Перевірка анонімності в мережі «Інтернет»

Максим Єрмоленко
головний судовий експерт, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, м. Київ, Україна, e-mail: yermomaur@ssu.gov.ua

Розглянуто методи перевірки рівня анонімності користувача, проведено аналіз засобів забезпечення анонімності (VPN, Tor, проксі тощо). Тези містять приклади з практики та сучасні тенденції розвитку цієї сфери.

Ключові слова: *VPN сервіси; мережа Tor; проксі-сервери.*

Anonymity Check on the Internet

Maksym Yermolenko

This report discusses methods for checking the level of user anonymity, analyzes tools for ensuring anonymity (VPN, TOR, proxies).The report includes practical examples and current trends in the development of this field.

Keywords: *VPN; Tor; Proxy.*

Анонімність в інтернеті означає можливість користувача діяти в мережі, не розкриваючи свою особистість. Для багатьох це важлива складова права на приватність і свободу слова. З одного боку, анонімність захищає користувачів від небажаного стеження, цензури або переслідувань за висловлювання; з іншого — нею можуть зловживати зловмисники для протиправних дій. Тому питання перевірки та забезпечення анонімності є актуальними: користувачі хочуть контролювати, яку інформацію про них видно в мережі, а держави та компанії встановлюють свої обмеження і правила.

Методи перевірки рівня анонімності користувача

Перед тим як покращувати свою анонімність, корисно оцінити, яка інформація про вас ву доступна онлайн. Існують спеціальні онлайн-сервіси, що даютьзмогу перевірити «слід» користувача в інтернеті. Вони показують дані, які ваш браузер і мережеве підключення розкривають вебсайтам. Популярні безкоштовні інструменти містять *Whoer.net, IPLeak.net, DNSLeakTest.com* та *BrowserLeaks.com.* Такі сервіси відображають вашу зовнішню *IP*-адресу, визначають *DNS*-сервери, через які йдуть запити, і перевіряють інші можливі витоки даних. Наприклад, якщо ви застосовуєте *VPN* чи проксі, на сайтах типу *Whoer* або *IPLeak* можна переконатися, що зовнішня *IP*-адреса відображається саме від *VPN/*проксі, а не ваша реальна. Зокрема, тест на витік *DNS* показує, чи не йдуть *DNS*-запити в обхід анонімайзера: якщо *DNS*-сервер у результатах збігається з *IP*-адресою *VPN*/проксі, то все налаштовано правильно; якщо ж видно *DNS* вашого провайдера, значить запити «прошиваються» повз захист і можуть розкривати вашу активність [1].

Кожен із таких сервісів дає різнобічну інформацію. Сайт *Whoer.net*,

приміром, докладно показує параметри з'єднання: *IP*-адресу та геолокацію, дані про провайдера, застосовувані *DNS*, наявність відкритих портів, установлені технології *(JavaScript, Flash, Java)*, мову та часовий пояс системи, тип операційної системи й браузера тощо [2]. *Whoer* навіть обчислює приблизний відсоток анонімності — інтегральну оцінку, наскільки ваше середовище «замасковане». Хоча цей відсоток умовний, він враховує різні чинники: збіг *IP* і *DNS*, відсутність витоків *WebRTC*, користування анонімною мережею *(Tor)* або проксі, унікальність налаштувань браузера тощо. Інший сервіс — *BrowserLeaks.com* — надає набір окремих тестів: перевірка *HTTP*-заголовків, витоку через *WebRTC* (ця технологія може видавати локальну *IP*-адресу), визначення Canvas-фінгерпринту, шрифтів, розширень, а також тест на витік через торрент (ідентифікація *IP* в *peer-to-peer* мережах). Застосовуючи кілька таких ресурсів разом, користувач може виявити всі основні «сліди», що їх залишає його пристрій.

Особливу увагу варто звернути на фінгерпринтінг браузера — визначення унікального набору характеристик браузера та пристрою (версія ОС, браузери, установлені плагіни, роздільність екрану, часовий пояс, мова, параметри *canvas/WebGL* тощо). Разом ці параметри часто утворюють унікальний відбиток, за яким користувача можна впізнати навіть без *cookies* або *IP*-адреси. Сервіс від *Electronic Frontier Foundation* під назвою *Cover Your Tracks* (раніше *Panopticlick*) дає змогу протестувати унікальність вашого браузера. За даними дослідження *EFF*, у вибірці понад 470 тисяч користувачів 83,6 % браузерів мали повністю унікальний фінгерпринт; ще ~5% були унікальні за повторного відвідування, тобто лише менш як 10% користувачів мали достатньо поширені параметри, щоб «змішатись з натовпом» [3]. Тому навіть якщо *IP*-адресу приховано, унікальна конфігурація системи може видати вашу особу. *Whoer.net* також надає інструмент перевірки фінгерпринту саме з цією метою: показати, наскільки унікальними є характеристики пристрою, які можуть бути використані для відстеження.

Отже, методи перевірки анонімності зводяться до виявлення всіх каналів витоку ідентифікаційних даних. Практичні кроки для користувача такі: зайти на кілька перевірочних сайтів, перевірити відображену *IP*-адресу й *DNS*, переконатися у відсутності *WebRTC* та інших витоків, оцінити свій фінгерпринт. Якщо тести показують справжню *IP*-адресу або *DNS* від провайдера, потрібно змінити налаштування *VPN*/проксі або скористатися іншим сервісом, який не допускає витоків. Отже, перевірка рівня анонімності є необхідним етапом для розуміння, наскільки ви захищені перед тим, як довіряти конфіденційні дії своїй «анонімності».

Застосування VPN, Tor, проксі-серверів та інших засобів для забезпечення анонімності

VPN (Virtual Private Network), мережа *Tor* та різноманітні проксі-сервери — це основні технології, які люди засто-

совують для підвищення своєї приватності й анонімності онлайн. Кожен із цих засобів має свої принципи роботи, сильні та слабкі сторони. Розглянемо їх по черзі, а також з'ясуємо, як їх комбінують і які сучасні тенденції їх застосування.

Найпростішим способом приховати свій реальний мережевий адрес є застосування проксі-сервера. Проксі виступає посередником між вашим пристроєм та інтернет-ресурсом: ви надсилаєте запит на проксі-сервер, а вже він відправляє його далі до сайту. В результаті сайт бачить *IP*-адресу проксі, а не вашу власну. У такий спосіб можна змінити свій видимий регіон (наприклад, обрати проксі в іншій країні) і сховати справжній *IP* від веб-ресурсу [3]. Проте проксі-сервери не забезпечують шифрування трафіку (якщо це не спеціальний проксі з шифруванням): ваші дані від комп'ютера до проксі йдуть відкритим текстом і можуть бути перехоплені. Тому, хоча *HTTP(S)*-проксі або *SOCKS*-проксі й допомагають приховати адресу, з позицій безпеки вони значно поступаються *VPN*. Як зазначає компанія *Avast*, проксі лише маскує *IP*, але не шифрує канал, через що трафік залишається вразливим для перехоплення або спостереження зловмисником. Проксі підходять для обходу простих блокувань або швидкої зміни *IP*, але не рекомендуються для передачі чутливої інформації (паролі, банківські дані тощо) без додаткового захисту.

VPN — це технологія, яка створює зашифрований тунель між пристроєм користувача і *VPN*-сервером, розташованим зазвичай в іншій мережі чи країні. Усі дані, що передаються через *VPN*, шифруються, тому навіть якщо їх перехопить інтернет-провайдер або хакер, вони не зможуть їх прочитати. На виході в інтернет буде видно *IP*-адресу *VPN*-сервера, а не справжню адресу користувача. Отже, *VPN* одночасно приховує *IP* і захищає трафік шифруванням. Сучасні *VPN*-сервіси зазвичай застосовують надійні протоколи (*OpenVPN, WireGuard* та ін.), що ускладнюють прослуховування трафіку. З позиції анонімності *VPN* має перевагу швидкості та простоти: швидкість інтернету майже не падає (порівняно з багатохоповими мережами як *Tor*), налаштування зручне навіть для нефахівців. Це зробило *VPN* надзвичайно популярним рішенням: станом на 2023 рік близько 31 % всіх інтернет-користувачів у світі регулярно користуються *VPN*-сервісами [4], причому основні причини — захист приватності, анонімний серфінг та безпечне спілкування.

Утім слід розуміти й обмеження *VPN* для повної анонімності. По-перше, ви довіряєте свій трафік *VPN*-провайдеру — він теоретично може логувати ваші дії. Тому важливо обирати надійні сервіси з політикою *no-logs* і гарною репутацією. По-друге, *VPN* не захищає від ідентифікації через акаунти: якщо ви заходите під своїм справжнім ім'ям у соцмережу або пошту, то залишаєтесь неанонімним незалежно від *VPN*. Так само *VPN* не завадить вебсайтам застосовувати фінгерпринтинг або встановлювати трекери. Отже, *VPN* — ефективний інструмент приватності, але не абсолютний щит: він приховає вас від пасивного спостереження

(провайдера, стороннього спостерігача) і підмінить вашу мережеву ідентичність, проте інші методи деанонімізації можуть лишитися дієвими.

Проєкт *Tor (The Onion Router)* був спеціально створений для забезпечення високого рівня анонімності в мережі. *Tor* прямо розв'язує проблему довіри до єдиного посередника (як у випадку з *VPN*): замість одного серверу трафік проходить через ланцюжок з декількох вузлів, кожен із яких знає лише свою попередню і наступну ланку. З'єднання в мережі *Tor* тришарове: спочатку трафік шифрується і прямує на вузол-*guard* (вхідний вузол), потім перенаправляється на проміжні *relay*-вузли і зрештою виходить через *exit*-вузол до цільового сайту. Кожен вузол «знімає» лише свій шар шифрування і не знає ні повного маршруту, ні особи користувача. У результаті сайт призначення бачить запит від *exit*-вузла (з його *IP*), а спостерігач у мережі не може простежити маршрут назад до користувача. *Tor*-браузер, побудований на *Firefox*, автоматично підключається до мережі *Tor* і вмикає додаткові засоби захисту (відключення плагінів, уніфікація браузерного середовища, захист від фінгерпринтингу тощо).

Головна перевага *Tor* — максимальна анонімність для масового користувача: ніхто з проміжних вузлів не знає, хто ви і які сайти відвідуєте, а кінцевий ресурс не знає, хто саме (який користувач) звертався, лише що запит прийшов із мережі *Tor*. Ця система добре захищає від відстеження та цензури; недарма *Tor* широко застосовують журналісти, правозахисники, активісти в країнах із жорсткими обмеженнями інтернету. Однак є й недоліки. По-перше, швидкодія: через багатократне шифрування і пересилання через кілька вузлів швидкість роботи в *Tor* значно нижча, ніж у звичайному інтернеті або *VPN*. Кожен запит може проходити довгий маршрут, тому, наприклад, завантаження сторінок відчутно повільніше [4]. По-друге, обмеження доступу: деякі вебсайти блокують відвідувачів з відомих *exit*-вузлів *Tor* (через часті випадки зловживань анонімністю для атак або шахрайства). По-третє, *Tor* не гарантує безпечності контенту: трафік шифрується лише всередині мережі *Tor*, а на виході *(exit)* він виходить у відкритий інтернет. Тому якщо сайт не застосовує *HTTPS*, зловмисний exit-вузол теоретично може переглянути або змінити незашифровані дані. Сам *Tor* не захистить і від помилок користувача: розкриття особистих даних вручну, завантаження файлів з експлойтами, користування своїм реальним іменем тощо.

Окрім *VPN*, проксі та *Tor*, існують й інші інструменти для анонімності, хоча вони менш популярні. Наприклад, мережа *I2P (Invisible Internet Project)* створює анонімне оверлейне середовище для сайтів і сервісів подібно до «цибулинного» маршрутування *Tor*, але працює дещо інакше та переважно для внутрішніх ресурсів *I2P*. Є також проєкти типу *Freenet*, які дають змогу публікувати й отримувати інформацію анонімно в розподіленому сховищі даних. Проте цим рішенням користується вузьке коло ентузіастів. Більш відомі підходи — браузери для анонімності (наприклад, *Tor Browser*, згаданий вище, або

спеціальні «антидетект» браузери, що мінімізують сліди) та операційні системи, орієнтовані на анонімність (як-от *Tails — Linux*-дистрибутив, що спрямовує весь трафік через *Tor*). Також можна комбінувати засоби: деякі користувачі вмикають *VPN* разом із *Tor* (наприклад, спочатку *VPN*, а поверх нього — *Tor*, щоб навіть провайдер не бачив факту користування *Tor*). Існують дискусії щодо схеми «*VPN* через Tor» чиабо «*Tor* через *VPN*» залежно від загроз, але в будь-якому разі комбінування ускладнює налаштування і часто впливає на швидкість.

Важливо розуміти, що жоден із методів не дає абсолютної гарантії анонімності. Як слушно зазначено в оглядовій статті, остаточний вибір залежить від того, який рівень приватності потрібен і скільки зусиль ви готові докласти [4]. Якщо потрібно просто змінити *IP* і трохи підвищити конфіденційність — вистачить проксі або звичайного *VPN*. Якщо ви переслідуєте мету максимально сховати свою особу (наприклад, в умовах репресивного режиму) — слід користуватися *Tor*, можливо, у поєднанні з додатковими заходами безпеки. До того ж не можна забувати про людський чинник: навіть найкращі технології не врятують, якщо користувач сам розкриє про себе інформацію.

Сучасна тенденція така, що інструменти анонімності стають доступнішими й масовішими. Ринок *VPN* зростає швидкими темпами, усе більше людей шифрують свій трафік навіть для повсякденних завдань (онлайн-банкінг, дистанційна робота). Зростає і технічна протидія анонімності: великі сайти впроваджують системи детектування *VPN* /проксі/ *Tor* за характерними ознаками підключення, щоб запобігти обходу геоблокувань або антиспаму. У відповідь сервіси впроваджують функції маскування (обфускації) трафіку *VPN* під звичайний. Отже, «гонитва озброєнь» між прагненням користувачів залишатися анонімними та бажанням провайдерів ідентифікувати кожного триває. Для користувача ж оптимальним є усвідомлене комбінування засобів: користування *VPN* / *Tor*, налаштування приватності браузера, менеджер паролів, блокування трекерів — усе це разом дає найкращий результат.

Анонімність в інтернеті — багатогранне явище, яке охоплює технічні, соціальні та правові аспекти. Перевірка рівня анонімності є першим кроком для кожного, хто прагне захистити свою приватність: за допомогою спеціальних онлайн-інструментів користувач може дізнатися, яку інформацію про нього видно в мережі (*IP*-адресу, *DNS*, параметри браузера тощо) і виявити потенційні витоки. На основі цього можна вибрати й налаштувати оптимальні засоби забезпечення анонімності. Сьогодні у розпорядженні користувачів є *VPN*-сервіси, проксі-сервери, мережа Tor та інші інструменти, кожен із яких має свої переваги. *VPN* та проксі приховують *IP*; *VPN* до того ж шифрує трафік; *Tor* дає дуже високий рівень укриття особи ціною зниження швидкості. Комбінація цих засобів і дотримання кращих практик (не розкривати особистих даних, ізолювати різні онлайн-активності) дають змогу досягти значного рівня анонімності.

Перелік джерел посилання

1. iProxy Online. *Швидкість, приватність проксі, підміна DN*. URL: https://iproxy.online/uk/faq/shvidkist-privatnist-proksi-pidmina-dns (дата звернення: 08.04.2025).
2. Whoer.net — *онлайн-сервіс для перевірки анонімності.* URL: https://whoer.net (дата звернення: 08.04.2025).
3. Buxton O. Proxy vs VPN vs Tor: What Are the Differences? URL: https://www.avast.com/c-vpn-proxy-tor-which-is-best (accessed: 08.04.2025).
4. Gajić A. *VPN* Statistics — 2023 Update. URL: https://99firms.com/blog/vpn-statistics/ (дата звернення: 08.04.2025.