

Віртуальна приватна мережа VPN (скорочення від [англ. Virtual Private Network](#)) — узагальнююча назва мереж, що створюються поверх інших мереж, які мають менший рівень довіри.

VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в [Інтернет](#).

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

Тунелювання може застосовуватися для декількох цілей:

- * передача через мережу пакетів, що належать протоколу, який у даній мережі не підтримується (наприклад, передача пакетів IPv6 через старі мережі, що підтримують тільки IPv4);
- * забезпечення слабкої форми конфіденційності (у першу чергу конфіденційності графіка) за рахунок приховування істинних адрес та іншої службової інформації;
- * забезпечення конфіденційності й цілісності переданих даних при використанні разом із криптографічними сервісами.

TheOnionRouter(TOR) - вільне і відкрите програмне забезпечення для реалізації другого покоління так званої "цибульної маршрутизації". Це система проксі-серверів, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від перехоплення інформації.

Загрози, пов'язані з використанням VPN.

- Недостатній рівень захисту даних забезпечується власниками VPN сервісами/
- Безкоштовні сервіси є менш захищеними ніж платні.
- Можливість крадіжки особистих даних.
- Передача даних невідомим адресатам.

Підручник В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест. Основи інформаційної безпеки <http://www.dut.edu.ua/ua/lib/1/category/729/view/1365>