

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра «Комп’ютерні інформаційні технології»

**Лабораторна робота №11**

**з дисципліни «Організація комп’ютерних мереж»**

**на тему: «Підключення до VPN сервера через локальну обчислювальну мережу (ЛОМ) (Windows 7).»**

Виконав:

Студент гр. ПЗ2011

Кулик С.В.

Прийняв:

Івченко Ю. М.

Дніпро, 2023

**Тема.** Підключення до VPN сервера через локальну обчислювальну мережу (ЛОМ) (Windows 7).

**Мета.** Ознайомитися і отримати практичні навички підключення до VPN сервера через ЛОМ.

**Порядок виконання роботи**

1. Ознайомитися з основними поняттями:  
    - локальна обчислювальна мережа (Local Area Network, LAN);  
    - набір протоколів для забезпечення захисту даних IP Security;  
    - протокол тунелювання другого рівня (Layer 2 Tunneling Protocol);  
    - протокол аутентифікації PAP (Password Authentication Protocol);  
    - віртуальна приватна мережа (Virtual Private Network, VPN);  
    - типи VPN-підключень;  
    - властивості VPN-підключень.
2. Налагодити VPN підключення в Windows, для чого виконати:  
    - створення нового мережевого підключення;  
    - перевірку поточного стану мережевого підключення;  
    - налагодження створеного VPN підключення;  
    - запуск і перевірку VPN підключення

**Теоретичні відомості**

Локальна обчислювальна мережа (ЛОМ, локальна мережа; Local Area Network, LAN) — комп’ютерна мережа, що охоплює відносно невелику територію або невелику групу будівель (дім, офіс, фірму, університет).

IPsec (сокращение от IP Security) — набір протоколів для забезпечення захисту даних, що передаються з використанням мережевого протоколу IP. Він дозволяє здійснювати підтвердження справжності (аутентифікацію), перевірку цілісності і/або шифрування IPпакетів. IPsec також включає в себе протоколи для захищеного обміну ключами в мережі Інтернет. В основному, застосовується для організації VPN –з’єднання.

Протокол тунелювання другого рівня (Layer 2 Tunneling Protocol, L2TP) — в комп’ютерних мережах тунельний протокол, що використовується для підтримки віртуальних приватних мереж (VPN). Головна перевага L2TP полягає в тому, що цей протокол дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 і Frame Relay. Тунелювання (від англ. tunnelling — «створення тунелю») в комп’ютерних мережах — процес, в ході якого створюється захищене логічне з’єднання між двома кінцевими точками за допомогою інкапсуляції різних протоколів. Тунелювання представляє собою метод побудови мереж, при якому один мережевий протокол інкапсулюється в інший. Від звичайних багаторівневих мережевих моделей (таких як OSI або TCP/IP) тунелювання відрізняється тим, що протокол, який інкапсулюється, відноситься до того ж або нижчого рівня, ніж той, що використовується в якості тунелю.

Суть тунелювання полягає в тому, щоб «упакувати» передану порцію даних разом з службовими полями, в новий «конверт» для забезпечення конфіденційності і цілісності всієї переданої порції, включаючи службові поля. Тунелювання може застосовуватися на мережевому і на прикладному рівнях. Комбінація тунелювання і шифрування дозволяє реалізувати закриті віртуальні приватні мережі (VPN). Тунелювання застосовується для узгодження транспортних протоколів або для створення захищеного з’єднання між вузлами мережі.

Протокол аутентифікації PAP (Password Authentication Protocol) — протокол простої перевірки справжності, що передбачає відправку імені користувача і пароля на сервер віддаленого доступу відкритим текстом (без шифрування).

Віртуальна приватна мережа (Virtual Private Network, VPN) є підключення типу «точка-точка» в приватній або публічній мережі, наприклад, в Інтернеті. VPN-клієнт використовує для віртуального звернення до віртуального порту VPN-сервера спеціальні протоколи на основі TCP/IP, які називаються тунельними протоколами. При звичайній реалізації VPN клієнт ініціює через Інтернет віртуальне підключення типу «точка-точка» до сервера віддаленого доступу. Сервер віддаленого доступу відповідає на виклик, виконує перевірку справжності викликаючої сторони і передає дані між VPN-клієнтом і приватною мережею організації.

Для емуляції каналу типу «точка-точка» до даних додається заголовок (виконується інкапсуляція). Цей заголовок містить відомості маршрутизації, які забезпечують проходження даних через загальну або публічну мережі до кінцевого пункту. Для емуляції приватного каналу і збереження конфіденційності передані дані шифруються. Пакети, що перехоплені в загальній або публічній мережі, неможливо розшифрувати без ключів шифрування. Такий канал, через який приватні дані передаються в інкапсульованому і зашифрованому виді, і називається VPN-підключенням.

Протокол IKE (Internet Key Exchange) — стандартний протокол IPsec, що використовується для забезпечення безпеки взаємодії в віртуальних приватних мережах. Призначення IKE — захищене узгодження і доставка ідентифікованого матеріалу для асоціації безпеки.

Типи VPN підключень

Існує два типи VPN-підключень:

* + VPN-підключення віддаленого доступу;
  + VPN-підключення типу «мережа-мережа».

**VPN-підключення віддаленого доступу**

VPN-підключення віддаленого доступу надає користувачам можливість працювати вдома або в дорозі, отримуючи доступ до сервера приватної мережі за допомогою інфраструктури публічної мережі, наприклад, Інтернету. З точки зору користувача, VPNпідключення є підключення типу «точка-точка» між комп’ютером (VPN-клієнтом) і сервером організації. Реальна інфраструктура загальної або публічної мережі не має значення, тому що дані передається подібно до того, як би вони передавалися через виділений приватний канал.

**VPN-підключення типу «мережа-мережа».**

VPN-підключення типу «мережа-мережа» (також називаються VPN-підключення типу «маршрутизатор-маршрутизатор») дозволяють організаціям встановлювати маршрутизовані підключення між окремими офісами (або між іншими організаціями) через публічну мережу, при цьому забезпечуючи безпеку зв’язку. Маршрутизоване VPNпідключення через Інтернет логічно подібне орендованому каналу глобальної мережі (WAN). У випадку, коли мережі з’єднані через Інтернет, як показано на наступному рисунку, маршрутизатор переадресовує пакети іншому маршрутизатору через VPNпідключення. З точки зору маршрутизаторів VPN-підключення працює як канал рівня передачі даних.

VPN-підключення типу «мережа-мережа» зв’язує два сегменти приватної мережі. Викликаючий маршрутизатор (VPN-клієнт) проходить перевірку справжності на відповідаючому маршрутизаторі (VPN-сервері) і, з метою взаємної перевірки справжності, відповідаючий маршрутизатор проходить перевірку справжності на викликаючому маршрутизаторі.

**VPN-підключення двох віддалених вузлів через Інтернет**

Властивості VPN-підключень

VPN-підключення, що використовують протоколи PPTP, L2TP/IPsec і SSTP, мають наступні властивості:

* інкапсуляція;
* перевірка справжності;
* шифрування даних.

**Інкапсуляція**

VPN-технологія забезпечує інкапсуляцію приватних даних з заголовком, що містить відомості маршрутизації для передачі цих даних через транзитну мережу.

**Перевірка справжності**

Існують три різних форми перевірки справжності для VPN-підключень.

1. Перевірка справжності на рівні користувача за протоколом PPP.

Для встановлення VPN-підключення VPN-сервер виконує перевірку справжності VPNклієнта, який намагається встановити підключення, на рівні користувача за протоколом PPP і перевіряє, чи має VPN-клієнт необхідну авторизацію. При взаємній перевірці справжності VPN-клієнт також виконує перевірку справжності VPN-сервера, що гарантує захист від комп’ютерів, що видають себе за VPN-сервери.

2. Перевірка справжності на рівні комп’ютера за протоколом IKE.

Для встановлення зіставлення безпеки IPsec VPN-клієнт і VPN-сервер використовують протокол IKE для обміну сертифікатами комп’ютерів або попереднім ключем. В обох випадках VPN-клієнт і VPN-сервер виконують взаємну перевірку справжності на рівні комп’ютера. Наполегливо рекомендується обирати перевірку справжності згідно з сертифікатом комп’ютера через більшу безпеку цього методу. Перевірка справжності на рівні комп’ютера виконується тільки для підключень L2TP/IPsec.

3. Перевірка справжності джерела даних і забезпечення цілісності даних.

Щоб впевнитися в тому, що джерелом відправлених через VPN-підключення даних є інша сторона VPN-підключення і що вони передані в незмінному виді, дані містять контрольну суму шифрування, що ґрунтується на ключі шифрування, який відомий тільки відправнику і отримувачу. Перевірка справжності джерела даних і забезпечення цілісності даних доступні тільки для підключень L2TP/IPsec.

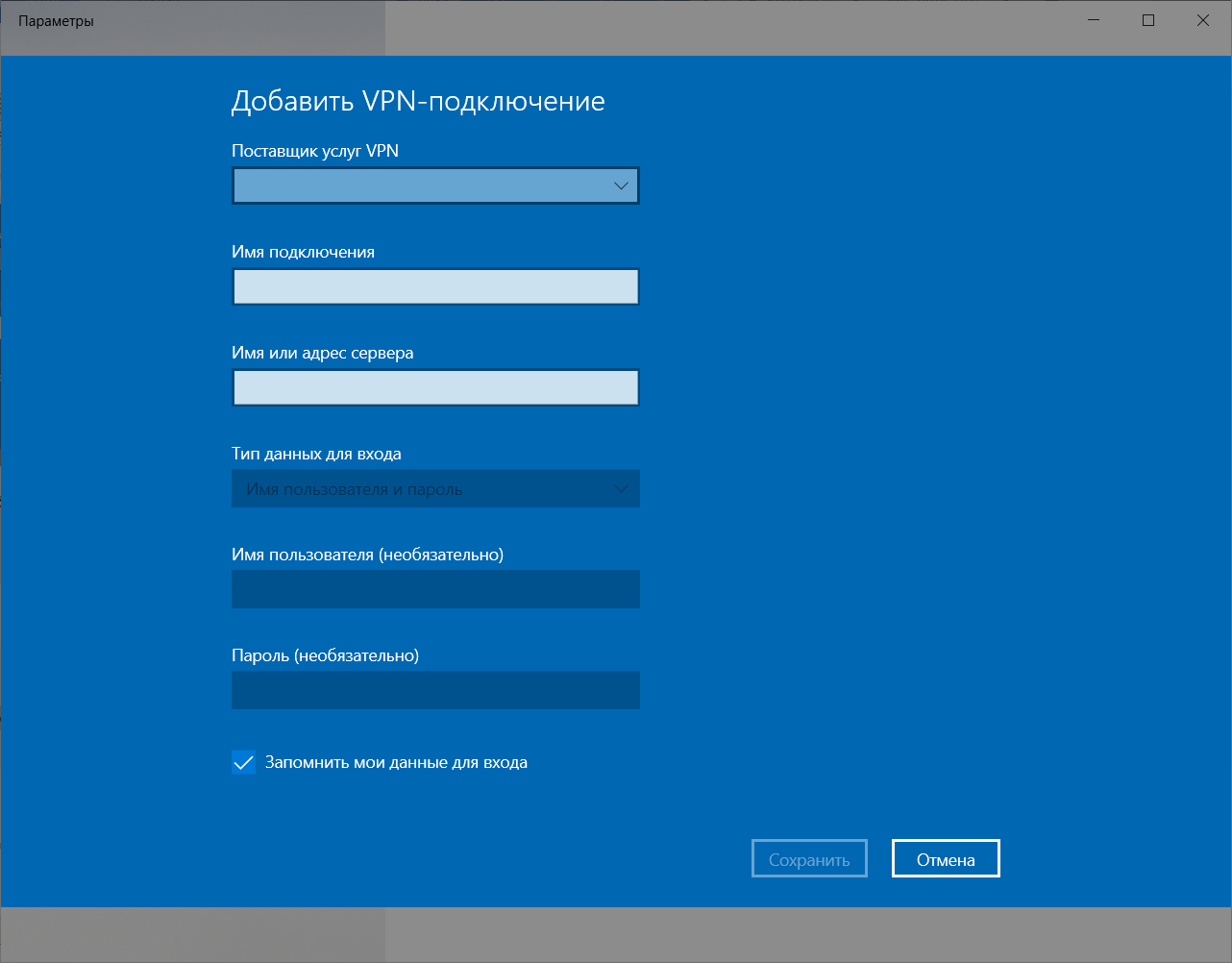
**Шифрування даних**

Для забезпечення конфіденційності даних при передачі через загальні або публічні транзитні мережі вони шифруються відправником і розшифровуються отримувачем. Успішність процесів шифрування і розшифрування гарантується в тому випадку, коли відправник і отримувач використовується загальний ключ шифрування.

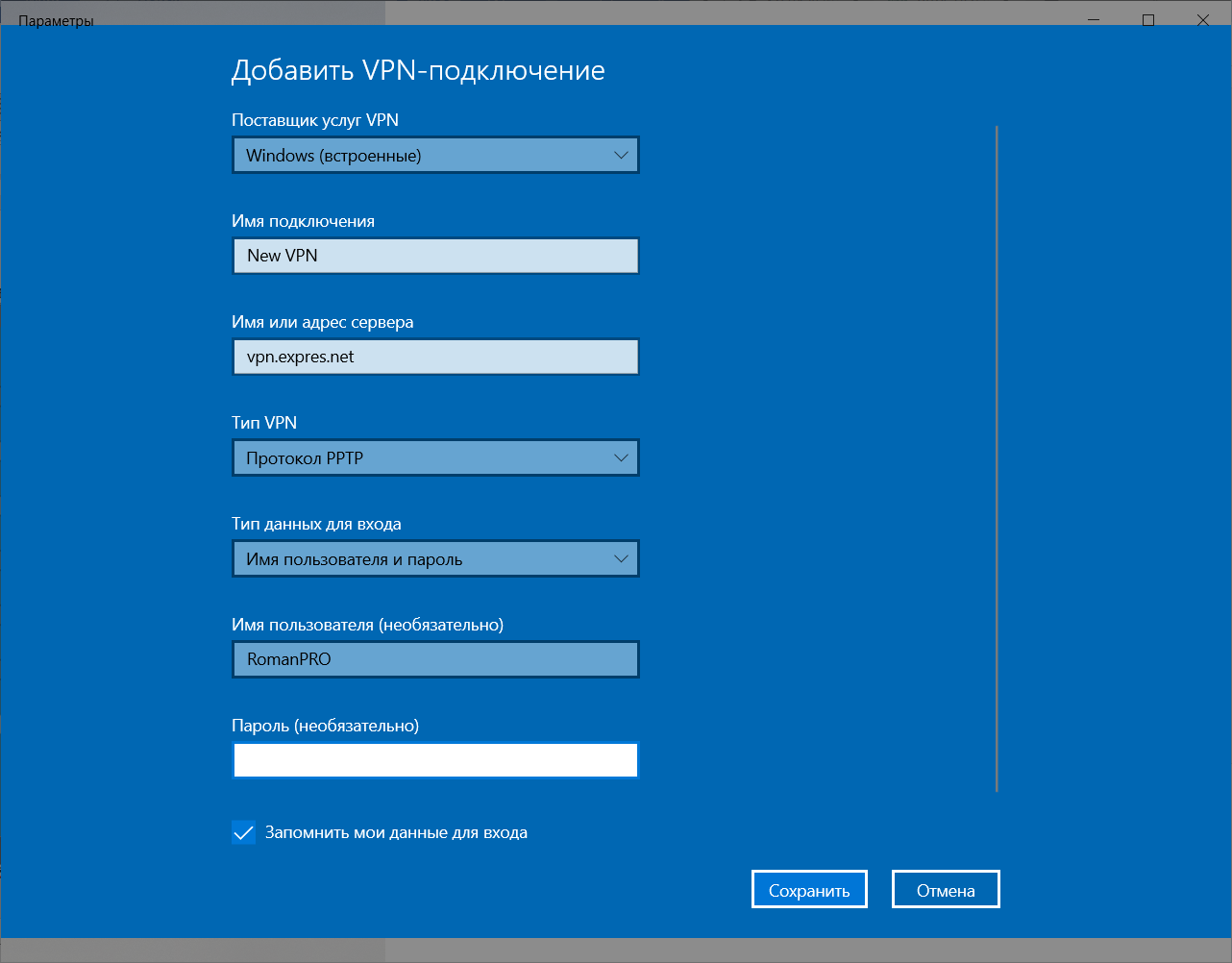
Зміст перехоплених пакетів, відправлених через VPN-підключення в транзитній мережі, зрозумілий тільки власникам загального ключа. Довжина ключа шифрування – це важливий параметр безпеки. Тому для гарантії конфіденційності даних рекомендується використовувати найбільший можливий ключ.

**Налагодження VPN підключення в Windows**

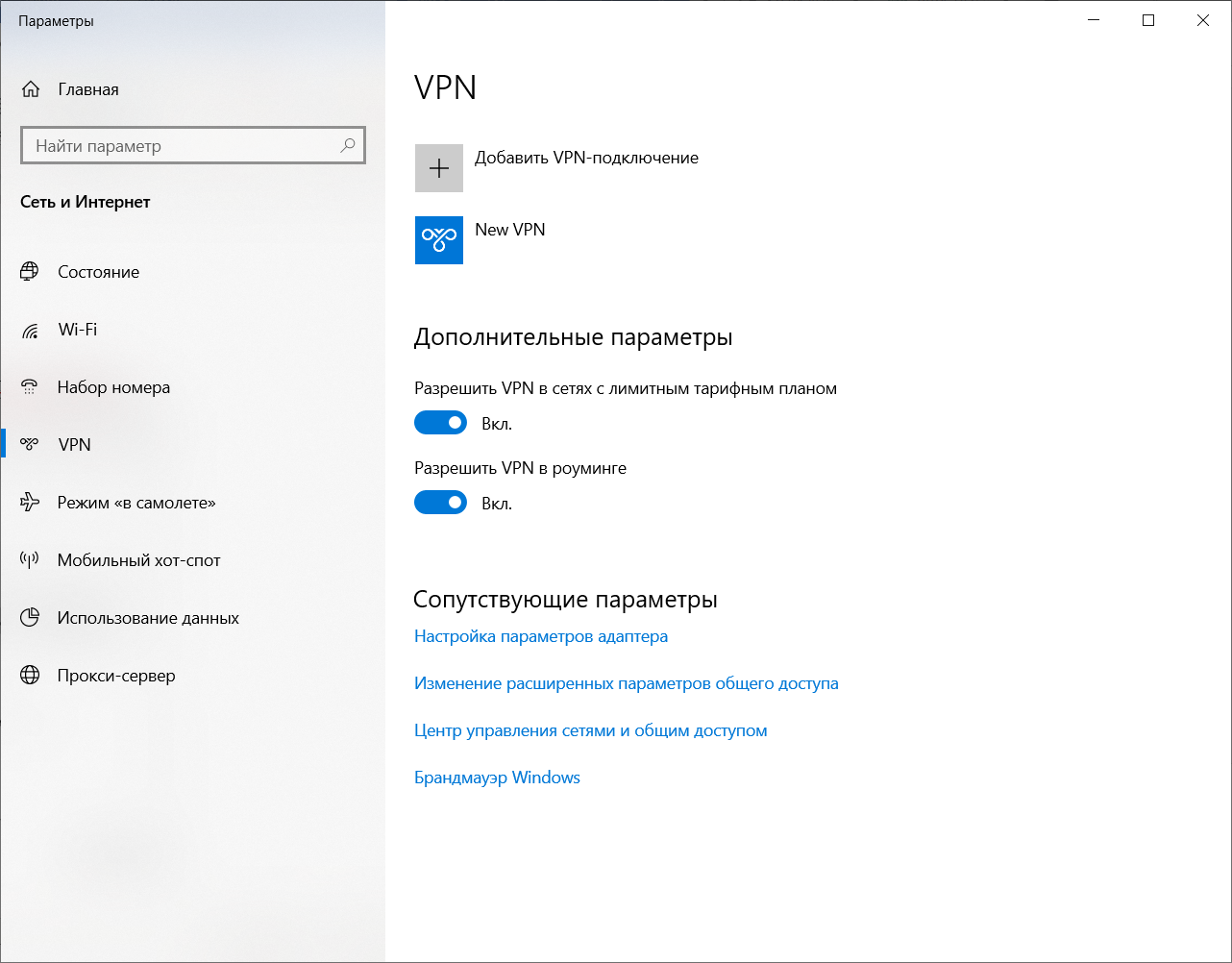
1. Створення нового мережевого підключення.



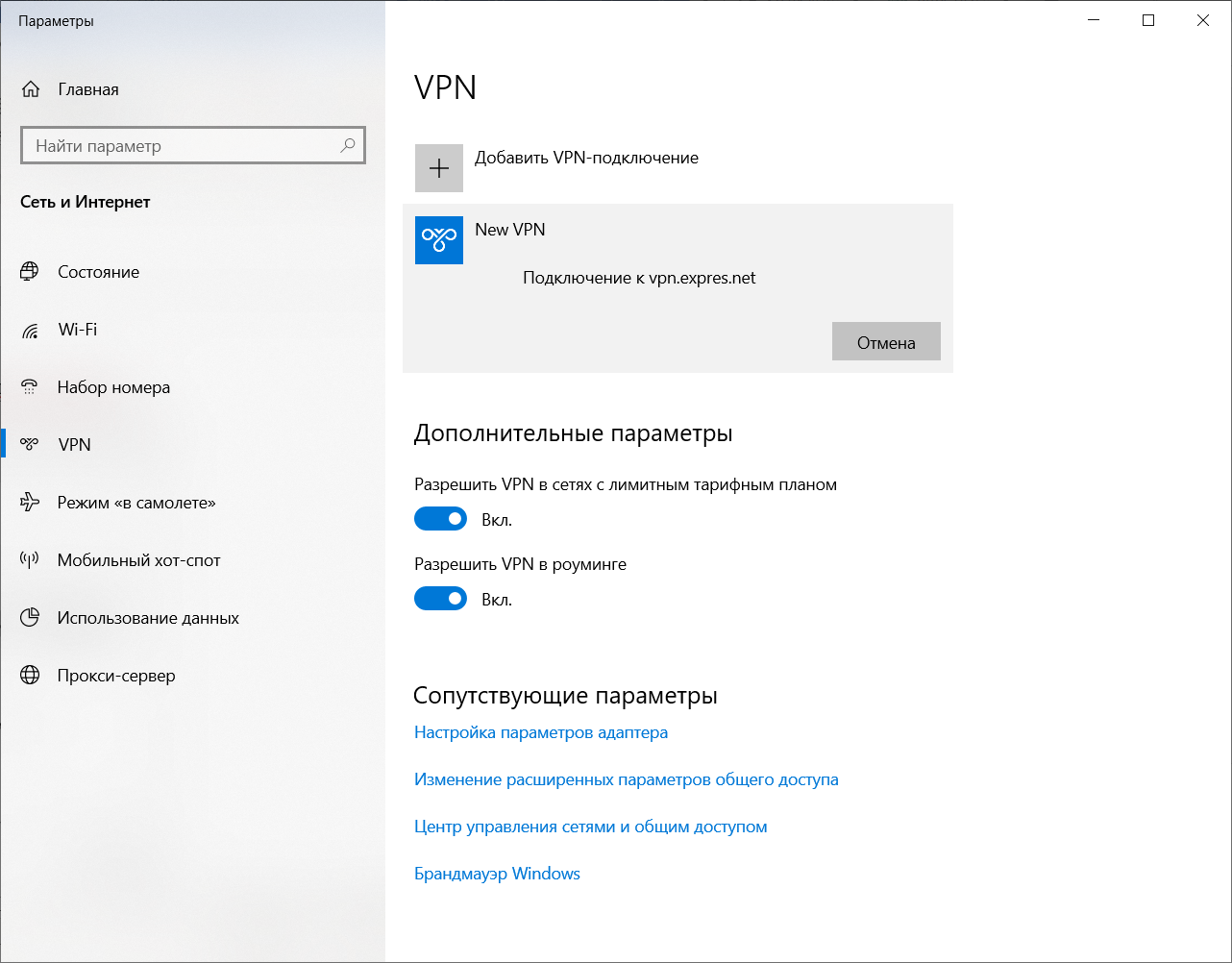
1. Перевірку поточного стану мережевого підключення



1. Налагодження створеного VPN підключення



1. Запуск і перевірку VPN підключення



**Висновок**

Підключення до VPN сервера через локальну обчислювальну мережу (ЛОМ) є важливим кроком у забезпеченні безпеки та приватності під час доступу до Інтернету. Цей процес передбачає налаштування віртуальної приватної мережі (VPN) на комп'ютері з операційною системою Windows 7, що дозволяє забезпечити шифрування трафіку та забезпечити анонімність під час передачі даних.

Отримання практичних навичок підключення до VPN сервера через ЛОМ на Windows 7 дозволяє користувачам безпечно та захищено користуватися мережевими ресурсами, зокрема, під час доступу до конфіденційної інформації або використання віддалених серверів.

Навички налаштування VPN на Windows 7 дозволяють користувачам підключатися до віддалених ресурсів з будь-якого місця з доступом до Інтернету, забезпечуючи безпеку і конфіденційність даних. Це особливо важливо в організаціях, де доступ до внутрішніх мережевих ресурсів здійснюється через ЛОМ.

**Контрольні питання**

**1. Що таке Інтернет, ідентифікатор місце розташування URL, Browser?**

**Інтернет** - всесвітня система об'єднаних комп'ютерних мереж, заснована на використанні протоколу IP і маршрутизації пакетів даних. Поняття часто згадується як «Всесвітня мережа» і «Глобальна мережа».

**Уніфіковані покажчик ресурсу (URL)** - система уніфікованих адресу електронних ресурсів, або одноманітно визначник місцезнаходження ресурсу (файлу). Використовується як стандарт запису посилань на об'єкти в Інтернеті.

**Браузер** - [програмне забезпечення](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) для [комп'ютера](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80) або іншого електронного пристрою, як правило, під'єднаного до [Інтернету](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), що дає можливість користувачеві взаємодіяти з текстом, малюнками або іншою інформацією на [гіпертекстовій](https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%BF%D0%B5%D1%80%D1%82%D0%B5%D0%BA%D1%81%D1%82) [вебсторінці](https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1%D1%81%D1%82%D0%BE%D1%80%D1%96%D0%BD%D0%BA%D0%B0). Тексти та малюнки можуть містити посилання на інші вебсторінки, розташовані на тому ж вебсайті або на інших вебсайтах. Вебпереглядач за допомогою [гіперпосилань](https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%BF%D0%B5%D1%80%D0%BF%D0%BE%D1%81%D0%B8%D0%BB%D0%B0%D0%BD%D0%BD%D1%8F) дозволяє користувачеві швидко та просто отримувати інформацію, розміщену на багатьох вебсторінках.

**2. Послуги Інтернет: WWW, FTP, електронна пошта, Telnet.**

**World Wide Web (скорочено WWW або Web)** - розподілена система, що надає доступ до пов'язаних між собою документів, розташованим на різних комп'ютерах, підключених до мережі Інтернет. Для позначення Всесвітньої павутини також використовують слово веб (англ. Web «павутина») і абревіатуру WWW.

Всесвітню павутину утворюють сотні мільйонів веб-серверів. Більшість ресурсів Всесвітньої павутини засноване на технології гіпертексту. Гіпертекстові документи, що розміщуються у Всесвітній павутині, називаються веб-сторінками.

**FTP (File Transfer Protocol)** - протокол передачі файлів по мережі, є одним з найстаріших прикладних протоколів, що з'явилися задовго до HTTP, і навіть до TCP / IP, в 1971 році; в перший час він працював над протоколом NCP. Він і сьогодні широко використовується для поширення ПО і доступу до віддалених хостів. На відміну від TFTP, гарантує передачу (або видачу помилки) за рахунок застосування квотної протоколу.

Протокол побудований на архітектурі «клієнт-сервер» і використовує різні мережеві з'єднання для передачі команд і даних між клієнтом і сервером. Користувачі FTP можуть пройти аутентифікацію, передаючи логін і пароль відкритим текстом, або ж, якщо це дозволено на сервері, вони можуть підключитися анонімно.

**TELNET (скор. від Teletype network)** - мережевий протокол для реалізації текстового термінального інтерфейсу по мережі (в сучасній формі - за допомогою транспорту TCP). Назва «telnet» мають також деякі утиліти, що реалізують клієнтську частину протоколу. Сучасний стандарт протоколу описаний в RFC 854.

Виконує функції протоколу прикладного рівня моделі OSI. Протокол telnet, поряд з ssh широко використовується для віддаленого адміністрування різними мережевими пристроями і програмними серверами.

**Електронна пошта** - технологія і служба з пересилки і отримання електронних повідомлень (званих «листи», «електронні листи» або «повідомлення») між користувачами комп'ютерної мережі (в тому числі - Інтернету).

**3. Протоколи IPsec, IKE. Протокол L2TP (тунелювання).**

**IPsec (сокращение от IP Security)** - набір протоколів для забезпечення захисту даних, що передаються з використанням мережевого протоколу IP. Він дозволяє здійснювати підтвердження справжності (аутентифікацію), перевірку цілісності і/або шифрування IPпакетів. IPsec також включає в себе протоколи для захищеного обміну ключами в мережі Інтернет. В основному, застосовується для організації VPN –з’єднання.

**IKE (Internet Key Exchange)** - стандартний протокол набору протоколів IPsec, який використовується для забезпечення безпеки взаємодії у віртуальних приватних мережах. Призначення IKE - захищене узгодження і доставка ідентифікованого матеріалу для "асоціації безпеки" (SA).

**Протокол L2TP (Layer 2 Tunneling Protocol, тунелювання другого рівня)** - в комп’ютерних мережах тунельний протокол, що використовується для підтримки віртуальних приватних мереж (VPN). Головна перевага L2TP полягає в тому, що цей протокол дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 і Frame Relay.

Від звичайних багаторівневих мережевих моделей (таких як OSI або TCP/IP) тунелювання відрізняється тим, що протокол, який інкапсулюється, відноситься до того ж або нижчого рівня, ніж той, що використовується в якості тунелю.

Суть тунелювання полягає в тому, щоб «упакувати» передану порцію даних разом з службовими полями, в новий «конверт» для забезпечення конфіденційності і цілісності всієї переданої порції, включаючи службові поля. Тунелювання може застосовуватися на мережевому і на прикладному рівнях. Комбінація тунелювання і шифрування дозволяє реалізувати закриті віртуальні приватні мережі (VPN). Тунелювання застосовується для 2 узгодження транспортних протоколів або для створення захищеного з’єднання між вузлами мережі.

**4. Типи VPN підключень.**

Існує два типи VPN-підключень:

* VPN-підключення віддаленого доступу;
* VPN-підключення типу «мережа-мережа».

**VPN-підключення віддаленого доступу** - надає користувачам можливість працювати вдома або в дорозі, отримуючи доступ до сервера приватної мережі за допомогою інфраструктури публічної мережі, наприклад, Інтернету. З точки зору користувача, VPN-підключення є підключення типу «точка-точка» між комп’ютером (VPN-клієнтом) і сервером організації. Реальна інфраструктура загальної або публічної мережі не має значення, тому що дані передається подібно до того, як би вони передавалися через виділений приватний канал.

**VPN-підключення типу «мережа-мережа»** - дозволяють організаціям встановлювати маршрутизовані підключення між окремими офісами (або між іншими організаціями) через публічну мережу, при цьому забезпечуючи безпеку зв’язку. Маршрутизоване VPN підключення через Інтернет логічно подібне орендованому каналу глобальної мережі (WAN). У випадку, коли мережі з’єднані через Інтернет, як показано на наступному рисунку, маршрутизатор переадресовує пакети іншому маршрутизатору через VPN підключення. З точки зору маршрутизаторів VPN-підключення працює як канал рівня передачі даних.

VPN-підключення типу «мережа-мережа» зв’язує два сегменти приватної мережі. Що викликає маршрутизатор (VPN-клієнт) проходить перевірку справжності на маршрутизаторі що відповідає (VPN-сервері) та, з метою взаємної перевірки справжності, маршрутизатор що відповідає проходить перевірку справжності на маршрутизаторі що викликає.

**5. Властивості VPN-підключень і використані протоколи.**

VPN-підключення, що використовують протоколи PPTP, L2TP/IPsec і SSTP, мають наступні властивості:

* інкапсуляція;
* перевірка справжності;
* шифрування даних.

**Інкапсуляція** - VPN-технологія забезпечує інкапсуляцію приватних даних з заголовком, що містить відомості маршрутизації для передачі цих даних через транзитну мережу.

**Перевірка справжності** - існують три різних форми перевірки справжності для VPN-підключень.

1) Перевірка справжності на рівні користувача за протоколом PPP. Для встановлення VPN-підключення VPN-сервер виконує перевірку справжності VPNклієнта, який намагається встановити підключення, на рівні користувача за протоколом PPP і перевіряє, чи має VPN-клієнт необхідну авторизацію. При взаємній перевірці справжності VPN-клієнт також виконує перевірку справжності VPN-сервера, що гарантує захист від комп’ютерів, що видають себе за VPN-сервери.

2) Перевірка справжності на рівні комп’ютера за протоколом IKE. Для встановлення зіставлення безпеки IPsec VPN-клієнт і VPN-сервер використовують протокол IKE для обміну сертифікатами комп’ютерів або попереднім ключем. В обох випадках VPN-клієнт і VPN-сервер виконують взаємну перевірку справжності на рівні комп’ютера. Наполегливо рекомендується обирати перевірку справжності згідно з сертифікатом комп’ютера через більшу безпеку цього методу. Перевірка справжності на рівні комп’ютера виконується тільки для підключень L2TP/IPsec.

3) Перевірка справжності джерела даних і забезпечення цілісності даних. Щоб впевнитися в тому, що джерелом відправлених через VPN-підключення даних є інша сторона VPN-підключення і що вони передані в незмінному виді, дані містять контрольну суму шифрування, що ґрунтується на ключі шифрування, який відомий тільки відправнику і отримувачу. Перевірка справжності джерела даних і забезпечення цілісності даних доступні тільки для підключень L2TP/IPsec.

**Шифрування даних** - для забезпечення конфіденційності даних при передачі через загальні або публічні транзитні мережі вони шифруються відправником і розшифровуються отримувачем. Успішність процесів шифрування і розшифрування гарантується в тому випадку, коли відправник і отримувач використовується загальний ключ шифрування. Зміст перехоплених пакетів, відправлених через VPN-підключення в транзитній мережі, зрозумілий тільки власникам загального ключа. Довжина ключа шифрування - це важливий параметр безпеки. Тому для гарантії конфіденційності даних рекомендується використовувати найбільший можливий ключ.