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

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«РОЗГОРТАННЯ ЗАСОБІВ АНОНІМІЗАЦІЇ НА ПРИКЛАДІ TOR»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека»
Григор'єв Олександр Володимирович

Керівник: професор, д.ф-м.н.
Василенко Микола Дмитрович

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

Одеса – 2024

ЗМІСТ

ВСТУП

Актуальність теми. Збільшення кількості цифрових загроз, таких як стеження, хакінг і цензура, спонукає користувачів шукати надійні способи захисту своєї приватності в інтернеті. Мережа TOR дозволяє забезпечити анонімність в Інтернеті шляхом маршрутизації інтернет-запитів через вузли, які розташовані по всьому світу, тим самим ускладнюючи простеження джерела трафіку.

Широка потреба в анонімності підкреслюється не тільки небажанням користувачів розкривати свою особистість або місцезнаходження, але й необхідністю уникнення державного нагляду або контролю з боку інших третіх сторін. Особливо це стосується журналістів, правозахисників і політичних активістів, для яких конфіденційність може бути питанням професійного виживання.

Анонімізація через TOR також має значення для бізнесу. Компанії використовують TOR для забезпечення безпечного віддаленого доступу до корпоративних мереж, особливо коли їхні співробітники працюють з нестабільних або небезпечних регіонів. Це дозволяє забезпечити захист корпоративних даних і мінімізувати ризики витоку інформації.

Наукове співтовариство також використовує TOR для забезпечення безпеки своїх досліджень, особливо в контекстах, де наукова діяльність може бути піддана репресіям або політичному контролю. Таким чином, анонімізація не лише захищає особисту інформацію, але й сприяє науковому прогресу.

Освітній сектор також відзначає переваги TOR, особливо в умовах, коли доступ до наукових матеріалів обмежений або цензурований. Студенти і викладачі можуть використовувати TOR для доступу до бібліотек, електронних ресурсів і освітніх платформ без страху перед можливими наслідками за їх інтелектуальну діяльність.

Мета дослідження аналізі технологій анонімізації з акцентом на системі TOR.

Для досягнення поставленої мети необхідно виконати такі **завдання:**

1) надати характеристику структури інтернета та анонімізація

2) дослідити основні етапи розвиток анонімних мереж
3) надати принципи роботи анонімних мереж
4) проаналізувати мережі TOR та її роботу з VPN
5) оцінити архітектуру мережі TOR і принципи роботи протоколу
6) визначити основні аспекти клієнтського програмного забезпечення на різних ОС
7) визначити практичні приклади використання TOR
8) скласти потенційні ризики використання TOR та їх мінімізація

Об'єкт дослідження системи анонімізації в мережі Інтернет.

Предмет дослідження технології та принципи роботи анонімізаційної мережі TOR, а також методи забезпечення анонімності та приватності її користувачів.

Практичне значення отриманих результатів полягає в підвищенні розуміння та ефективності використання анонімізаційних технологій на прикладі мережі Tor. Завдяки аналізу архітектури та безпекових аспектів Tor, можливо виявити та усунути потенційні вразливості, що значно збільшить захист користувачів від небажаного стеження та інших форм втручання. Отримані дані допоможуть розробникам і фахівцям у сфері кібербезпеки створювати більш безпечні та надійні інструменти для анонімізації. Також результати дослідження можуть використовуватися для освіти та підготовки спеціалістів, які працюють у сферах, де конфіденційність є критично важливою.

1 ПОНЯТТЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ TOR

1.1 Структура інтернета та анонімізація

Інтернет являє собою глобальну мережу, яка з'єднує мільярди пристроїв по всьому світу, формуючи складну і динамічну систему комунікацій. Він складається з безлічі маленьких та великих мереж, що включають приватні комп'ютери, мобільні телефони, планшети, і сервери, які спілкуються через комплекс взаємодій між локальними мережами, інтернет-провайдерами, точками обміну трафіком, та дата-центрами. Всі ці компоненти зв'язані між собою через великі мережеві магістралі, включаючи підводні кабелі, що пролягають на дні океанів та морів, забезпечуючи миттєвий обмін інформацією на величезні відстані.

У цій складній мережі велике значення має анонімність, яка дозволяє користувачам зберігати конфіденційність, обходити цензуру та захищати особисті дані від несанкціонованого доступу. Анонімізація в інтернеті досягається за допомогою віртуальних приватних мереж (VPN), які шифрують трафік користувачів та приховують їх реальні IP-адреси за IP-адресами VPN-серверів. Також широко використовується система TOR, що надає можливість передачі даних через розподілену мережу вузлів, замасковуючи дійсне джерело і призначення інформації, яка передається. Додаткову безпеку забезпечує шифрування, яке захищає дані на всьому їх шляху від відправника до одержувача [1].

Проте, потрібно пам'ятати, що анонімність в мережі може бути використана як в законних, так і в незаконних цілях, що вимагає ретельного підходу до регулювання технологій анонімізації. Освічений користувач мережі повинен бути свідомим всіх потенційних ризиків та користей, що випливають з використання таких технологій, щоб забезпечити максимальний захист своєї особистості та даних.

Структура інтернету та процеси анонімізації в інтернеті є двома важливими аспектами сучасної цифрової ери. Розглянемо кожен з них детальніше.

Інтернет складається з величезної кількості взаємопов'язаних мереж, які включають мільярди пристроїв по всьому світу. Основні елементи структури інтернету включають:

1. Кінцеві пристрої та клієнтські системи - приватні комп'ютери, мобільні телефони, планшети, та інші пристрої, які використовують люди для доступу до інтернету.
2. Локальні мережі (LAN) та вай-фай мережі - малі мережі в офісах, будинках тощо, які з'єднують кінцеві пристрої з інтернетом.
3. Інтернет-провайдери (ISP) - компанії, які надають інтернет-послуги та з'єднують локальні мережі з глобальною системою інтернету.
4. Точки обміну трафіком (IXP) і основні мережеві магістралі - великі мережеві вузли, де трафік між різними інтернет-провайдерами обмінюється
5. Дата-центри та сервери - сервери зберігають веб-сторінки, додатки, і бази даних, які ми використовуємо через інтернет.
6. Підводні комунікаційні кабелі - кабелі, розміщені на дні океанів, які з'єднують мережі різних континентів.
7. Протоколи (TCP/IP, HTTP, HTTPS, FTP, і т.д.) - стандарти, які регулюють передачу даних в інтернеті [2].

Анонімізація в інтернеті – це процеси та методи, які дозволяють користувачам захищати свою особистість і діяльність в мережі. Основні методи анонімізації можна побачити в таблиці 1.1.

Таблиця 1.1 – Методи анонимізації [3]

№	Метод	Опис
1	Віртуальні Приватні Мережі (VPN)	VPN створює зашифроване з'єднання між пристроєм користувача та сервером VPN, приховуючи IP-адресу користувача за IP-адресою VPN-сервера.

2	TOR (The Onion Router)	TOR дозволяє користувачам відправляти трафік через розподілену мережу вузлів, ефективно маскуючи походження та призначення даних.
3	Шифрування	Дані можуть бути зашифровані на кінцевому пристрої перед тим, як будуть відправлені через інтернет, щоб захистити їх від перехоплення.
4	Проксі-сервери	Проксі діють як посередники між користувачем та інтернетом, приховуючи реальні IP-адреси користувачів.
5	Платформи для анонімного перегляду	Інструменти типу "Incognito" режим в браузерах можуть допомогти приховати історію перегляду, але не замінюють повноцінні анонімізаційні технології.
6	Спеціалізовані операційні системи	Системи, як Tails або Whonix, розроблені для того, щоб максимально зберегти анонімність користувачів.

Анонімізація в інтернеті захищає право користувачів на приватне життя, допомагає обійти цензуру, і забезпечує безпеку в мережі. Однак, важливо розуміти, що повна анонімність важко досяжна і може бути використана як для законних, так і для незаконних цілей.

Інтернет являє собою глобальну мережу, яка з'єднує мільярди пристроїв по всьому світу, формуючи складну і динамічну систему комунікацій. Він складається з безлічі маленьких та великих мереж, що включають приватні комп'ютери, мобільні телефони, планшети, і сервери, які спілкуються через комплекс взаємодій між локальними мережами, інтернет-провайдерами, точками обміну трафіком, та дата-центрами. Всі ці компоненти зв'язані між собою через великі мережеві магістралі, включаючи підводні кабелі, що пролягають на дні океанів та морів, забезпечуючи миттєвий обмін інформацією на величезні відстані.

У цій складній мережі велике значення має анонімність, яка дозволяє користувачам зберігати конфіденційність, обходити цензуру та захищати особисті дані від несанкціонованого доступу. Анонімізація в інтернеті досягається за допомогою віртуальних приватних мереж (VPN) [4], які шифрують трафік користувачів та приховують їх реальні IP-адреси за IP-адресами VPN-серверів. Також широко використовується система TOR, що надає можливість передачі даних через розподілену мережу вузлів, замасковуючи дійсне джерело і призначення інформації, яка передається. Додаткову безпеку забезпечує шифрування, яке захищає дані на всьому їх шляху від відправника до одержувача.

Проте, потрібно пам'ятати, що анонімність в мережі може бути використана як в законних, так і в незаконних цілях, що вимагає ретельного підходу до регулювання технологій анонімізації. Освічений користувач мережі повинен бути свідомим всіх потенційних ризиків та користей, що випливають з використання таких технологій, щоб забезпечити максимальний захист своєї особистості та даних.

Така детальна структура інтернету і різноманітні способи анонімізації підкреслюють не лише технологічні можливості сучасності, але й складність викликів, що стоять перед кожним користувачем у глобальному веб-просторі.

1.2 Історія та розвиток анонімних мереж

Історія та розвиток анонімних мереж є складним і багатогранним процесом, який розпочався ще у 1970-х роках і продовжується донині. Основною метою анонімних мереж є забезпечення приватності та анонімності користувачів в інтернеті. Вони дозволяють користувачам приховувати свою фактичну IP-адресу, географічне розташування та іншу ідентифікаційну інформацію, надаючи можливість обмінюватися інформацією або використовувати інтернет-ресурси без ризику відстеження.

Зародження ідеї анонімних мереж відбулося у часи, коли інтернет ще тільки розвивався. Перші дослідження у цій області були направлені на створення засобів

захисту персональних даних користувачів від несанкціонованого доступу. Важливим кроком стало створення технології віртуальних приватних мереж (VPN), які дозволяли створювати зашифровані з'єднання між комп'ютерами в інтернеті, ефективно "маскуючи" реальну IP-адресу користувача [5].

Надзвичайний розвиток анонімних мереж припадає на 2000-ті роки з появою TOR (The Onion Router). TOR став відомий завдяки своїй здатності директорій маршрутизації інтернет-трафіку через різні сервери, розташовані по всьому світу, що робило майже неможливим відслідковування вихідних точок з'єднань. Система TOR використовує так звану технологію "лукової маршрутизації", при якій дані зашифровуються декілька разів і проходять через кілька вузлів мережі, кожен з яких розшифровує шар шифрування, перш ніж передати дані наступному вузлу.

Разом з ростом популярності TOR, з'явилися інші анонімні мережі, такі як I2P (Invisible Internet Project), який спеціалізується на створенні внутрішньої анонімної мережі, де користувачі можуть взаємодіяти у відносно захищеному середовищі. I2P шифрує користувацькі дані в пакетах і дозволяє користувачам відправляти їх через власну мережу серверів, ускладнюючи відстеження [6]. Принцип роботи I2P бачимо на рисунку 1.1.

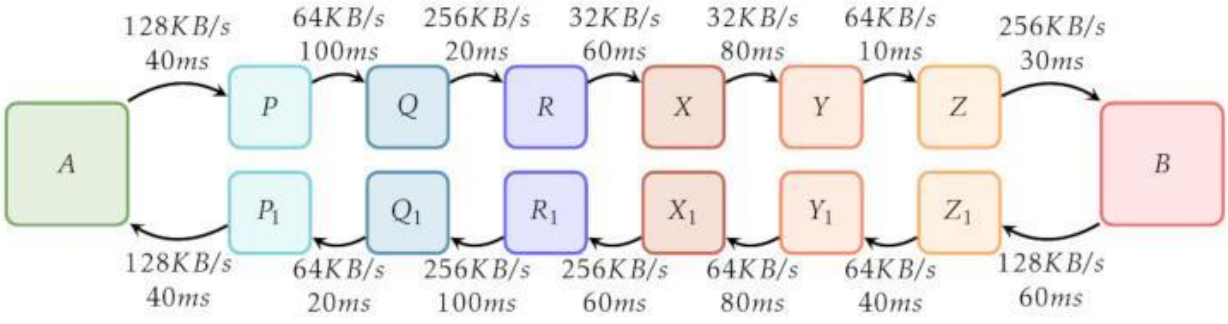

Рисунок 1.1 Принцип роботи I2P [6]

Технології анонімних мереж неперервно вдосконалюються, але вони також стикаються з численними викликами, включаючи спроби урядових і комерційних організацій розробити методи "розкриття" анонімності користувачів. Це призвело

до "гонитви озброєнь" між розробниками анонімних мереж та тими, хто намагається компрометувати їхню ефективність.

Наразі, анонімні мережі використовуються не тільки для захисту приватності звичайних користувачів, але й для захисту журналістів, правозахисників та інших осіб, які працюють у небезпечних умовах або країнах з обмеженим доступом до свободи слова. Анонімні мережі також стали популярним засобом для обходу цензури в інтернеті, дозволяючи користувачам вільно отримувати та передавати інформацію, недоступну через традиційні медіа.

Враховуючи їхню важливість у сучасному світі, де інформаційна безпека стає все більш критичною, анонімні мережі продовжуватимуть розвиватися, адаптуючись до нових викликів і технологічних можливостей.

Однією з ключових причин, чому анонімні мережі набули такої великої популярності та необхідності, є зростання цифрового спостереження та збільшення обсягів збору даних комерційними та урядовими організаціями. В епоху великих даних, коли інформація стала одним із найважливіших ресурсів, приватність в інтернеті опинилася під загрозою. Це спонукало до пошуку рішень, які б могли гарантувати анонімність та безпеку в інтернеті, де користувачі могли б вільно обмінюватися інформацією без страху бути ідентифікованими або відслідкованими.

З іншого боку, анонімні мережі часто стають об'єктом критики та контроверсій через їх використання в сумнівних та нелегальних цілях. Темні сторони інтернету, такі як Dark Web (рис. 1.2), часто асоціюються з анонімними мережами, адже вони надають платформу для продажу наркотиків, зброї та інших незаконних товарів та послуг. Це створює великі виклики для правоохоронних органів у всьому світі, оскільки анонімність користувачів значно ускладнює процес ідентифікації та притягнення до відповідальності порушників закону.

Незважаючи на ці виклики, розвиток анонімних мереж продовжує йти вперед, водночас розвиваючи нові технології захисту даних та приватності. Однією з останніх інновацій є впровадження блокчейн технологій у сферу анонімних мереж, що відкриває нові можливості для створення розподілених,

нецентралізованих систем, які можуть забезпечити ще вищий рівень анонімності та безпеки.

Ключовим аспектом майбутнього розвитку анонімних мереж буде знаходження балансу між необхідністю забезпечення приватності та анонімності користувачів та потребою забезпечення національної безпеки та запобігання злочинності. Технології постійно змінюються, і як суспільство, так і технічна спільнота мають адаптуватися до цих змін, знаходячи оптимальні шляхи вирішення цих складних проблем.

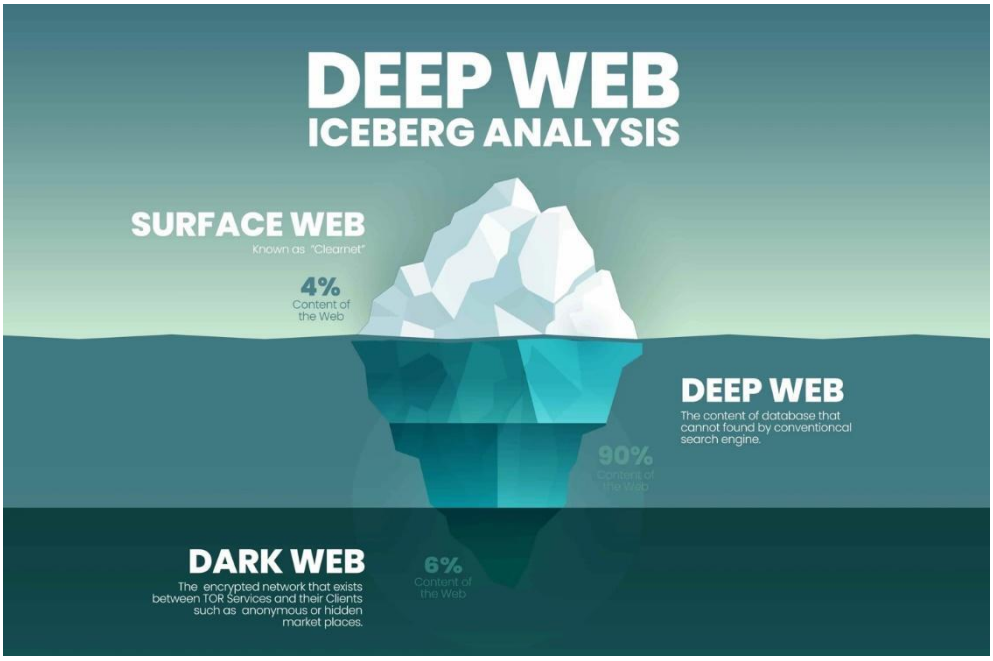

Рисунок 1.2 «Глубокий інтернет» [7]

Проблематика регулювання анонімних мереж і забезпечення законного і безпечного їх використання залишається актуальною, викликаючи гарячі дебати на рівні державних і міжнародних організацій. Ідеальне рішення повинно враховувати права і свободи індивідуумів, а також колективні інтереси безпеки і порядку.

Важливим аспектом є і розвиток технологій шифрування, які лежать в основі анонімних мереж. Прогрес у квантових обчисленнях може в майбутньому змінити правила гри, оскільки здатність квантових комп'ютерів розшифровувати сучасні криптографічні системи може зробити багато з них застарілими. Це ставить під

сумнів майбутнє приватності та анонімності в цифровому світі і вимагає розробки нових, більш стійких методів шифрування.

Попри проблеми, анонімні мережі сприяють підтримці вільного обміну інформацією, що є життєво важливим для демократичних суспільств. Вони допомагають забезпечувати приватність користувачів, які живуть у країнах з репресивними режимами, і підтримують свободу преси та вираження думок. Таким чином, анонімні мережі виступають не тільки як технічний інструмент, але й як засіб політичного і соціального вираження.

Що ж стосується майбутнього, розвиток анонімних мереж вимагатиме нових інноваційних підходів для забезпечення їх стійкості до потенційних загроз, таких як квантове декодування, і адаптації до постійно змінюваних умов цифрового світу. Також потрібно буде виробити механізми взаємодії з правоохоронними і регулюючими органами для забезпечення законності їх використання, що дозволить гармонійно інтегрувати анонімні мережі в суспільне життя, мінімізуючи ризики і максимізуючи переваги для всіх користувачів.

1.3 Принципи роботи анонімних мереж

Анонімні мережі — це спеціалізовані мережеві системи, які дозволяють користувачам залишатися анонімними у глобальній мережі, захищаючи їхню особистість та дані від сторонніх поглядів. Створені з метою забезпечення конфіденційності та безпеки, ці мережі використовують різноманітні техніки шифрування та маршрутизації, щоб замаскувати трафік користувача та ускладнити будь-які спроби його відстеження.

На сьогоднішній день, TOR, знаний як The Onion Router, є однією з найвідоміших анонімних мереж. Він використовує так звану маршрутизацію через "луковичні шари", де дані проходять через ряд випадково вибраних вузлів, кожен з яких додає або видаляє шар шифрування, завдяки чому слід користувача стає практично неможливо простежити. Tor також застосовує службу директорії для

оновлення статусів вузлів, що допомагає оптимізувати та безпечно вибирати маршрути для даних.

I2P, або Invisible Internet Project, пропонує альтернативний підхід, фокусуючись на забезпеченні безпеки внутрішніх з'єднань між користувачами. Відмінною особливістю I2P є гарлічне шифрування, яке одночасно шифрує декілька повідомлень, забезпечуючи вищий рівень анонімності та ефективність передачі даних. Мережа використовує комплексні тунелі, які дозволяють даним проходити через множину вузлів, додатково захищаючи інформацію від зовнішнього втручання [8].

Freenet вибудовує свою роботу на принципах peer-to-peer, де кожен учасник мережі виступає як міні-сервер для розподілу та зберігання шифрованих копій файлів. Це робить мережу особливо стійкою до цензури та блокування, оскільки відсутній єдиний контрольний центр або точка входу, яку можна було б вимкнути або заблокувати.

VPN, хоч і не є чисто анонімною мережею, відіграє важливу роль у захисті приватності користувачів. Шифрування з'єднань від кінця до кінця та приховування реальних IP-адрес користувачів допомагає уникнути відстеження та інтерцепції даних, тим самим забезпечуючи безпечний простір для обміну інформацією.

Кожна з цих мереж використовує свої унікальні методи та протоколи для забезпечення максимальної анонімності та безпеки користувачів, відповідаючи на постійно зростаючу потребу у захисті особистої інформації в цифровому світі.

Анонімні мережі дозволяють користувачам захищати свою особистість та приватність під час користування Інтернетом. Ці мережі використовують різні технології та протоколи для забезпечення анонімності та безпеки. Ось основні принципи роботи декількох популярних анонімних мереж:

TOR - найбільш відома анонімна мережа, що використовує техніку маршрутизації лука, щоб забезпечити анонімність:

1. Маршрутизація лука - дані передаються через випадково вибрані вузли (вузли TOR), кожен з яких додає або знімає шар шифрування, схоже на лущення цибулини.
2. Вузли в'єднання, середні вузли, та виходи - трафік проходить через вузол в'єднання, один або декілька середніх вузлів, і нарешті через вихідний вузол, де він виходить у відкритий Інтернет.
3. Шифрування - кожен вузол шифрує та розшифровує інформацію, забезпечуючи, що жоден окремий вузол не може простежити шлях від початку до кінця.
4. Служба директорії - вузли оновлюють свої статуси в центральному репозиторії, що допомагає вибирати оптимальний маршрут [9].

I2P—це анонімна мережа, спеціалізована на забезпеченні безпечних внутрішніх з'єднань між користувачами:

1. Гарлічне шифрування (Garlic Encryption) - шифрування декількох повідомлень разом для забезпечення кращої анонімності та ефективності.
2. Тунелі - використовуються два типи тунелів—вхідні та вихідні. Трафік проходить через кілька тунелів для забезпечення анонімності.
3. Декілька шарів шифрування - схоже на TOR, але з більшою кількістю шарів та складнішими алгоритмами.

Freenet використовує peer-to-peer принципи для розподілу даних у вигляді шифрованого кешування:

1. Розподілене зберігання - кожен вузол мережі зберігає частину загальних даних.
2. Динамічна маршрутизація - трафік направляється за допомогою алгоритмів маршрутизації, заснованих на викликах та попиті, не за фіксованими шляхами.
3. Сповільнення трафіку (traffic throttling) - для захисту приватності трафік може бути уповільнений.

Хоча VPN не є чисто анонімною мережею, вона важлива для забезпечення приватності:

1. Шифроване з'єднання - всі дані, що передаються через VPN, шифруються від вашого пристрою до VPN сервера.
2. Сховище IP адреси - VPN приховує вашу реальну IP адресу, замінюючи її IP адресою VPN сервера.
3. Захист від стеження – шифрування та заміна IP затруднюють відстеження вашої діяльності в Інтернеті.

Загальні риси анонімних мереж:

1. Множинне шифрування - застосування кількох шарів шифрування для забезпечення безпеки та анонімності.
2. Децентралізація - відсутність центрального контролюючого органу, що знижує ризик цензури та блокування.
3. Алгоритми маршрутизації - використання складних алгоритмів для забезпечення анонімності маршрутів передачі даних [8].

Кожна з цих мереж має свої особливості та оптимальні сценарії використання, але всі вони спрямовані на забезпечення більшої приватності користувачів у мережі.

В цілому, анонімні мережі використовують складні технології шифрування і маршрутизації для забезпечення того, щоб користувачі могли безпечно та конфіденційно взаємодіяти в цифровому світі. Множинне шифрування, децентралізація, і сложні алгоритми маршрутизації спільно забезпечують фундаментальні засоби для захисту приватності користувачів у сучасному Інтернет-просторі. Це не просто технічні рішення, а важливі інструменти для збереження особистих прав і свобод в епоху цифрової інформації.

У світлі зростаючих загроз цифровій приватності та безпеці, анонімні мережі стають не просто корисними інструментами, але й необхідністю для захисту особистої інформації користувачів. Використання мереж як TOR, I2P, Freenet та VPN може значно ускладнити відстеження активності користувачів, забезпечити конфіденційність передачі даних і обходити цензуру, відкриваючи доступ до вільної інформації без страху перед репресіями або втручанням ззовні.

Така анонімність є особливо важливою в умовах сучасного цифрового ландшафту, де уряди та великі корпорації постійно шукають способи збору і аналізу особистих даних. Анонімні мережі надають можливість протистояти цій тенденції, дозволяючи зберігати приватність, захищати особисту свободу та сприяти вільному обміну інформацією.

Завдяки їх здатності забезпечити множинне шифрування та децентралізовану маршрутизацію, анонімні мережі виступають як бастіони в боротьбі за цифрові права та свободи в усьому світі. Отже, розуміння та активне використання цих інструментів є критично важливими для всіх, хто цінує свою цифрову анонімність та безпеку. Вони не тільки підвищують нашу індивідуальну захищеність, але й колективно сприяють підтримці вільного і відкритого Інтернету, доступного і безпечного для всіх його користувачів.

2 ОГЛЯД АПАРАТНОЇ ТА ПРОГРАМНОЇ ЧАСТИНА ПРОЄКТУ

2.1 Характеристики мережі TOR та робота з VPN

TOR (The Onion Router) — це комплексна система для анонімного веб-серфінгу, яка дозволяє користувачам зберігати конфіденційність та безпеку їхніх онлайн активностей від сторонніх очей, включаючи інтернет-провайдерів та урядові структури. Система TOR використовує масив добровільних серверів, відомих як вузли, для створення шифрованого мережевого маршруту, через який проходить трафік, замасковуючи інформацію про місцезнаходження користувача і зміст даних. Головна сторінка сайту зображена на рисунку 2.1.

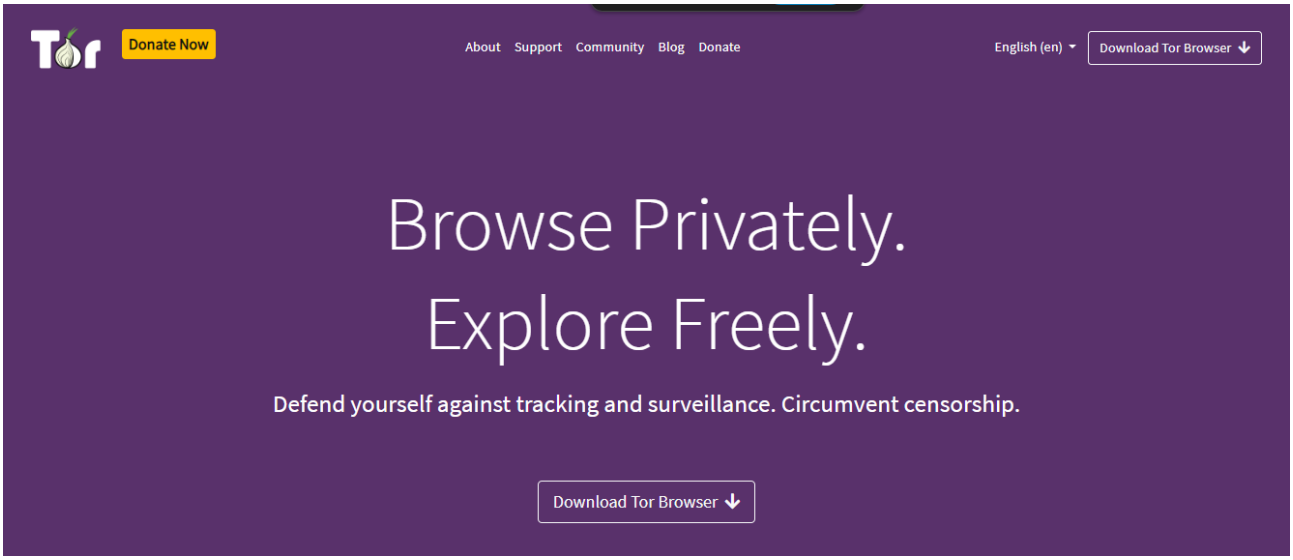

Рисунок 2.1 Головна сторінка TOR [10]

TOR маршрутизує інтернет-запити через сложний ланцюжок вузлів (роутерів), які шифрують вхідні та вихідні дані на кожному етапі, з кожним наступним шаром шифрування, що накладається на попередній, схоже на шари цибулі. Це додає міцні шари анонімності, перешкоджаючи будь-кому відслідковувати діяльність від кінцевого користувача до остаточного призначення веб-запитів.

У 1990-х роках постало усвідомлення, що Інтернет, у своїй первісній конструкції, не забезпечує адекватного рівня захисту персональних даних користувачів, а також відкритий для різного роду нагляду та контролю. Особливо це стало зрозуміло, коли в 1995 році Девід Гольдшлаг, Майк Рід і Пол Сайверсон з Науково-дослідної лабораторії ВМС США (NRL) розпочали проєкт із розробки новітнього методу анонімного входу в Інтернет. Їхнім завданням було створення системи, яка дозволила б зберігати ідентичність користувачів в секреті навіть у випадку активних спроб їх ідентифікації чи відстеження [10].

Їх робота призвела до розробки прототипів маршрутизації, які використовували принцип "цибулевого шифрування". Суть методу полягала в множинному перенаправленні інтернет-трафіку через різні сервери, знаходжені по всьому світу, та шифруванні даних на кожному кроці їх передачі. Це стало основою для майбутньої системи TOR (The Onion Router), яка мала на меті забезпечення найвищого рівня конфіденційності в інтернеті.

На початку 2000-х років проєкт залучив нові сили, зокрема Роджера Дінгледіна, свіжого випускника Массачусетського технологічного інституту (MIT). Разом з Полом Сайверсоном, вони розпочали інтенсивну роботу над вдосконаленням цибулевої маршрутизації. Роджер Дінгледін вніс значний вклад у проект, що тепер відомий як "Проект Тор", щоб підкреслити його відмінність від інших схожих ініціатив. Незабаром до команди приєднався Нік Метьюсон, також випускник MIT і колишній однокурсник Роджера, який значно підсилив розробницький потенціал проекту.

Робота над TOR включала створення складної архітектури серверів, які б виконували функції в'язки для передачі шифрованих даних. Ці сервери, відомі як вузли TOR, були розподілені географічно по всьому світу, що забезпечувало рівень анонімності, недоступний в інших мережах. Кожен шар шифрування, доданий на кожному вузлі, додатково зміцнював безпеку даних, перешкоджаючи можливості їх перехоплення або аналізу.

Протягом наступних років "Проект Тор" розвивався і здобув підтримку в академічних колах та серед правозахисних організацій, які вбачали в ньому

потужний інструмент для захисту права на приватне життя в цифрову епоху. Сьогодні TOR використовується мільйонами людей по всьому світу як засіб захисту їх анонімності онлайн, дозволяючи уникати цензури та спостереження, незалежно від політичних або географічних обмежень.

Кожен вузол мережі здійснює шифрування трафіку, створюючи так зване цибулеве шифрування, де дані захищені на кожному етапі своєї передачі. Зміна вузлів в ланцюжку відбувається кожні 10 хвилин або при кожному новому з'єднанні, що робить ідентифікацію конкретного користувача складнішою.

Вразливість траєкторії трафіку особливо критична на останньому вихідному вузлі, де можливе перехоплення HTTP-пакетів, що несуть інформацію про відвідувані ресурси. Такі дані можуть включати URL-адреси з заголовку запиту Referer. Одним із рішень цієї проблеми є використання HTTPS-протоколу, який дозволяє захищати дані на останньому етапі передачі.

Завдяки великій кількості користувачів, яка майже досягла 2 мільйонів щомісяця, та більш ніж 6000 волонтерських серверів щодня, мережа TOR забезпечує високий рівень анонімності. Це оверлейна мережа, де кожен цибулевий роутер запущений як звичайний процес без спеціальних прав.

Цибулевий проксі (ЦП), який кожен користувач запускає на своєму пристрої, відповідає за отримання директорій, налаштування та підтримку з’єднань. Використовуючи TCP потоки, ці ЦП пересилають дані через захищені ланцюги з’єднань, де кожен пакет даних має фіксовану довжину 512 байт і складається з заголовка та тіла [11].

TOR використовує цибулеву маршрутизацію для створення захищених ланцюгів, де кожен ретранслятор знає тільки передоднього та наступного в ланцюзі, не володіючи інформацією про повний шлях пакету. Це дозволяє користувачам анонімно доступати інтернет та відвідувати приховані служби TOR.

Часта помилка користувачів полягає в неправильному розумінні анонімізації трафіку при використанні не через TOR браузери, такі як Chrome. TOR захищає лише трафік, що проходить через нього. Разом з браузером TOR рекомендується

використання Firefox з плагіном TORbutton для кращого контролю над анонімністю і вимкнення ризикованих плагінів.

Для забезпечення максимальної анонімності досвідчені користувачі застосовують оперативну систему Linux Tails (The Amnesic Incognito Live System), яка може запускатися з USB-накопичувача, зберігаючи анонімність усіх підключень через TOR і не залишаючи жодних слідів на використовуваному пристрої.

У світі цифрової анонімності і безпеки, TOR і VPN є двома основними інструментами, що допомагають захистити особисті дані та обходити цензуру. Обидва варіанти, TOR-through-VPN та VPN-through-TOR, мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб користувача. Детально переваги та недоліки варіантів використання TOR та VPN складено в таблиці 2.1.

Таблиця 2.1 – Види взаємодії TOR та VPN [12]

Вид	Переваги	Недоліки
TOR-through-VPN	Інтернет-провайдер відстежує лише активність VPN, не знаючи про використання TOR. Захист від вузлів входу TOR: Вузли входу TOR бачитимуть IP-адресу VPN, а не вашу реальну IP-адресу, що підвищує анонімність.	VPN знає вашу IP-адресу, це створює потенційну точку вразливості, оскільки VPN може вести журнали користувачів. Ризик на виході TOR: Хоча вхідний вузол не бачить вашу IP, вихідний вузол TOR може бути під контролем зловмисників і використовуватись для перехоплення даних.
VPN-through-TOR	З цією конфігурацією, ні VPN, ні Інтернет-провайдер, ні будь-яка інша сторона не зможе	Необхідно знайти VPN-провайдера, який дозволяє таке з'єднання та налаштувати його відповідним чином.

	відслідковувати вашу діяльність до мережі TOR. Захист від зловмисних виходів TOR: Використання VPN після TOR гарантує, що вихідний вузол TOR не бачить вашу реальну IP-адресу і не може перехоплювати ваші дані.	Обмеження швидкості: Обидва, TOR і VPN, сповільнюють інтернет-з'єднання, і їх комбінація може знизити швидкість інтернету до неприйнятних рівнів для деяких користувачів.

У варіанті TOR-through-VPN, трафік спочатку проходить через VPN-сервер, а потім через мережу TOR перед тим, як досягти інтернету. Це відмінний спосіб приховати від вашого Інтернет-провайдера факт використання TOR, оскільки вони бачитимуть лише зашифроване з'єднання до VPN.

На відміну від TOR-through-VPN, схема VPN-through-TOR передбачає спочатку вхід у мережу TOR, а потім підключення до VPN. Це важливо для тих, хто хоче забезпечити максимальний рівень анонімності.

Вибір між TOR-through-VPN та VPN-through-TOR залежить від вашої потреби в анонімності та типу вашої діяльності в інтернеті. Якщо ваш основний пріоритет — приховати використання TOR від Інтернет-провайдера, то TOR-through-VPN буде відповідним варіантом. Якщо ж ви хочете максимально захистити свої дані на кожному етапі транзакції, тоді VPN-through-TOR є більш переважним.

2.2 Архітектура мережі TOR і принципи роботи протоколу

TOR забезпечує конфіденційність за допомогою унікальної архітектури, що базується на принципах маршрутизації через "цибулинні" шари. Ця мережа складається з трьох основних типів вузлів: вхідних (або захисних) реле, проміжних

реле та вихідних реле [13]. В окремих випадках для обходу блокувань, встановлених корпораціями або урядовими установами, використовуються мостові вузли, які дозволяють з'єднання з мережею, коли стандартні вхідні або вихідні вузли заблоковані. Загальні характеристики вхідних, серединніх та вихідних вузлів описано в таблиці 2.2.

Таблиця 2.2 Види вузлів TOR [14]

№	Вузли	Характеристика
1.	Вхідні вузли (Entry Guards)	Ці вузли відомі користувачу і служать першою точкою входу в мережу TOR. Вони знають реальну IP-адресу користувача, але не знають конечного призначення запитів.
2.	Серединні вузли (Middle Relays)	Забезпечують продовження передачі даних від вхідного до вихідного вузла, приховуючи ключові деталі транзакції.
3.	Вихідні вузли (Exit Nodes)	Остання точка передачі даних з мережі TOR до веб-сайту. Вихідний вузол може бачити трафік, який виходить з мережі TOR, але не знає реальної IP-адреси користувача, що значно ускладнює спроби відстеження.

Вхідний вузол служить головним воротами до мережі TOR. Клієнт, який має намір з'єднатися з цією мережею, спершу встановлює зв'язок з захисним реле, яке є єдиною точкою, здатною визначити реальну IP-адресу користувача. Інформація про захисні вузли регулярно оновлюється і доступна у відкритих джерелах. Однак, існують ризики, пов’язані з можливістю контролю зловмисниками деяких реле, що може призвести до зловживань.

Захисні вузли, як правило, оновлюються кожні два до трьох місяців, щоб запобігти атакам на анонімність. Під час зміни реле в активному сеансі, захисний вузол залишається незмінним для забезпечення додаткової безпеки.

Проміжне реле відіграє ключову роль у передачі даних, діючи як центральна ланка в ланцюгу TOR. Дані, які проходять через проміжні реле, шифруються, що унеможливлює визначення повного маршруту передачі кожним окремим вузлом. Це забезпечує високий рівень захисту і приватності. Проміжні реле не мають можливості діяти як вихідні вузли, тому не можуть бути визначені як точка походження або призначення трафіку, що мінімізує їхню відповідальність за переданий контент [14].

Вихідний вузол є останнім елементом у ланцюгу TOR, кінцевою точкою передачі даних до призначення. Цей вузол зазвичай асоціюється з певними ризиками, оскільки він відкрито виступає як джерело трафіку, що робить його IP-адресу видимою для отримувача. Власники вихідних вузлів повинні бути готові до юридичних викликів, зокрема щодо запитів на видалення контенту або юридичних повідомлень. Прицнип функціонування усього ланцюга TOR зображено на рисунку 2.2.

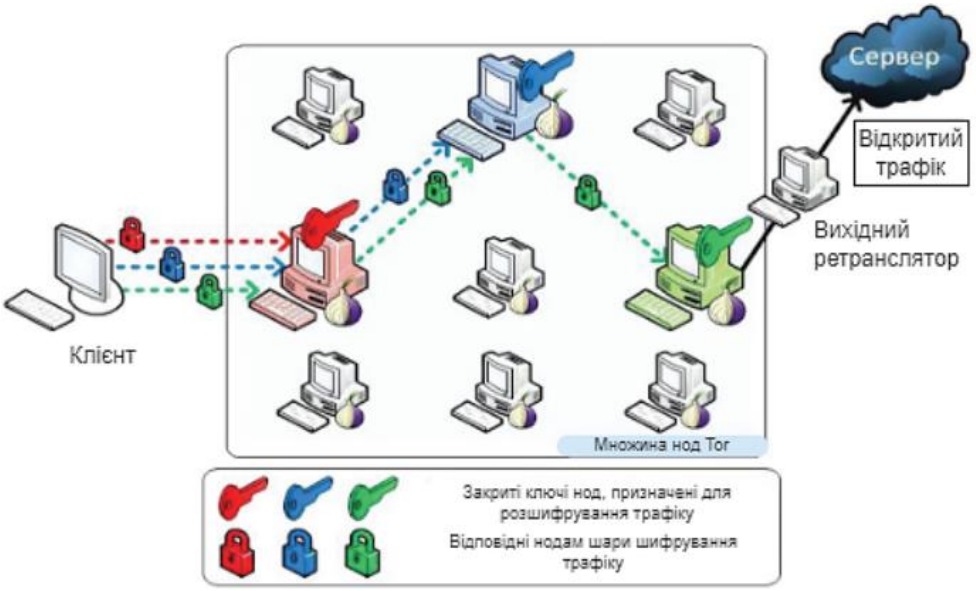

Рисунок 2.2 Принцип функціонування ланцюга TOR [14]

I

Мостові вузли, що не перераховані у загальнодоступному каталозі, використовуються для обходу фільтрації доступу до мережі TOR, яку можуть встановити уряди або корпорації. Ці вузли допомагають користувачам з'єднуватися

з мережею, коли загальнодоступні вузли заблоковані, наприклад, у Китаї. Щоб використовувати мостовий вузол, потрібно налаштувати спеціальні параметри конфігурації.

Інтернет-провайдери, корпоративні організації, і уряди часто встановлюють фільтри, які блокують доступ до мережі TOR, аби контролювати анонімність та конфіденційність користувачів в інтернеті. Один із прикладів такої практики - Китай, де уряд ефективно блокує всі загальнодоступні вузли TOR, ускладнюючи використання цієї мережі в межах країни. В таких умовах, щоб обійти блокування і забезпечити доступ до TOR, використовуються спеціальні налаштування через так звані мостові вузли (Bridge nodes) [15].

Мостові вузли - це приватні вузли в мережі TOR, які не відображаються у загальнодоступному списку вузлів. Ці вузли допомагають користувачам обійти блокування TOR, оскільки адреси цих вузлів не відомі цензорам, що ускладнює їх блокування. Мостові вузли є важливим інструментом для забезпечення доступу до TOR в країнах зі строгим інтернет-цензурованим режимом, таких як Китай, Іран, та Росія.

Для того щоб використовувати мостові вузли для доступу до мережі TOR, потрібно виконати наступні кроки:

1. Завантаження та інсталяція TOR Browser:
2. Спершу потрібно завантажити та встановити TOR Browser з офіційного сайту TOR Project.
3. Для отримання адрес мостових вузлів ви можете відвідати сторінку bridges.TORproject.org або надіслати запит на адресу bridges@TORproject.org з текстом "get bridges". Вам будуть надіслані адреси мостових вузлів, які можна використовувати.
4. При першому запуску TOR Browser, виберіть опцію “Configure” і вказівку на те, що у вашій країні мережа TOR може бути заблокована. Потім виберіть опцію “Use a bridge”, і ви зможете ввести один із отриманих адрес мостових вузлів.

5. Введіть одну або декілька адрес мостових вузлів, які ви отримали. Це можуть бути різні типи мостів, такі як obfs4, meek-azure, або інші, які забезпечують різні рівні обфускації трафіку.

6. Після введення адрес мостових вузлів, продовжуйте налаштування та дозвольте TOR Browser завершити конфігурацію. Якщо все зроблено правильно, ваше підключення до мережі TOR буде виконано через мостовий вузол, що дозволить вам обійти блокування і забезпечить анонімний доступ до інтернету.

Використання мостових вузлів є ефективним способом для обходу блокувань і цензури у країнах з обмеженим доступом до інтернету. Такий метод забезпечує користувачам можливість вільного та безпечного використання інтернет-ресурсів, незалежно від геополітичних обмежень.

2.3 Клієнтське програмне забезпечення на різних ОС

Програмне забезпечення TOR (The Onion Router) є безкоштовним інструментом для анонімного користування інтернетом та обходу цензури, який доступний для багатьох операційних систем, включаючи Windows, macOS, Linux, а також Android і iOS через мобільні додатки. У цій статті ми розглянемо особливості клієнтського програмного забезпечення TOR для різних ОС. Особливості використання складено в таблиці 2.3.

Таблиця 2.3 – Використання TOR на різних ОС

№	ОС	Принцип роботи
1.	Windows	На Windows клієнт TOR може бути встановлений через TOR Browser, який базується на Firefox і містить всі необхідні налаштування для забезпечення анонімності. Встановлення полягає у завантаженні і запуску файлу інсталятора з офіційного сайту проекту. TOR Browser автоматично налаштовується і включає все необхідне для миттєвого входу в мережу TOR, зокрема, і інтеграцію з системою NoScript для

		блокування JavaScript та HTTPS Everywhere для шифрування з'єднань.
2.	macOS	Для користувачів macOS, TOR також доступний у формі TOR Browser, який легко інсталюється з драг-енд-дроп інсталяцією в папку "Додатки". Так само як і для Windows, версія для macOS містить всі захисні механізми та додаткові налаштування для забезпечення анонімності і безпеки даних.
3.	Linux	У Linux існує кілька способів встановлення TOR, зокрема через пакети для різних дистрибутивів (наприклад, через apt для Ubuntu або yum для Fedora) або компіляція з джерельних кодів. TOR Browser для Linux, як правило, включає ті ж функції, що й для інших платформ, і також забезпечує високий рівень захисту користувача.
4.	Android	На Android TOR доступний через додаток Orbot, який є VPN-службою, що маршрутизує весь трафік через мережу TOR, і TOR Browser для Android. Ці додатки дозволяють користувачам мобільних пристроїв безпечно та анонімно користуватися інтернетом, обходити блокування та захищати особисті дані.

На операційній системі Windows клієнт мережі TOR можна встановити за допомогою TOR Browser, який є спеціалізованим веб-браузером, розробленим на базі Mozilla Firefox. Він призначений для забезпечення конфіденційності та анонімності користувачів у мережі Інтернет шляхом маршрутизації трафіку через розподілену мережу серверів, відомих як вузли TOR. Ця технологія дозволяє користувачам обходити цензуру і забезпечує захист від мережевого спостереження та аналізу трафіку [16].

Процес встановлення TOR Browser на Windows простий і не вимагає спеціальних технічних знань від користувача. Першим кроком є відвідування офіційного сайту проекту TOR, де користувачі можуть завантажити файл інсталятора для Windows. Після завантаження файлу інсталятора його потрібно

запустити, що ініціює процес встановлення. Протягом процесу встановлення користувачам можуть бути запропоновані додаткові опції налаштування, але в більшості випадків стандартні налаштування виявляються адекватними для забезпечення безпечного та анонімного серфінгу.

TOR Browser автоматично налаштовується на використання мережі TOR і включає в себе ряд важливих заходів безпеки та приватності. Серед них — інтеграція з розширенням NoScript, яке дозволяє користувачам керувати виконанням JavaScript на відвідуваних веб-сайтах. Це зменшує ризик використання JavaScript для здійснення мережевих атак або відстеження користувачів. Крім того, TOR Browser містить розширення HTTPS Everywhere, яке змушує веб-сайти використовувати зашифроване з'єднання, коли це можливо, забезпечуючи додатковий рівень захисту даних користувачів.

Для користувачів macOS, процес завантаження та встановлення TOR Browser виглядає наступним чином:

1. Перехід на сторінку завантаження TOR Browser:

Відкрийте ваш браузер та перейдіть на офіційну сторінку завантаження TOR Browser за адресою https://www.TORproject.org/download/. Це гарантує, що ви отримаєте останню та найбезпечнішу версію браузера.

2. Завантаження файлу для macOS:

На сторінці завантаження знайдіть секцію для завантаження версії для macOS та натисніть на посилання файла з розширенням .dmg. Файл автоматично завантажиться на ваш комп’ютер.

3. Перевірка підпису файла (рекомендовано):

Для забезпечення того, що файл не був змінений або пошкоджений під час передачі, рекомендується перевірити його цифровий підпис. Це можна зробити за допомогою програми GPG Suite, яка дозволяє перевірити підпис та впевнитись у автентичності файла.

4. Встановлення програми:

Після завершення завантаження, знайдіть файл .dmg у папці завантажень та двічі клікніть по ньому для відкриття. Відкриється вікно з інструкціями та TOR Browser у формі додатка.

5. Перетягніть іконку TOR Browser у вашу папку "Програми" (Applications), щоб завершити процес інсталяції.

Додатково, можливо вам знадобиться підтвердити встановлення, вводячи пароль адміністратора або дозволяючи встановлення з невизначених джерел в налаштуваннях системи безпеки macOS.

6. Запуск TOR Browser:

Після встановлення, відкрийте папку "Програми" та клікніть по іконці TOR Browser для його запуску.

При першому запуску може з'явитися діалогове вікно, яке запитає дозвіл на відкриття програми, оскільки вона була завантажена з Інтернету. Підтвердіть вашу згоду, та продовжіть.

Встановлення TOR на Linux є важливим кроком для користувачів, які прагнуть забезпечити анонімність та безпеку під час інтернет-серфінгу. TOR (The Onion Router) дозволяє користувачам захищати свою приватність в інтернеті шляхом направлення трафіку через розподілену мережу серверів, забезпечуючи анонімність та ускладнення слідкування діяльності користувача [17].

Способи встановлення TOR на Linux:

1. Встановлення через пакетний менеджер:

- Debian/Ubuntu:

- Використання `apt`:

sudo apt update

sudo apt install TOR TORbrowser-launcher

- Цей спосіб є найпростішим та рекомендованим для новачків, оскільки пакети підтримуються спільнотою і зазвичай є актуальними.

- Fedora/Red Hat:

- Використання `dnf` (раніше `yum`):

```
sudo dnf install TOR
```

- Для встановлення TOR Browser, може знадобитись додавання зовнішнього репозиторію або використання Flatpak.

- Arch Linux:

- Використання `pacman`:

sudo pacman -S TOR

- Також можна встановити `TORbrowser-launcher` з AUR для отримання TOR Browser.

2. Компіляція з джерельних кодів:

- Скачування останньої версії джерельного коду з офіційного [сайту TOR](https://www.TORproject.org/download/TOR/).

- Компіляція з коду забезпечує більш гнучке налаштування та можливість використання останніх розробок, але це вимагає більше часу та розуміння процесу:

```
tar -xvf TOR-*.tar.gz
cd TOR-*
./configure
make
sudo make install
```

Забезпечення анонімності в інтернеті є критично важливим в наш час, і TOR є одним з найнадійніших інструментів для цього. Встановлення та використання TOR на Linux допоможе користувачам залишатися анонімними та безпечними під час онлайн активності.

На Android, доступ до мережі TOR здійснюється через два основні додатки: Orbot і TOR Browser. Orbot є VPN-службою, яка використовує технологію TOR для маршрутизації весь інтернет-трафіку користувача через розподілену мережу серверів, відомих як вузли TOR. Це дозволяє користувачам зберігати анонімність та безпеку під час інтернет-сесій, захищаючи їхні особисті дані від стеження та інтерцепції. Orbot також може бути налаштований для використання окремих або всіх додатків на пристрої.

TOR Browser для Android пропонує схожу функціональність, але у форматі браузера, спеціально адаптованого для анонімного веб-серфінгу. Цей браузер

автоматично маршрутизує веб-запити через мережу TOR, ефективно блокуючи сторонні спроби стеження за активністю користувача і допомагаючи обходити цензуру інтернету. Такий підхід дозволяє відкрити доступ до веб-сайтів, які можуть бути заблоковані в певних країнах або регіонах, забезпечуючи свободу інформації.

Користування Orbot і TOR Browser на Android є особливо корисним у країнах зі строгими законами щодо інтернету, де уряди блокують доступ до певного контенту або здійснюють масовий нагляд за інтернет-активністю своїх громадян. Окрім забезпечення доступу до заблокованих ресурсів, ці додатки також захищають від потенційних кібератак і зловмисного програмного забезпечення, яке часто розповсюджується через незахищені або інфіковані веб-сайти.

Використання TOR через Orbot і TOR Browser на Android має певні нюанси. Перш за все, швидкість інтернету може значно знизитися через те, що дані відправляються через ряд випадково вибраних вузлів TOR перед досягненням кінцевого пункту. Також, для забезпечення повної анонімності і безпеки користувачам необхідно дотримуватися рекомендацій щодо безпеки, як-от вимкнення JavaScript в TOR Browser, не використання браузерних розширень, які можуть витікати інформацію, та регулярне очищення cookies і кешу.

Комбіноване використання Orbot і TOR Browser на мобільному пристрої Android є ефективним способом забезпечення приватності в інтернеті, дозволяючи користувачам відчувати себе в безпеці під час онлайн-активностей, зокрема при відправці чутливих даних, таких як логіни, паролі, фінансова інформація, тощо.

Користувачам всіх платформ рекомендується завжди завантажувати останню версію TOR Browser з офіційного сайту проекту, щоб гарантувати максимальну безпеку і анонімність. Також важливо регулярно оновлювати програмне забезпечення, щоб уникнути потенційних уразливостей, які можуть бути використані для деанонімізації користувачів.

Клієнтське програмне забезпечення TOR на різних ОС забезпечує потужний інструмент для забезпечення приватності і безпеки в інтернеті, дозволяючи користувачам вільно доступати інформацію та обходити гео-рестрикції без ризику особистої інформації.

3 ПРАКТИЧНЕ ВИКОРИСТАННЯ TOR І РИЗИКИ

3.1 Анонімізація трафіку: практичні приклади використання TOR

TOR це інструмент, що стає опорою для активістів, журналістів та всіх, хто цінує свою приватність у цифровій ері. Але разом із цими перевагами приходять і виклики, включаючи потенційні ризики безпеки та використання для злочинних цілей. Розуміння та використання TOR потребує обачливості та розсудливості, але його роль у забезпеченні приватності та анонімності в Інтернеті надзвичайно важлива у сучасному цифровому світі.

Анонімізація трафіку за допомогою TOR (The Onion Router) - це популярний метод забезпечення приватності та анонімності в Інтернеті. Ось декілька практичних прикладів використання TOR:

1. Анонімне перегляд веб-сторінок - один з найпоширеніших використань TOR - це анонімний перегляд веб-сайтів. Користувачі можуть скористатися TOR для доступу до веб-ресурсів без ризику викриття їх місцезнаходження чи ідентичності.
2. Захист від слідування - користувачі можуть використовувати TOR для уникнення слідування їхніх онлайн-дій. Це особливо корисно у країнах, де інтернетова діяльність може бути моніторена або обмежена.
3. Анонімне спілкування - TOR може бути використаний для анонімного спілкування в мережі. Це може бути корисно для журналістів, активістів чи осіб, які працюють з конфіденційною інформацією.
4. Обхід цензури - у країнах з обмеженим доступом до Інтернету користувачі можуть використовувати TOR для обхіду цензури та отримання доступу до заблокованих ресурсів.
5. Захист особистих даних - TOR допомагає захистити особисті дані користувача від зловмисників, що намагаються використати їх для кібератак чи ідентифікації.

6. Створення анонімного веб-сайту - користувачі можуть використовувати TOR для створення анонімних веб-сайтів, які не можна відслідкувати до конкретного сервера чи місцезнаходження.

Звичайно, використання TOR має свої обмеження і потенційні недоліки, такі як повільна швидкість мережі та можливість використання для злочинних дій. Також важливо розуміти, що TOR не є повністю анонімною мережею, і користувачі повинні дотримуватися правил безпеки під час його використання.

Приклад коду на мові Python, який демонструє, як використовувати бібліотеку requests разом з TOR для анонімного запиту до веб-сайту:

```
import requests
import socks
import socket
# Налаштовуємо SOCKS проксі для використання TOR
socks.set_default_proxy(socks.SOCKS5, "localhost", 9050)  # Порт 9050 - стандартний порт, на якому працює TOR
socket.socket = socks.socksocket  # Перенаправляємо всі сокет-з'єднання через проксі TOR
# URL веб-сайту, який ми хочемо відвідати
url = "http://example.com"
# Виконуємо GET-запит до веб-сайту через TOR
response = requests.get(url)
# Виводимо вміст відповіді
print(response.text)
```

Перед виконанням цього коду переконайтеся, що ви встановили бібліотеку requests та pysocks, і що TOR запущено на вашому комп'ютері. Крім того, цей приклад передбачає, що TOR працює на стандартному порті 9050 на вашому комп'ютері. Якщо TOR працює на іншому порті, змініть 9050 на відповідне значення.

Цей код встановлює SOCKS5 проксі на локальному комп'ютері і налаштовує всі сокет-з'єднання використовувати цей проксі.

Потім він виконує GET-запит до вказаного URL через TOR і виводить вміст відповіді.

3.2 Потенційні ризики та їх мінімізація

Використання TOR може поставити користувачів перед різними потенційними ризиками, включаючи безпеку, приватність та юридичні аспекти. Одним з основних ризиків є можливість використання TOR для здійснення злочинних дій, таких як злочини проти дітей, наркоторгівля, злочини з бойовою зброєю тощо. Це може призвести до негативного ставлення з боку правоохоронних органів, якщо ваш трафік буде виявлено і відстежено. Крім того, використання TOR може знизити швидкість з'єднання через додатковий рівень обробки і маршрутизації трафіку. Також існує ризик виявлення вашої реальної IP-адреси через витік даних або атаки на приватність, особливо якщо ви використовуєте TOR разом із сайтами, які не захищені протоколом HTTPS.

Мінімізація цих ризиків включає використання додаткових заходів безпеки, таких як віртуальні приватні мережі (VPN) разом з TOR для додаткового шифрування трафіку і захисту від витоку даних. Важливо слідкувати за правилами безпеки, не використовувати TOR для незаконних дій і уникати передачі конфіденційної інформації через мережу TOR, якщо це може бути небезпечним. Також необхідно враховувати юридичні аспекти використання TOR у вашій країні і дотримуватися місцевого законодавства.

Додатковими заходами для мінімізації ризиків є використання оновлених версій програмного забезпечення TOR і забезпечення правильної конфігурації параметрів приватності. Користувачам слід регулярно оновлювати TOR і використовувати рекомендації щодо забезпечення приватності, які надаються розробниками. Важливо уникати використання плагінів браузера або інших додаткових компонентів, які можуть вплинути на безпеку або анонімність при використанні TOR, оскільки деякі плагіни можуть витікати інформацію про реальну IP-адресу користувача або інші конфіденційні дані. Зазвичай використання TOR з вимкненим JavaScript також може знизити ризик витоку інформації через браузерні уразливості. Деякі уразливості браузера можуть використовуватися для отримання інформації про реальну IP-адресу користувача або інші деталі системи.

Особливу увагу слід приділити правильній настройці і застосуванню правил файрвола та інших засобів безпеки на комп'ютері користувача. Це допоможе уникнути можливих атак на систему через TOR або викриття конфіденційних даних через інші вектори. Загалом, правильне використання TOR, спільно з додатковими заходами безпеки та обережністю, може значно знизити ризики і забезпечити більш високий рівень приватності та анонімності в Інтернеті. Для налаштування TOR-сервісу для роботи через SOCKS5 проксі спершу потрібно встановити та налаштувати TOR-сервіс. Спочатку встановіть TOR командою `sudo apt install tor`. Після цього створіть або відредагуйте файл конфігурації `torrc` у папці `/etc/tor/`.

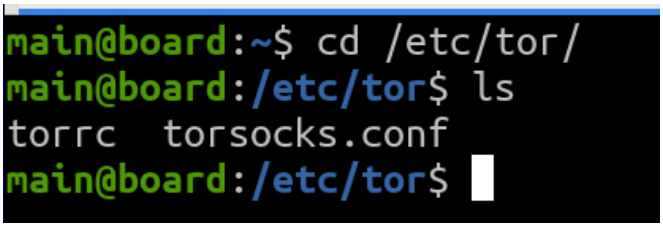

Рисунок 3.1 Файли конфігурації torrc

На рисунку 3.1 показано, що файл конфігурації `torrc` включає налаштування для роботи з SOCKS5 проксі, яке дозволяє TOR приймати з'єднання на порту 9050.

На рисунку 3.2 зображено приклад конфігурації `torrc`.

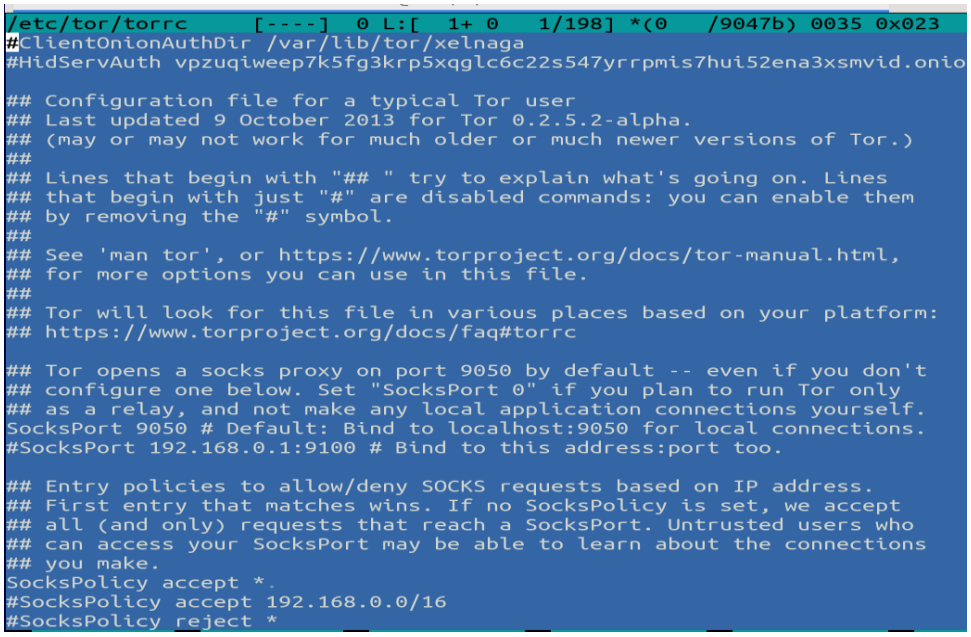

Рисунок 3.2 – Приклад конфігурації torrc

У цій конфігурації Tor прийматиме з'єднання на порту 9050 для надання проксі-сервера SOCKS. Це означає, що будь-які програми, налаштовані для використання проксі-сервера SOCKS на цьому порту, будуть маршрутизувати свій трафік через мережу Tor.

Таким чином, коли ми запускаємо Tor з цією конфігурацією, будь-які програми, які налаштовані на використання локального SOCKS-проксі на порту 9050, автоматично надсилатимуть свої дані через мережу Tor, забезпечуючи анонімність та приховування вашої вихідної IP-адреси.

Однак у цій конфігурації будь-який клієнт, який намагається підключитися до Tor-сервера на порту 9050, буде прийнятий.
Слід зазначити, що таке налаштування може становити ризик безпеки, оскільки воно дозволяє будь-якому користувачеві підключатися до вашого Tor-проксі. Якщо ви хочете обмежити доступ до певних IP-адрес або діапазонів, замість "*" можна використовувати конкретні IP-адреси або підмережі.

```
/etc/tor/torrc     [----]  0 L:[  1+ 0   1/198] *(0   /9047b) 0035 0x023
#ClientOnionAuthDir /var/lib/tor/xelnaga
#HidServAuth vpzuqiweep7k5fg3krp5xqglc6c22s547yrrpmis7hui52ena3xsmvid.onion

## Configuration file for a typical Tor user
## Last updated 9 October 2013 for Tor 0.2.5.2-alpha.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc

## Tor opens a socks proxy on port 9050 by default -- even if you don't
## configure one below. Set "SocksPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
SocksPort 9050 # Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.

## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SocksPolicy is set, we accept
## all (and only) requests that reach a SocksPort. Untrusted users who
## can access your SocksPort may be able to learn about the connections
## you make.
SocksPolicy accept *
#SocksPolicy accept 192.168.0.0/16
#SocksPolicy reject *
```

Рисунок 3.3 – Перезапуск TOR

На цьому скріншоті показано, як перезапустити службу TOR, використовуючи команду `systemctl`. Для перезапуску служби TOR необхідно виконати наступну команду: `sudo systemctl restart tor`. Після цього можна перевірити логи служби, щоб переконатися, що вона працює коректно. Для перевірки логів слід використати команду `sudo tail -f /var/log/tor/notices.log`, яка дозволяє в реальному часі стежити за записами у файлі логів. Це допомагає виявити можливі помилки або проблеми, що виникають під час роботи TOR.

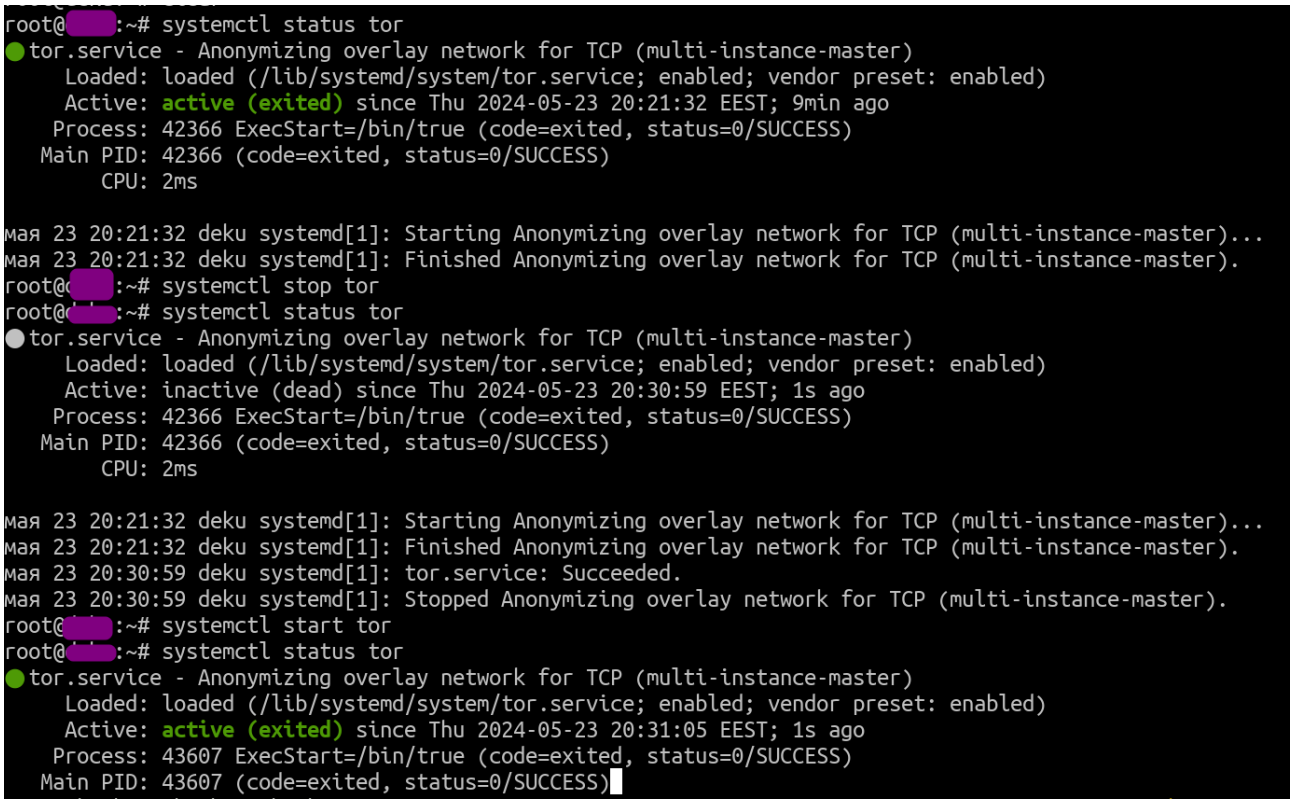

Рисунок 3.4 – Перевірка логінів

Перевірка логів є важливим кроком для переконання, що TOR запущено і працює коректно. Для цього необхідно переглянути відповідні журнали та знайти підтвердження успішного запуску TOR, що забезпечить його правильну роботу.

Для налаштування Python для роботи з TOR необхідно встановити відповідні бібліотеки. Це можна зробити за допомогою команди в терміналі. Відкрийте термінал і введіть наступну команду:

```bash
python3 -m pip install requests pysocks```

Ця команда встановить бібліотеки `requests` та `pysocks`, які є необхідними для взаємодії Python з мережею TOR. Після успішної інсталяції ви зможете використовувати ці бібліотеки для роботи з TOR у ваших Python-скриптах.

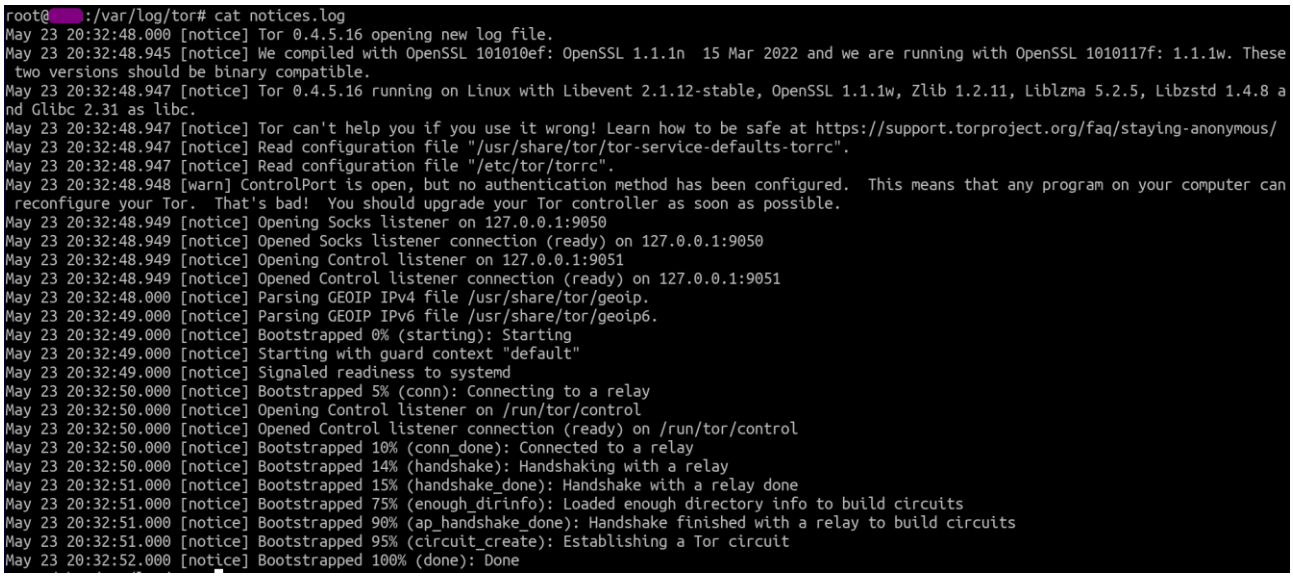


Рисунок 3.5 – Установка бібліотек

На скріншоті видно процес встановлення бібліотек `requests` та `pysocks`. Для створення та активації віртуального середовища, виконайте наступні команди. Спочатку використовуйте команду `python3 -m venv tor`, щоб створити віртуальне середовище з назвою `tor`. Після цього активуйте його командою `source tor/bin/activate`. Ці дії дозволять вам ізольовано працювати з необхідними бібліотеками та пакетами в межах створеного віртуального середовища.

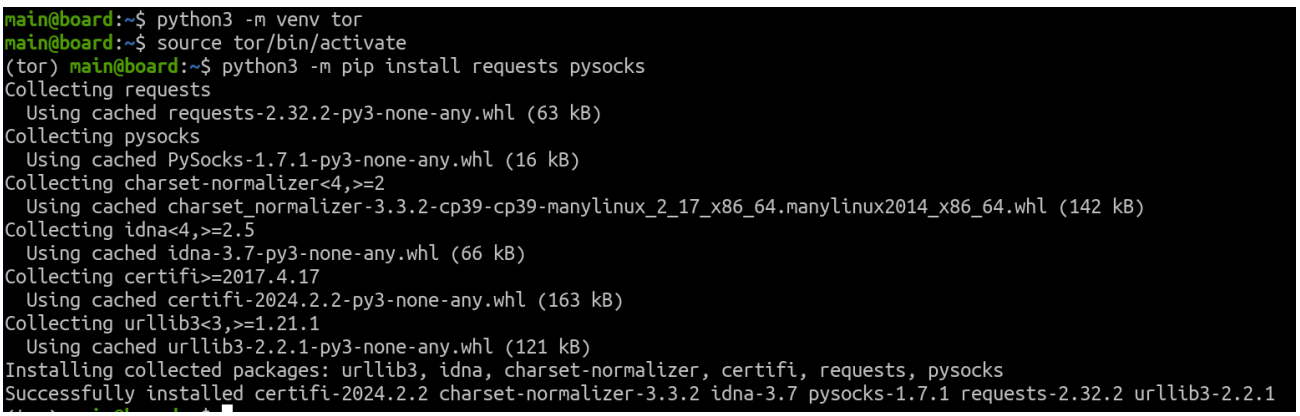
```

Рисунок 3.6 – Віртуальне середовище

Щоб створити та активувати віртуальне середовище для Python, виконайте наступні кроки. Спочатку переконайтеся, що у вас встановлений Python та менеджер пакетів pip. Відкрийте термінал і перейдіть до директорії, де ви хочете створити віртуальне середовище. Виконайте команду `python -m venv env`, щоб створити нове віртуальне середовище, де `env` - це ім'я директорії, яка буде містити файли віртуального середовища. Після створення віртуального середовища активуйте його командою `source env/bin/activate` для Unix або `env\Scripts\activate` для Windows. Активне віртуальне середовище дозволяє встановлювати та використовувати пакети ізольовано від системних.

Для виконання запиту через TOR, вам потрібно буде використати бібліотеку `requests` разом із налаштуванням проксі-сервера для маршрутизації через TOR. Переконайтеся, що у вас встановлений та запущений TOR, який зазвичай слухає на порту 9050. Після цього використовуйте наступний код для виконання HTTP-запиту:

```python
import requests

proxies = {'http': "socks5h://localhost:9050"}
response = requests.get('http://example.org', proxies=proxies)
print(response.text)
```

Цей код використовує бібліотеку `requests` для надсилання HTTP-запиту до сайту `http://example.org` через проксі-сервер TOR, налаштований на `localhost:9050`. Відповідь сервера буде виведена у термінал.

```
>>> import requests
>>> proxies = {'http': "socks5h://localhost:9050"}
>>> s = requests.get('http://example.org', proxies=proxies)
>>> print(s.text)
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
```

Рисунок 3.7 – Приклад запиту

На рисунку 3.7 показано результат виконання запиту через TOR, де видно відповідь сервера.

Перед виконанням цього коду переконайтеся, що ви встановили бібліотеки `requests` та `pysocks`, і що TOR запущено на вашому комп'ютері. Крім того, цей приклад передбачає, що TOR працює на стандартному порту 9050 на комп'ютері. Якщо TOR працює на іншому порту, змініть 9050 на відповідне значення.

Цей код встановлює SOCKS5 проксі на локальному комп'ютері і налаштовує всі сокет-з'єднання використовувати цей проксі. Потім він виконує GET-запит до вказаного URL через TOR і виводить вміст відповіді.

Таким чином, дотримуючись правил безпеки та використовуючи додаткові заходи, такі як VPN та правильні налаштування TOR, можна значно знизити ризики, пов'язані з використанням цієї технології**.**

ВИСНОВОК

Анонімні мережі, зокрема TOR, відіграють значну роль у забезпеченні приватності та безпеки користувачів в інтернеті. Оглянувши теоретичні аспекти анонімізації, історію та розвиток анонімних мереж, а також принципи їх роботи, ми можемо зрозуміти, яким чином ці системи працюють і як вони допомагають користувачам залишатися анонімними в мережі.

TOR, зокрема, відзначається своєю складною архітектурою та протоколом, що дозволяє захищати конфіденційність даних користувачів шляхом маршрутизації їх трафіку через різні вузли мережі. Програмне забезпечення TOR доступне на різних операційних системах, що робить його доступним для широкого кола користувачів.

Практичне використання TOR може бути корисним для забезпечення анонімності при перегляді веб-сторінок, обміні повідомленнями або виконанні інших онлайн-дій. Однак, варто бути обізнаним із потенційними ризиками, пов'язаними з використанням анонімних мереж, такими як можливість зловживання або відстеження діяльності користувача.

Для більш глибокого розуміння практичного використання TOR важливо враховувати, що ця мережа не є абсолютним засобом анонімізації. Хоча TOR допомагає приховати ідентифікаційні дані користувача, він не гарантує повну анонімність. Наприклад, використання TOR може залишити сліди, які за допомогою додаткових технік аналізу можуть бути пов'язані з конкретним користувачем.

Крім того, варто пам'ятати, що деякі дії, здійснені через TOR, можуть бути незаконними в деяких юрисдикціях. Наприклад, деякі дії, пов'язані зі злочинністю або порушенням авторських прав, залишаються неприпустимими, навіть якщо вони виконані через анонімні мережі.

Для мінімізації ризиків при використанні TOR було рекомендовано застосовувати додаткові заходи безпеки, такі як використання віртуальних приватних мереж (VPN), оновлення програмного забезпечення, налаштування параметрів приватності та використання захищених протоколів. Також важливо

слідкувати за правилами безпеки, уникати використання небезпечних плагінів та правильного налаштування файрвола.

Проведений аналіз та практичні приклади налаштування TOR на різних операційних системах, а також використання TOR в Python, допомогли краще зрозуміти механізми роботи цієї мережі та засоби захисту від можливих загроз.

Загальний висновок полягає в тому, що TOR та інші анонімні мережі є важливими інструментами для захисту приватності та безпеки в онлайн-середовищі, проте їх використання повинне супроводжуватися обізнаністю із можливими ризиками та заходами для їх мінімізації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Хижняк Є. Ідентифікація особистості злочинця за віртуальними слідами в мережі інтернет. *Підприємництво, господарство і право*, 2017. №17. С. 217-221.
2. Підгорний, П.В. Експертна система ідентифікації користувачів мережі Інтернет. *Лаврик*. Суми: СумДУ, 2020. 79 с.
3. Білашенко Д. В. Способи анонімності в інтернеті / Д. В. Білашенко, Ю. М. Онищенко. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. С. 17-18.
4. Що таке VPN? URL: https://nordvpn.com/uk/what-is-a-vpn/
5. Комп'ютерні мережі частина 1 навчальний посібник: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с
6. I2P: Принципи функціонування основних сервісів мережі. URL: http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1504-i2p-principles-of-basic-network-services
7. Інформаційна безпека та інформаційні технології: збірник тез доповідей VI Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів, (м. Львів, 30 листоп. 2023 року). Львів, ЛДУ БЖД, 2023, 489 с.
8. Карабан Д. Р.; Жаровський Р. О. Методи забезпечення анонімності в інтернеті. Використанні мережі інтернет, 2023. С. 237.
9. Козак Р. О. Аналіз засобів забезпечення анонімності в мережі інтернет / Р. О. Козак // *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2014. № 1. С. 100-105.

10. Про Tor Browser. URL: https://tb-manual.torproject.org/uk/about/
11. Види проксі: Все, що вам потрібно знати. URL: https://www.rapidseedbox.com/uk/blog/types-of-proxy
12. Що таке браузер Tor: чим він цікавий для учасників криптоспільноти. URL: https://incrypted.com/ua/shcho-take-tor-brauzer/
13. Архітектура сучасних комп'ютерних мереж: Методичний посібник.— Вінниця: УНІВЕРСУМ-Вінниця, 2008. 98 с.
14. Погромська Г., Чернищук Г. Реалізація аплету для анонімізації трафіку за допомогою мережі TOR. *Геометричне моделювання та інформаційні технології*, 2018. №1. С. 98-104.
15. The Tor Architecture and its Inherent Security Implications. URL: https://medium.com/@gkaufmann/the-tor-architecture-and-its-inherent-security-implications-61f45fd42b01
16. TOR браузер: як зберегти анонімність в мережі. [Електроний Ресурс] – Режим доступу до ресурсу: https://znaj.ua/society/282872-tor-brauzer-yak-zberegti-anonimnist-v-merezhi
17. What Does Node Mean? [Електроний Ресурс] – Режим доступу до ресурсу: https://www.trenchlesspedia.com/definition/3097/node
18. Node Guard. [Електроний Ресурс] – Режим доступу до ресурсу:https://www.npmjs.com/package/node-guard
19. «Debian/Ubuntu setup» [Електроний ресурс] – Режим доступу до ресурсу: https://community.torproject.org/relay/setup/guard/debian-ubuntu/
20. «Why and how I can enable Tor Package Repository in Debian?» [Електроний ресурс] – Режим доступу до ресурсу: https://support.torproject.org/apt/tor-deb-repo/