НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи
фахового молодшого бакалавра

на тему: **Огляд і порівняння ключових протоколів віртуальних приватних мереж (VPN)**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Яцинич Владислав Вячеславович

Керівник	_____ (підпис)	Володимир ПЛІШ
Нормоконтролер	_____ (підпис)	Володимир ПЛІШ
Рецензент	_____ (підпис)	Анатолій РОМАНЮК
Голова ЕК	_____ (підпис)	Андрій ВАХ
Члени ЕК	_____ (підпис)	Ігор ТИБЕЛЬ
	_____ (підпис)	Володимир ПЛІШ

Дипломна робота захищена в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія	***Телекомунікації***
Освітньо-професійний ступінь	***Фаховий молодший бакалавр***
Освітньо-професійна програма	***Телекомунікації та комп'ютерні технології***
Спеціальність	***172 Телекомунікації та радіотехніка***

ЗАТВЕРДЖУЮ
Завідувач відділення
«Телекомунікацій та
комп'ютерних технологій»
_____ Ігор ТИБЕЛЬ
« 25 » квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ ЗДОБУВАЧУ

Яциничу Владиславу Вячеславовичу
(прізвище, ім'я та по батькові)

1.Тема роботи *Огляд і порівняння ключових протоколів віртуальних приватних мереж (VPN)*

керівник роботи *Володимир ПЛІШ викладач вищої категорії, викладач-методист*
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом директора від " 20 " березня 2025 року № 20-СТ

2. Строк подання студентом роботи "10" червня 2025 року

3. Вихідні дані до роботи *3.1 Характеристика, протоколи, функції та проблеми VPN;*

3.2 Зробити дослідження та аналіз сучасних VPN.

3.3 Проаналізувати альтернативні підходи до впровадження VPN мереж;

3.4 Порівняти особливості та характеристики п'яти різних протоколів VPN

4. Зміст розрахунково-пояснювальної записки

4.1 Мета та завдання використання VPN мереж.

4.2 Різновиди VPN та їх особливості.

4.3 Стратегії забезпечення конфіденційності в віртуальних приватних мережах.

4.4Техніко-економічне обгрунтування.

4.5 Охорона праці та безпека життедіяльності

5. Перелік графічного матеріалу

5.1.	*Структура віртуальних приватних мереж VPN*
5.2.	*Забезпечення аутентифікація користувачів у VPN мережах*
5.3.	*Класифікація VPN*
5.4.	*Структурна організація мережі, що ґрунтується на протоколі PPTP*
5.5	*Стандартне використання віртуальної приватної мережі*

6. Консультанти розділів дипломної роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	Завдання отримав
Техніко-економічне обґрунтовування	*Мар'яна СМУК викладач вищої категорії*	*25.04.2025р.*	*25.04.2025р*
Охорона праці та безпека життєдіяльності	*Олена МЕЛЬНИКОВА викладач першої категорії*	*25.04.2025р.*	*25.04.2025р.*

7. Дата видачі завдання « 25» квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання	Примітка
1	*Вступ.*	*25.04-01.05*	
2	*Мета та завдання використання VPN мереж*	*02.05-08.05*	
3	*Різновиди VPN та їх особливості.*	*09.05-15.05*	
4	*Стратегії забезпечення конфіденційності в віртуальних приватних мережах.*	*16.05-22.05*	
5	*Техніко – економічне обґрунтування*	*23.05-29.05*	
6	*Охорона праці та безпека життєдіяльності*	*30.05-03.06*	
7	*Висновки*	*04.06-05.06*	
8	*Підготовка графічного матеріалу.*	*06.06-09.06*	

Здобувач _____ *Владислав ЯЦИНИЧ*
(підпис) (ім'я, прізвище)

Керівник роботи _____ *Володимир ПЛІШ*
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина дипломної роботи: 90 с., 32 рис., 6 табл., 9 джерел.

Об’єкт дослідження – є віртуальні мережі VPN.

Мета роботи – є підвищення ефективності захисту корпоративних і публічних мереж з використанням нових технології VPN

Метод дослідження – аналітичний з використанням комп’ютерних технологій.

В дані роботі було досліджено структуру та принципи роботи основних протоколів VPN, а також їх ефективність за допомогою порівняння різних показників, таких як швидкість передачі даних, рівень шифрування, використання доступної пропускної здатності каналів і сумісність з операційними системами.

За результатами дослідження, протокол OpenVPN видається найбільш підходящим для задоволення вимог безпеки мережі від зловмисників. Він володіє високим рівнем шифрування даних, що забезпечує надійний захист, та відомий своєю високою швидкістю передачі інформації, незважаючи на високий рівень безпеки, що надається

VPN, TCP/IP, PPTP, ТУНЕЛЬ, IPSEC, ПАКЕТИ, ЗАХИСТ ІНФОРМАЦІЇ, TCP/IP, AES, AH, L2TP, IP.

ЗМІСТ

ВСТУП

У сучасному світі все більше уваги приділяється використанню технологій віддаленого доступу для спільної роботи та обміну даними між різними локаціями. Це особливо важливо для підрозділів автоматизації підприємств. У зв'язку з цим, наявність VPN-сервера в комп'ютерних мережах стає необхідністю. Він дозволяє віддаленим користувачам отримувати доступ до ресурсів приватної мережі через публічні канали зв'язку. Крім того, VPN використовується для забезпечення безпеки під час передачі конфіденційної інформації в локальній мережі, що допомагає уникнути її витоку або крадіжки під час транспортування через мережу.

Бізнес-людям часто доводиться подорожувати, доступ до важливої інформації може бути критично важливим. Це може бути інформація, збережена на особистому або корпоративному комп'ютері. Для отримання доступу до цієї інформації використання традиційних методів, таких як модем та телефонна лінія, може бути дорогим, особливо у випадку міжнародних подорожей.

У таких випадках використання технології VPN (Virtual Private Network) стає вигідним рішенням. VPN дозволяє здійснювати віддалений доступ до мережі через Інтернет, що є більш доступним та ефективним способом порівняно з використанням телефонних ліній. Для організації віддаленого доступу до приватної мережі за допомогою VPN потрібен лише доступ до Інтернету та реально діюча IP-адреса. Це робить доступ до мережі з будь-якого місця земної кулі зручним та доступним, за умови знання IP-адреси, логіну та паролю [1].

Сьогодні організація VPN-каналів для забезпечення зв'язку співробітників, які працюють віддалено, стала стандартною практикою для будь-якого адміністратора мережі. VPN, або віртуальна приватна мережа, з'єднує окремі комп'ютери або локальні мережі в єдину віртуальну мережу, що гарантує цілісність та безпеку передаваних даних. Вона працює на основі властивостей приватної мережі, але дозволяє передавати дані між комп'ютерами через будь-яку проміжну мережу, наприклад, Інтернет [2].

Використання VPN забезпечує ряд економічних переваг порівняно з іншими методами дистанційного доступу. Будь-який користувач, який має доступ до Інтернету, може легко підключитися до корпоративної мережі своєї фірми. Важливо відзначити, що доступність даних не означає їхню незахищеність. VPN є системою безпеки, що захищає всю корпоративну інформацію від несанкціонованого доступу.

У першу чергу, дані передаються у зашифрованому вигляді, доступ до яких може мати лише особа з відповідним ключем. Підтвердження справжності включає перевірку цілісності даних та ідентифікацію користувачів, що залучені до VPN.

Забезпечення безпеки інформації є суттєвим фактором будь-якої передачі даних. На сьогодні це одна з найважливіших складових роботи системного адміністратора. Із зростанням розміру мережевого підрозділу компанії збільшується ризик перехоплення інформації, тому що потрібно забезпечити відповідну безпеку каналів підприємства.

Таким чином, створення віртуальних приватних комп'ютерних мереж, використання технології шифрування інформації є важливими технічними завданнями для забезпечення безпеки та конфіденційності даних.

.

1 МЕТА ТА ЗАВДАННЯ ВИКОРИСТАННЯ VPN МЕРЕЖ

1.1 Основні завдання застосування VPN технології

В останні часи термін VPN став поширеним у обговореннях про захист даних в мережі, що вкрай важливо. Хоча раніше технологія VPN була новітнім винаходом у високих технологіях, сьогодні вона стала обов'язковим інструментом для будь-якої організації або користувача, який бажає зберегти конфіденційність своїх даних серед інших користувачів. По суті, технологія VPN забезпечує захист даних у мережі, що є критичним у сучасному цифровому середовищі.

Рисунок 1.1 – Структура віртуальних приватних мереж VPN

Віртуальна приватна мережа (VPN) – це набір технологій, що забезпечує безпечне та зашифроване з'єднання через ненадійну мережу, таку як Інтернет. VPN використовує протоколи тунелювання для зашифрування даних під час передачі та їхнього розшифрування на приймальному кінці. Щоб забезпечити додатковий рівень безпеки, вихідні та приймаючі мережеві адреси також можуть бути зашифровані.

Завдяки технології VPN всі дії користувача в Інтернеті можуть бути шифровані. Всі дані, які користувач надсилає та отримує, захищені. Якщо користувач використовує VPN для доступу до мережі, зловмиснику буде важко

визначити, з якої адреси підключенося користувач, оскільки він бачитиме лише один з багатьох VPN-маршрутизаторів.

VPN широко використовуються для надання віддаленому корпоративному персоналу, співробітникам великих компаній та мандрівникам-бізнесменам доступу до ресурсів, що розміщені в їхніх внутрішніх мережах. Для отримання доступу до обмежених ресурсів через VPN, користувачі повинні мати права на використання VPN-клієнта та проходити аутентифікацію за допомогою одного чи декількох факторів, таких як пароль, токен безпеки або біометричні дані.

У сучасний час використання віддаленого доступу за допомогою VPN між віддаленими ресурсами набуває все більшої популярності. Це стає важливим питанням не лише для підрозділів автоматизації на підприємствах, але і для будь-якої компанії загалом. У зв'язку з цим, наявність VPN-сервера у комп'ютерних мережах стає необхідністю, що дозволяє користувачам отримувати доступ до всіх ресурсів приватної захищеної мережі через публічні мережі. Крім того, VPN-сервер може використовуватися для підвищення безпеки передачі даних у внутрішній мережі, зменшуючи ризик витоку або крадіжки інформації, що транспортується через Інтернет.

За роки з моменту впровадження технології, спостерігається зростання популярності використання VPN серед приватних користувачів. У сучасному бізнесі, незалежно від його масштабів, VPN стає необхідним інструментом для забезпечення безпеки та захисту конфіденційної інформації в процесі комунікацій та передачі даних.

Віртуальна приватна мережа використовується для розширення приватної мережі через публічну інфраструктуру, таку як Інтернет. Вона дозволяє користувачам з різних місцезнаходжень з'єднуватися з локальною мережею захищеним тунелюванням. Це особливо важливо для підприємств з розгалуженою інфраструктурою, оскільки більші розділи можуть збільшувати ризики безпеки. Забезпечення безпеки каналів зв'язку стає пріоритетом в таких умовах, запобігаючи можливість несанкціонованого доступу до конфіденційної інформації.

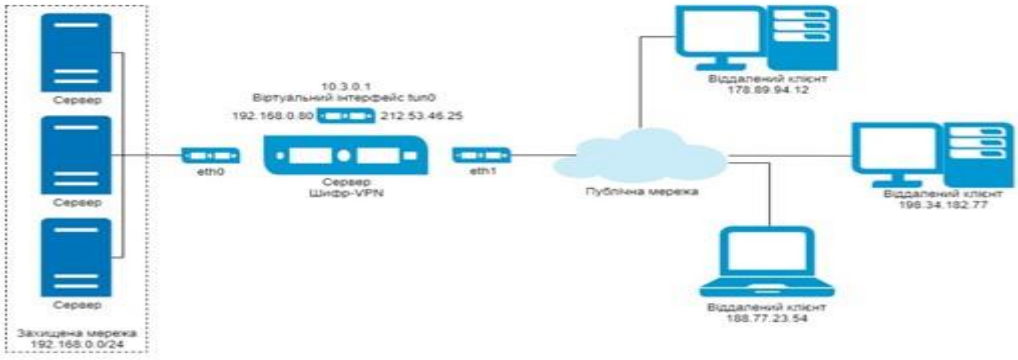

Рисунок 1.2 – Структурна схема мережі VPN організацій

У кожної компанії виникає потреба у безпечній передачі даних між своїми відділеннями, а також у захисті цих даних. Створення власних каналів доступу не завжди доступно з фінансової точки зору. Тут на допомогу приходить технологія VPN, яка дозволяє об'єднати всі підрозділи та офіси, забезпечуючи високий рівень безпеки та гнучкість мережі. VPN побудовані на основі публічної мережі, такої як Інтернет. Хоча Інтернет має свої недоліки, в тому числі і можливість порушення безпеки та конфіденційності, VPN забезпечують захист трафіку через Інтернет та передачу даних всередині локальної мережі. Використання віртуальних мереж дозволяє значно заощадити кошти порівняно з власними глобальними мережами.

Одним з головних завдань використання технології VPN є захист конфіденційної корпоративної інформації, яка передається через відкриті мережі. Відкриті канали можуть бути захищені лише за допомогою криптографічних методів. Виділені лінії, незважаючи на свою велику пропускну спроможність, не мають значних переваг у забезпеченні безпеки. Існує ризик, що вони можуть бути пошкоджені або підключені несанкціоновано в неконтрольованих зонах. Принцип роботи VPN не суперечить основним мережевим протоколам і технологіям. Зокрема, при установці з'єднання для віддаленого доступу клієнт використовує стандартний протокол PPP. У разі використання віртуальних виділених ліній між локальними мережами, їх роутери також обмінюються пакетами PPP. Однак новаторським моментом є пересилка даних через безпечний, зашифрований тунель, який організований в межах загальнодоступної мережі.

Тунелювання в мережевій технології дозволяє передавати пакети даних одного протоколу через іншу мережу, використовуючи інший протокол. Це дозволяє вирішувати проблеми взаємодії різнотипних мереж, забезпечуючи цілісність і конфіденційність даних та примирюючи різні протоколи або схеми адресації.

Для впровадження VPN в корпоративну мережу існують різні підходи, включаючи програмне забезпечення. Створення віртуальної приватної мережі можна порівняти з прокладанням кабелю через глобальну мережу.

Один із найпоширеніших методів тунелювання VPN – це інкапсуляція мережевого протоколу IP в PPP і подальша інкапсуляція у протокол тунелювання. Цей підхід відомий як тунелювання другого рівня через використання протоколу на цьому рівні.

Тунелювання – це технологія, що дозволяє передавати дані одного протоколу через інший протокол в логічному середовищі. Це відкриває можливість вирішувати проблеми взаємодії різнотипних мереж, забезпечуючи безпеку і конфіденційність передачі даних, а також узгодження зовнішніх протоколів і схем адресації.

Мережева інфраструктура корпорації може бути легко підготовлена до використання VPN за допомогою різних програмних рішень. У плані аналогії, організація віртуальної приватної мережі подібна до прокладання кабелю через глобальну мережу.

Серед найбільш поширених методів створення VPN є інкапсуляція мережевого протоколу IP в PPP і подальша інкапсуляція у протокол тунелювання. Цей підхід відомий як тунелювання другого рівня, оскільки він використовує протокол на другому рівні мережевої моделі OSI.

Основні характеристики корпоративних мереж, такі як їх глобальність та масштабованість, створюють серйозні виклики для забезпечення їхньої безпеки та надійності. Протоколи сімейства TCP/IP, хоч і широко використовувані, були розроблені у часи, коли проблеми безпеки мереж не стояли настільки гостро, як сьогодні. Це призвело до того, що вони переважно спроектовані для забезпечення

функціональності та легкості налаштування, а не для максимального рівня захисту.

У сучасному світі Інтернету з'явилося безліч інструментів і методів для несанкціонованого доступу та крадіжки даних в корпоративних мережах. З ростом кількості підключених до Інтернету пристроїв і збільшенням кількості компаній, які використовують Інтернет для своєї діяльності, збільшується і кількість інцидентів, пов'язаних із порушенням безпеки даних.

На сьогоднішній день існує широкий спектр загроз різного походження, які можуть становити різний рівень загрози для інформації в корпоративних мережах.

Загрози походження можуть бути наслідком зловмисних дій осіб, які мають різні мотивації і використовують різні методи для здійснення широкого спектру загроз. Розрізняються два типи загроз: об'єктивні, пов'язані з недостатністю елементів системи, та суб'єктивні, що виникають внаслідок дій розвідувальних служб іноземних держав, промислового шпигунства, кримінальних елементів та недобросовісних працівників системи.

Джерелами загроз можуть бути зловмисники, технічні об'єкти, програми та алгоритми, технологічні схеми обробки даних і зовнішнє середовище.

Основні причини витоку інформації включають:

– порушення персоналом норм, вимог та правил експлуатації систем безпеки інформації;

– помилки в проектуванні системи захисту;

– проведення зловмисною стороною технічної розвідки.

Недотримання персоналом норм та вимог експлуатації може бути як навмисним, так і не навмисним. Від розвідки зловмисною стороною цей випадок відрізняється тим, що в даному разі особисті мотиви рухають особа, яка здійснює несанкціоновані дії. Причини витоку інформації тісно пов'язані з видами такого витоку, як розголошення, несанкціонований доступ та отримання захищеної інформації розвідувальними службами.

Розголошення інформації визначається як неправомірна передача захищених даних споживачам, які не мають права на доступ до цих даних.

Несанкціонований доступ означає отримання захищеної інформації зацікавленим суб'єктом з порушенням встановлених правовими документами або власником інформації прав або правил доступу до захищених даних. Цим зацікавленим суб'єктом може бути держава, юридична особа, група фізичних осіб (включаючи громадські організації) або окрема особа, наприклад, хакер.

Отримання захищеної інформації розвідками може здійснюватися за допомогою технічних засобів (технічна розвідка) або шляхом агентурних операцій (агентурна розвідка).

Канал витоку інформації – це сукупність джерел, матеріальних носіїв або середовищ, які поширюють вказану інформацію сигналом, а також засобів виділення інформації з сигналу або носія. Однією з основних характеристик каналу є місцезнаходження засобів виділення інформації з сигналу або носія, які можуть бути розташовані як у межах контрольованої зони, охоплюючи систему, так і поза нею.

Інформацію, яка потребує захисту, необхідно передавати з пункту А до пункту Б таким чином, щоб зловмисники не могли отримати до неї доступ. Це досить реальна ситуація, яка часто виникає на практиці, особливо в останні часи. Пункти А і Б можуть бути окремими вузлами або цілими сегментами мережі.

При передачі інформації між мережами в якості захисту може використовуватися виділений канал зв'язку, який належить компанії, інформація якої потребує захисту. Однак підтримка таких каналів зв'язку є дуже витратним заходом.

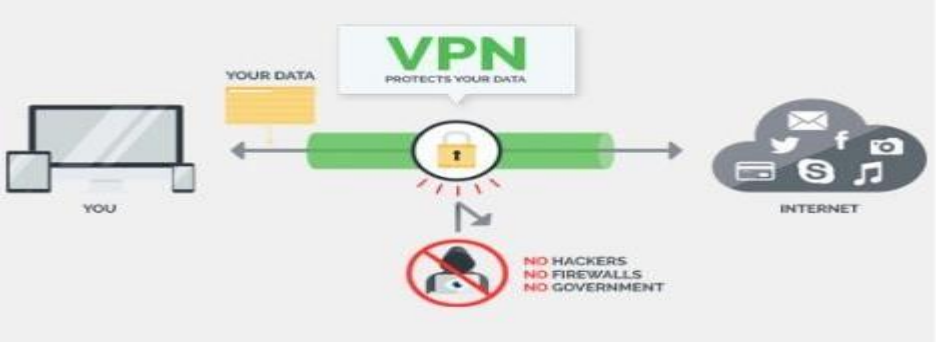

Рисунок 1.3 – Графічне зображення концепції безпечного VPN-каналу

Забезпечити конфіденційність передачі даних можна ефективно та економічно, використовуючи звичайні канали зв'язку, такі як Інтернет. Проте необхідно забезпечити віддаленість або прихованість від потоку трафіку інших компаній, що циркулює в мережі. Потреба у конфіденційній передачі даних може виникати як у глобальних мережах, так і в локальних, де потрібно відділити один тип трафіку від іншого, наприклад, білінговий трафік від трафіку інформаційно-технологічної системи.

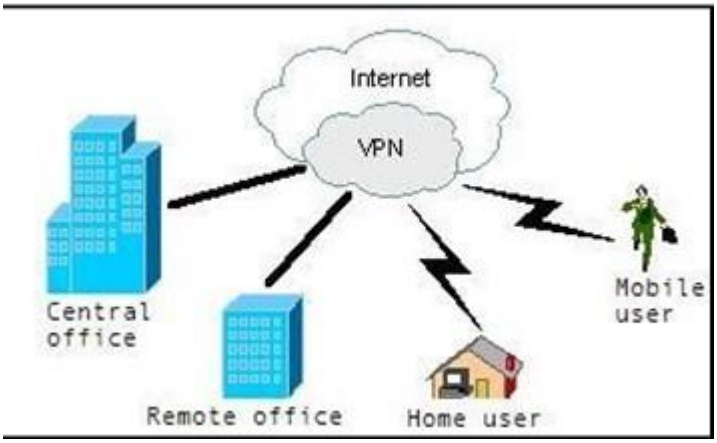

Рисунок 1.4 – Складові структури організаційної мережі

Одна з ключових особливостей технології VPN полягає у можливості забезпечення віддаленого доступу через Інтернет, що є економічно вигідним і ефективним рішенням. Для налагодження віддаленого доступу до приватної мережі за допомогою VPN потрібні лише доступ до Інтернету, реальна IP-адреса та відповідне програмне забезпечення. Це дозволяє будь-якому користувачеві з будь-якого куточка світу отримати доступ до захищеної мережі за умови знання відповідних авторизаційних даних.

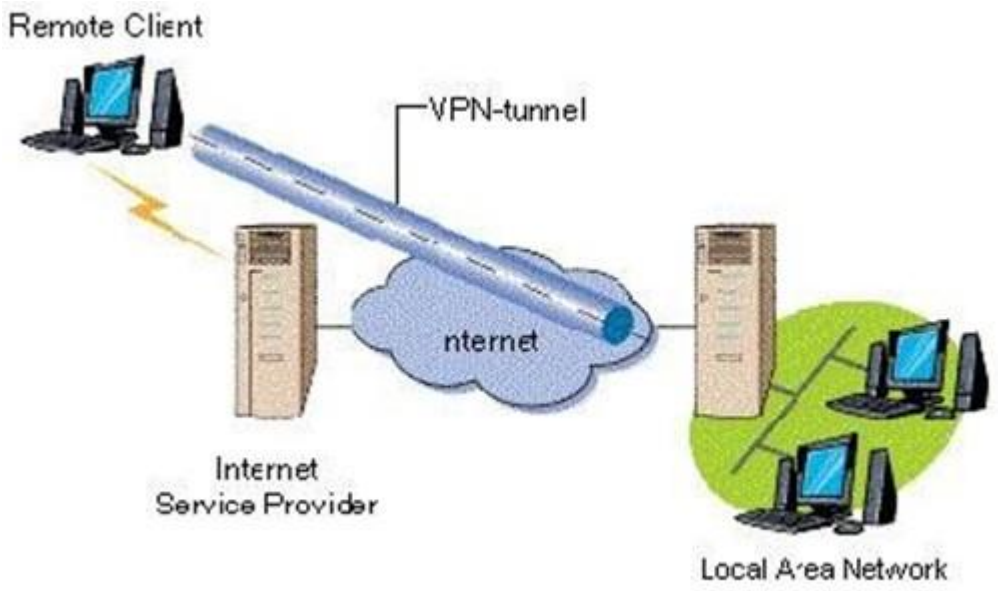

Рисунок 1.5 – Підключення користувача з віддаленої локації до корпоративної локальної мережі

Якщо потрібно забезпечити конфіденційність переміщення інформації в розподілених мережах і забезпечити захист від зловмисників, то використання VPN є відмінним вибором. Одна з основних переваг VPN полягає у забезпеченні захищеності всієї мережі шляхом простого застосування без необхідності великої кількості IP-адрес або зміни інфраструктури при зміні провайдера.

VPN також дозволяє легко забезпечити віддалений доступ до головних філіалів для клієнтів або забезпечити повний і безпечний доступ до локальної мережі. Замість турбування про складні IP-адреси та інфраструктуру, VPN дозволяє зосередитися лише на конфігурації маршрутизатора.

Використання VPN є відносно дешевим методом з'єднання фізично віддалених мереж, оскільки не потрібно оплачувати WAN-конектів, а весь трафік між мережами передається через Інтернет.

1.2 Ключові елементи мереж VPN

Основні принципи VPN базуються на трьох методах, які використовуються для забезпечення безпеки в мережах:

– Тунелювання, цей метод дозволяє передавати шифровані дані між двома точками таким чином, що для відправника і отримувача даних вся мережева інфраструктура, що лежить між ними, залишається невидимою.

– Аутентифікація, цей процес впізнавання дозволяє визначити, що користувач або пристрій є вповноваженим для доступу до мережі. Це забезпечує контроль над тим, хто має право використовувати мережу.

– Шифрування, даний метод забезпечує захист конфіденційності даних, що передаються через мережу, шляхом перетворення їх у незрозумілий формат за допомогою спеціального алгоритму шифрування. Таким чином, навіть якщо зловмисник отримає доступ до даних, він не зможе їх розшифрувати без відповідного ключа.

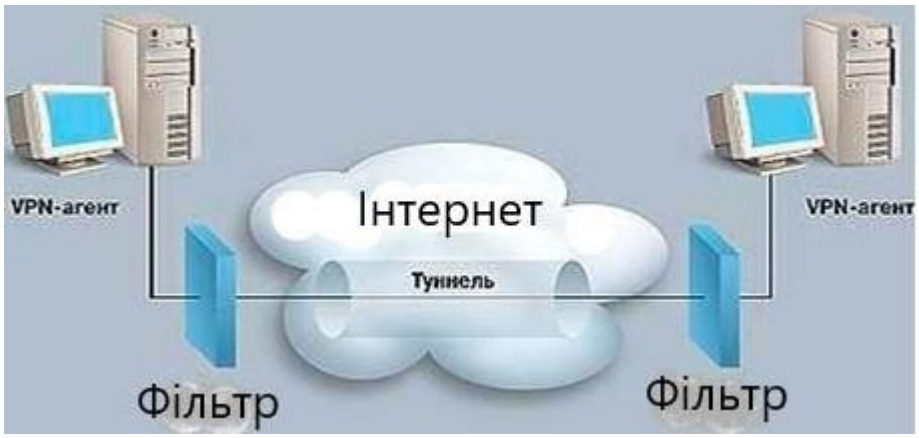

Рисунок 1.6 – Впровадження VPN з використанням методу тунелювання

Тунельне транспортне середовище використовується для перехоплення та передачі даних між двома мережевими вузлами, забезпечуючи їхнє безпечне з'єднання через відкритий Інтернет. Цей метод дозволяє з'єднати вузли таким чином, що вони здаються підключеними до однієї локальної мережі з точки зору програмного забезпечення, яке на них працює. Однак слід пам'ятати, що тунельна інфраструктура проходить через безліч проміжних маршрутизаторів глобальної мережі.

Такий підхід має свої обмеження та проблеми. Перша з них полягає в тому, що інформація, яка передається через тунель, може бути піддана перехопленню зловмисниками.

Використання тунелювання дозволяє передавати пакети даних через загальнодоступну мережу як у звичайному з'єднанні "точка-точка". Кожній парі "відправник-отримувач даних" встановлюється свій тунель - безпечне логічне з'єднання, яке дозволяє інкапсулювати дані одного протоколу в пакети іншого. Основні компоненти тунелю включають в себе відправника (ініціатора з'єднання), маршрутизатор мережі, тунельний комутатор і один або кілька тунельних термінаторів.

Однак, якщо передавана інформація є конфіденційною (наприклад, номери банківських карток, фінансові звіти, особисті дані), існує реальна загроза її компрометації, що може мати серйозні наслідки. Зловмисники можуть модифікувати передані через тунель дані так, що одержувач не зможе перевірити їх достовірність.

Однак ці проблеми можуть бути вирішені за допомогою сучасних засобів криптографічного захисту інформації. Наприклад, метод електронного цифрового підпису (ЕЦП) дозволяє запобігти внесенню несанкціонованих змін в пакет з даними на шляху його проходження через тунель. Захист переданих даних від несанкціонованого перегляду забезпечується за допомогою сильних алгоритмів шифрування.

1.2.1 Аутентифікація

Однією з основних функцій VPN є забезпечення безпеки. У VPN всі дані від комп'ютерів-клієнтів передаються через Інтернет до VPN-сервера. Цей сервер може розташовуватися на великій відстані від клієнтського комп'ютера, і дані, що прямують до мережі організації, проходять через обладнання багатьох провайдерів. Однак, як можна переконатися, що дані не були перехоплені або змінені під час передачі? Для цього використовуються різноманітні методи

аутентифікації і шифрування, які забезпечують конфіденційність та цілісність переданих даних.

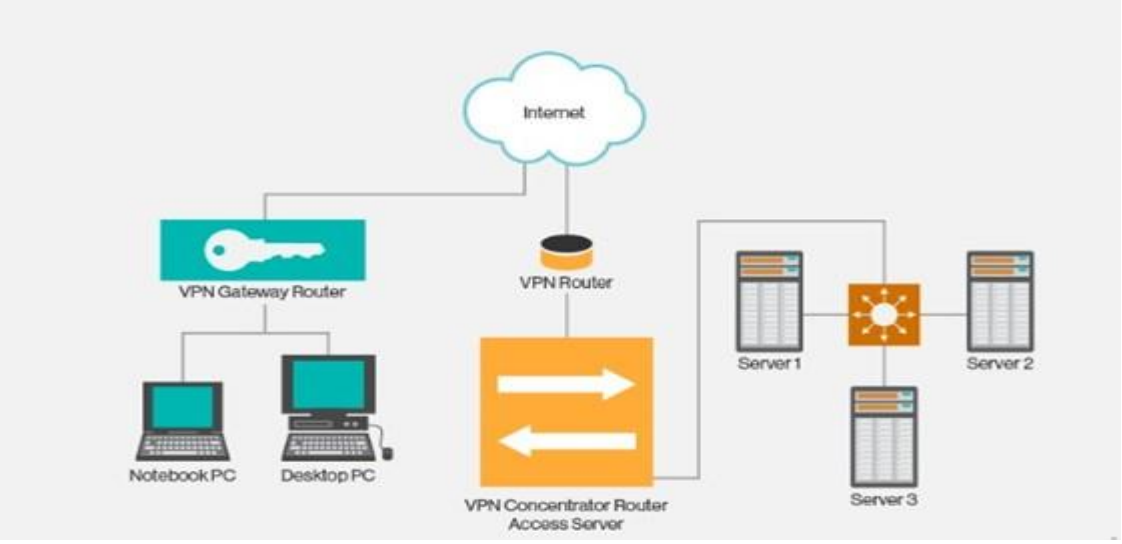

Рисунок 1.7 – Забезпечення аутентифікація користувачів у VPN мережах

Для аутентифікації користувачів в протоколі PPTP можна використовувати різні методи, такі як EAP (Extensible Authentication Protocol), MSCHAP (Microsoft Challenge Handshake Authentication Protocol) версії 1 і 2, CHAP (Challenge Handshake Authentication Protocol), SPAP (Shiva Password Authentication Protocol) та PAP (Password Authentication Protocol). Протоколи MSCHAP версії 2 і Transport Layer Security (EAP-TLS) вважаються найбільш надійними, оскільки вони забезпечують взаємну аутентифікацію, дозволяючи VPN-серверу і клієнту ідентифікувати один одного.

Незважаючи на те, що PPTP забезпечує певний рівень безпеки, L2TP поверх IPSec вважається надійнішим. L2TP поверх IPSec дозволяє аутентифікацію на рівнях «користувач» і «комп'ютер», а також забезпечує аутентифікацію і шифрування всіх даних.

Аутентифікація може здійснюватися шляхом передачі паролю у відкритому вигляді або за допомогою схеми запит-відгук. У цій схемі клієнт надсилає пароль серверу, і сервер порівнює його зі своєю базою даних для підтвердження доступу. Відкрита аутентифікація в наш час практично не використовується.

Метод запит-відгук є більш поширеним в аутентифікації користувачів. У загальному вигляді цей процес включає наступні кроки:

– клієнт надсилає запит на аутентифікацію серверу;

– сервер надсилає відповідь клієнту (виклик);

– клієнт хешує свій пароль, шифрує відповідь і передає її серверу.

Такий же процес виконується сервером, який порівнює результат з відповіддю клієнта.

Якщо зашифрований запит співпадає, аутентифікація вважається успішною.

При аутентифікації користувачів і серверів у VPN мережах, протокол L2TP поверх IPSec використовує локальні сертифікати, які отримані від служби сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють захищений коннект ESP SA (security association). Після завершення процесу аутентифікації комп'ютера L2TP (поверх IPSec) виконує аутентифікацію на рівні користувача. Для цього можна використовувати будь-який протокол, включаючи PAP, який передає ім'я користувача та пароль у незашифрованому вигляді. При цьому аутентифікація вважається безпечною, оскільки L2TP поверх IPSec шифрує всю сесію. Однак, застосування протоколу MSCHAP для аутентифікації користувача, який використовує різні ключі шифрування для аутентифікації комп'ютера і користувача, може збільшити рівень захисту.

1.2.2 Шифрування

Шифрування забезпечує високий рівень захисту, що ускладнює отримання доступу до пакетів під час їх пересилання через Інтернет.

Рисунок 1.8 – Подання захищеного каналу VPN в мережах

Наразі існують два методи шифрування, які підтримуються:

1. Протокол шифрування MPPE або Microsoft Point-to-Point Encryption, який сумісний лише з MSCHAP.

2. EAP-TLS автоматично вибирає довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером.

MPPE працює з ключами різної довжини – 32, 40, 56, 64, 72, 128 або 256 біт. Операційні системи Windows підтримують шифрування лише з ключами довжиною 32 або 40 біт, тому в середовищі Windows рекомендується вибирати довжину ключа, яка підтримується усіма пристроями.

Протокол MPPE був розроблений для зв'язку точка-точка, де пакети передаються послідовно і втрата пакетів неможлива. Однак при побудові віртуальних мереж через загальнодоступні мережі ці умови не виконуються, оскільки пакети даних часто надходять до одержувача не в тій послідовності, в якій були відправлені. Тому PPTP використовує порядкові номери пакетів для зміни ключа шифрування. Це дозволяє виконувати дешифрування незалежно від порядку прийнятих пакетів.

Обидва протоколи реалізовані як у Microsoft Windows, так і в інших операційних системах, таких як Linux. Однак алгоритми роботи VPN можуть істотно відрізнятися залежно від конкретної реалізації.

З'єднання за допомогою тунелювання, аутентифікації та шифрування дозволяє передавати дані між двома точками через загальнодоступну мережу, емулюючи роботу приватної (локальної) мережі. Іншими словами, ці засоби дозволяють побудувати віртуальну приватну мережу.

Додатковим приємним ефектом VPN-з'єднання є можливість (і навіть необхідність) використання системи адресації, прийнятої в локальній мережі. На практиці, реалізація віртуальної приватної мережі виглядає так: у локальній обчислювальній мережі офісу фірми встановлюється сервер VPN. Віддалений користувач (або маршрутизатор, якщо здійснюється з'єднання двох офісів) ініціює процедуру з'єднання з сервером за допомогою клієнтського програмного забезпечення VPN. Після аутентифікації користувача настає друга фаза -

узгодження деталей забезпечення безпеки з'єднання між клієнтом і сервером. Після цього організується VPN-з'єднання, яке забезпечує обмін інформацією між клієнтом і сервером, забезпечуючи шифрування, дешифрування та перевірку цілісності кожного пакета даних.

Однією з головних проблем мереж VPN є відсутність загальноприйнятих стандартів для аутентифікації та обміну шифрованими даними. Ці стандарти все ще перебувають у процесі розробки, тому продукти різних виробників не завжди можуть встановлювати VPN-з'єднання та автоматично обмінюватися ключами. Ця проблема ускладнює поширення VPN, оскільки важко змусити різні компанії використовувати продукцію одного виробника. Як наслідок, утворення мереж партнерів, так званих extranet-мереж, стає складним завданням.

У цьому розділі розглянуто загальні аспекти технології VPN для організації підключення до мережі передачі даних, побудови розподільної мережі та забезпечення віддаленого доступу до мережі. Схеми віддаленого доступу можуть варіюватися за типом підтримуваних служб для віддалених клієнтів, таких як доступ до файлів, баз даних, або принтерів, аналогічно до роботи у локальній мережі. Цей режим відомий як режим віддаленого вузла. Іноді віддалений доступ може включати обмін повідомленнями електронної пошти з центральною мережею, щоб автоматично отримувати корпоративні дані, наприклад, з бази даних.

Серед різноманітних форм віддаленого доступу до комп'ютера особливе місце займає метод, за якого користувач може працювати з комп'ютером віддалено так, ніби він управляє ним безпосередньо через локальний термінал. У цьому режимі він може запускати програми на віддаленому комп'ютері та отримувати результати в реальному часі. Цей тип доступу зазвичай розділяють на термінальний доступ і віддалене управління.

2 РІЗНОВИДИ VPN ТА ЇХ ОСОБЛИВОСТІ

2.1 Види VPN та їх опис

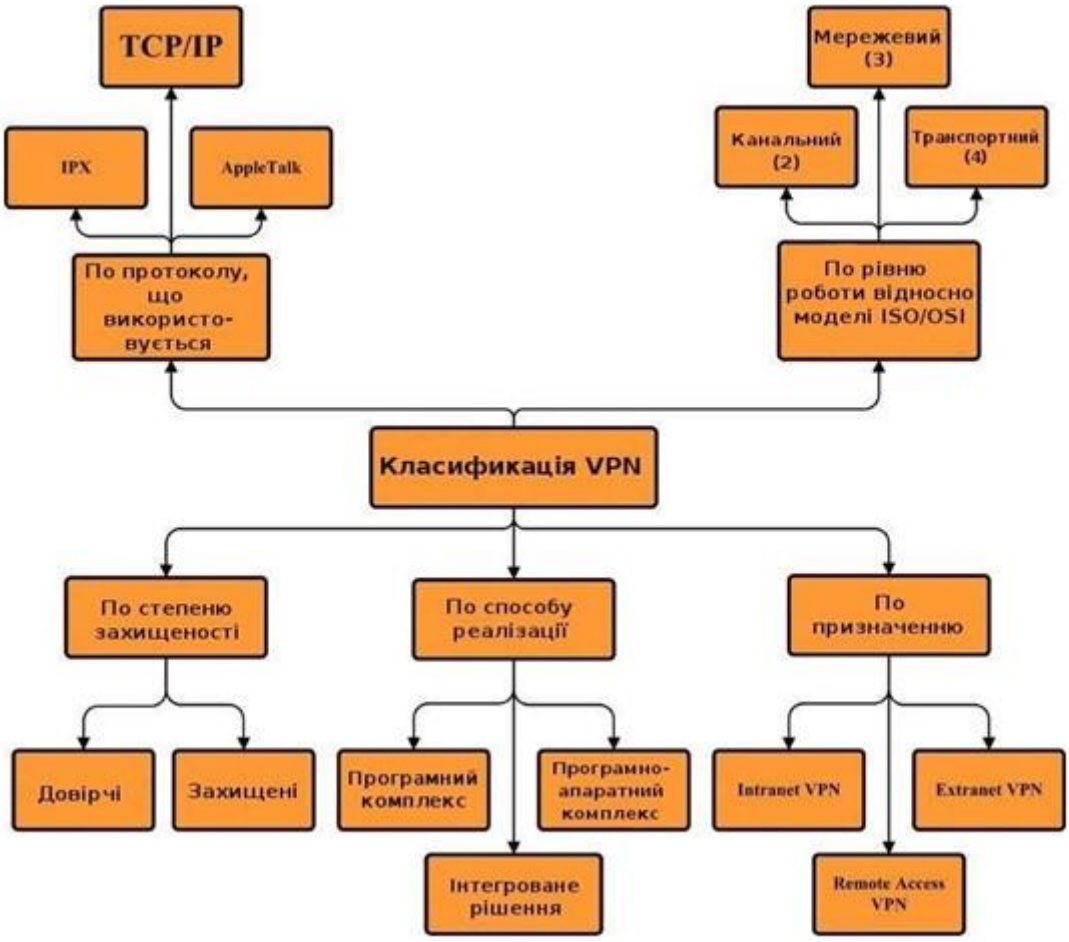

Рисунок 2.1 – Класифікація VPN

Класифікація VPN та їх основні параметри:

1. За рівнем захисту даних:

– VPN з шифруванням на рівні даних (Data Link Layer VPN);

– VPN з шифруванням на рівні мережі (Network Layer VPN);

– VPN з шифруванням на рівні застосунків (Application Layer VPN).

2. За методом реалізації:

– клієнт-серверні VPN;

– ьережеві VPN;

– тунельні VPN.

3. За призначенням:

– віддалений доступ до корпоративних ресурсів;

– забезпечення безпеки публічних мереж;

– з'єднання між офісами компанії.

4. За використовуваним протоколом:

– PPTP (Point-to-Point Tunneling Protocol);

– L2TP (Layer 2 Tunneling Protocol);

– IPSec (Internet Protocol Security).

– SSL/TLS (Secure Socket Layer/Transport Layer Security).

5. За рівнем роботи відносно стеку протоколів OSI:

– VPN на рівні мережевого протоколу (Network Layer VPN);

– VPN на рівні транспортного або прикладного протоколу (Transport/Application Layer VPN).

Існують дві основні категорії VPN мереж:

– Захищені VPN мережі – це найпоширеніший тип приватних мереж, який дозволяє створити надійну підмережу на базі ненадійної інфраструктури, такої як Інтернет. Приклади таких захищених VPN включають IPSec, OpenVPN та PPTP.

– Довірчі VPN мережі, цей тип використовується тоді, коли існуюче передавальне середовище можна вважати довірчим, і головна мета - створити віртуальну підмережу в рамках більшої мережі. У таких ситуаціях проблеми безпеки можуть не виникати. Приклади таких VPN включають MPLS і L2TP, які можуть використовуватися з іншими протоколами, такими як IPSec.

Щодо реалізації VPN мереж, вони можуть бути реалізовані наступними способами:

– Спеціалізоване програмно-апаратне забезпечення. Використання спеціальних комплексів програмно-апаратних засобів для реалізації VPN мереж. Цей підхід забезпечує високу продуктивність і високий рівень захисту даних.

– Програмне забезпечення для ПК. Використання спеціального програмного забезпечення на персональних комп'ютерах для створення VPN з'єднань.

– Інтегровані рішення VPN. Використання комплексних систем, які включають в себе функції VPN, а також фільтрацію мережевого трафіку, організацію мережевих екранів і забезпечення якості обслуговування.

За призначенням VPN можна класифікувати наступним чином:

– Intranet VPN. Використовуються для об'єднання різних розподілених філій або підрозділів в єдину захищену мережу організації. Ці мережі дозволяють обмінюватися даними між філіями через відкриті канали зв'язку, забезпечуючи високий рівень захисту і конфіденційності.

– Remote Access VPN. Використовуються для створення захищеного каналу між корпоративною мережею (наприклад, центральним офісом або філією) і окремим користувачем, який підключається до корпоративних ресурсів з домашнього комп'ютера або під час відрядження за допомогою ноутбука. Ці VPN дозволяють користувачам отримувати доступ до корпоративних ресурсів з будь-якого місця, де є Інтернет-з'єднання.

– Extranet VPN. Використовуються для з'єднання зовнішніх користувачів, таких як замовники або клієнти, з мережею підприємства. З урахуванням нижчого рівня довіри до цих користувачів порівняно зі співробітниками компанії, забезпечується високий рівень безпеки, обмежуючи доступ до особливо цінної та конфіденційної інформації.

Розробники програмного забезпечення все більше віддають перевагу використанню протоколу TCP/IP для побудови віртуальних приватних мереж (VPN). На сьогоднішній день більшість VPN-рішень підтримує протокол TCP/IP, оскільки він є широко поширеним і надійним.

По рівню роботи відносно стека протоколів OSI.

Мережі VPN зазвичай будуються на рівні канального, мережевого та транспортного рівнів стека протоколів OSI.

На канальному рівні використовуються протоколи тунелювання даних, такі як L2TP (Layer 2 Tunneling Protocol) і PPTP (Point-to-Point Tunneling Protocol). Ці

протоколи забезпечують авторизацію і аутентифікацію користувачів, а також шифрування даних.

Очікується, що в найближчому майбутньому буде зростання використання протоколу тунелювання другого рівня (L2TP), оскільки він дозволяє побудувати надійні та безпечні віртуальні приватні мережі.

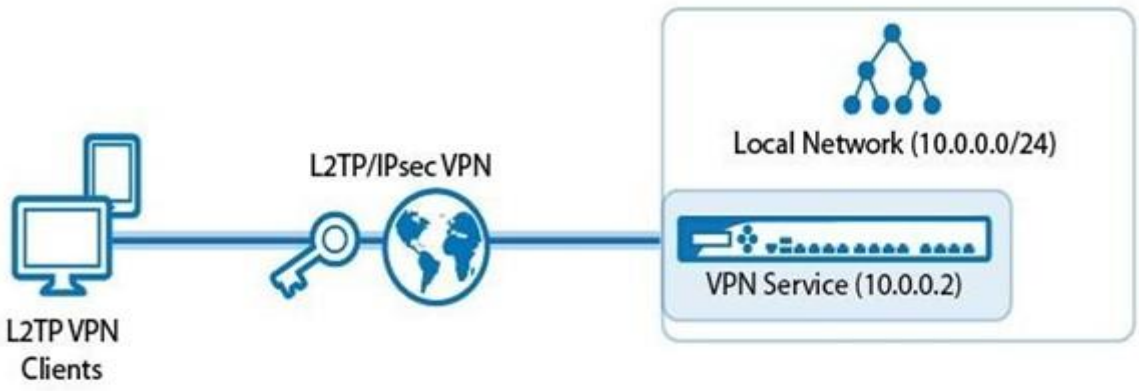

Рисунок 2.2 – Канальний рівень

L2TP виник внаслідок поєднання можливостей протоколів PPTP і L2F (Layer 2 Forwarding). PPTP дозволяє передавати пакети PPP через тунель, а L2F - пакети SLIP і PPP. L2TP вбирає в себе найкращі характеристики обох цих протоколів, надаючи можливість створювати тунелі не лише в IP-мережах, а й у мережах, таких як ATM, X.25 і Frame Relay.

У L2TP в якості транспортного протоколу використовується UDP, а формат повідомлень однаковий як для управління тунелем, так і для передачі даних. В реалізації Microsoft L2TP використовує пакети UDP для контролю тунелю, що містять зашифровані пакети PPP. Надійність доставки гарантується за допомогою контролю послідовності пакетів.

Існують суттєві відмінності між функціональними можливостями протоколів PPTP і L2TP. L2TP може бути використаний не лише в IP-мережах, але і в інших середовищах. Службові повідомлення для створення тунелю і передачі даних використовують однаковий формат та протоколи. Навпаки, PPTP

застосовується лише в IP-мережах, і для його роботи необхідне окреме TCP-з'єднання.

L2TP поверх IPSec надає більшу безпеку, ніж PPTP, і може забезпечити майже 100% захисту важливих даних організації. Особливості L2TP роблять його дуже перспективним протоколом для побудови віртуальних мереж.

Протокол тунелювання другого рівня (L2TP) – це протокол тунелювання на основі RFC, який є галузевим стандартом і вперше підтримується в клієнтських та серверних операційних системах. У відміну від PPTP, L2TP не використовує Encryption-Point-to-Point-Encryption (MPPE) для шифрування дейтаграм протоколу «точка-точка» (PPP), але покладається на безпеку протоколу шифрування IPSec. Комбінація L2TP та IPSec відома як L2TP/IPSec, яка надає послуги шифрування та інкапсуляції приватних даних в рамках віртуальної приватної мережі (VPN).

L2TP використовує два види пакетів: керуючі та інформаційні. Керуючі пакети використовуються для встановлення та підтримки тунелів, тоді як інформаційні повідомлення використовуються для інкапсуляції PPP-кадрів, які передаються через тунель. Керуючі повідомлення забезпечують надійний контроль доставки, щоб гарантувати надійність передачі. В разі втрати інформаційні повідомлення не будуть повторно відправлені.

Таблиця 2.1 – Структура протоколу

PPP кадри	
L2TP інформаційні повідомлення	L2TP управляючі повідомлення
L2TP інформаційний канал (ненадійний)	L2TP канал управління (надійний)
Транспортування пакетів (UDP, FR, ATM тощо)	

Таблиця 2.2 – Формат заголовка

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16						31
T	L	x	x	S	x	O	P	x	x	x	x	Версія				Довжина(опц)						
ID тунелю																ID сесії						
Ns (опц)																Nr (опц)						
Offset Size (опц)																Offset Pad (опц).....						
Payload data																						

Характеристики заголовка L2TP визначаються різними бітами та полями:

– біт типу (T) вказує на тип пакета: 0 для інформаційних повідомлень і 1 для керуючих;

– бт довжини (L) показує наявність поля довжини: 1 для керуючих повідомлень;

– зарезервовані біти (x) призначені для майбутніх застосувань;

– біт послідовності (S) вказує на присутність полів Ns і Nr;

– біт зсуву (O) показує, чи присутнє поле величини зміщення;

– біт пріоритету (P) вказує на пріоритет повідомлення в черзі: 0 для керуючих і 1 для інформаційних;

– поле Ver вказує версію заголовка L2TP;

– значення 1 використовується для виявлення пакетів L2F серед потоку L2TP-пакетів. Пакети з невідомим значенням поля Ver відкидаються;

– опціональне поле Довжина вказує загальну довжину повідомлення в октетах;

– ID-тунелю визначає ідентифікатор керуючого з'єднання;

– ID-сесії визначає ідентифікатор для сесії даного тунелю;

– поля Ns і Nr вказують порядкові номери повідомлень інформації або керування;

– поле величина зсуву (Offset Size), якщо присутнє, визначає кількість октетів після заголовка L2TP, де починається поле даних. Вміст поля зсуву не визначено.

Процес встановлення PPP-сесії тунелювання L2TP складається з двох основних етапів:

1. Встановлення керуючого каналу для тунелю:

– Цей етап передбачає створення керуючого з'єднання між LAC (L2TP Access Concentrator) і LNS (L2TP Network Server) перед початком будь-яких сесій.

– Під час встановлення керуючого з'єднання відбувається ідентифікація партнера, визначення версії L2TP, визначення можливостей каналу та обмін кадрами.

– Важливою частиною цього процесу є безпечна аутентифікація тунелю, яка забезпечується простою, але ефективною системою схожою на CHAP.

2. Формування сесії:

– Після успішного встановлення керуючого з'єднання можуть бути сформовані індивідуальні сесії.

– Кожна сесія відповідає одному потоку PPP між LAC і LNS.

– Відмінність від встановлення керуючого з'єднання полягає в тому, що процес встановлення сесії є асиметричним щодо LAC і LNS.

– LAC запитує доступ до сесії для вхідних запитів, тоді як LNS запитує LAC запустити сесію для роботи з вихідними запитами.

Після формування тунелю, PPP-кадри, які надходять від віддаленої системи і отримані LAC, звільняються від CRC, канальних заголовків тощо, інкапсулюються в L2TP та пересилаються через відповідний тунель. LNS отримує L2TP-пакет і обробляє інкапсульований PPP-кадр так, якщо він надійшов через локальний інтерфейс PPP.

Кожне вихідне повідомлення має в собі ID сесії і тунелю, які асоційовані з певною сесією та тунелем і вказані партнером у відповідних полях заголовка.

Якщо розглядати L2TP та IPSec з точки зору VPN, обидва ці протоколи мають бути підтримані як VPN-клієнтом, так і VPN-сервером. L2TP встановлюється за допомогою протоколу TCP/IP. Залежно від налаштувань маршрутизатора та віддаленого доступу, L2TP може бути налаштований на п'ять або 128 портів L2TP.

На сьогоднішній день одним з найпоширеніших протоколів VPN є PPTP, що означає протокол тунелювання точка-точка або Point-to-Point Tunneling Protocol. PPTP, використовуючи стандарти TCP/IP, ґрунтується на застарілому протоколі PPP (Point-to-Point Protocol). Під час передачі даних PPTP створює тунель через мережу до сервера приймача, що дозволяє передавати пакети PPP віддаленого користувача через цей тунель. Сервер і робоча станція використовують віртуальну приватну мережу, незалежно від того, наскільки безпечною або доступною є глобальна мережа між ними.

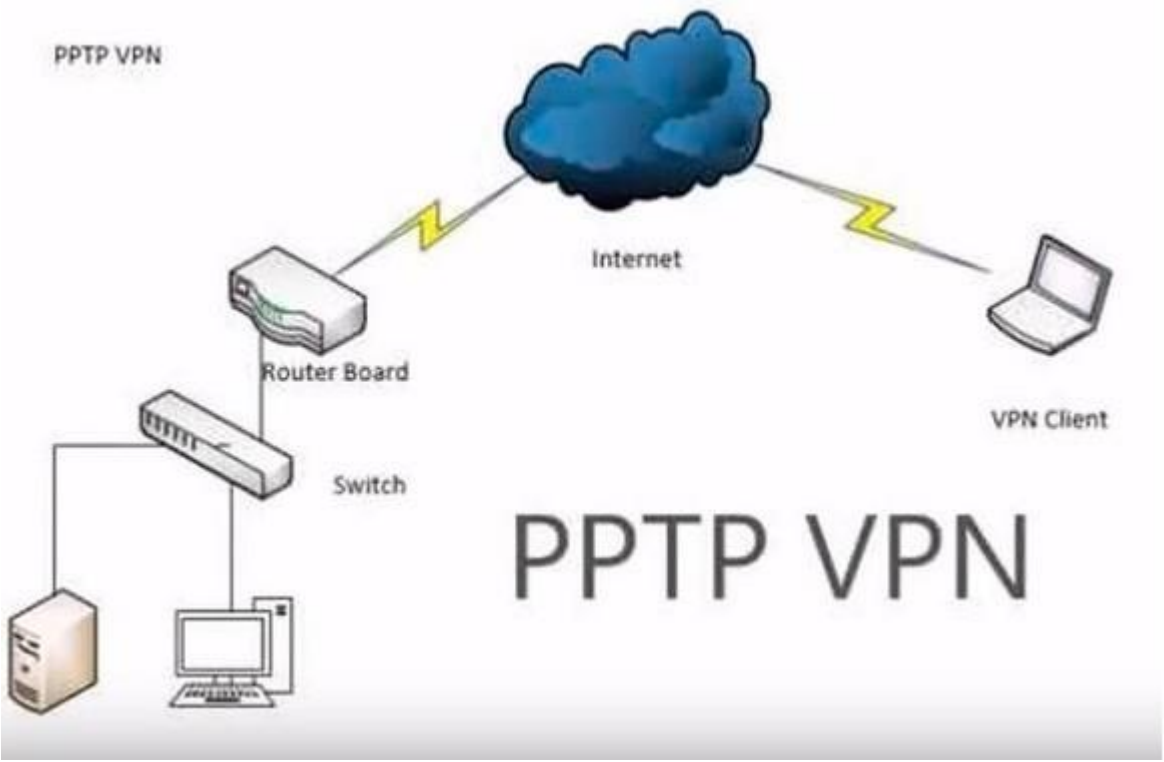

Рисунок 2.3 – Структурна організація мережі, що ґрунтується на протоколі PPTP

Навіть при обмеженні протоколу PPTP лише для пристроїв під управлінням Windows, він дозволяє компаніям безпечно взаємодіяти з існуючими мережевими структурами, не порушуючи власну систему безпеки. Це дає можливість віддаленим користувачам підключатися до Інтернету через місцевого провайдера за допомогою аналогового або каналу ISDN та встановлювати захищене з'єднання з сервером NT. Таким чином, компаніям не потрібно вкладати значні кошти у підтримку пулу модемів для віддаленого доступу. PPTP є тунельним протоколом

типу точка-точка, який дозволяє комп'ютерам створювати безпечний тунель до сервера в стандартній мережі, що не має захисту.

Рисунок 2.4 – Структурна пакета PPTP

PPTP використовується для інкапсуляції IP-пакетів для їх передачі через IP-мережу. Клієнти PPTP встановлюють керуюче тунельне з'єднання, використовуючи порт призначення на транспортному рівні OSI. Після налагодження тунелю між комп'ютером-клієнтом і сервером відбувається обмін службовими пакетами. Крім керуючого з'єднання PPTP, яке забезпечує функціональність каналу, створюється ще одне з'єднання для передачі даних через тунель.

Інкапсуляція даних перед їх відправленням через тунель відбувається у два етапи:

1. Отримані дані інкапсулюються протоколами верхніх рівнів під час першого проходу.

2. Далі дані досягають транспортного рівня. Однак, їх не можна відправити безпосередньо, оскільки це відповідальність канального рівня OSI. Тому PPTP шифрує корисне навантаження пакета і виконує функції другого рівня, які зазвичай належать PPP. Це включає додавання до PPTP-пакету заголовка та закінчення PPP.

Після інкапсуляції кадра PPP у пакет Generic Routing Encapsulation (GRE), який належить мережевому рівню, PPTP продовжує процес інкапсуляції, передавши цей пакет через IP-мережу. GRE дозволяє інкапсулювати різні мережеві протоколи, такі як IPX, AppleTalk, DECnet, щоб вони могли бути передані по IP-мережі. Однак, хоча GRE не здатний створювати сесії або

забезпечувати захист даних від зловмисників, PPTP забезпечує можливість керувати тунельними з'єднаннями для цих цілей.

Після інкапсуляції у кадр з IP-заголовком, що містить адреси відправника і одержувача пакету, PPTP додає PPP заголовок і закінчення. На додаток, структура даних для пересилання по тунелю PPTP показана на діаграмі у додатку 3.

Коли дані надсилаються через тунель, система-одержувач видаляє всі службові заголовки, залишаючи тільки дані PPP.

MPLS VPN – це набір методів, які використовують мультипротокольну комутацію міток (MPLS) для створення віртуальних приватних мереж (VPN). Використання MPLS VPN дозволяє гнучко транспортувати та маршрутизувати різноманітний мережевий трафік через мережу MPLS. В мережах MPLS VPN зараз розгорнуто три типи VPN-мереж:

– точка-точка (псевдопровід);

– рівень 2 (VPLS);

– рівень 3 (VPRN).

MPLS працює на рівні, що знаходиться між канальним і третім мережевим рівнями моделі OSI, тому його часто називають протоколом канально-мережевого рівня. В точкових MPLS VPN використовуються віртуальні орендовані лінії (VLL), щоб забезпечити з'єднання Layer2 «точка-точка» між двома сайтами. Кадри Ethernet, TDM та ATM можуть бути інкапсульовані в межах цих VLL.

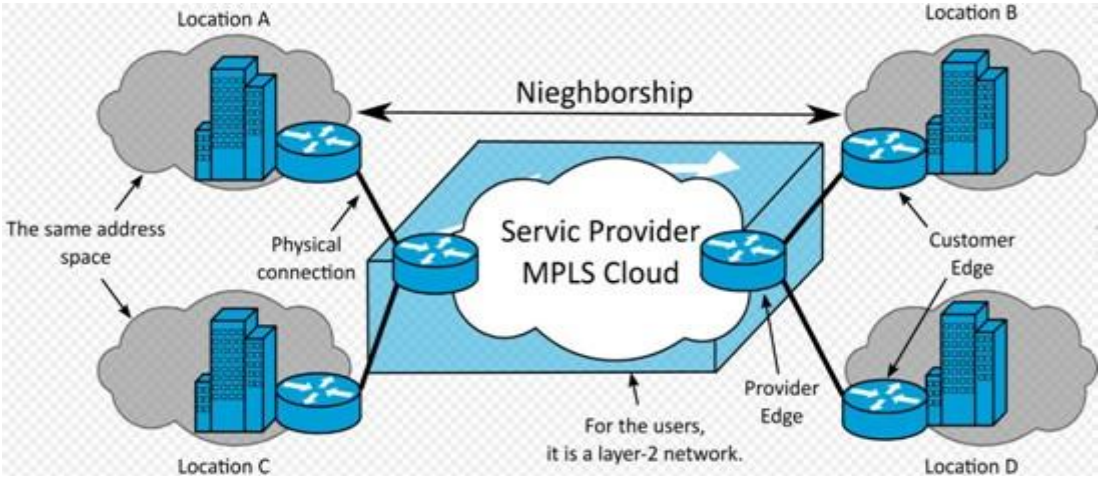

Рисунок 2.5 – Структурна організація мережі MPLS

MPLS VPN операційна в двох зонах: у мережі IP-клієнтів та внутрішній (магістральній) інфраструктурі MPLS провайдера, яка служить для інтеграції мереж клієнтів.

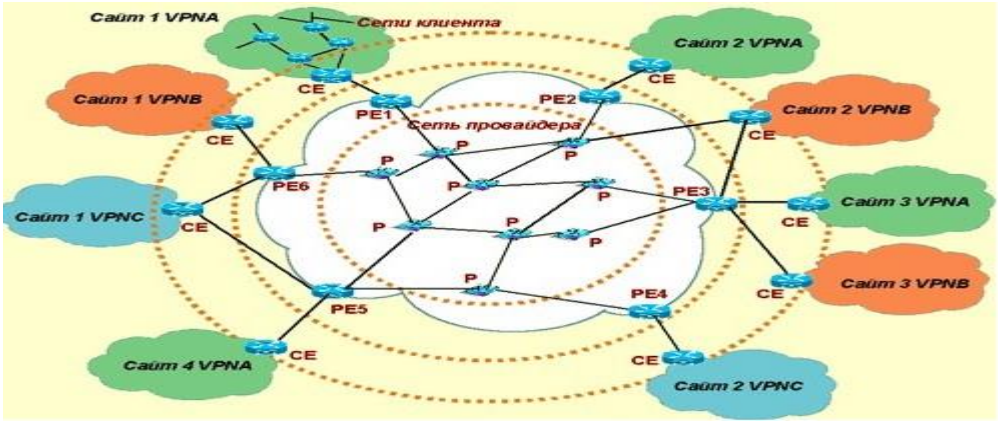

Рисунок 2.6 – Елементи системи MPLS VPN

Зазвичай, у корпоративних мережах, де кожен клієнт може мати кілька мережевих IP-адрес, і кожен з них може включати декілька підмереж зі своїми маршрутами, такі частини мережі часто називаються "сайтами". Сайти, що належать одному клієнту, обмінюються IP-пакетами, що дозволяє створити віртуальну приватну мережу для цього клієнта.

Наприклад, у корпоративній мережі з центральним офісом і віддаленими філіями може бути кілька сайтів. Для забезпечення обміну маршрутною інформацією між цими сайтами зазвичай використовується внутрішній протокол маршрутизації (Internal Gateway Protocol, IGP), такий як RIP, OSPF або IS-IS, який працює в межах автономної системи.

2.2 Мережевий рівень протоколу

На рівні мережі використовується протокол IPSec для забезпечення шифрування та конфіденційності даних, а також аутентифікації абонентів. Використання протоколу IPSec дозволяє здійснити повнофункціональний доступ, еквівалентний фізичному підключенню до корпоративної мережі. Для налаштування віртуальної приватної мережі (VPN) кожен учасник повинен

налаштувати певні параметри IPSec, тобто кожен клієнт повинен мати програмне забезпечення, що реалізує IPSec.

IPsec розроблений з метою забезпечення сумісного та високоякісного криптографічного захисту для IPv4 та IPv6. Він надає ряд служб безпеки, включаючи контроль доступу, цілісність даних, аутентифікацію джерела даних, захист від повторних атак, шифрування та обмежену конфіденційність потоку трафіку. Ці послуги забезпечуються на рівні IP, що дозволяє захистити протоколи IP та/або верхній рівень мережевого стеку.

Для досягнення цих цілей використовуються два протоколи безпеки руху: заголовок автентифікації (AH) та корисне навантаження інкапсуляції безпеки (ESP), а також криптографічний ключ для процедур управління протоколами. Вибір протоколів IPsec та їх конфігурація зазвичай залежить від вимог до безпеки та системних вимог користувачів, додатків та/або сайтів будь-якої організації.

Правильно впроваджені та налаштовані ці механізми не мають негативного впливу на користувачів, хости та інші компоненти мережі Інтернет, які не використовують ці механізми безпеки для захисту свого трафіку. Крім того, ці механізми розроблені таким чином, що їх можна використовувати незалежно від вибору алгоритму. Ця модульність дозволяє вибирати різні комбінації алгоритмів, не впливаючи на інші аспекти реалізації. Наприклад, різні спільноти користувачів можуть обирати різні набори алгоритмів шифрування даних в залежності від потреби.

Стандартний набір алгоритмів за замовчуванням спрямований на полегшення сумісності в глобальному Інтернеті. Використання цих алгоритмів разом з протоколами захисту трафіку IPsec та протоколами управління ключами дозволяє розробникам систем та додатків ефективно впроваджувати високоякісні технології криптографічної безпеки.

Компанії не бажають передавати фінансову або іншу конфіденційну інформацію відкритими каналами передачі даних. VPN-канали захищені потужними алгоритмами шифрування, які вбудовані в стандарти протоколу безпеки IPsec. IPSec, або Internet Protocol Security, як стандарт, був обраний

міжнародним співтовариством, зокрема групою IETF - Internet Engineering Task Force, для створення основ безпеки для Інтернет-протоколу (IP). Протокол IPSec забезпечує захист на мережевому рівні і вимагає підтримки стандарту IPSec тільки від пристроїв, що спілкуються між собою по обидві сторони з'єднання. Інші пристрої, розташовані між ними, просто маршрутизують IP-пакети.

Рисунок 2.7 – Архітектура IPSec

Програмні заходи безпеки, такі як Internet Protocol Security (IPsec) і Internet Security Association and Key Management Protocol (ISAKMP), використовуються для створення захищених з'єднань у віртуальних приватних мережах (VPN). Ці заходи гарантують безпечні зв'язки між віддаленими користувачами та корпоративною інфраструктурою. Кожне забезпечене з'єднання, яке використовується для передачі даних, відоме як "тунель". Продукт ASA використовує стандарти тунелювання ISAKMP та IPsec для керування цими тунелями. Основні функції ISAKMP та IPsec включають:

– параметри тунелювання;

– встановлення туннелю;

– аутентифікацію користувачів і даних;

– управління безпековими ключами;

– шифрування та дешифрування даних;

– управління передачею даних через туннель;

– керування потоком даних на вхід та вихід як кінцева точка тунелю або маршрутизатора.

IPsec використовується для створення VPN-з'єднань між віддаленими користувачами та локальною мережею, а також для забезпечення безпеки з'єднань між клієнтами та локальною мережею. У термінології IPsec, клієнт на одному рівні розглядається як віддалений клієнт або інший безпечний шлюз.

При виборі рівня реалізації захищеного каналу виникає декілька аргументів. З одного боку, вибір верхнього рівня незалежний від видів транспортування (вибір мережевого та канального протоколу), а з іншого - для кожного рівня потрібні окремі налаштування та конфігурація. Вибір нижчих рівнів має плюс у їх універсальності та огляді для запропонованого, але мінус у залежності від конкретного протоколу (наприклад, PPP або Ethernet). IPsec є компромісним рівнем: він розміщений на мережевому рівні, використовуючи IP як найвищий розширений протокол цього рівня. Це робить IPsec більш гнучким, оскільки він може захищати будь-які протоколи, що базуються на TCP та UDP. У той же час він є прозорим для більшої кількості пропозицій.

При налаштуванні тунелю IPsec відбувається узгодження асоціації безпеки, яка відповідає за автентифікацію, шифрування, інкапсуляцію та управління ключами. Цей процес розділяється на дві фази: перша - встановлення тунелю (IKE SA), і друга - керування трафіком всередині тунелю (IPsec SA). VPN, що з'єднує локальні мережі між різними географічними місцями, використовує підключення IPsec LAN-LAN.

Тунелі IPsec між точками представляють собою набори налаштувань, які встановлюються для кожного з'єднання. SA (Security Associations) визначають протоколи та алгоритми для захисту конфіденційних даних, а також вказують ключі, що використовуються між відповідними точками. IPsec SA відповідають за контроль над фактичною передачею трафіку користувача.

Між точками узгоджуються налаштування, які використовуються для кожного SA. Кожна SA складається з наступного:

– набори перетворень IKEv1 або IKEv2;

– криптографічні параметри;

– ACL (списки керування доступом);

– тунельні групи;

– політика передфрагментації.

Створення безпечного каналу зв'язку може мати різні варіанти реалізації на різних рівнях OSI.

IPsec представляє собою набір стандартів Інтернету та є специфікацією, що працює на рівні IP-протоколу. Основу IPsec складають три ключові протоколи:

– Протокол аутентифікації заголовка (AH), який гарантує цілісність передачі даних, аутентифікацію відправника та можливість виявлення повторних пакетів.

– Протокол захисту корисного навантаження (ESP), який забезпечує конфіденційність (шифрування) передаваної інформації, а також може виконувати функції AH, забезпечуючи аутентифікацію та захист від повторної передачі пакетів. При використанні ESP слід вказати набір безпекових сервісів, які включають в себе опціональні функції.

– Протокол управління ключами та безпекою Інтернету (ISAKMP) - це протокол, який використовується для встановлення з'єднання, взаємної аутентифікації та обміну ключами. ISAKMP включає в себе різні механізми обміну ключами, включаючи стандартні протоколи, такі як Internet Key Exchange, Kerberized Internet Negotiation of Keys або DNS записи типу IPSECKEY.

Заголовок аутентифікації (AH) є важливою складовою безпеки мережі, що може бути додатковою опцією пакету IP. AH зазвичай вставляється між основним заголовком IP та самими даними пакету. Його наявність не впливає на передачу інформації на транспортному та вищих рівнях мережевої стеки. Основне призначення AH полягає у захисті від атак, спрямованих на недозволену зміну

змісту пакета, включаючи підміну IP-адреси вихідного рівня. Протоколи вищих рівнів можуть бути адаптовані для перевірки автентичності отриманих даних.

Формат AH досить простий, включаючи 96-бітовий заголовок і довільну кількість даних, організованих у 32-бітові слова. Назви полів чітко відображають їхню призначеність: Next Header вказує на наступний заголовок, Payload Len визначає довжину пакета, SPI вказує на контекст безпеки, а поле Sequence Number містить послідовний номер пакета.

IPsec має два режими функціонування: транспортний і тунельний, кожен з яких використовується відповідно до вимог конкретної ситуації мережі.

Рисунок 2.8 – Структура заголовка аутентифікації AH

При використанні інкапсуляції зашифрованих даних, заголовок ESP з'являється як останній опціональний заголовок в пакеті. Оскільки головною метою ESP є забезпечення конфіденційності даних, різні типи інформації можуть потребувати застосування різних алгоритмів шифрування. Тому формат ESP може змінюватися в залежності від використовуваних криптографічних алгоритмів.

Проте, обов'язковими полями ESP є SPI, що вказує на контекст безпеки, і поле Sequence Number, яке містить послідовний номер пакета. Поле "ESP Authentication Data" (контрольна сума) не є обов'язковим у заголовку ESP.

Отримувач пакету ESP розшифровує ESP заголовок і використовує параметри та дані використаного алгоритму шифрування для декодування інформації на транспортному рівні.

У транспортному режимі шифруються (або підписуються) лише дані IP-пакета, зберігаючи вихідний заголовок. Цей режим зазвичай використовується для з'єднання між хостами і може також використовуватися для захисту тунелів між шлюзами, які були організовані за іншими протоколами (наприклад, L2TP).

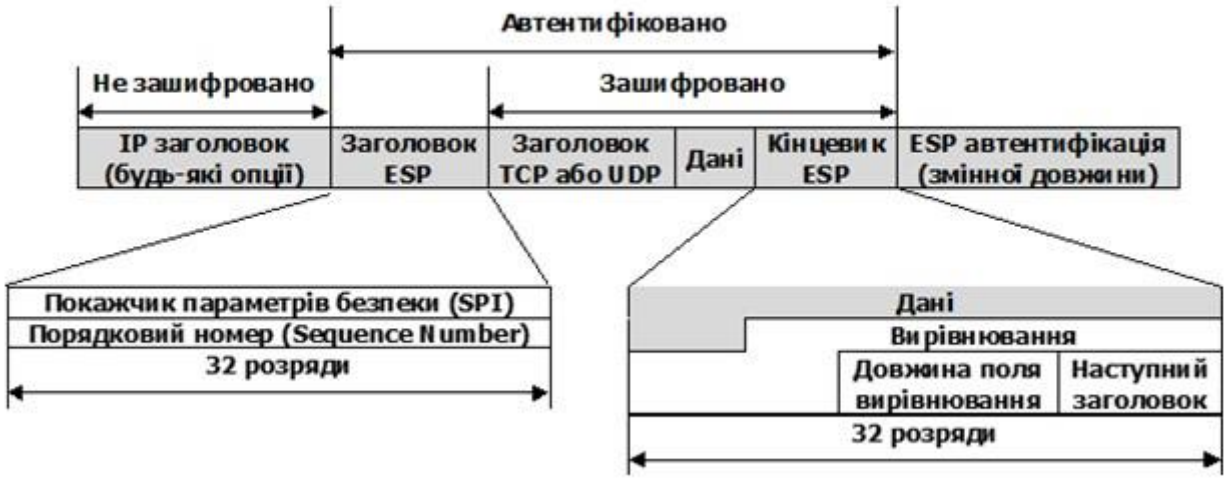

Рисунок 2.8 – Структура заголовка ESP

У тунельному режимі весь вихідний IP-пакет, включаючи дані, заголовок та маршрутну інформацію, шифрується і потім вставляється в поле даних нового пакета, що представляє собою інкапсуляцію. Такий режим дозволяє підключати віддалені комп'ютери до віртуальних приватних мереж або забезпечує безпечну передачу даних через відкриті канали зв'язку, такі як Інтернет, між шлюзами для об'єднання різних частин віртуальної приватної мережі.

Режими IPsec не виключають один одного. На одному вузлі деякі безпекові асоціації можуть використовувати транспортний режим, тоді як інші можуть використовувати тунельний режим.

Рисунок 2.10 – Організація та функціонування засобів захисту в рамках IPSec

Транспортний режим IPSec застосовується для зашифрування тільки поля даних IP-пакету, яке містить протоколи транспортного рівня, такі як TCP, UDP, а також ICMP, які в свою чергу містять інформацію про різноманітні прикладні служби. Прикладом використання транспортного режиму є передача електронної пошти. Усі проміжні вузли на шляху пакету від відправника до одержувача використовують лише відкриту інформацію мережевого рівня та, можливо, деякі опціональні заголовки пакету (у IPv6).

Недоліком транспортного режиму є відсутність механізмів приховування конкретних відправника та одержувача пакету, а також можливість проведення аналізу трафіку. Результатом такого аналізу може стати отримання інформації про обсяги та напрямки передачі інформації, області інтересів абонентів та навіть розташування керівників.

Тунельний режим IPSec використовується для шифрування всього IP-пакету, включаючи його заголовок мережевого рівня. Цей режим застосовується в ситуаціях, коли необхідно приховати обмін інформацією організації зі зовнішнім світом. У такому випадку адресні поля заголовка мережевого рівня пакету, який використовує тунельний режим, заповнюються за допомогою фаєрвола організації і не містять інформації про конкретного відправника пакета. При

передачі інформації зі зовнішнього світу в локальну мережу організації в якості адреси призначення використовується мережева адреса брандмауера. Після розшифрування фаєрволом початкового заголовка мережевого рівня пакет направляється до його одержувача.

Security Association (SA) представляє собою з'єднання, яке забезпечує безпеку трафіку, який передається через нього. Обидва комп'ютери на кожній стороні SA зберігають режим, протокол, алгоритми та ключі, що використовуються в SA. Кожен SA використовується лише в одному напрямку, тому для двостороннього зв'язку потрібно два SA. Кожен SA реалізує один режим і протокол; таким чином, якщо для одного пакету необхідно використовувати два протоколи (наприклад, AH і ESP), то потрібно два SA.

База даних політики безпеки (SPD) зберігає політику безпеки, яка визначає, які дії слід виконати для кожного пакету даних. Ці дії можуть включати відкидання пакета, не обробку пакета з використанням IPSec або обробку пакета за допомогою IPSec. У випадку останнього в SPD також вказується, який Security Association (SA) слід використовувати (якщо відповідний SA вже був створений) або з якими параметрами потрібно створити новий SA.

Протокол обміну ключами Internet Key Exchange (IKE) є стандартним протоколом для управління ключами в IPSec. Він виконує встановлення як Security Association (SA) для ISAKMP, так і для IPSec. IKE забезпечує початкову аутентифікацію сторін та обмін загальними секретними ключами. Крім того, IKE підтримує різноманітні примітивні функції, включаючи хеш-функції та псевдовипадкові функції (PRF).

IKE є основним протоколом, який об'єднує всі компоненти IPSec в єдину систему. Він забезпечує надійну початкову аутентифікацію сторін та обмін загальними секретними ключами. Існує можливість ручного встановлення ключів для сесій, але цей підхід рідко використовується і не рекомендується. Зазвичай IKE працює через порт 500 UDP.

Існує дві версії протоколу обміну ключами для IPSec: оригінальний IKE та більш новий IKEv2. Ці протоколи мають свої відмінності в специфікаціях та

функціонуванні. Наприклад, IKEv2 встановлює параметри з'єднання за одну фазу, яка складається з декількох кроків. У той час як процес роботи оригінального IKE можна розбити на дві фази.

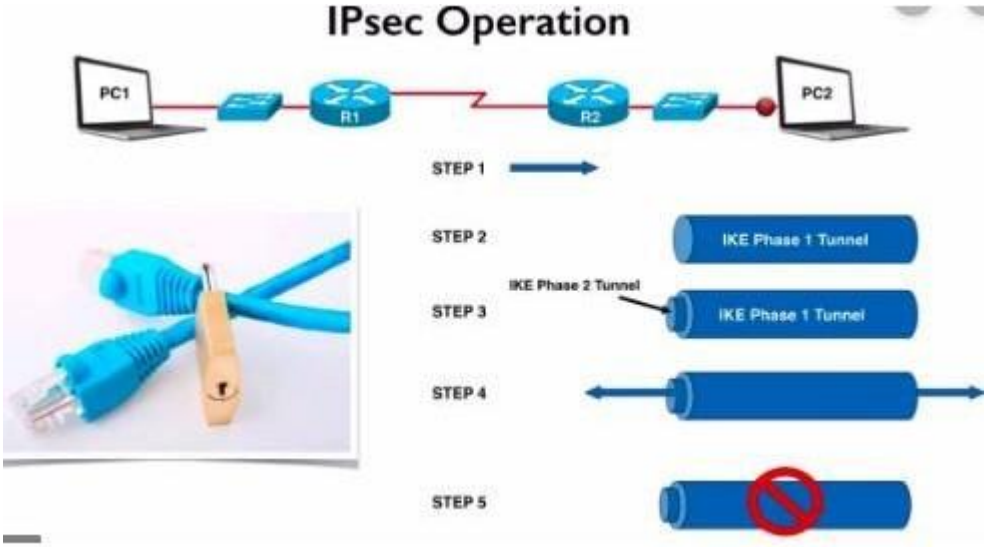

Рисунок 2.11 – Перша фаза протоколу обміну ключами Internet Key Exchange (IKE)

У першій фазі IKE встановлюється безпечний канал між двома вузлами, який відомий як асоціація безпеки IKE (IKE SA). Ця фаза може пройти у двох режимах:

1. Основний режим:

– Включає три двосторонні обміни між відправником і отримувачем.

– Під час першого обміну визначаються алгоритми та хеш-функції для захисту IKE з'єднання шляхом узгодження IKE SA кожного вузла.

– Вузли також взаємно перевіряють свою ідентифікацію, відправляючи та підтверджуючи послідовність псевдовипадкових чисел.

– Зашифровані IP-адреси використовуються для перевірки ідентичності протилежного боку.

– В результаті основного режиму створюється безпечний канал для подальшого обміну ISAKMP, який визначає порядок дій для аутентифікації з'єднання вузлів, створення та управління Security Association (SA), генерації

ключів та запобігання загроз, таких як DoS-атаки або атаки повторного відтворення.

Агресивний режим" встановлення IKE спрощує процес і вимагає менше обміну повідомленнями, що призводить до зменшення кількості переданих пакетів. Перше повідомлення містить практично всю необхідну інформацію для встановлення IKE SA, включаючи відкритий ключ Діффі-Хеллмана, що використовується для синхронізації пакетів, ідентифікатор пакета, який підтверджується іншим учасником. Одержувач у відповідь надсилає все необхідне для завершення обміну. Першому вузлу потрібно лише підтвердити з'єднання.

З точки зору безпеки агресивний режим менш надійний, оскільки учасники починають обмінюватися інформацією до встановлення безпечного каналу, що може призвести до несанкціонованого перехоплення даних. Проте, цей режим працює швидше, ніж основний. Згідно зі стандартом IKE, будь-яка реалізація повинна підтримувати основний режим, а підтримка агресивного режиму вважається вкрай бажаною.

Друга фаза.

У фазі два IKE використовує лише швидкий режим, який відбувається після успішного встановлення безпечного каналу під час першої фази. Швидкий режим призначений для узгодження загальної політики IPsec, отримання загальних секретних ключів для алгоритмів протоколів IPsec (AH або ESP) і встановлення IPsec SA.

Використання послідовних номерів гарантує захист від атак повторного відтворення. Швидкий режим також використовується для перегляду поточних IPsec SA і вибору нових, коли час життя SA закінчується. Зазвичай швидкий режим оновлює загальні секретні ключі, використовуючи алгоритм Діффі-Хеллмана з першої фази.

У використанні псеводслучайних функцій наразі замість спеціальних PRF застосовується хеш-функція в конструкції HMAC (HMAC - механізм аутентифікації повідомлень за допомогою хеш-функцій). Для обчислення HMAC потрібна криптографічна хеш-функція (означимо її як H) і секретний ключ K.

Довжина ключа K може бути менше або рівна довжині блоків у байтах, які використовуються для хешування.

SPD є дуже гнучким механізмом управління, який дозволяє ефективно керувати обробкою кожного пакету. Пакети класифікуються за різними полями, і SPD може перевіряти одне або кілька полів для визначення відповідних дій. Це може призвести до того, що весь трафік між двома вузлами буде передаватися за допомогою одного SA, або окремі SA будуть використовуватися для кожного додатка, або навіть для кожного TCP з'єднання.

Протокол ISAKMP встановлює загальну структуру для протоколів, які використовуються для встановлення Security Association (SA) і здійснення інших операцій з керування ключами. ISAKMP підтримує різні Області Інтерпретації (DOI), одна з яких є IPSec-DOI. Він не надає повного протоколу, але забезпечує "будівельні блоки" для різних DOI і протоколів обміну ключами.

Протокол Oakley визначає методи встановлення ключа, використовуючи алгоритм обміну ключами Діффі-Хеллмана. Він підтримує ідеальну пряму безпеку (Perfect Forward Secrecy - PFS), що означає, що навіть при компрометації будь-якого ключа в системі неможливо розшифрувати весь трафік.

Для розпочатку обміну даними між двома сторонами необхідно встановити безпечне з'єднання, відоме як Security Association (SA). Концепція SA є основою IPsec і визначає, як сторони використовуватимуть сервіси для забезпечення захищеного спільного використання. SA є симплексним (однонаправленим) і для взаємодії сторонам необхідно встановити два з'єднання.

Протоколи IPsec дозволяють створювати SA для передачі трафіку між всіма хостами, що взаємодіють через цей канал, або навіть для кожного TCP-з'єднання. Це дає можливість вибирати рівень деталізації захисту.

Процес встановлення з'єднання розпочинається з взаємної аутентифікації сторін, вибору параметрів (типу аутентифікації, шифрування, перевірки цільових даних) і необхідності передачі даних (AH або ESP). Потім вибираються конкретні алгоритми (наприклад, для шифрування, хешування), деякі з яких є стандартними

(наприклад, DES для шифрування, MD5 або SHA-1 для хешування), а інші можуть бути надані виробниками продуктів, які використовують IPsec.

При обробці вихідних IPSec пакетів, якщо передавальний модуль визначає, що пакет пов'язаний з Security Association (SA), що вимагає обробки ESP, то починається відповідний процес. Залежно від режиму (транспортний або тунельний), обробка вихідного IP-пакету відрізняється.

У транспортному режимі IPsec модуль використовує ESP-заголовок та ESP-кінцевик для обрамлення протоколу верхнього рівня (наприклад, TCP або UDP), залишаючи заголовок IP-пакету незмінним.

У тунельному режимі IP-пакет спочатку обрамлюється ESP-заголовком і ESP-кінцевиком (інкапсуляція), а потім зовнішнім IP-заголовком (який може відрізнятися від вихідного, наприклад, коли IPsec модуль встановлений на шлюзі).

Після обрамлення проводиться шифрування: в транспортному режимі шифрується лише протокол верхнього рівня (тобто дані після IP-заголовка вихідного пакету), у тунельному режимі - весь вихідний IP-пакет.

Передавальний модуль IPsec визначає алгоритм шифрування і секретний ключ з запису про SA. Стандарти IPsec дозволяють використання алгоритмів шифрування Triple DES, AES і Blowfish, якщо їх підтримують обидві сторони. В іншому випадку використовується DES, визначений в RFC 2405.

Щоб забезпечити правильне шифрування, розмір відкритого тексту повинен бути кратним певному числу байтів, тому перед шифруванням доповнюється шифруваний текст. Зашифровані дані поміщаються в поле Payload Data, а довжина доповнення - в поле Pad Length.

Далі обчислюється Sequence Number, а потім контрольна сума (ICV). Контрольна сума обчислюється тільки по полях ESP-пакета, враховуючи поле ICV. Перед обчисленням контрольної суми воно заповнюється нулями.

Алгоритм обчислення ICV визначається з запису про SA, пов'язаним з обробленим пакетом.

Після отримання пакета, що містить ESP-протокол, приймальний модуль IPsec шукає відповідне захищене віртуальне з'єднання (SA) в базі даних SA,

використовуючи IP-адресу одержувача, протокол безпеки (ESP) і індекс SPI. Якщо відповідного SA не знайдено, пакет відкидається.

Знайдене SA вказує, чи використовується послуга захисту від повторної передачі пакетів, тобто чи необхідно перевіряти поле Sequence Number. Якщо послуга використовується, то поле перевіряється. Для цього використовується метод ковзного вікна. Приймальний модуль IPsec формує вікно шириною W. Ліва межа вікна відповідає мінімальному послідовному номеру N коректно прийнятого пакета. Пакети з полями Sequence Number, які знаходяться між N + 1 і N + W, приймаються коректно. Якщо отриманий пакет перевищує ліву межу вікна, він відкидається.

Після цього, якщо SA підтримує послугу аутентифікації, приймальний модуль IPsec обчислює ICV за відповідними полями прийнятого пакета, використовуючи алгоритм аутентифікації, який він дізнається з запису про SA, і порівнює отриманий результат зі значенням ICV, що міститься в полі "Integrity Check Value". Якщо значення ICV співпадає з отриманим результатом, пакет вважається дійсним. У разі невідповідності пакет відкидається.

Після цього проводиться розшифрування пакету. Приймальний модуль IPsec використовує алгоритм шифрування і секретний ключ, які він дізнається з запису про SA. Перевірка контрольної суми і процедура розшифрування можуть проводитися паралельно, проте процедура перевірки контрольної суми повинна завершитися раніше, і якщо вона не пройшла, розшифрування припиняється. Це дозволяє швидше виявляти пошкоджені пакети і підвищує рівень захисту від DOS-атак.

Після розшифрування пакет передається для подальшої обробки відповідно до поля Next Header.

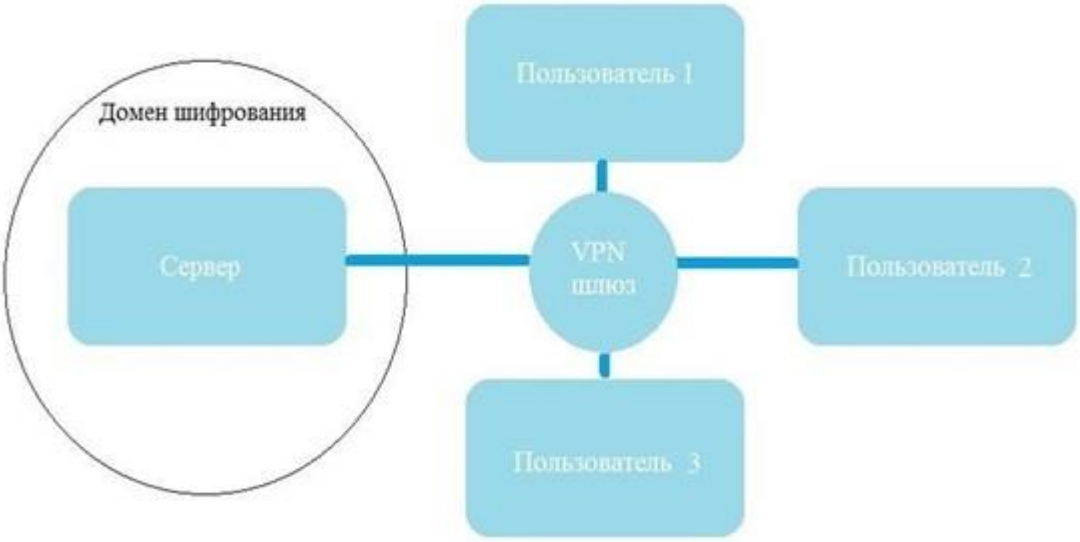

Рисунок 2.12 – Розподіл абонентів через шлюз з використанням маршрутизатора

Протокол IPsec переважно використовується для налаштування віртуальних приватних мереж (VPN), де протоколи ESP і AH працюють у режимі тунелювання. У додаток до цього, за допомогою налаштування політики безпеки, IPsec можна використовувати для забезпечення мережевого доступу. Брандмауер функціонує як контрольний пункт, який відстежує та фільтрує пройдені через нього пакети відповідно до встановлених правил. Набір правил налаштовується, і брандмауер перевіряє всі пакети, які проходять через нього. Якщо пакети відповідають цим правилам, то брандмауер обробляє їх відповідно до встановлених правил. Наприклад, він може блокувати або відкидати певні пакети, таким чином запобігаючи потенційним загрозам. Налаштувавши політику безпеки належним чином, можна, наприклад, обмежити веб-трафік, блокуючи пакети з HTTP або HTTPS протоколами. IPsec також може використовуватися для захисту серверів, де блокуються всі пакети, за винятком тих, які необхідні для коректного функціонування сервера. Наприклад, для веб-сервера можна блокувати весь трафік, за винятком з'єднань через порт 80 для протоколу TCP, або через порт 443 для протоколу TCP у випадках використання HTTPS.

За допомогою IPsec забезпечується безпечний доступ користувачів до сервера. Коли протокол ESP використовується, всі звернення до сервера і його відповіді шифруються. Проте за VPN-шлюзом, який є частиною домену шифрування, передаються відкриті повідомлення. Крім того, інші сценарії використання IPsec включають шифрування трафіку між файловим сервером і комп'ютерами в локальній мережі за допомогою IPsec у транспортному режимі, а також створення з'єднання між двома офісами за допомогою IPsec у тунельному режимі.

У сучасний час існують різні пропозиції щодо інкапсуляції одного протоколу в іншому. Деякі варіанти інкапсуляції пропонуються для транспортування IP через IP з метою реалізації політики безпеки. GRE є одним з таких протоколів, схожих на зазначені вище варіанти, проте він має більш загальний характер.

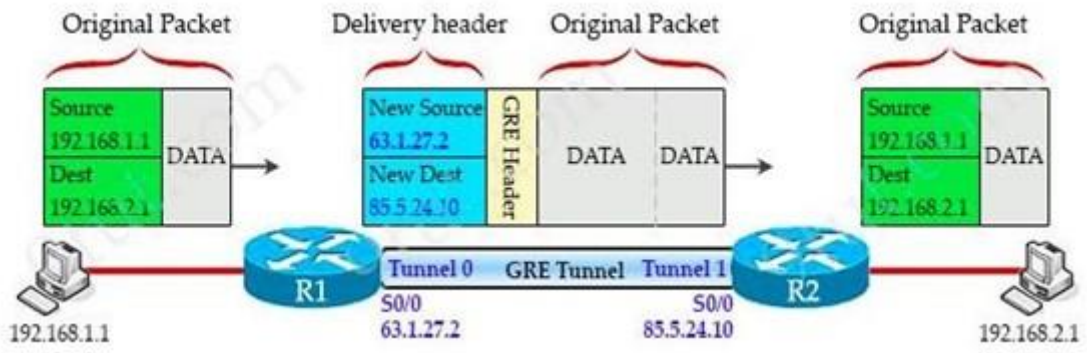

Рисунок 2.12 – Створення VPN за допомогою GRE

У різноманітних сценаріях застосування протоколу, виявляються важливі нюанси, які варто враховувати. Ця пропозиція ставить перед собою завдання бути більш універсальною, оскільки конкретні випадки інкапсуляції "X над Y" можуть бути обмежені. З метою спрощення процесу інкапсуляції протокол пропонує механізм загального призначення, що спрямований на зменшення складності інкапсуляції до більш керованого рівня.

У найбільш узагальненому випадку система опрацьовує пакет, який потрібно інкапсулювати та доставити до визначеного пункту призначення. Цей пакет називається корисним навантаженням. Спочатку корисне навантаження інкапсулюється в пакет GRE. Отриманий пакет GRE потім може бути додатково інкапсульований у інший протокол для подальшої передачі. Цей зовнішній протокол відомий як протокол доставки.

Капсульований пакет GRE має вигляд:

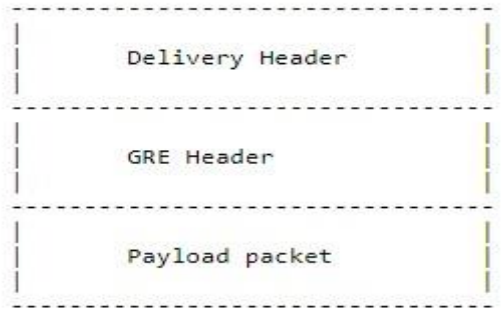

Рисунок 2.13.Вигляд GRE пакета

Заголовок пакету GRE має вигляд:

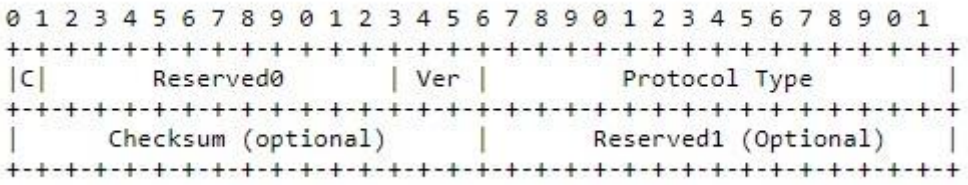

Рисунок 2.14 – Заголовок GRE пакета

2.3 Принципи організації структури мережі VPN

Існує кілька варіантів реалізації віртуальних приватних мереж (VPN), і вибір конкретного рішення повинен враховувати фактори продуктивності та обмеження доступних ресурсів для побудови VPN. Наприклад, якщо маршрутизатор вже працює на межі своїх можливостей у звичайному режимі,

додавання VPN-тунелів та застосування шифрування може призвести до перевантаження системи, що вплине на продуктивність всієї мережі. У таких випадках може бути доцільним використання спеціалізованого обладнання для побудови VPN, або врахування програмних рішень з обмеженими ресурсами.

Основними варіантами побудови VPN є:

1. Віддалений доступ (Remote Access VPN):

– Цей тип VPN дозволяє віддаленим користувачам підключатися до мережі з будь-якого місця за допомогою Інтернету.

– Зазвичай використовуються спеціальні програмні клієнти або вбудовані в операційні системи засоби для забезпечення безпеки підключення.

2. Мережа між сайтами (Site-to-Site VPN):

– Цей тип VPN з'єднує дві або більше віддалені мережі між собою, створюючи безпечне з'єднання через Інтернет.

– Використовується для з'єднання філій організації з центральним офісом або для підключення віддалених даних центрів.

2.3.1 Remote access VPN

Remote access VPN" - це тип віртуальної приватної мережі, в якому тунель створюється між програмою-клієнтом, встановленою на комп'ютері користувача (наприклад, Cisco AnyConnect), та серверним пристроєм, який обробляє підключення від різних клієнтів (наприклад, VPN-концентратор, маршрутизатор, Cisco ASA або інший пристрій, обраний організацією).

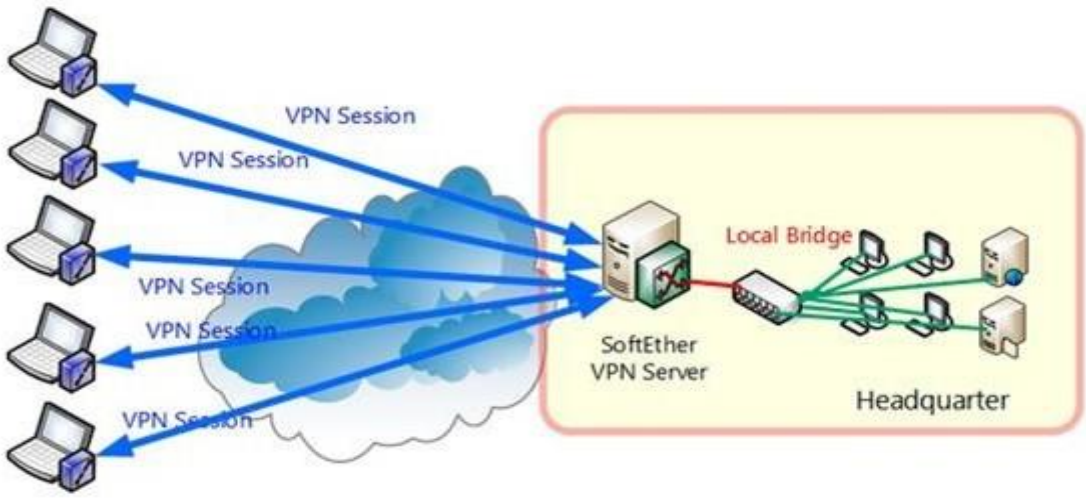

Рисунок 2.15 – Структура Remote access VPN

VPN з віддаленим доступом" – це технологія, яка спрямована на забезпечення безпеки підключення віддалених користувачів до локальної мережі компанії. Спочатку вони були розроблені для забезпечення безпечного доступу до ресурсів компанії з будь-якої точки світу для віддалених працівників. Віддалені користувачі можуть отримати доступ до захищених ресурсів у мережі компанії з будь-якого місця. Головна мета VPN з віддаленим доступом - це забезпечити безпеку даних. Для цього використовується NAS або VPN-шлюз для аутентифікації облікових даних будь-якого пристрою, який намагається підключитися до VPN.

Для віддаленого доступу до VPN зазвичай потрібне клієнтське програмне забезпечення. Це програмне забезпечення клієнта VPN спілкується з шлюзом VPN, що автентифікує користувача як віддаленого користувача та створює захищений "віртуальний" тунель між локальною мережею та шлюзом.

Після створення тунелю будь-які дані, що ви надсилаєте з цього пристрою, інкапсулюються та шифруються VPN вашого віддаленого доступу, а потім надсилаються до шлюзу VPN, який знаходиться поза межами віддаленої локальної мережі. Далі шлюз VPN розшифровує ваш трафік і пересилає дані в локальну мережу.

Не тільки весь трафік, що надсилається через віртуальний тунель, захищений, але також будь-який трафік, який користувач отримує від локальної мережі або її серверів, також проходить через цей тунель у зворотному напрямку і захищений. Шлюз VPN шифрує вхідний трафік (до користувача), який потім отримує клієнт VPN.

2.3.2 Site-to-site VPN

Мережа VPN типу "Site-to-Site" передбачає, що мережева структура складається з двох вузлів (наприклад, маршрутизаторів), які забезпечують з'єднання через тунель. У цьому сценарії користувачі розташовані за зазначеними вузлами в локальних мережах, і їм не потрібно встановлювати будь-яке спеціалізоване програмне забезпечення на своїх комп'ютерах.

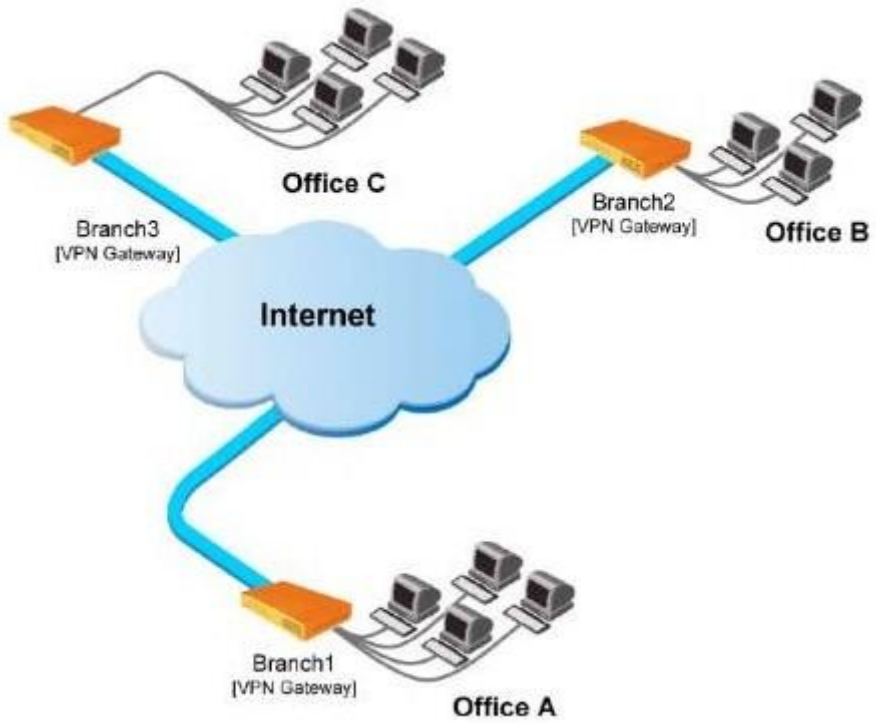

Рисунок 2.16 – Структура Site-to-site VPN

Порівняно з VPN з віддаленим доступом, VPN site-to-site забезпечують надійне з'єднання двох або більше локальних мереж, які знаходяться у різних

фізичних місцях. VPN від сайту до сайту використовують доступний Інтернет для розширення мережі вашої компанії на кілька офісів або філій.

Існують два основних типи VPN від сайту до сайту: інтранет та екстранет. Інтранет VPN ґрунтуються на внутрішній мережі компанії і використовуються для об'єднання локальних мереж кількох офісів у єдину приватну мережу, яка відома як WAN (Wide Area Network).

З іншого боку, VPN, що базуються на екстранеті, дозволяють компаніям використовувати загальнодоступний Інтернет для підключення своєї локальної мережі до мереж інших компаній, клієнтів або громад. Це дозволяє компаніям обмінюватися інформацією зі своїми партнерами, зберігаючи при цьому свою власну локальну мережу (intranet).

VPN site-to-site створює захищені тунелі між шлюзами VPN різних локальних мереж (або мережі головного офісу) для забезпечення безпечного обміну даними. Віддаленим пристроям не потрібен клієнт VPN, оскільки весь трафік автоматично пройде через шлюзи VPN.

Шлюзи VPN відповідають за автентифікацію користувачів та мереж, а також за шифрування та цілісність даних. Вони приймають зашифровані дані, розшифровують їх та передають до цільових пристроїв у мережі.

Створений тунель VPN від сайту до сайту дозволяє компаніям обмінюватися мережевими ресурсами та інформацією між головним офісом та віддаленими відділеннями. Пристрої в різних локальних мережах можуть взаємодіяти між собою так, ніби вони знаходяться в одній мережі, що сприяє ефективності та зручності управління.

Існують два ключових підходи до створення VPN від сайту до сайту: VPN на базі Інтернету та MPLS (Multiprotocol Label Switching) VPN. Обидва методи забезпечують безпечний обмін даними між різними локальними мережами, проте вони використовують різні технології та мережеві засоби для досягнення цієї мети.

2.4 Альтернативні підходи до впровадження VPN мереж

2.4.1 VPN на основі брандмауерів

Брандмауери різних виробників зазвичай підтримують функціонал тунелювання та шифрування даних. Більшість таких продуктів використовують вбудований модуль шифрування для захисту трафіку, що проходить через брандмауер. Однак, цей метод може мати обмеження у продуктивності, оскільки ефективність роботи брандмауера часто залежить від характеристик використаного апаратного забезпечення.

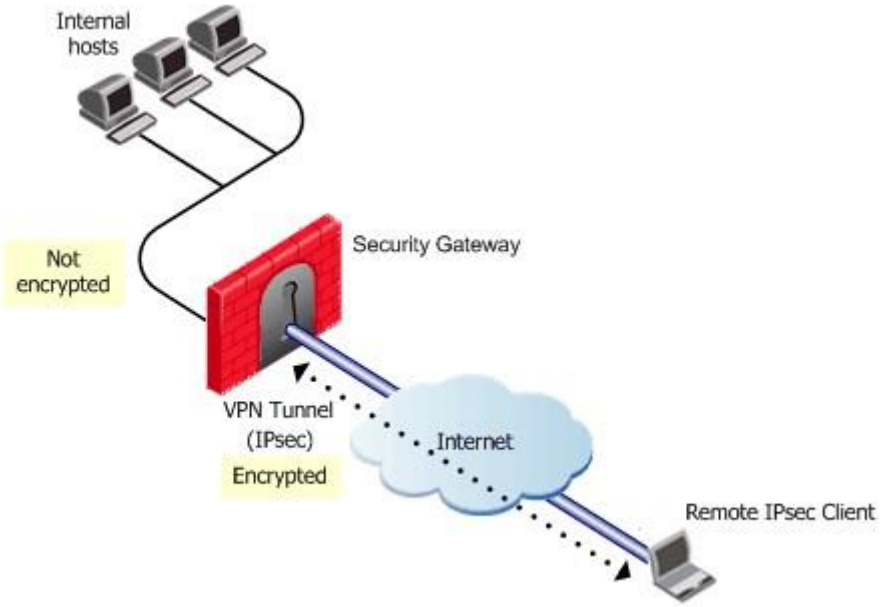

Рисунок 2.17 – VPN на основі брандмауерів

При застосуванні брандмауерів на базі ПК, важливо враховувати, що такі рішення найбільш ефективні для невеликих мереж з обмеженим обсягом передаваної інформації.

Один із прикладів такого типу VPN - це FireWall-1 від Check Point Software Technologies. Цей продукт використовує стандартний підхід на базі IPSec для створення VPN. Припливаючий трафік спочатку розшифровується брандмауером, а потім застосовуються звичайні правила управління доступом.

2.4.2 VPN на базі маршрутизаторів

Ще одним методом створення VPN є використання маршрутизаторів для створення захищених каналів зв'язку. Оскільки весь трафік, який покидає локальну мережу, проходить через маршрутизатор, це може бути ефективним рішенням для застосування шифрування прямо на рівні маршрутизатора рис. 2.18.

Прикладом обладнання для створення VPN на маршрутизаторах є пристрої від компанії Cisco Systems. Починаючи з версії програмного забезпечення IOS 11.3, маршрутизатори Cisco підтримують протоколи L2TP і IPSec. Крім простого шифрування інформації, що проходить через них, маршрутизатори Cisco також забезпечують інші функції VPN, такі як ідентифікація при встановленні тунельного з'єднання та обмін ключами.

Рисунок 2.18 – VPN на основі маршрутизаторів

Для підвищення продуктивності маршрутизатора можна використовувати додаткові модулі шифрування, такі як ESA. Крім того, компанія Cisco Systems пропонує спеціалізовані пристрої для VPN, серед яких є Cisco 1720 VPN Access Router, призначений для застосування в малих та середніх компаніях, а також в окремих підрозділах великих організацій.

2.4.3 VPN на базі програмного забезпечення

Іншим способом побудови VPN є використання чисто програмних рішень. Такі рішення базуються на спеціалізованому програмному забезпеченні, яке

працює на окремому комп'ютері і, в більшості випадків, виконує роль проксі-сервера. Цей комп'ютер може бути розташований за брандмауером, що забезпечує додатковий рівень захисту.

Прикладом такого програмного рішення є продукт Tunnel 97 від компанії Digital. Клієнт підключається до сервера Tunnel 97, який його аутентифікує та обмінюється ключами. Шифрування здійснюється за допомогою 56 або 128-бітних ключів, які генеруються під час встановлення з'єднання. Потім зашифровані пакети інкапсулюються в інші IP-пакети та надсилаються на сервер. Крім того, програмне забезпечення автоматично генерує нові ключі кожні 30 хвилин, що підвищує безпеку з'єднання.

Рисунок 2.19 – VPN на основі програмного забезпечення

Перевагами програмного забезпечення AltaVista Tunnel 97 є його легка установка та зручне управління. Недоліками цієї системи можуть бути відзначені нестандартна архітектура (власний алгоритм обміну ключами) та обмежена продуктивність.

2.5 Характеристики топологій VPN мереж та їхні описи

Зазвичай, при налаштуванні VPN використовують підключення типу "точка-точка" до конкретного сервера або встановлюють Ethernet-тунель із визначеним сервером, при якому тунелі призначають певну підмережу. Сервер VPN в цьому випадку виконує функції маршрутизації та фільтрування трафіку для доступу до локальної мережі через VPN.

Цей підхід забезпечує можливість фільтрації трафіку в залежності від методу підключення (наприклад, застосування різних фільтрів для локальної мережі та для віддалених користувачів), але не потребує налаштування маршрутизації. Віддалені машини безпосередньо підключаються до локальної мережі, бачать ресурси і можуть використовувати широкосмуговий доступ навіть без додаткового налаштування. Через такий VPN вони можуть бачити всі комп'ютери локальної мережі Windows і всі доступні XDMCP-сервери за допомогою XDMCP broadcast.

VPN-з'єднання завжди ґрунтуються на каналі типу "точка-точка", відомому як тунель. Цей тунель створюється в незахищеній мережі, зазвичай, як Інтернет. Канал "точка-точка" передбачає, що з'єднання встановлюється між двома комп'ютерами, які називаються вузлами або пірами. Кожен вузол відповідає за шифрування даних перед їхнім введенням у тунель і розшифрування після виходу з нього.

Незважаючи на те, що VPN-тунель завжди створюється між двома точками, кожен вузол може встановлювати додаткові тунелі з іншими вузлами. Наприклад, якщо трьом віддаленим станціям потрібно з'єднатися з одним офісом, будуть створені три окремі VPN-тунелі до цього офісу. Проте один і той же вузол може бути peer для всіх цих тунелів. Це можливо, оскільки вузол може шифрувати та розшифровувати дані від імені всієї мережі, як показано на рис. 1.20.

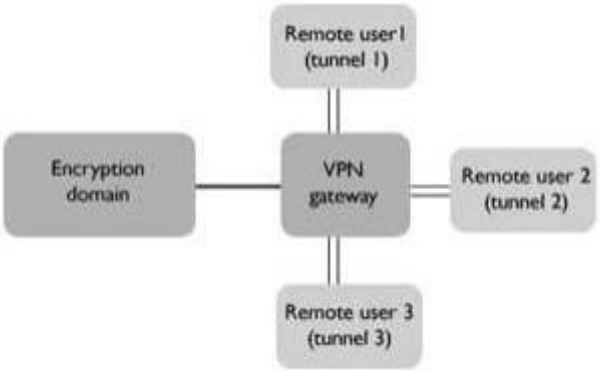

Рисунок 2.20 – Рознесення користувачів за допомогою шлюза

У даному випадку VPN-вузол відомий як VPN-шлюз, а мережа, що за ним розташована, відома як діапазон шифрування (encryption domain). Використання шлюзів має свої переваги з кількох причин. По-перше, всі користувачі пройшовши через цей пристрій, полегшують завдання управління політикою безпеки та контролю над вхідним та вихідним трафіком мережі. По-друге, індивідуальні тунелі до кожної робочої станції швидко можуть стати складними для управління (оскільки тунель є каналом типу точка-точка). У разі наявності шлюзу користувач встановлює з'єднання з ним, що надає йому доступ до мережі (діапазону шифрування).

Цікаво відзначити, що всередині діапазону шифрування саме шифрування не відбувається. Це через те, що ця частина мережі вважається безпечною та перебуває під безпосереднім контролем на відміну від Інтернету. Це також стосується з'єднання офісів за допомогою VPN-шлюзів. Таким чином, забезпечується шифрування лише тієї інформації, яка передається через небезпечний канал між офісами.

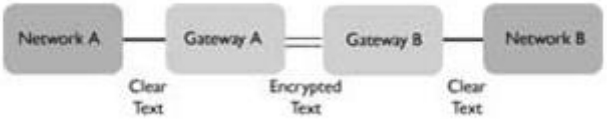

Рисунок 2.21 – VPN на основі незахищеної мережі

Мережа А вважається початковою точкою VPN-з'єднання, а мережа В - кінцевою точкою. Коли користувач мережі А відправляє дані в мережу В через VPN, дані спочатку зашифровуються VPN-шлюзом А і потім передаються через захищений тунель до VPN-шлюзу В. Там вони розшифровуються і доставляються до призначення. Використання тунелю означає, що всі дані між мережами шифруються та маскуються за допомогою нового IP-заголовка, який містить IP-адреси обох VPN-шлюзів. Це ускладнює перехоплення та визначення джерела та призначення даних для сторонніх спостерігачів.

Тунелювання дозволяє пакетам даних транзитувати через загальнодоступну мережу, як у звичайному з'єднанні. Між кожною парою "відправник-отримувач" встановлюється безпечний тунель - логічне з'єднання, яке дозволяє приховувати дані одного протоколу в пакетах іншого. Основні компоненти тунелювання включають:

– ініціатор;

– маршрутизатор мережі;

– тунельний комутатор;

– один або кілька тунельних термінаторів.

Принцип роботи VPN може суперечити деяким основним мережним технологіям і протоколам. Наприклад, при встановленні з'єднання віддаленого доступу клієнт відправляє потік пакетів стандартного протоколу PPP на сервер. При організації віртуальних виділених ліній між локальними мережами їх маршрутизатори також обмінюються пакетами PPP. Проте, принципово новим моментом є пересилання пакетів через безпечний тунель, організований в межах загальнодоступної мережі. Тунелювання дозволяє передавати пакети одного протоколу через логічне середовище, що використовує інший протокол. Це дозволяє вирішувати проблеми взаємодії кількох типів мереж, включаючи забезпечення цілісності і конфіденційності даних, а також пристосування до різних протоколів або схем адресації.

Існуючу мережеву інфраструктуру корпорації можна підготувати до використання VPN як за допомогою програмного, так і апаратного забезпечення.

Організацію віртуальної приватної мережі можна порівняти з прокладанням кабелю через глобальну мережу. Зазвичай, безпосереднє з'єднання між віддаленим користувачем і кінцевим пристроєм утворюється по протоколу PPP.

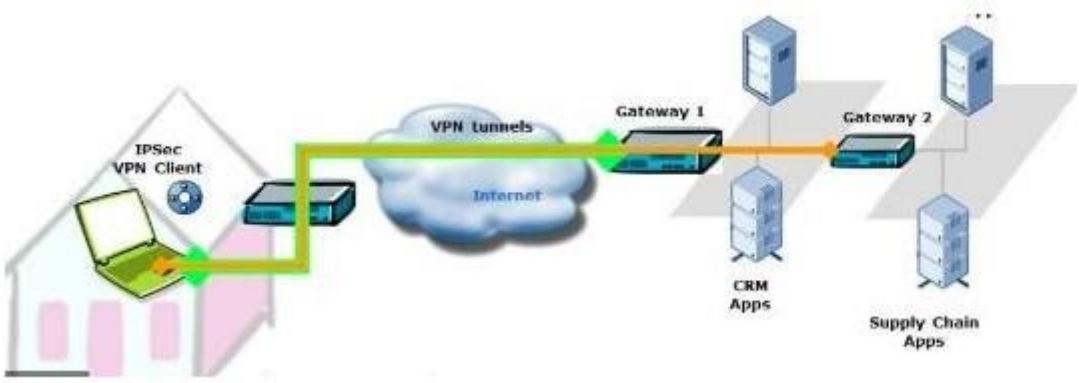

Рисунок 2.22 – Стандартне використання віртуальної приватної мережі

Рисунок 2.22. надає ілюстрацію стандартного використання VPN, яке дозволяє віддаленим користувачам, що працюють віддалено або з перенесеним комп'ютером, мати доступ до ресурсів офісної мережі. Для цього користувачеві необхідно мати встановлене програмне забезпечення - VPN-клієнт, яке забезпечить створення VPN-тунелю до віддаленого VPN-шлюзу. У даному сценарії використовується режим тунелю, оскільки користувач бажає отримати доступ до ресурсів домену, а не просто до самого шлюзу. Використання режиму транспорту актуальне лише у випадку, коли потрібно, щоб один комп'ютер отримав доступ до іншого безпосередньо.

Існує різноманітність VPN-шлюзів і VPN-клієнтів, які можуть бути реалізовані як апаратне забезпечення або програмне забезпечення, що встановлюється на маршрутизаторах або комп'ютерах. Наприклад, операційна система FreeBSD постачається з ПЗ для створення VPN-шлюзу та налаштування VPN-клієнта. Також існують VPN-рішення від компанії Microsoft.

Незалежно від використаного програмного забезпечення, всі VPN працюють за такими основними принципами:

1. Кожен вузол ідентифікується перед створенням тунелю, щоб забезпечити відправку шифрованих даних на вірний вузол.

2. Обидва вузли мають попередньо налаштовані політики, які визначають, які протоколи можуть бути використані для шифрування та забезпечення цілісності даних.

3. Вузли порівнюють політики, щоб домовитися про використані алгоритми. Якщо досягнуто згоди, тунель встановлюється.

4. Після досягнення згоди по алгоритмах генерується ключ, який буде використаний в симетричному алгоритмі для шифрування та розшифрування даних.

3 СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ В ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ

3.1 Вразливості мереж передачі даних

Ризики безпеки пов'язані зі застарілими протоколами, такими як TCP/IP, які були розроблені в епоху, коли безпека мережі не була пріоритетом. У той час користувачі Інтернету були мало зацікавлені в забезпеченні захисту, і протоколи не мали ефективних механізмів для відстоювання від можливих атак. Наприклад, протоколи FTP і Telnet, які передбачають аутентифікацію, передавали паролі у відкритому вигляді через мережу, що робило їх вразливими до перехоплення та зловживання зловмисниками.

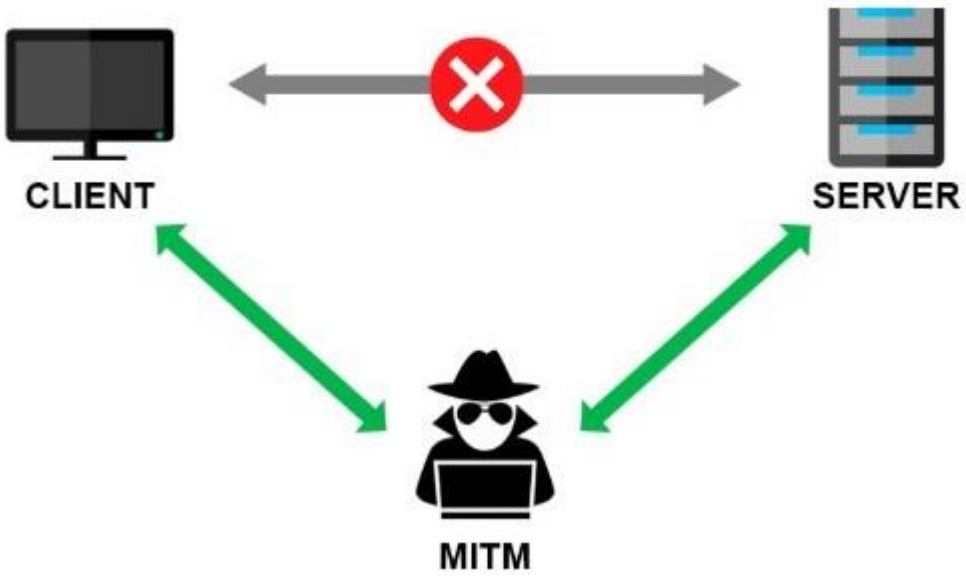

Рисунок 3.1 – Загроза MITM атаки

Під підключенням до мережі розуміється з'єднання комп'ютера з зовнішнім середовищем для взаємодії з іншими ресурсами. В таких випадках неможливо повністю гарантувати, що доступ до комп'ютера та інформації в ньому обмежений лише для користувача або авторизованих осіб з мережі.

Коли комп'ютер підключений до локальної мережі, потенційно можливий несанкціонований доступ до нього та інформації в ньому зі сторони інших користувачів локальної мережі.

При з'єднанні локальної мережі з іншими мережами можливий несанкціонований доступ не лише з локальної мережі, а й з віддалених мереж.

Якщо комп'ютер підключено безпосередньо до зовнішньої мережі через провайдера, наприклад, через модем до Інтернету, для віддаленої взаємодії з локальною мережею, комп'ютер та інформація в ньому можуть стати доступними хакерам з Інтернету. Це також може відкрити доступ до ресурсів локальної мережі зловмисникам.

Зазвичай, для захисту від несанкціонованого доступу застосовуються або вбудовані засоби розмежування доступу операційної системи, або спеціалізовані програмні засоби безпеки, або криптографічні системи, що використовуються на рівні окремих програм. Часто використовують комбінацію цих методів.

Але навіть при використанні цих заходів немає гарантії повної безпеки під час мережевих атак. Це пояснюється наступними причинами:

– Операційні системи, особливо такі як Windows, є складними програмними продуктами, розробка яких ведеться великими командами. Важко провести детальний аналіз таких систем. Тому неможливо довести відсутність у них вразливостей або недокументованих можливостей, якими можна скористатися через мережеві атаки.

– У багатозадачних операційних системах, зокрема Windows, одночасно працює багато різних додатків, для яких також складно гарантувати відсутність вразливостей, які можуть бути використані для отримання доступу до інформаційних ресурсів через мережеві атаки.

– У сучасних системах існує безліч механізмів для віддаленого завантаження та запуску виконуваних програм, контроль над якими є складним завданням.

3.2 Захищені шляхи комунікації

У порівнянні з захищеними каналами, віртуальні приватні мережі (VPN) є більш масштабним і ефективним засобом захисту трафіку. VPN створюють свого роду тунель між користувачем і мережею, що надає відчуття приватності від зовнішнього світу. Однією з основних переваг VPN є захищеність трафіку від потенційних атак користувачів публічної мережі. Крім того, VPN дозволяють користувачам мати власний адресний простір і забезпечувати якість обслуговування, аналогічну якості виділеного каналу.

Віртуальна приватна мережа на основі шифрування представляє собою захищену мережу, створену підприємством в публічній мережі з метою з'єднання різних філійних підрозділів. У сутності, технологія VPN використовує захищені канали, що дозволяють об'єднати не лише дві, але будь-яку кількість клієнтських мереж.

Технології VPN на базі шифрування включають в себе шифрування, аутентифікацію і створення тунелів. Шифрування забезпечує конфіденційність корпоративних даних під час їх передачі через публічну мережу. Аутентифікація гарантує, що системи (користувачі) на обох кінцях VPN перевіряють ідентичність один одного. Створення тунелів надає можливість передавати зашифровані пакети через відкриту публічну мережу.

Для підвищення рівня захищеності віртуальних приватних мереж можна поєднувати технології VPN на основі шифрування з технологіями VPN, що базуються на розмежуванні трафіку.

При виборі засобів для побудови захищених віртуальних мереж важливо враховувати ряд характеристик, таких як функціональна повнота, надійність, гнучкість, продуктивність, керованість і сумісність. Існує кілька способів організації VPN зі своїми перевагами та недоліками:

1. VPN на базі маршрутизаторів:

– Підтримка VPN може бути вбудована в маршрутизатори, що не потребує додаткових витрат на придбання спеціальних пристроїв.

– Спрощується адміністрування VPN.

2. Програмне забезпечення VPN для брандмауерів:

– Можливий контроль трафіку в тунелі.

– Ефективне адміністрування захищеними віртуальними мережами.

– Комплексний захист інформаційного обміну.

3. VPN на базі спеціалізованого програмного забезпечення:

– Можливість модернізації і оновлення версій.

– Оперативне усунення помилок.

– Не потрібно спеціальних апаратних засобів.

4. VPN на базі апаратних засобів:

– Висока продуктивність.

– Легкість конфігурації і обслуговування.

– Тонке налаштування для досягнення найвищої продуктивності.

IPSec може використовуватися у транспортному або тунельному режимі для забезпечення безпеки з'єднань. У транспортному режимі IPSec застосовується для захисту зв'язку між двома точками, наприклад, між двома комп'ютерами в межах однієї локальної мережі. У тунельному режимі IPSec використовується для з'єднання двох віддалених офісів та надання доступу комп'ютера до віддаленого офісу.

У транспортному режимі IPSec залишає IP-заголовок незмінним (за винятком номера протоколу) і захищає дані після нього. У тунельному режимі IPSec додає новий IP-заголовок до пакету, захищаючи колишній IP-заголовок і дані після нього.

IPSec став визнаним стандартом для безпечної комунікації по IP. Він широко використовується як розширення для IPv4 і є невід'ємною частиною IPv6. Цей протокол забезпечує конфіденційність, цілісність і аутентифікацію даних. Аутентифікація здійснюється за допомогою загальних секретних ключів або цифрових підписів, а обмін ключами забезпечується через протокол обміну ключами Internet (IKE).

Поміж звичайними конфігураціями VPN існують ще дві сфери використання стандарту IPSec: динамічні з'єднання між хостами через Інтернет та захист внутрішнього трафіку в локальній мережі.

IPSec може бути використаний для налагодження надійного каналу зв'язку прямо між взаємодіючими хостами без потреби у додатковому обладнанні. Це досягається через створення з'єднання між хостами за допомогою протоколу IPSec, використовуючи транспортний режим. У цьому режимі фрейм IPSec додається до вихідного пакету IP після IP-заголовка. На відміну від тунельного режиму, жодні додаткові IP-заголовки не додаються. Такий підхід потребує реалізації підтримки IPSec у стеках IP на обох хостах.

Для пропуску захищеного трафіку IP через міжмережеві екрани мереж партнерів, адміністраторам слід відкрити UDP-порт 500 для протоколів IKE і NAT Traversal. Останнє забезпечує неперервність інформаційного обміну по протоколу IPSec при проходженні через обладнання NAT.

Протокол NAT Traversal (NAT-T) інкапсулює трафік IPSec, створюючи пакети UDP, які коректно пересилаються через NAT. Для цього NAT-T додає додатковий UDP-заголовок перед пакетом IPSec, щоб він оброблявся як звичайний пакет UDP і приймач не проводив ніяких перевірок цілісності. Після прибуття пакету на приймача заголовок UDP видаляється, і пакет даних продовжує свій шлях як інкапсульований пакет IPSec.

Протокол IPSec дозволяє створювати захищені комунікаційні канали в локальній мережі. Його прозорість полегшує імплементацію, не потребуючи значних модифікацій у додатках.

IPSec можна поступово впроваджувати в існуючі мережеві середовища. На перехідному етапі адміністратор має можливість дозволити незахищені з'єднання з хостами, які ще не можуть підтримувати IPSec.

При захисті трафіку локальної мережі віддалені користувачі майже ніколи не використовують IPSec-VPN для зв'язку з локальною мережею. Для того, щоб вони могли користуватися захищеними службами, використовується ітеративна техніка тунелювання.

Під час ітеративного тунелювання кожен хост має дві або більше асоціацій безпеки, згідно з якими відбувається обмін даними з іншими хостами. Цей процес може бути невидимим для хоста, наприклад, якщо хости встановлюють з'єднання в транспортному режимі від одного сегмента до іншого через IPSec-тунель, який проходить через VPN між двома філіями.

У сучасних підприємствах, коли виникає потреба в захищеному каналі зв'язку всередині локальної мережі або між віддаленими офісами, зазвичай вдаються до використання технологій для створення віртуальних мереж. Проте важливо усвідомлювати, що такі рішення мають свої обмеження, і абсолютний захист інформації може бути досягнутий лише за умови розробки та впровадження комплексних програмних, апаратних та організаційних заходів, адаптованих під конкретні потреби об'єкта інформаційної діяльності.

SSL VPN – це інноваційний підхід до захищеного з'єднання, який базується на використанні криптографічного протоколу для забезпечення аутентифікації, перевірки та шифрування переданих пакетів інформації. Цей метод забезпечує надійний та безпечний обмін даними, при цьому він є економічно вигідним та не потребує постійних налаштувань. Хоча спочатку SSL розглядалося як альтернатива, сьогодні воно є самостійним рішенням. Однією з його переваг є сумісність з будь-якими операційними системами, та не потреба встановлення додаткового програмного забезпечення.

3.3 Порівняння особливостей та характеристик п'яти різних протоколів VPN

3.3.1 PPTP (Point-to-Point Tunneling Protocol)

Використання програм VPN (Virtual Private Network) є важливим засобом забезпечення приватності веб-перегляду та захисту конфіденційності даних. Це досягається через зміну IP-адреси та шифрування даних за допомогою різних протоколів VPN. Однак вибір оптимального протоколу може бути складним, оскільки кожен протокол має свої особливості та призначення. У даній

обговорюваній темі, ми розглянемо п'ять найпоширеніших протоколів VPN, описавши їх переваги та недоліки. Коли організація вирішує використовувати VPN, важливо врахувати, що кожен протокол має свої унікальні особливості, які визначають, як він обробляє конфіденційні дані, забезпечуючи баланс між продуктивністю та безпекою.

Таблиця 3.1 – Характеристики PPTP

Сумісність платформи	Windows, macOS, Android, iOS, Linux та ін
Шифрування VPN	До 128-розрядних.
Шифрування стандарту безпеки VPN	Відомі вразливості.
Швидкість VPN	Висока швидкість через нижчий рівень шифрування)

PPTP, або протокол точка-точка тунелювання, вважається одним з найдавніших протоколів VPN, і його специфікація була опублікована в кінці 90-х років. Хоча цей протокол вважається простим у налаштуванні та має широку підтримку, він також має деякі обмеження та застереження.

Основна версія PPTP не має вбудованих механізмів автентифікації та шифрування. Проте сучасні реалізації, особливо ті, що постачаються разом з операційною системою Windows, використовують стек технологій PPTP, який включає різні варіанти шифрування та забезпечує вищий рівень безпеки.

PPTP відзначається високою швидкістю порівняно з більш сучасними та сильно зашифрованими протоколами, що робить його відмінним вибором для широкополосних застосувань, наприклад, для потокового відео. Проте існує серйозна проблема безпеки з PPTP, оскільки її захист був порушений протягом багатьох років. Це викликало розвиток багатьох нових протоколів з огляду на серйозні вразливості PPTP.

Хоча PPTP може захистити від крадіжки звичайного трафіку, державні структури або організації з великими ресурсами можуть легко проникнути в систему і отримати доступ до даних. Через це, для більшості потреб у

конфіденційності та безпеці, PPTP вважається застарілою технологією. Якщо організація має потребу в надійній захисті, рекомендується обрати інший протокол VPN. Для розблокування заблокованих веб-сайтів може бути краще використовувати інші технології, такі як Smart DNS або Proxy, які не претендують на надання високого рівня конфіденційності та безпеки, але забезпечують географічне розблокування.

3.3.2 L2TP/IPsec (Layer 2 Tunneling Protocol)

L2TP зазвичай поєднується з протоколом безпеки IPsec (IP Security), який відповідає за забезпечення безпеки з'єднання між комп'ютером та VPN-сервером. IPsec використовується для аутентифікації користувача та шифрування передачі даних. Цей протокол забезпечує високий рівень безпеки, надійно захищаючи дані від несанкціонованого доступу та перехоплення.

Таблиця 3.2 – Характеристики L2TP/IPsec

Сумісність із платформою	Windows, macOS, Android, iOS, Linux та ін.
Шифрування VPN	До 256-бітного.
Сильне шифрування VPN Security	Сильна цілісність даних.
Швидкість VPN	Відносно повільна завдяки обробці даних процесором.

Насправді, L2TP є більш безпечним порівняно з PPTP, оскільки він не став жертвою багатьох вразливостей. Особливо ефективним є L2TP/IPsec, який об'єднується у стандарт і широко використовується сьогодні. Як і PPTP, L2TP має широку підтримку серед клієнтів та сервісів. Однак однією з основних проблем L2TP є можливість блокування, оскільки він використовує обмежену кількість мережевих портів. Для заблокування VPN досить просто закрити ці порти.

Нарешті, коли мова йде про вибір стандарту шифрування для L2TP/IPsec, ви зазвичай маєте два варіанти. Один з них - 3DES, але через відомі вразливості його зараз майже не використовують. Основний стандарт для L2TP/IPsec (і VPN

загалом) – це AES. Зокрема, 256-бітний AES надзвичайно надійний і практично неможливий до взлому з використанням сучасних обчислювальних технологій.

Загалом, L2TP/IPsec є чудовим вибором для пересічного користувача Інтернету, оскільки він забезпечує високий рівень безпеки та надійності.

3.3.3 SSTP (Secure Socket Tunneling Protocol)

SSTP – це один з протоколів VPN, який відомий своєю надійністю та захищеністю від атак, спрямованих на блокування VPN, які можуть виникати при використанні інших протоколів, таких як L2TP. Важливо зауважити, що SSTP головним чином асоційований з операційною системою Windows, тому його ефективність може бути обмеженою на інших платформах. Хоча існує підтримка для macOS та Linux, налаштування можуть вимагати додаткових зусиль. Якщо організація використовує VPN з важливості на платформу Windows, то варто розглянути використання SSTP.

Таблиця 3.3 – Характеристики SSTP

Сумісність із платформою	Windows, macOS, Android, Linux та ін.
Шифрування VPN	До 256-бітного.
Сильне шифрування VPN Security	Шифрування SSL включено
Шифрування SSL включено	Повільна швидкість (завдяки високому рівню безпеки).

SSTP вперше з'явився разом з випуском пакету оновлень 1 для Windows Vista. Цей протокол є власністю Microsoft і був розроблений ними. Однак це може становити проблему для деяких користувачів, оскільки внутрішній механізм роботи стандарту залишається закритим. Хоча фактичних доказів про можливість втручання Microsoft або уряду США немає, це питання варто мати на увазі, особливо якщо організація прагне забезпечити максимальний рівень захисту мережі.

SSTP використовує стандарт шифрування SSL 3.0, який має кілька відомих проблем безпеки. Microsoft вже в 2014 році випустила офіційне повідомлення про безпеку SSL 3.0, відзначаючи його проблематичний характер.

Однією з основних переваг SSTP є можливість подолати багато форм блокування VPN, оскільки він може використовувати загальний порт (TCP 443), який часто використовується для веб-сайтів з протоколом SSL. Це дає можливість обхід блокування VPN для більшості користувачів, оскільки Windows є поширеною операційною системою. Проте, якщо ви шукаєте альтернативний протокол з безпекою та надійністю, який не пов'язаний з Microsoft, варто розглянути OpenVPN.

3.3.4 OpenVPN

OpenVPN – це один з найбільш популярних і надійних протоколів VPN, коли йдеться про забезпечення конфіденційності в Інтернеті. Він базується на відкритому коді, що дозволяє забезпечити високий рівень безпеки та пристосування до змін у кібербезпеці.

OpenVPN базується на протоколах OpenSSL та TLS, а також використовує деякі додаткові технології для забезпечення надійності та безпеки. На відміну від деяких інших протоколів VPN, таких як PPTP та SSTP, OpenVPN не має вбудованої підтримки для певних операційних систем або апаратних платформ. Це означає, що для використання OpenVPN може знадобитися встановлення стороннього VPN-клієнта, що може бути як перевагою, так і обмеженням в залежності від потреб користувача.

OpenVPN широко використовується провідними постачальниками VPN, оскільки вони зазвичай розробляють власні клієнти VPN. Проте варто зазначити, що відсутність підтримки для певних платформ може обмежити доступність сервісу для користувачів. Незважаючи на це, існують загальні клієнти OpenVPN, які працюють на більшості платформ. Проте використання таких загальних клієнтів може збільшити ризик вразливостей із-за можливих задніх дверей,

оскільки користувачі повинні довіряти як своєму постачальнику VPN, так і розробникам загальних клієнтів.

Хоча OpenVPN оптимально працює на ряді UDP-портів, він також може функціонувати через порт TCP 443. Це дозволяє використовувати шифрований трафік HTTPS і уникнути блокування VPN на основі портів. Завдяки бібліотеці OpenSSL, OpenVPN має доступ до всіх шифрувальних технологій, включених до цієї бібліотеки, хоча в основному використовується шифрування AES з достатньою довжиною ключа.

У підсумку, OpenVPN вважається найбільш гнучким і безпечним протоколом VPN, доступним на сьогоднішній день. Якщо постачальник VPN добре розуміє технологію та належним чином її впроваджує, використання OpenVPN зазвичай є оптимальним вибором. Проте рекомендується спробувати OpenVPN в першу чергу, якщо це можливо, перш ніж розглядати інші альтернативи.

4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок капітальних витрат на розробку

Капітальні витрати на розробку становлять:

$$К=К1+К2 \quad (4.1)$$

де: К1– витрати на розробку, грн.;

К2– витрати на налагодження і дослідну експлуатацію програмного засобу на ПК, грн.;

4.2 Складові структури витрат на розробку

Складові структури витрат на розробку та реалізацію розробки розраховуються за формулою:

$$К1=Зз+Нз+Ві, \quad (4.2)$$

де: Зз – загальна зарплата розробників, грн;

Нз – нарахування на зарплату, грн;

Ві – інші витрати, грн;

Для проведення розрахунків зарплати (Зз) необхідно визначити спеціальність робітників, чисельність робітників і трудомісткість цих робіт. Для розробки проектного рішення потрібно чотири спеціалісти розробники:

– Керівник проекту(К);

–Студент-дипломник(СД);

– Консультант з економічне ї частини(КЕ);

– Консультант з охорони праці(КОП);

Згідно з штатним розписом сума витрат на оплату праці робітників, з 01.01.2025р. складає:

– Керівник (викладач вищої категорії) – 107,93 грн/год;

– Консультант з економічної частини (викладач вищої категорії) – 107,93 грн/год;

– Консультант з охорони праці(викладач першої категорії) 93,70 грн/год;

– Час витрачений керівником – tk = 14 годин.

– Час витрачений консультантом з охорони праці – tko= 1 година.

– Час витрачений консультантом з економічної частини–tke = 1 година.

– Час витрачений студентом дипломником tc = 3×50= 150 годин.

Витрати на оплату праці керівника проекту:

Ск = 14 роб.год.× 107,93 грн.год.=1511,02 грн.

Витрати на оплату праці консультанта з економічної частини:

Ске = 1 роб.год.×107,93грн.год.= 107,93 грн.

Витрати на оплату праці консультанта з охорони праці :

Ско = 1 роб.год×93,70грн.год.= 93,70грн.

Денна оплата студента дипломника :

1510/173=8,73 грн.

1510 – стипендія

173 – місячний фонд робочого часу, годин.

Витрати на оплату праці студента дипломника

Сс = 8,73×150= 1310 грн.

Витрати на оплату праці робітників проектустановлять

Зз= Ск+Ске+Ско+Сс= 1511,02 +107,93 +93,70 +1310= 3022,65 грн.

Нарахування на зарплату визначаються в розмірі 22% від фонду оплати праці

Нз = Зз×22% = (3022,65 ×22)/100 = 664,98 грн.

де 22 – норматив нарахування на зарплату, %

Інші витрати Ві відображають витрати які, не враховані в попередніх статтях витрат. Ці витрати розраховуються згідно структури витрат(5%)

Ві = 0.05×(Зз+Нз)= 0.05×(3022,65 +664,98)=1843,93 грн.

К1 = Зз+Нз+Ві= 3022,65 +664,98 +1843,93 =5578,56 грн.

4.3 Витрати на відлагодження розробки

Витрати на від лагодження та дослідну експлуатацію розробки

$$К2 = Sм\text{-}г. \times t \quad (4.3)$$

де Sм-г. – вартість однієї машино-години роботи конкретно ПК, грн./год.;

t–машинний час, витрачений на накладку та дослідну експлуатацію програмного засобу, год.

Вартісь 1 машинно-години роботи ПК розраховуємо за складовими витрат на таку роботу:

$$Sм\text{-}г =(А+Ен)/Фд \quad (4.4)$$

де А – амортизація використаного ПК, грн;

Ен – вартість електроенергії, яку споживає ПК, грн.;

Фд – дійсний час від лагодження програми, год.;

Розрахунок складових вартості 1 машино-години роботи ПК:

а) амортизація ПК становить

А= (Кт×На)/100 = (670,31 ×15%)/100= 100,55 грн.

Де Кт – вартість використання ПК, грн..

На – норма амортизації (На=15%)

Кт = (Кс×Тексп)/Твик = (14625×2,2)/48= 670,31 грн.

де Кс – вартість компютероної системи,грн.

Тексп – період експлуатації системи 2.2 місяців(50 робочих днів)

Твик – термін корисного використання 4 роки (48 місяців):

Кс= Ркомп×Р$ = 500×41,00=14625 грн.

де Ркомп –вартість комп'ютерної системи у доларах США;

Р$ – курс долара США по курсу НБУ на момент купівлі системи.

б) вартість використання електроенергії розраховується за формулою:

Ен = (Р×Тф)×Фд×Квик=(0,25 ×5,60)×150×0,8=154,8грн.

де Р – потужність обчислювальної системи, кВт (Р=0,25)

Квик – коефіцієнт використання ПК

Тф – ціна за 1кВт/год.,грн..(Тф = 5,16 грн.)

Фд – дійсний час від лагодження програми

Фд = пр.д.×Тсер= 50р.дн.×3год. = 150год.

Де пр.д. – кількість робочих днів ПК

Тсер = 3 год – середній щоденний час роботи ПК

Отже вартість 1 машино-години роботи і від лагодження на ПК становить

Sм-г=(100,55+154,8)/150= 1,70 грн.

Таким чином сумарні витрати на від лагодження і дослідну експлуатацію проектного рішення становлять:

К2=Sм-г×Фд= 1.70×150=255 грн.

Отже, капітальні витрати на розробку проектного рішення за формулою становлять:

К=К1+К2 = 5578,56 + 255 = 5833,56 грн.

Загальний кошторис витрат на розробку проектного рішення приведений в таблиці 4.1

Таблиця 4.1 – Кошторис витрат на розробку проектного рішення

Складові елементи витрат	Умовне позначення	Сума витрат, грн
Витрати на оплату праці	Зз	3022,65
Нарахування на зарплату	Нз	664,98
Інші витрати	Ві	1843,93
Разом	К1	5578,56
Витрати на відлагодження	К2	255
Разом К=К1+К2	К	5833,56

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ

5.1 Загальні положення

Визначення поняття охорони праці дається в ст. 1 Закону України від 14 жовтня 1992 р. «Про охорону праці». Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. В поняття охорони праці входять і всі ті заходи, що спеціально призначені для створення особливих полегшених умов праці для жінок і неповнолітніх, а також працівників зі зниженою працездатністю. Охорону праці і здоров'я громадян віднесено до пріоритетних напрямків соціальної політики України. Так, Конституція України одним з основних соціальних прав громадян визначає право кожного на належні, безпечні й здорові умови праці, встановлює, що використання праці жінок і неповнолітніх на небезпечних для їхнього здоров'я роботах забороняється. Завдання охорони праці:

– проектування підприємств, технологічних процесів і конструювання обладнання з обов'язковим виконанням вимог охорони праці;

– знаходження оптимальних співвідношень між різними факторами виробничого середовища, що дозволяє забезпечити мінімум несприятливого впливу їх на здоров'я працівників;

– розробка конкретних заходів щодо покращення умов праці та забезпечення її безпеки на основі застосування у виробництві новітніх досягнень науки і техніки;

– застосування раціональних засобів захисту працівників від впливу несприятливих факторів виробничого середовища, а також втілення організаційних заходів, які нейтралізують або послаблюють ступінь їх впливу на організм людини;

– розробка та застосування методів і засобів оцінки ефективності заходів з охорони праці, що плануються і здійснюються.

5.2 Організація охорони праці на підприємстві

На сучасному етапі науково-технічного розвитку нашої держави питання охорони праці на підприємствах є одним із найактуальніших.

Належна організація охорони праці, яка відповідає вимогам нормативно-правових актів, є основним заходом профілактики та запобігання виробничому травматизму й професійній захворюваності. Крім того, кожним трудовим договором передбачаються зобов’язання роботодавця щодо забезпечення найманих працівників безпечними умовами праці.

Законодавство України покладає на всіх роботодавців обов'язок щодо забезпечення безпечних і нешкідливих умов праці. Витрати на охорону праці на підприємстві згідно зі ст. 19 Закону повинні становити не менше 0,5% від фонду оплати праці за попередній рік, а за невиконання законодавства про охорону праці до підприємства можуть бути застосовані санкції аж до заборони його експлуатації.

Для того щоб не поставити під загрозу існування підприємства, роботодавцю необхідно:

– створити службу охорони праці.

Згідно зі ст. 15 Закону така служба обов'язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці, затвердженого наказом Держкомітету з нагляду за охороною праці від 15.11.2004 № 255. На підставі цього документа також має бути розроблено Положення про службу охорони праці цього підприємства, визначено структуру такої служби, її чисельність, основні завдання, функції та права її працівників. На підприємствах із кількістю працівників менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку.

– Розробити та затвердити на підприємстві положення, інструкції та інші акти з охорони праці.

Обов'язок роботодавця стосовно розробки та затвердження документів, які повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майдан-чиках і робочих місцях, передбачений ст. 13 Закону про охорону праці.

– Організувати проведення інструктажів з питань охорони праці.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 КЗпП зобов'язаний проінформувати його під розпис про умови праці, наявні на його робочому місці, у тому числі про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров'я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

– Забезпечити навчання і перевірку знань з питань охорони праці.

Згідно зі ст. 18 Закону працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, проходять спеціальне навчання і перевірку знань відповідних нормативно-правових актів з охорони праці. Таке навчання з питань охорони праці може проводитись як безпосередньо на підприємстві, так і навчальним центром.

– Подбати про проведення медичних оглядів.

Згідно зі ст. 169 КЗпП роботодавець зобов'язаний за свої кошти організувати проведення попереднього (при прийнятті на роботу) та періодичних (протягом трудової діяльності) медоглядів працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі. Також він зобов'язаний проводити щорічний обов'язковий медогляд осіб віком до 21 року.

– Забезпечити працівників засобами індивідуального захисту.

На роботах із шкідливими й небезпечними умовами праці, а також на роботах, пов'язаних із забрудненням або несприятливими температурними умовами, працівникам згідно зі ст. 164 КЗпП необхідно безкоштовно видавати спеціальний одяг, взуття та інші ЗІЗ.

– Провести атестацію робочих місць.

На підприємствах, де технологічний процес, використовуване обладнання, сировина, матеріали є потенційними джерелами шкідливих і небезпечних виробничих факторів, які можуть негативно впливати на стан здоров'я працюючих, повинна проводитись атестація робочих місць за умовами праці. Така атестація повинна проводитися атестаційною комісією, склад і повноваження якої визначаються наказом по підприємству в строки, передбачені колективним договором, але не рідше одного разу на 5 років. Порядок проведення такої атестації передбачений постановою КМУ від 01.08.1992 № 442. Відомості про результати атестації заносяться в картку умов праці.

– Налагодити облік нещасних випадків.

Згідно зі ст. 22 Закону «Про охорону праці» роботодавець зобов'язаний організувати розслідування та вести облік нещасних випадків, професійних захворювань і аварій у порядку, встановленому постановою КМУ від 30.11.2011 № 1232. За результатами такого розслідування роботодавець повинен складати акт за формою Н-5 (якщо нещасний випадок визнано таким, що не пов'язаний з виробництвом) або Н-1 (якщо він визнаний пов'язаним з виробництвом). Один із примірників повинен видатися потерпілому або іншій зацікавленій особі не пізніше трьох днів з моменту закінчення розслідування.

5.3 Заходи безпеки на робочому місці

Конструкція робочого місця, його розміри та взаємне розташування його елементів повинні відповідати антропометричним, фізіологічним І психофізіологічним характеристикам людини, а також характеру роботи.

Організація робочих місць повинна забезпечувати стійке положення та вільність рухів працівника, безпеку виконання трудових операції виключати або допускати лише в деяких випадках роботу в незручну позиціях, котрі зумовлюють підвищену втомлюваність.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого; всі необхідні для роботи предмети повинні знаходитись поряд з працівником, але не заважати йому;

– ті предмети, котрими користуються частіше, розташовуються ближче, ніж ті предмети, котрими користуються рідше;

– предмети, котрі беруть лівою рукою, повинні знаходитись зліва а ті предмети, котрі беруть правою рукою, повинні знаходитись справа;

– якщо використовують обидві руки, то місце розташування інструментів вибирається з врахуванням зручності захоплювання його двома руками;

– небезпечніше, з точки зору можливості травмування обладнання повинне розташовуватись вище, ніж менш небезпечне. Однак слід враховувати, що важкі предмети під час роботи зручніше опускати, ніж піднімати.

5.4 Санітарно-гігієнічні вимоги

Санітарно-гігієнічні вимоги до умов праці під час виконання роботи мають відповідати визначеним нормативам:

– параметри мікроклімату у приміщенні забезпечували комфортне самопочуття організму. Параметри мікроклімату закритих приміщень унормовані за санітарні норми ДСН 3.3.6.042-99.

– освітлення приміщень та робочих місць забезпечене відповідно до встановлених вимог. Відносно вікна робоче місце розміщено так, що природне світло збоку, переважно з лівого та забезпечувало коефіцієнт природної освітленості не нижче 1,5 %. Освітленість за штучного освітлення в площині робочої поверхні становила 300 – 500 Лк. Відношення яскравості робочих поверхонь було 3:1, а яскравість робочих поверхонь і стін (іншого обладнання) – 5:1. Використана система вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

– Дотримані вимоги до рівнів шуму та вібрації. Було дотримано допустимих рівнів звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях встановлені санітарними нормами виробничого 17 шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

– Надходження свіжого повітря регульоване, виходячи із відповідних нормативних.

– Передбачений захист від шуму та вібрацій.

Дотримані заходи особистої гігієни на робочому місці (підтримання чистоти, миття рук тощо). Заходи особистої гігієни на робочому місці передбачають щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього трудового розпорядку.

ВИСНОВКИ

В сучасних умовах забезпечення безпеки інформації стає важливим завданням, і все більше уваги приділяється використанню технології VPN.

З моїх досліджень випливає, що для забезпечення надійності передачі даних через VPN з використанням OpenVPN рекомендується використовувати найбільшу можливу довжину ключа шифрування.

Аналізуючи проблеми інформаційної безпеки в мережах, зокрема віртуальних приватних мережах (VPN), стає очевидним, що такі системи повинні виявляти внутрішні та зовнішні загрози і вторгнення, фільтрувати зовнішній трафік, контролювати використання корпоративних мережевих ресурсів і запобігати витокам конфіденційної інформації. Для цього важливо мати інформацію про структуру та характеристики трафіку, що дозволяє розробити набір правил для класифікації нормальних та аномальних компонентів трафіку. Це підвищить безпеку мереж шляхом оперативної реакції на відомі загрози та аномальні ситуації, а також за допомогою ідентифікації діючих мережевих додатків або процесів та управління ними для забезпечення доступності необхідних мережевим спільнотам інформаційних сервісів.

Отже, очевидно, що вирішення проблеми зв'язку «тунелювання + аутентифікація + шифрування» є критичним для побудови безпечної VPN-мережі.

Для повсякденної роботи в мережі зазвичай підходять протоколи OpenVPN, L2TP/IPsec і IKEv2. Також варто згадати про SSTP, особливо якщо ви працюєте на пристрої з операційною системою Windows. Проте слід пам'ятати, що SSTP може бути уразливішим порівняно з іншими протоколами.

Ефективний захист можливий лише з використанням протоколу, який не має вразливостей та слабких місць. Наразі OpenVPN є єдиним варіантом, який задовольняє ці вимоги. Крім того, цей протокол підтримується на різних платформах, що робить його дуже привабливим для користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. VPN протоколы [Електронний ресурс] – Режим доступу до ресурсу: https://www.cactusvpn.com/ru/beginners-guide-to-vpn/vpn-protocol/

2. Virtual private network (VPN) [Електронний ресурс] – Режим доступу до ресурсу:

https://en.wikipedia.org/wiki/Virtual_private_network

3. Браун С. Віртуальні приватні мережі. – М.: Радіо та зв'язок, 2001.

4. A Framework for IP Based Virtual Private Networks [Електронний ресурс] – Режим доступу до ресурсу: http://www.ietf.org/rfc/rfc2764.txt

5. Pure hardware VPNs rule high-availability tests [Електронний ресурс] – Режим доступу до ресурсу: https:

//web.archive.org/web/20070923013848/http://www.networkworld.com/reviews/2000/1211rev.html

6. Douglas Crawford. OpenVPN over TCP vs. UDP: what is the difference, and which should I choose? [Електронний ресурс] – Режим доступу до ресурсу: https://www.bestvpn.com/blog/7359/openvpn-tcp-vs-udp-difference-choose/

7. IPSec — протокол захисту мережевого трафіку на IP-рівні. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ixbt.com/comm/ipsecure.shtml

8. Базова реалізація бібліотек для роботи з IPsec для Unix-подібних систем [Електронний ресурс] – Режим доступу до ресурсу:

http://ipsec-tools.sourceforge.net/

9. Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Н. Г. Медведев, Д.В. Москалик - К: Европ.. ун-та, 2002.

КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ