# 10.3. Віртуальна приватна мережа VPN

VPN (Virtual Private Network - віртуальна приватна мережа) - це безпечне, зашифроване підключення між двома мережами або між окремим користувачем і мережею. Мережі VPN дозволяють користуватися Інтернетом, зберігаючи конфіденційність (рис.1).



Рис.1. Технологія VPN

Технологія VPN працює як невидимка - маскує користувача і зберігає анонімність. Всі дії користувача приховані в зашифрованих даних і надійно заховані за іншою IP-адресою. При входженні користувача в інтернет через VPN, видно не справжнє джерело підключення, а один з численних VPN-маршрутизаторів.

Технології VPN допомагають наблизитися до цієї анонімності, не вдаючись до використання мережі TOR, в якій підключення блукає по широкій мережі ретрансляторів, постійно змінюючи виконання дій в інтернеті, щоб на них ніхто не міг сфокусуватися. Мережі VPN такий протокол не використовують, але вони забезпечують достатній захист під час переміщення користувача по мережі інтернет.

Мережний нейтралітет - це принцип, згідно з яким постачальники послуг інтернету повинні працювати з усіма даними однаково, без дискримінації та врахування особистих переваг. У 2017 році Федеральна комісія із зв'язку США скасувала мережний нейтралітет, що означає виникнення будь-яких умов або упередженості в залежності від дій користувача в мережі.

Тепер провайдери США можуть продати номер соціального страхування, інформацію про геолокацію, здоров'я, історії пошуку в інтернеті і будь-які відомості про користувача, які вони збирають, тому, хто більше заплатить. Мережа VPN допомагає зберегти конфіденційність користувача навіть від канального провайдера Інтернету, щоб ніхто не зміг відстежити його дії або побачити дані.

Вагомою причиною використовувати VPN - це зростання числа загальнодоступних точок доступу Wi-Fi, де відкривається простір для зловмисників, щоб шпигувати за користувачами. Великий ризик виникає при здійсненні покупок і вказанні даних картки через безкоштовну мережу Wi-Fi.

У мережі VPN кілька переваг. Оскільки користувач є анонімом, ніхто не дізнається, місце знаходження. Він може вибрати одну з IP-адрес і країну, звідки буде перебувати в мережі. Якщо постачальник служби VPN досить надійний, він запропонує хороший вибір IP-адрес з різними географічними положеннями. Наприклад, якщо користувач буде в Парижі і зіткнеться з обмеженням доступу за географічною ознакою до сайту, який зазвичай відвідує в Україні, тоді слід вибрати в службі VPN IP-адресу з України, у віртуального браузера з'являться українські номери і доступ буде надано.

### Переваги мережі VPN

* **Дивитися трансляції з будь-якої точки світу.** Якщо користувач перебуває за кордоном і намагається увійти в обліковий запис для трансляцій, якою користується в своїй країні, то може виявити, що деякі шоу не працюють. Але якщо вибрати IP-адресу, що розташована на батьківщині, то все улюблені шоу будуть доступними.
* **Отримувати доступ до заблокованих веб-сайтів.** Деякі установи (школи, бібліотеки, офіси) обмежують доступ до певних веб-сторінок, наприклад до соціальних мереж, але зашифроване VPN-підключення пройде крізь всі бар'єри.
* **Обійти цінову дискримінацію.** Цінова дискримінація - це коли, за один і той же товар, різні групи споживачів платять різні кошти. Перша причина - виходячи з місця перебування користувача. У великих містах вартість життя вище, а це означає, що вище і доходи. Маркетологи це знають і програмують свої сайти так, щоб люди з цих регіонів бачили більш високі ціни (такий підхід часто зустрічається серед авіаліній). Друга причина дискримінації: провайдери та інші сервіси відстежують покупки і переваги своїх клієнтів. Дізнавшись, що клієнт регулярно купує певний товар, вони теоретично можуть продати цю інформацію виробнику товару, який підвищить для цього клієнта ціну, оскільки знає, що він точно його купить. Завдяки конфіденційності та анонімності в мережі VPN користувач буде вільний від подібного цільового впливу.
* **Позбавитися від стеження.** Не надавати такої можливості зловмисникам, кіберзлочинцям, корпораціям і навіть власному постачальнику послуг інтернету стежити за собою.

### Недоліки мережі VPN

* **Можливо уповільнення роботи.** При підключенні через VPN потік даних проходить більше етапів, ніж зазвичай, що може викликати помітне уповільнення роботи. Оскільки це популярна скарга щодо VPN, розробники взяли це до відома. Багато з них настільки досягли успіху в оптимізації швидкості і продуктивності, що їх користувачі VPN можуть без найменших проблем грати в ігри і дивитися трансляції.
* **Труднощі, пов'язані з QoS.** QoS означає «якість обслуговування» і описує продуктивність служби або мережі. Для мереж VPN поки немає будь-якого стандарту, який можна заміряти і повідомити показники. А оскільки немає показників для аналізу, потрібно покладатися на професійні огляди та відгуки користувачів, щоб дізнатися, які служби є надійними.
* **Блокування VPN.** Деякі компанії розуміють, що мережі VPN надають їх користувачам багато можливостей. Щоб протистояти цьому, вони починають блокувати доступ для відомих IP-адрес VPN. Проте, служби VPN натомість використовують нові IP-адреси.
* **Відсутність повної конфіденційності.** Хоча мережа VPN справляється з шифруванням і збереженням конфіденційності користувача, файли cookie, що знаходяться у браузері все одно можуть його впізнати. Виходом буде вимкнення збереження cookie.

### Сумісність VPN з пристроями

На всіх пристроях, що підключаються до Інтернету, можна скористатися перевагами конфіденційності, яка забезпечується мережею VPN. Служби VPN зазвичай пропонують можливість підключення для кількох пристроїв одночасно.



Рис.2. Підключення VPN для кількох пристроїв одночасно

Комп'ютери, планшети і телефони підключити до мережі VPN нескладно, однак з пристроями Інтернету речей все не так просто. Для них кращим варіантом буде встановити маршрутизатор із захистом VPN. Тоді і вхідні і вихідні дані будуть захищені. Деякі маршрутизатори продаються з уже вбудованим ПЗ для VPN.

## Принцип функціонування мережі VPN

При використанні віртуальної приватної мережі ніхто не побачить реальну IP-адресу, оскільки замість неї тепер буде розпізнаватися адреса VPN (рис.3).

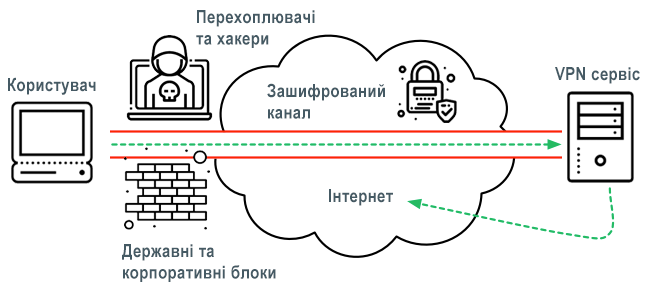


Рис. 3. Принцип функціонування мережі VPN

Саме підключення до Інтернету буде зашифровано, тому, ніхто не побачить дані, які користувач завантажуєте, вивантажує або надсилає. Шифрування - це спосіб перетворення тексту в складний набір кодів. Існує три основних види шифрування: хешування, симетричне і асиметричне шифрування. В кожного виду свої переваги і недоліки, але всі вони шифрують дані так, що в чужих руках вони будуть марними.

Додатковий рівень захисту, який є у більшості служб VPN - їх власна система DNS. DNS - система доменних імен - це телефонна книга інтернету, в якій текстові URL-адреси ототожнені з відповідними IP-адресами. Система DNS дозволяє замість довгої послідовності цифр вводити назву сайту, наприклад site.ua. Кіберзлочинці можуть спостерігати за запитами DNS, щоб відстежувати дії користувача в інтернеті, але система DNS в службах VPN розроблена так, щоб за допомогою додаткового шифрування перешкодити їм.

Слід пам'ятати, що не вся інформація шифрується. У різних VPN-провайдерів можуть відрізнятися такі характеристики як ступінь шифрування, приховування факту підключення до сервера, зберігання логів (журнал, в який зберігається інформація про відвідуваних сайтах, реальні IP адреси тощо) і співпраця при видачі інформації третім особам.

Якщо VPN-провайдер взагалі не записує логи, то передавати третім особам просто нічого. А приховування факту підключення до сервера - вже більш рідкісна послуга. При некоректному підключенні або різкому розриві з'єднання може статися витік частини даних.

### Розвиток мережі VPN

Спочатку мережі VPN були споживчим продуктом, як сьогодні. Компанія Microsoft розробила першу мережу VPN в 1996 році, щоб співробітники могли отримати доступ до внутрішньої мережі компанії з дому. Так виникли віддалені робочі місця.

Це, природно, дозволило збільшити продуктивність праці в компанії. Інші компанії почали теж впроваджувати цю технологію. Сьогодні такий вид мережі VPN використовується широко. Це стандартний функціональний засіб сучасного бізнес-середовища в усьому світі.

В подальшому захист VPN, що забезпечує конфіденційність, оцінили і в споживчому секторі. Розробники побачили, що цей захищений «тунель», за яким можна пересуватися в мережі, міг би використовуватися для з'єднання з найбільшою мережею в світі - всесвітньою павутиною. Багато користувачів хочуть зберегти конфіденційність і анонімність в інтернеті. Мережі VPN стали готовим рішенням.

## Різні види мереж VPN

Існує два основних види мереж VPN.

**Шлюз захищеного віддаленого доступу до VPN** дозволяє користувачам підключитися до іншої мережі (до інтернету або внутрішньої системі своєї компанії) за приватним зашифрованим тунелем (рис.4).

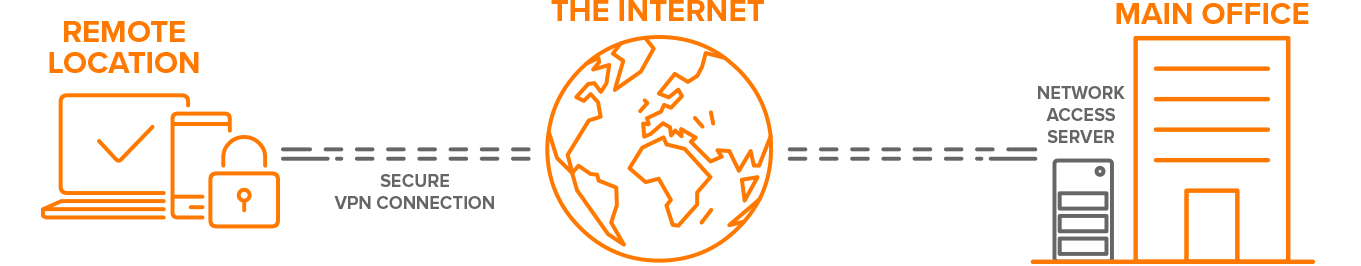


Рис.4. Шлюз захищеного віддаленого доступу до VPN

**VPN типу «мережа-мережа»**, яку називають VPN між маршрутизаторами. Цей вид мережі VPN в основному використовується в корпоративному середовищі, особливо якщо у підприємства є штаб-квартири з різним розташуванням. VPN типу «мережа-мережа» використовується для створення закритої внутрішньої мережі, де всі офіси можуть підключатися один до одного. Ця технологія відома як інтранет.

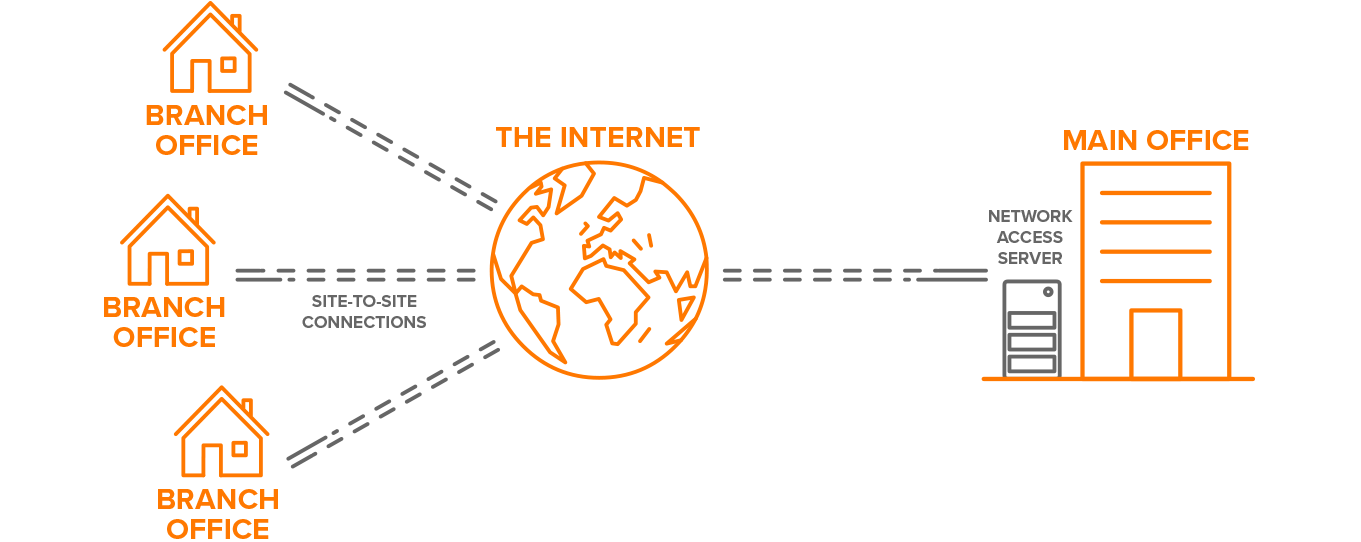


Рис.5. VPN типу «мережа-мережа»

Існує кілька протоколів VPN, тобто способів забезпечення безпеки. Найстаріший з них - PPTP (протокол тунелювання «точка-точка»), який вважається одним з самих ненадійних протоколів. Решта - IPSec, L2TP, SSL, TLS, SSH і OpenVPN. Багато хто віддає перевагу протоколу OpenVPN, оскільки це програмне забезпечення з відкритим вихідним кодом. Якщо в там буде виявлено вразливість, то її швидко виправлять.

## Вибір VPN

При виборі VPN є кілька варіантів. Деякі вважають за краще випробувати VPN безкоштовно. Безкоштовні мережі VPN відмінно підійдуть, якщо потрібно розібратися, як працює VPN.

Після випробувань можна купити повну версію (за невелику плату отримати підвищену пропускну здатність, сервери, необхідні для доступу до будь-яких матеріалів з будь-якої точки світу, і повний захист в безкоштовних мережах Wi-Fi).

Перед покупкою слід випробувати пробну версію, для з’ясування слабких місць, що можуть бути:

* Використовуються ненадійні протоколи, такі як PPTP.
* Кількість серверів менше, тому пропускна здатність поділяється з іншими користувачами, через що зменшується швидкість.
* Може міститися реклама.
* Можуть бути встановлені обмеження на скачування.

Платні служби VPN мають серйозну перевагу, але всі вони різні. Нижче описано, що слід врахувати при пошуку ідеальної програми VPN.

* **Репутація.** Щоб з'ясувати, наскільки ефективно працює VPN, варто почитати відгуки користувачів і фахівців. Оскільки правила для постачальників послуг інтернету щодо конфіденційності були скасовані, тому від того часу з'явилося багато фальшивих мереж VPN. Варто переконатися, що обрана мережа є справжньою.
* **Загальні IP-адреси.** Вибирати мережу VPN з загальними IP-адресами. Бути одним з багатьох анонімних користувачів - це додатковий рівень захисту конфіденційності.
* **Сервери.** Чим більше серверів, тим швидше перегляд веб-сторінок, оскільки чим ближче ви до сервера, тим швидше і надійніше ваше підключення.
* **Шифрування.** AES-256 (Advanced Encryption Standard) - найвищий стандарт шифрування на поточний момент. Його практично неможливо зламати, оскільки у нього незлічима кількість комбінацій.
* **Протокол.** Намагатися не використовувати ненадійні протоколи, такі як PPTP, обирати надійний OpenVPN.
* **Журнали даних.** Служба VPN повинна вказувати, що вона не зберігає журнали даних (тобто власний звіт про дії користувача в Інтернеті). Щоб дізнатися, чи збирає служба VPN інформацію про клієнтів, варто прочитати її політику.
* **Підтримка клієнтів.** Кращі постачальники VPN мають службу підтримки клієнтів, яка завжди готова допомогти, якщо виникне якась проблема.
* **Функції.** Переконатися, що обрана програма VPN сумісна з усім, що необхідно користувачеві. Наприклад, деякі програми VPN не дозволяють використовувати BitTorrent, мають обмеження при скачуванні (лише певну кількість завантажень), пропонують блокування реклами, мережні екрани, аварійні вимикачі, одночасне підключення тощо. Користувачеві слід визначитися, що найкраще підходить саме для його потреб в Інтернеті.
* **Безкоштовна пробна версія.** В багатьох програмах VPN є можливість отримати безкоштовну пробну версію для перевірки зручності використання і продуктивності мережі VPN, перш ніж за неї платити.

### Використання VPN в браузері

У випадку використання звичайного браузером можна застосувати кілька підходів:

1. Встановити VPN-клієнт (програму) на комп’ютер.
2. Додати розширення для браузера через Webstore.
3. Використовувати безкоштовний VPN, вбудований в браузері Opera.

Щоб встановити VPN-клієнт, необхідно завантажити програму в інтернеті, наприклад, «Betternet». Запуском інсталяційного файлу встановлюється клієнт. В клієнті потрібно лише натиснути: «Connect». Програма автоматично видає рандомну IP-адресу і не можна вибрати країну. Деякі клієнти мають можливість одночасного запуску з ОС, в іншому випадку доведеться запускати самому.

Для додавання розширення потрібно пройти реєстрацію. Такий підхід є зручним, оскільки потрібно лише увімкнути іконку, вибрати країну і починати веб-серфінг. На даний момент існують тисячі подібних програм, наприклад «Hotspot Shield».

Про VPN розширення для різних браузерів можна прочитати на цьому [ресурсі](https://help-wifi.com/programmy-brauzery/vpn-dlya-chrome-opera-firefox-i-yandeks-brauzera-dostup-k-zablokirovannym-sajtam/).

### VPN на мобільних пристроях

Використання VPN на смартфонах або планшетах з операційною системою ОС, наприклад, iOS або Андроїд реалізується через мобільні додатки. На Android, наприклад, це OpenVPN, а на iOS - це Cloak. Так само на iPhone і iPad можна використовувати безкоштовний і перевірений Opera VPN для iOS. Додатки завантажуються з Play Market або AppStore і встановлюються на пристрій. Після активації VPN вибирається профіль, отримується IP-адреса і проводиться з'єднання через VPN.

## Контрольні запитання

1. Який принцип покладено в функціонування VPN?
2. Що таке мережний нейтралітет?
3. Назвати основні види мереж VPN.
4. Чи забезпечується сумісність VPN з різними пристроями?
5. Критерії вибору VPN.
6. Як можна використати в браузері VPN?
7. Як використати VPN в мобільних пристроях?

## Літературні джерела

1. Що таке VPN и як це працює <https://blog.avast.com/ru/chto-takoe-vpn-i-kak-eto-rabotaet-bazovoe-rukovodstvo-avast>
2. Як працює VPN <https://blog.themarfa.name/kak-rabotaiet-vpn-i-pochiemu-eto-luchshie-tor-ili-proxy/>
3. VPN: просто про складне <https://habr.com/ru/post/534250/>
4. Що таке VPN <https://help-wifi.com/poleznoe-i-interesnoe/chto-takoe-vpn-dlya-chego-on-nuzhen-i-kak-polzovatsya/>
5. Порівняльний огляд реалізацій технології VPN https://1cloud.ru/help/network/comparevpntypes
6. VPN-протоколи [https://ru.vpnmentor.com/blog /какой-vpn-протокол-стоит-использовать/](https://ru.vpnmentor.com/blog%20/какой-vpn-протокол-стоит-использовать/)
7. VPN для Chrome, Opera, Firefox <https://help-wifi.com/programmy-brauzery/vpn-dlya-chrome-opera-firefox-i-yandeks-brauzera-dostup-k-zablokirovannym-sajtam/>