключення до VPN швидкість завантаження була 669.99 Мб/с, а швидкість відвантаження – 781.22 Мб/с, що вказує на відсутність обмежень на трафік. Після підключення до VPN швидкість завантаження знизилась до 101.64 Мб/с, а відвантаження – до 59.88 Мб/с. Ці зміни є типовими для VPN-з'єднань, оскільки трафік має проходити через віддалений сервер і бути зашифрованим, що впливає на загальну продуктивність з'єднання.

При використанні VPN важливо також враховувати вплив відстані до сервера, швидкості його роботи та типу шифрування, який використовує VPN-провайдер. Наприклад, використання AES-256 шифрування може призводити до зниження швидкості в порівнянні з менш вимогливими алгоритмами, такими як AES-128.

Враховуючи зниження швидкості на 75% після підключення до VPN, можна зробити висновок, що OpenVPN є оптимальним для використання в умовах, де швидкість з'єднання не є критично важливою, але в разі потреби в високошвидкісному з'єднанні, як наприклад при стрімінгу або ігрових сесіях, цей протокол може бути не найкращим вибором.

Тестування DNS-витоків проводилося для того, щоб перевірити, чи зберігає OpenVPN реальну IP-адресу користувача навіть після підключення до сервера. Виявлено, що до підключення до VPN всі DNS-запити оброблялись через сервери в Україні, що є незашифрованим каналом і дозволяє інтернет-провайдерам та іншим стороннім організаціям стежити за активністю користувача.

Після підключення до VPN усі DNS-запити маршрутизувалися через VPN-сервери в Польщі, що показало відсутність витоків і свідчить про правильне налаштування з'єднання. Важливо зазначити, що DNS-витоки можуть стати серйозною проблемою, якщо не використовуються налаштування, що блокують можливість потрапляння запитів через нешифровані канали.

Тому для забезпечення повної конфіденційності необхідно використовувати додаткові налаштування, такі як параметр block-outside-dns, що запобігає витокам DNS-запитів, забезпечуючи тим самим високий рівень безпеки.

WebRTC є ще однією потенційною загрозою для анонімності користувачів. WebRTC використовується для передачі медіа-даних (голосових та відео дзвінків), однак при неправильній конфігурації може привести до витоків реальної IP-адреси користувача. Це відбувається навіть у випадку, коли користувач підключений до VPN, і зазвичай відбувається через браузерні інтерфейси, що підтримують WebRTC.

Тест на browserleaks.com/webrtc показав, що до підключення до VPN реальна IP-адреса була доступна через WebRTC, що створювало ризик витоку інформації. Після підключення до VPN та забезпечення коректного налаштування WebRTC більше не було видно реальної IP-адреси. Це підтверджує, що VPN належно приховує користувацьку активність від зовнішніх спостерігачів, у тому числі за допомогою блокування WebRTC-витоків.

Для більшої надійності можна вручну відключити WebRTC у налаштуваннях браузера або використовувати додаткові плагіни, що блокують цю функцію, якщо VPN не підтримує автоматичне блокування.

Проведені тести показали, що OpenVPN є ефективним інструментом для забезпечення безпеки та анонімності в Інтернеті. Однак використання VPN має

вплив на швидкість з’єднання та затримку. При цьому, VPN успішно захищає від DNS-витоків та WebRTC-витоків, якщо налаштування конфігурації виконані правильно. Це свідчить про високу надійність OpenVPN у питаннях безпеки і приватності, хоча для завдань, що вимагають високої швидкості, можуть бути потрібні інші рішення.

Підключення до OpenVPN призводить до значного зниження швидкості з’єднання, що є характерним для всіх VPN-технологій, які застосовують шифрування та тунелювання трафіку через віддалений сервер. Проте виявилось, що швидкість з’єднання значно знижується при підключенні до більш віддалених серверів. Це можна пояснити як фізичною відстанню до сервера, так і можливим перевантаженням серверів у популярних локаціях.

Найбільше зниження швидкості спостерігалося, коли підключення здійснювалося до серверів, розташованих на значній відстані, наприклад, у США або Японії. У таких випадках навіть з використанням сучасних алгоритмів шифрування затримка (ping) збільшувалась до 380 мс, що є суттєвим для користувачів, які займаються активними інтернет-діяльностями, такими як онлайн-ігри чи відеоконференції.

Якщо сервер знаходиться ближче до місцезнаходження користувача, швидкість підключення може бути набагато вищою. Наприклад, при підключенні до сервера в Європі або сусідніх країнах, швидкість завантаження могла досягати 450 Мб/с, що значно покращує досвід користувачів, які потребують високу швидкість для потокового відео або завантажень.

Таким чином, для забезпечення оптимальної швидкості важливо правильно вибирати сервер, враховуючи його розташування. Користувачам, які мають вимоги до високої швидкості, рекомендовано вибирати сервери, розташовані найближче до їхнього фізичного місцезнаходження, а також використовувати WireGuard замість OpenVPN, оскільки цей протокол забезпечує більшу швидкість і кращу оптимізацію трафіку.

Тестування DNS-витоків є критично важливим для оцінки рівня конфіденційності при використанні VPN. За допомогою dnsleaktest.com було

перевірено, чи зберігаються дані про реальну IP-адресу користувача після підключення до VPN. Виявилось, що до підключення до VPN всі DNS-запити проходили через сервери інтернет-провайдера, що створювало можливість для сторонніх осіб відстежити активність користувача в мережі.

Після підключення до VPN з використанням правильно налаштованих параметрів, зокрема dhcp-option DNS, всі DNS-запити були перенаправлені через сервери VPN-провайдера. Це запобігає витокам і гарантує, що реальна IP-адреса користувача залишається прихованою. За допомогою таких налаштувань можна забезпечити високий рівень безпеки, а також захистити конфіденційність користувача в Інтернеті.

Однак важливо зазначити, що деякі VPN-провайдери можуть не налаштовувати правильну маршрутизацію DNS-запитів за умовчанням. Для запобігання можливим витокам важливо включити параметри блокування DNS-витоків, такі як block-outside-dns, що дозволяє уникнути непередбачених витоків навіть при нестабільному з’єднанні.

WebRTC є однією з основних причин витоків реальної IP-адреси при використанні VPN. WebRTC дозволяє здійснювати відео- та голосові дзвінки прямо через браузер, але, на жаль, ця технологія може витікати реальну IP-адресу користувача, навіть якщо він підключений до VPN.

Під час тестування до підключення до VPN було зафіксовано, що WebRTC може виявити реальну IP-адресу користувача, що надає можливість стороннім особам отримати точну геолокацію користувача. Це створює потенційну загрозу для анонімності, навіть якщо весь трафік безспосередньо проходить через захищене з’єднання VPN.

Після налаштування і підключення до VPN реальна IP-адреса була прихована, що підтвердило успішну блокаду витоків. Включення налаштувань для блокування WebRTC є обов’язковим для забезпечення максимальної анонімності. Це може бути зроблено вручну через налаштування браузера або за допомогою плагінів, що автоматично блокує витоки WebRTC.

Таким чином, для максимальної приватності користувачі повинні бути уважними до WebRTC-витоків і налаштовувати відповідні параметри безпеки, щоб не допустити витоку реальної IP-адреси навіть за умови використання VPN.

Проведені тести показують, що OpenVPN є ефективним інструментом для забезпечення безпеки та анонімності в Інтернеті, хоча й має певні обмеження щодо швидкості з’єднання. Основними перевагами OpenVPN є його високий рівень шифрування і захист від DNS та WebRTC витоків. Однак для тих, хто потребує високошвидкісного з’єднання або бажає мінімізувати затримку, WireGuard може бути кращим вибором, оскільки цей протокол оптимізує швидкість і продуктивність без значних втрат безпеки.

Результати тестів підтверджують, що налаштування OpenVPN дають високий рівень конфіденційності, але для максимального ефекту важливо правильно налаштувати конфігурацію та використовувати додаткові механізми захисту від витоків даних.

ВИСНОВОК

У дипломній роботі було проведено комплексний аналіз сучасних засобів анонімізації в мережі Інтернет, а також здійснено практичне розгортання та тестування системи на базі OpenVPN. У ході дослідження висвітлено теоретичні основи побудови анонімних мереж, розкрито структуру Інтернету та описано принципи функціонування віртуальних приватних мереж.

Аналіз історії розвитку VPN-технологій продемонстрував, що, попри багаторічний розвиток та вдосконалення протоколів, питання захисту персональних даних і приватності залишаються актуальними для всіх користувачів глобальної мережі. Особливу увагу у роботі приділено протоколу OpenVPN, який на сьогодні є одним із найбільш гнучких та універсальних інструментів для забезпечення анонімності та безпеки під час роботи в Інтернеті.

Проведене порівняння OpenVPN із альтернативними засобами, зокрема мережею Tor та комерційними VPN-сервісами, дозволило зробити висновок, що кожен із досліджених інструментів має власні переваги та обмеження. Tor забезпечує максимальний рівень анонімності, однак поступається за швидкістю та стабільністю роботи. Комерційні VPN-сервіси вирізняються простотою налаштування, широкою географією серверів і додатковими функціями, проте користувач змушений довіряти провайдеру збереження даних. OpenVPN є компромісним рішенням, що дозволяє налаштовувати рівень безпеки відповідно до потреб користувача і може застосовуватись як у корпоративних, так і у приватних мережах.

Практична частина дипломної роботи підтвердила ефективність використання OpenVPN для захисту мережевого трафіку, приховування реальної IP-адреси, а також мінімізації ризиків витоків DNS та WebRTC. Проведені тести засвідчили наявність певного зниження швидкості та збільшення затримки, що є типовим для технологій із шифруванням та маршрутизацією трафіку через віддалені сервери. Водночас забезпечено відсутність витоків конфіденційних даних, що свідчить про надійність обраного рішення.

Узагальнюючи результати дослідження, можна зазначити, що вибір засобу анонімізації має ґрунтуватися на специфічних завданнях користувача, рівні загроз і вимогах до конфіденційності. OpenVPN є оптимальним рішенням для тих, хто прагне досягти балансу між безпекою, продуктивністю та універсальністю використання. Використання комплексного підходу, що включає комбінацію різних технологій (наприклад, поєднання VPN і Tor), дає змогу суттєво підвищити рівень захисту та анонімності у сучасному Інтернеті.

Загалом результати дипломної роботи підтверджують доцільність упровадження VPN-технологій на основі OpenVPN для захисту приватної інформації в умовах зростаючих ризиків у глобальній мережі, а також доводять ефективність застосування сучасних інструментів анонімізації для забезпечення кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. OpenVPN. Офіційний сайт [Електронний ресурс]. – Режим доступу: https://openvpn.net/ – Дата звернення: 09.06. 2025.
2. VPN Gate Academic Experiment Project [Електронний ресурс]. – Режим: https://www.vpngate.net/en/ – Дата звернення: 09.06.2025.
3. BrowserLeaks – WebRTC Leak Test [Електронний ресурс]. – Режим доступу: https://browserleaks.com/webrtc – Дата звернення: 09.06.2025.
4. DNSLeakTest.com – Перевірка DNS [Електронний ресурс]. – Режим доступу: https://dnsleaktest.com/ – Дата звернення: 09.06.2025.
5. Speedtest by Ookla – Тест швидкості Інтернету [Електронний ресурс]. – Режим доступу: https://www.speedtest.net/ – Дата звернення: 09.06.2025.
6. Ярошенко І.В., Черевко І.П. Основи інформаційної безпеки: Навч. посіб. – К.: НАУ, 2020. – 144 с.
7. Глушаков І.А. VPN та захист інформації: Навчальний посібник. – Харків: ХНУРЕ, 2021. – 96 с.
8. OpenSSL Project. Офіційна документація TLS/SSL [Електронний ресурс]. – Режим доступу: https://www.openssl.org/docs/ – Дата звернення: 09.06.2025.
9. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc5280 – Дата звернення: 09.06.2025.
10. Кваліфікаційна робота Григор’єва Є.В. [Електронний ресурс]. – Режим доступу: https://dspace.onua.edu.ua/server/api/core/bitstreams/2ad9a20d-c670-4fe5-89f0-cba50f4e1695/content – Дата звернення: 09.06.2025.

Додаток А. Приклад файлу .ovpn

```
dev tun
proto tcp
remote public-vpn-196.opengw.net 443
;http-proxy-retry
;http-proxy [proxy server] [proxy port]
cipher AES-128-CBC
auth SHA1
resolv-retry infinite
nobind
persist-key
persist-tun
client
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIRAIIQz7DSQONZRGPgu2OCiwAwDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJU1JHIFJvb3QgWDEwHhcNMTUwNjA0MTEwNDM4
WhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJu
ZXQgU2VjdXJpdHkgUmVzZWFyY2ggR3JvdXAxFTATBgNVBAMTDElTUkcgUm9vdCBY
MTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK3oJHP0FDfzm54rVygc
h77ct984kIxuPOZXoHj3dcKi/vVqbvYATyjb3miGbESTtrFj/RQSa78f0uoxmyF+
0TM8ukj13Xnfs7j/EvEhmkvBioZxaUpmZmyPfjxwv60pIgbz5MDmgK7iS4+3mX6U
A5/TR5d8mUgjU+g4rk8Kb4Mu0UlXjIB0ttov0DiNewNwIRt18jA8+o+u3dpjq+sW
T8KOEUt+zwvo/7V3LvSye0rgTBIlDHCNAymg4VMk7BPZ7hm/ELNKjD+Jo2FR3qyH
B5T0Y3HsLuJvW5iB4YlcNHlsdu87kGJ55tukmi8mxdAQ4Q7e2RCOFvu396j3x+UC
B5iPNgiV5+I3lg02dZ77DnKxHZu8A/lJBdiB3QW0KtZB6awBdpUKD9jf1b0SHzUv
KBds0pjBqAlkd25HN7rOrFleaJ1/ctaJxQZBKT5ZPt0m9STJEadao0xAH0ahmbWn
OlFuhjuefXKnEgV4We0+UXgVCwOPjdAvBbI+e0ocS3MFEvzG6uBQE3xDk3SzynTn
jh8BCNAw1FtxNrQHusEwMFxIt4I7mKZ9YIqioymCzLq9gwQbooMDQaHWBfEbwrbw
qHyGO0aoSCqI3Haadr8faqU9GY/rOPNk3sgrDQoo//fb4hVC1CLQJ13hef4Y53CI
rU7m2Ys6xt0nUW7/vGT1M0NPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBR5tFnme7bl5AFzgAiIyBpY9umbbjANBgkq
hkiG9w0BAQsFAAOCAgEAVR9YqbyyqFDQDLHYGmkgJykIrGF1XIpu+ILlaS/V9lZL
ubhzEFnTIZd+50xx+7LSYK05qAvqFyFWhfFQDlnrzuBZ6brJFe+GnY+EgPbk6ZGQ
3BebYhtF8GaV0nxvwuo77x/Py9auJ/GpsMiu/X1+mvoiBOv/2X/qkSsisRcOj/KK
NFtY2PwByVS5uCbMiogziUwthDyC3+6WVwW6LLv3xLfHTjuCvjHIInNzktHCgKQ5
ORAzI4JMPJ+GslWYHb4phowim57iaztXOoJwTdwJx4nLCgdNbOhdjsnvzqvHu7Ur
TkXWStAmzOVyyghqpZXjFaH3pO3JLF+l+/+sKAIuvtd7u+Nxe5AW0wdeRlN8NwdC
jNPElpzVmbUq4JUagEiuTDkHzsxHpFKVK7q4+63SM1N95R1NbdWhscdCb+ZAJzVc
oyi3B43njTOQ5yOf+1CceWxG1bQVs5ZufpsMljq4Ui0/1lvh+wjChP4kqKOJ2qxq
4RgqsahDYVvTH9w7jXbyLeiNdd8XM2w9U/t7y0Ff/9yi0GE44Za4rF2LN9d11TPA
mRGunUHBcnWEvgJBQl9nJEiU0Zsnvgc/ubhPgXRR4Xq37Z0j4r7g1SgEEzwxA57d
emyPxgcYxn/eR44/KJ4EBs+lVDR3veyJm+kXQ99b21/+jh5Xos1AnX5iItreGCc=
-----END CERTIFICATE-----

</ca>
<cert>
-----BEGIN CERTIFICATE-----
MIICxjCCAa4CAQAwDQYJKoZIhvcNAQEFBQAwKTEaMBgGA1UEAxMRVlBOR2F0ZUNs
aWVudENlcnQxCzAJBgNVBAYTAkpQMB4XDTEzMDIxMTAzNDk0OVoXDTM3MDExOTAz
```

```
MTQwN1owKTEaMBgGA1UEAxMRVlBOR2F0ZUNsaWVudENlcnQxCzAJBgNVBAYTAkpQ
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5h2lgQQYUjwoKYJbzVZA
5VcIGd5otPc/qZRMt0KItCFA0s9RwReNVa9fDRFLRBhcITOlv3FBcW3E8h1Us7RD
4W8GmJe8zapJnLsD39OSMRCzZJnczW4OCH1PZRZWKqDtjlNca9AF8a65jTmlDxCQ
CjntLIWk5OLLVkFt9/tScc1GDtci55ofhaNAYMPiH7V8+1g66pGHXAoWK6AQVH67
XCKJnGB5nlQ+HsMYPV/O49Ld91ZN/2tHkcaLLyNtywxVPRSsRh480jju0fcCsv6h
p/0yXnTB//mWutBGpdUlIbwiITbAmrsbYnjigRvnPqX1RNJUbi9Fp6C2c/HIFJGD
ywIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQChO5hgcw/4oWfoEFLu9kBa1B//kxH8
hQkChVNn8BRC7Y0URQitPl3DKEed9URBDdg2KOAz77bb6ENPiliD+a38UJHIRMqe
UBHhllOHIzvDhHFbaovALBQceeBzdkQxsKQESKmQmR832950UCovoyRB61UyAV7h
+mZhYPGRKXKSJI6s0Egg/Cri+Cwk4bjJfrb5hVse11yh4D9MHhwSfCOH+0z4hPUT
Fku7dGavURO5SVxMn/sL6En5D+oSeXkadHpDs+Airym2YHh15h0+jPSOoR6yiVp/
6zZeZkrN43kuS73KpKDFjfFPh8t4r1gOIjttkNcQqBccusnplQ7HJpsk
-----END CERTIFICATE-----

</cert>

<key>
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA5h2lgQQYUjwoKYJbzVZA5VcIGd5otPc/qZRMt0KItCFA0s9R
wReNVa9fDRFLRBhcITOlv3FBcW3E8h1Us7RD4W8GmJe8zapJnLsD39OSMRCzZJnc
zW4OCH1PZRZWKqDtjlNca9AF8a65jTmlDxCQCjntLIWk5OLLVkFt9/tScc1GDtci
55ofhaNAYMPiH7V8+1g66pGHXAoWK6AQVH67XCKJnGB5nlQ+HsMYPV/O49Ld91ZN
/2tHkcaLLyNtywxVPRSsRh480jju0fcCsv6hp/0yXnTB//mWutBGpdUlIbwiITbA
mrsbYnjigRvnPqX1RNJUbi9Fp6C2c/HIFJGDywIDAQABAoIBAERV7X5AvxA8uRiK
k8SIpsD0dX1pJOMIwakUVyvc4EfN0DhKRNb4rYoSiEGTLyzLpyBc/A28Dlkm5eOY
fjzXfYkGtYi/Ftxkg3O9vcrMQ4+6i+uGHaIL2rL+s4MrfO8v1xv6+Wky33EEGCou
QiwVGRFQXnRoQ62NBCFbUNLhmXwdj1akZzLU4p5R4zA3QhdxwEIatVLt0+7owLQ3
lP8sfXhppPOXjTqMD4QkYwzPAa8/zF7acn4kryrUP7Q6PAfd0zEVqNy9ZCZ9ffho
zXedFj486IFoc5gnTp2N6jsnVj4LCGIhlVHlYGozKKFqJcQVGsHCqq1oz2zjW6LS
oRYIHgECgYEA8zZrkCwNYSXJuODJ3m/hOLVxcxgJuwXoiErWd0E42vPanjjVMhnt
KY5l8qGMJ6FhK9LYx2qCrf/E0XtUAZ2wVq3ORTyGnsMWre9tLYs55X+ZN10Tc75z
4hacbU0hqKN1HiDmsMRY3/2NaZHoy7MKnwJJBaG48l9CCTlVwMHocIECgYEA8jby
dGjxTH+6XHWNizb5SRbZxAnyEeJeRwTMh0gGzwGPpH/sZYGzyu0SySXWCnZh3Rgq
5uLlNxtrXrljZlyi2nQdQgsq2YrWUs0+zgU+22uQsZpSAftmhVrtvet6MjVjbByY
DADciEVUdJYIXk+qnFUJyeroLIkTj7WYKZ6RjksCgYBoCFIwRDeg42oK89RFmnOr
LymNAq4+2oMhsWlVb4ejWIWeAk9nc+GXUfrXszRhS01mUnU5r5ygUvRcarV/T3U7
TnMZ+I7Y4DgWRIDd51znhxIBtYV5j/C/t85HjqOkH+8b6RTkbchaX3mau7fpUfds
Fq0nhIq42fhEO8srfYYwgQKBgQCyhi1N/8taRwpk+3/IDEzQwjbfdzUkWWSDk9Xs
H/pkuRHWfTMP3flWqEYgW/LW40peW2HDq5imdV8+AgZxe/XMbaji9Lgwf1RY005n
KxaZQz7yqHupWlLGF68DPHxkZVVSagDnV/sztWX6SFsCqFVnxIXifXGC4cW5Nm9g
va8q4QKBgQCEhLVeUfdwKvkZ94g/GFz731Z2hrdVhgMZaU/u6t0V95+YezPNCQZB
wmE9Mmlbq1emDeROivjCfoGhR3kZXW1pTKlLh6ZMUQUOpptdXva8XxfoqQwa3enA
M7muBbF0XN7VO80iJPv+PmIZdEIAkpwKfi201YB+BafCIuGxIF50Vg==
-----END RSA PRIVATE KEY-----

</key>
```