

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КОРИСТУВАЧА В МЕРЕЖІ ІНТЕРНЕТ

Папазов К.О.

Науковий керівник – к.т.н., доц. Олешко І.В.

Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків,
Українаe-mail: kyrylo.papazov@nure.ua

This paper examines the different methods of providing user anonymity in the Internet, including proxy servers, virtual private networks (VPN) and Onion routing. The paper evaluates and compares these methods according to the criteria of anonymity level, speed, cost and ease of use. The paper also discusses the advantages and disadvantages of each method, as well as the specific needs of users. The paper concludes that VPNs are the “golden mean” that offer a balance between anonymity, internet connection speed and technical complexity. However, the choice of a particular method depends on the user’s preferences and goals.

В епоху цифрової інформації, анонімність в Інтернеті стає все більш актуальною темою. Користувачі прагнуть залишатися анонімними, щоб захистити свою приватність, уникнути небажаного контенту та забезпечити свободу вираження своїх думок без страху переслідування.

Анонімність в Інтернеті – це стан, коли ідентичність користувача не відома або не може бути встановлена. Користувач, який залишається анонімним, може переглядати, завантажувати та використовувати Інтернет-ресурси, не розкриваючи свою особисту інформацію. Це може бути важливо для захисту приватності, свободи слова та уникнення цензури.

Одним з методів забезпечення анонімності є використання проксі-сервера. Проксі-сервер – проміжний сервер у комп’ютерних мережах, що виконує роль посередника між користувачем і цільовим сервером, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб і отримувати відповіді. Простими словами, проксі-сервер ховає IP-адресу користувача і звертається до сайтів за допомогою іншої IP-адреси. Хоча проксі-сервери можуть забезпечити певний рівень анонімності, вони мають обмеження, наприклад, вони не шифрують трафік, що може стати проблемою, якщо користувач передає чутливу інформацію.

Віртуальна приватна мережа (VPN) – це доступне програмне забезпечення, яке забезпечує конфіденційність Інтернету. VPN створює зашифрований тунель між пристроєм користувача і всесвітньою мережею, щоб діяльність в Інтернеті була прихована від хакерів, Інтернет-провайдерів (ISP) та інших.

VPN з’єднують пристрій користувача та мережу, як правило, публічну, через зашифрований тунель. Тунель шифрує онлайн-активність користувача та

приховує його IP-адресу, замінюючи її IP-адресою приватного сервера, до якого користувач підключається. Більшість VPN використовує 256-бітне шифрування AES, яке є поточним стандартом у галузі. Щоб передати дані з пристрою на приватний сервер, мережі VPN використовують Інтернет-протоколи, які розміщують дані в пакетах і забезпечують їх надсилання в належному порядку. Якщо VPN виходить з ладу, більшість із них оснащена перемикачами, які закривають усі вікна чи програми з веб-трафіком, залишаючи користувача захищеним і конфіденційним у мережі.

Ще одним важливим та доволі потужним методом забезпечення анонімності в Інтернеті є Onion routing, який найбільш відомий завдяки мережі Tor. Tor – це мережа віртуальних тунелів, які дозволяють покращити приватність і безпеку в інтернеті. Архітектура Tor базується на принципі розподіленої мережі. Вона складається з тисяч волонтерських ретрансляторів по всьому світу, які передають трафік від одного до іншого. Кожен ретранслятор додає шар шифрування до даних, що забезпечує анонімність користувача. Коли дані досягають свого кінцевого пункту, кожен шар шифрування знімається, щоб відновити оригінальні дані. Це гарантує, що жоден окремих вузол в мережі Tor не знає і про джерело, і про призначення даних, що забезпечує високий рівень анонімності. Таким чином ті, хто зацікавлений особою користувача, бачитимуть підключення з мережі Tor замість справжньої IP-адреси, допоки користувач сам не залишить інформацію про себе в мережі.

Хоча Tor забезпечує високий рівень анонімності, він також має обмеження такі, як повільна швидкість, можливість стати ціллю для зловмисника, а також ризику, пов'язані з відвідуванням .onion сайтів.

Враховуючи те, що повна анонімність в Інтернеті є майже неможливою, в таблиці 1 наведено порівняння розглянутих методів за рівнем анонімності, впливом на швидкість інтернет з'єднання, вартістю впровадження та простотою використання. З таблиці можна зробити висновок, що кожен метод має свої сильні та слабкі сторони, які залежать від критеріїв порівняння. Проксі-сервери надають середній рівень анонімності, не впливають значно на швидкість інтернет з'єднання, але потребують впевненого вміння керувати пристроями. VPN забезпечують високий рівень анонімності, середній вплив на швидкість інтернет з'єднання, але коштують гроші. Onion routing надає максимальний рівень анонімності, але значно знижує швидкість інтернет з'єднання, а також має ризику, пов'язані з відвідуванням .onion сайтів. Вибір конкретного методу залежить від специфічних потреб користувача.

Враховуючи вищезазначене, можна зробити висновок, що анонімність в Інтернеті є важливим аспектом цифрової безпеки. Проксі-сервери, VPN та Onion routing надають різні рівні анонімності та мають свої переваги та недоліки. Віртуальні приватні мережі (VPN) вважаються “золотою серединою”, оскільки вони забезпечують баланс між анонімністю, швидкістю

інтернет-з'єднання та технічною складністю. Однак вибір конкретного методу залежить від специфічних потреб користувача. Незважаючи на те, що повна анонімність в Інтернеті є майже неможливою, використання цих методів поодиночки або в поєднанні може значно підвищити приватність користувача в мережі.

Таблиця 1 – Порівняння методів забезпечення анонімності в мережі інтернет

Критерії порівняння	Проксі-сервери	VPN	Onion routing
Рівень анонімності	Середній	Високий	Максимальний
Вплив на швидкість інтернет з'єднання	Не значний, в залежності від навантаження серверів та відстані до них	Середній вплив, в залежності від навантаження серверів та відстані до них	Значний
Вартість	Від 0.80\$ в місяць; є безкоштовні, але зі значними обмеженнями	Надійні сервіси від 5\$ в місяць; є безкоштовні, але зі значними обмеженнями	Безкоштовно
Простота використання	Потребує впевненого вміння керувати пристроями	Потребує вміння встановлювати додатки на пристрої	Потребує вміння встановлювати додатки на пристрої

Список використаних джерел

1. A 2024 Guide to VPNs : вебсайт. URL: <https://www.security.org/vpn/> (дата звернення 04.03.2024).
2. How can we help? | Tor Project | Support : вебсайт. URL: <https://support.torproject.org/> (дата звернення 04.03.2024).
3. Proxy server : вебсайт. URL: https://en.wikipedia.org/wiki/Proxy_server (дата звернення 04.03.2024).
4. Сердюков Д. В., Северінов О. В., Сидоренко З. М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023. Т. 1, С. 70.