

Що таке VPN насправді

Він змінює того, хто може тебе бачити, а не те, чи може хтось узагалі.

Простіше кажучи: VPN не дає твоєму інтернет-провайдеру чи Wi-Fi в аеропорту бачити, куди ти підключаєшся. Ця інформація не зникає: вона передається компанії VPN, яка тепер її бачить. Те, що вже передавалося зашифрованим, як пошта чи банк, було зашифрованим і раніше. Він служить для кількох конкретних завдань, а продають його часто так, ніби він вирішує значно більше.

Роками я чув про VPN і не звертав на них уваги, так само як і на антивіруси: я не користуюсь антивірусом, або майже ніколи. У мене є копії всього в трьох місцях у реальному часі, і я дуже уважний до того, що завантажую, за якими посиланнями переходжу та які сайти відвідую. Це не стовідсоткова безпека, але для мене це працює. Одного разу я побачив пропозицію VPN трохи більше ніж за два євро на місяць і підписався з цікавості. Працює добре, але став у пригоді мало: наприклад, протестувати сервіс, який тоді відкривався лише у США. Чи почуваюся я в більшій безпеці? Ні. Якщо мені знову запропонують його за цю ціну, можливо, подовжу; якщо ні — ні. Це лише мій досвід, він нічого не доводить. Тому я запитав себе, що саме робить VPN. Ось як я це зрозумів.

Уяви, що ти опускаєш листа в поштову скриньку з чітко видимою адресою одержувача. Листоноша бачить, кому ти його надсилаєш, навіть якщо не може прочитати його, коли конверт запечатаний. Цей листоноша — твій інтернет-провайдер. VPN вкладає твій лист в інший конверт, адресований посереднику, який розкриває його та пересилає далі. Твій звичний листоноша більше не бачить справжньої адреси. Він бачить лише те, що ти пишеш цьому посереднику.

Той, хто контролює мережу, з якої ти підключаєшся (наприклад, Wi-Fi в аеропорту), перестає бачити, куди ти заходиш. Але посередник тепер бачить те, що раніше бачив твій провайдер, а іноді й більше, адже весь твій трафік проходить через нього. Стеження не зникає: воно переходить до інших рук. Звідси й назва.

Крім того, майже все, що ти робиш сьогодні (наприклад, перевіряєш пошту або заходиш у банк), уже передається зашифрованим до кінцевого сервера завдяки замочку у браузері. Це відбувається як з VPN, так і без нього. VPN додає захист лише на першій ділянці — до свого власного сервера. Звідти шлях залишається звичайним.

Ось чому є речі, яких він не може тобі пообіцяти, навіть якщо його іноді так рекламують. Якщо ти увійшов у свою пошту чи в банк, цей сервіс знає, що це ти, з VPN чи без. Він також не гарантує, що ніхто не стежить за твоїм трафіком: змінюється лише той, хто стежить. Заява компанії про те, що вона «не веде журналів», — це обіцянка, точнісінько так, як коли велика платформа каже «ваші повідомлення зашифровані, ми їх не читаємо». Аудит може підтвердити це в певний момент, але це залишається питанням твоєї довіри до обіцянки, а не тим, чого неможливо порушити за самою структурою.

І вміст бесіди залишається таким самим. Якщо твій додаток для повідомлень уже шифрує наскрізно, VPN нічого не додає. Якщо ні — VPN цього теж не виправить: він захищає шлях повідомлення, а не те, що додаток або його сервер зроблять із ним після прибуття.

Ніщо з цього не робить його непотрібним. Приховати місце свого підключення від публічного Wi-Fi, від провайдера, який хотів би продати цю історію, або від країни, яка блокує сервіс, — це реальна робота, і він виконує її добре. Маркетинг, щоправда, зазвичай обіцяє більше, ніж цей рівень здатен дати.

Питання, яке варто собі поставити щодо VPN або будь-якого сервісу, що обіцяє захист, звучить не «чи це зашифровано?». Напевно так, принаймні на одній ділянці. Питання в іншому: кому я віддаю ту довіру, яку відібрав в іншого? І що в мене залишиться, якщо вона виявиться невиправданою?

VPN, коли він добре виконує свою роботу, лише змінює посередника у твоєму підключенні. Такий додаток, як Solo2, чиї повідомлення не проходять через жоден сервер, повністю прибирає посередника з розмови. Вони не конкурують: вони вирішують різні проблеми.

Плутати їх — дуже поширений спосіб вважати себе більш захищеним, ніж ти є насправді.

Від редакції: коли в цих Cuadernos згадуються компанії або продукти, це робиться не для того, щоб когось звинуватити. Ті, хто їх створює, роблять роботу, якою користуються і яку цінують мільйони людей. Ми вказуємо на структурну проблему — модель, а не бренд. Бренди з'являються як приклад, тому що вони впізнавані для читача.

Джерела та додаткова література

- Протокол HTTPS і транспортне шифрування є відкритими стандартами, публічно задокументованими IETF.
- У цій самій збірці: «Коли посередині нікого немає» та «Ви не анонімні» розкривають під іншими кутами ту саму відмінність між структурою та обіцянкою.

[← Попередній](#) [Ти не анонімний](#)

Останні матеріали

- [Роздуми · 29 червня 2026 р. Ти не анонімний](#)
- [Рефлексія · 27 травня 2026 р. Те, що підпис не може виправити](#)
- [Аналіз · 26 травня 2026 р. Реальна vs уявна конфіденційність: питання, які варто собі поставити](#)

Візьми цю статтю з собою куди завгодно.

[↓ Markdown](#) [↓ Звичайний текст](#) [↓ PDF](#)

Файл буде завантажено на твій пристрій. Звідти ти можеш зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за тебе.

Сургучна печатка · SHA-256 aea9f8d148074c0892c117db62b94c4d005e16db75ca969e29432678f66ef50a
[Можливості](#) [Ціни](#) [Встановити](#) [Новини](#) [Блог](#) [Pro](#) [Допомога](#) [Про нас](#) [Контакти](#)
[Прозорість](#) [Верифікація](#) [Приватність](#) [Умови](#) [Файли cookie](#)

Cuadernos Lacre · Видання [Menzuri Gestión S.L.](#) · автор R.Eugenio · під редакцією команди [Solo2](#).

Цей сайт не використовує куки. Усе, що завантажує твій браузер, написане або контрольоване нами та розміщене на наших європейських серверах: анонімний лічильник відвідувань (Utmati, самостійно розміщений) і мінімум JavaScript, необхідний для вибору мови та твого налаштування світлої/темної теми, яке зберігається на твоєму власному пристрої. Без сторонніх ресурсів, без трекерів, без профілювання, без поширення даних. Якщо ти хочеш стежити за нами: [RSS](#).