МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри ЗЗІ
_____ В.В. Козловський

«____»_____ 2020 р.

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Захист мереж від несанкціонованого доступу з використанням технології VPN

Автор: В.С. Олійник

Науковий керівник: к.т.н., доцент Ю.В. Баланюк

Нормоконтролер: д.т.н., професор М.О. Шутко

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітнього ступеня: «Магістр»

Спеціальність: 125 Кібербезпека

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗЗІ

_____ В.В. Козловський

«____»_____ 2020 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
студента Олійника Вадима Сергійовича

1. Тема: Захист мереж від несанкціонованого доступу з використанням технології VPN

затверджена наказом ректора від 13.10.2020 р. № 1994/ст.

2. Термін виконання: з 05 жовтня 2020р. по 27 грудня 2020р.

3. Вихідні дані: характеристика, протоколи, функції та проблеми VPN; аналіз способів їх захисту каналів корпоративних мереж на базі VPN рішень та концепція побудови віртуальних захищених мереж VPN; дослідження та аналіз сучасних VPN.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):

1. Значення та проблеми застосування VPN

2. Допустимі концепції та конфігурації для побудови захищеної мережі VPN

3. Захист мереж від несанкціонованого доступу з використанням технології VPN

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі		Виконано
2.	Аналіз літературних джерел		Виконано
3.	Обґрунтування рішення		Виконано
4.	Збір інформації		Виконано
5.	Значення та проблеми застосування VPN		Виконано
6.	Допустимі концепції та конфігурації для побудови захищеної мережі VPN		Виконано
7.	Захист мереж від несанкціонованого доступу з використанням технології VPN		Виконано
8.	Оформлення і друк пояснювальної записки		Виконано
9.	Оформлення презентації		Виконано
10.	Отримання рецензій від опонентів		Виконано
11.	Захист в ЕК		

Дипломник В.С. Олійник

(підпис, дата)

Дипломний керівник Ю.В. Баланюк

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 72 сторінки, має 6 рисунків, 1 таблиця. Список використаних джерел містить 42 найменування і займає 5 сторінок.

Метою кваліфікаційної роботи є захист мереж від несанкціонованого доступу з використанням технології VPN.

Підсумком роботи є надання рекомендацій щодо застосування технології VPN.

Ключові слова: VPN, МЕТОДИ ЗАХИСТ ІНФОРМАЦІЇ, ПРОТОКОЛИ VPN, МЕРЕЖІ VPN, КОНФІГУРАЦІЯ VPN.

ЗМІСТ

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ 6
ВСТУП 7
РОЗДІЛ 1 ЗНАЧЕННЯ ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ VPN 9
1.1 Загальні характеристики VPN 9
1.2 Протоколи VPN 10
1.3 Функції та компоненти VPN 12
1.4 Мережі VPN та проблеми їх захисту 12
1.5 Висновки до першого розділу 18
Розділ 2 ДОПУСТИМІ КОНЦЕПЦІЇ ТА КОНФІГУРАЦІЇ ДЛЯ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ VPN 20
2.1 Способи захисту каналів корпоративних мереж на базі VPN рішень 20
2.2 Концепція побудови віртуальних захищених мереж VPN 27
2.3 Конфігурація VPN для безпечної передачі даних 39
2.4 Висновки до другого розділу 41
Розділ 3 ЗАХИСТ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN 43
3.1 Методи захисту інформації в мережах VPN 43
3.2 VPN від Avast 49
3.3 VPN від Сайфер 51
3.4 VPN від Автор 56
3.5 Висновки до третього розділу 57
ВИСНОВКИ 59
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 62
ДОДАТОК А 67

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

CERT – Computer emergency response team
CHAP – Challenge handshake authentication protocol
EAP – Extensible authentication protocol
EAP-TLS – Transport layer security
IKE – Internet key exchange
IPSec – Internet protocol security
L2F – Layer-2 forwarding
L2TP – Layer-2 tunneling protocol
LAN – Local area network
LCP – Link Control Protocol
MPLS – Multiprotocol label switching
MPPE – Microsoft Point-to-Point Encryption
MSCHAP – Microsoft challenge handshake authentication protocol
PAP – Password authentication protocol
PPP – Point-to-Point Protocol
PPTP – Point-to-Point Tunneling Protocol
SA – Security association
SPAP – Shiva password authentication protocol
SSL – Secure sockets layer
VPN – Virtual private network
ІБ – Інформаційна безпека
ІТ – Інформаційні технології
КЕП – Кваліфікований електронний підпис
КМ – Корпоративних мереж
КСМ – Комп’ютерні системи та мережі
НСД – Несанкціонований доступ
ОС – Операційні системи
ПЕОМ – Персональна електронна обчислювальна машина
ПЗ – Програмне забезпечення

ВСТУП

Virtual Private Network (VPN) – віртуальна приватна мережа, котра формується поверх інших мереж із меншим рівнем довіри. VPN, формується між двома вузлами та надає можливість клієнту, який приєднався бути учасником віддаленої мережі та користуватись її сервісами (внутрішніми сайтами, базами даних, принтерами, політиками виходу в Інтернет). Безпека передачі інформації через загальнодоступні мережі реалізуються завдяки шифрування, у результаті формується закритий для сторонніх канал обміну інформацією. Технологія VPN пов'язує мережі в єдину мережу із застосування непідконтрольних каналів. Провайдери пропонують власні послуги для розгортання власної VPN-мережі. VPN вважається клієнт-серверною технологією [41].

Сучасні технології для обробки, передачі та збору інформації спряють для розвитку загроз, таких як можливість втрати, модифікації та розкриття даних, котрі направляються кінцевим користувачам. Забезпечення інформаційної безпеки (ІБ) комп'ютерних систем і мереж (КСМ) є одним з перспективних напрямків розвитку ІТ. Комп'ютерні інформаційні технології (ІТ) змінюють наше життя. Інформація була і буде товаром, який можна придбати, продати, обміняти. А вартість інформації завжди перевищує вартість купівлі та обслуговування КСМ [41].

ІБ КСМ забезпечує конфіденційність, цілісність та доступність даних, котрі обробляються, компонентів та ресурсів такої системи. При розробці КСМ варто зауважити на можливі наслідки при поломках та їх ліквідація, тому комп'ютерна безпека є надважливою, тому дана тематика є **актуальною**.

Заходи, які спрямовані на забезпечення комп'ютерної безпеки, які включають у собі технічні, організаційні та правові. Захист інформаційної системи від втручання, котрі шкодять власникам чи користувачам інформації, у залежності від доступності, цілісності, конфіденційності [41].

Сучасна ІС – система, котра складається з компонентів, які

пов’язуються між собою та обмінюються даними. Кожен компонент піддається зовнішньому впливу чи поломка. Якщо інформація є важливою, то захист її повинен дорівнювати її вартості [41].

Метою є захист мереж від несанкціонованого доступу з використанням технології VPN.

У процесі підготовки кваліфікаційної роботи були поставлені наступні **задачі**:

- Дослідження протоколів, функцій та проблеми VPN;
- Аналіз способів їх захисту каналів корпоративних мереж на базі VPN рішень та концепція побудови віртуальних захищених мереж VPN;
- Дослідження та аналіз сучасних VPN

Об’єкт дослідження. Мережі.

Предмет дослідження. Технології VPN.

Новизна роботи. Рекомендації щодо застосування технології VPN.

Практична цінність. Аналіз, який проведено у роботі дозволить для організації підібрати найактуальніший VPN.

РОЗДІЛ 1 ЗНАЧЕННЯ ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ VPN

1.1 Загальні характеристики VPN

У залежності від протоколів та призначень, VPN надає можливість поєднати три види вузлів: вузол-вузол, вузол-мережу та мережу-мережу [25].

Застосування технології із використанням мережі Internet як передавача IP-трафіку. Мережі VPN мають вирішувати задачі для підключення кінцевого користувача до віддаленої мережі та поєднання кількох локальних мереж. Структура даної технології включає канали глобальної мережі, захищені протоколи та маршрутизатори [25].

VPN пристрій знаходиться між внутрішньою мережею та мережею Інтернет на кожному кінці з'єднання. При передачі інформації через VPN, вони потрапляють на вхід VPN та після повного проходження через неї та з'являються у точці призначення. Процес вважається «туннелюванням» – формування логічного тунелю у мережі Інтернет, котрий поєднує 2 точки. зА допомогою застосування «тунелюванню» особиста інформація є невидимою для інших користувачів Інтернету. Перед попаданням інформації до інтернет-тунелю, дані зашифровуються, і це їм надає додатковий захист [25].

Протоколи шифрування використовуються у залежності від того протоколу тунелювання, який підтримується VPN-рішенням. Характеристика VPN-рішення – це є діапазон підтримуваних протоколів автентифікації. Найрозповсюдженішим стандартом є сімейство стандартів X.509. Тобто, вдосконаливши VPN протоколом автентифікації можна гарантувати її захист та не допустити несанкціонованого доступу (НСД). Технологія VPN набрала такої популярності, що це є обов'язковим для побудови комплексної системи захисту інформації (КСЗІ), для роботи у державних та не державних організаціях чи структурах не лише в організації, а й поза нею. У зв'язку з карантинними заходами, велика кількість організацій перейшла на віддалену роботу, тому для захисту даних, які надсилаються через мережу Інтернет чи для підключення до сервісів [25].

VPN мають певні відмінності, у порівняні з іншими, якщо точніше

звернення мережі організації не встановлюючи комутоване з’єднання та уникнення виділених ліній [9].

Користувач маючи доступ до Інтернету може підключитися до мережі офісу, але загальнодоступність даних зовсім не означає, що вони не є незахищеними. Система безпеки VPN – це захист корпоративної інформації від НСД. Так як інформація передається у зашифрованому вигляді, доступ до яких має лише їх власник. Алгоритм розповсюджений для зашифрування є Triple DES (притаманне потрійне шифрування – використання 3-х ключів) [9].

Достовірність підтверджується через перевірку цілісності даних та ідентифікації користувачів, які задіяні у VPN. Це дає можливість отримати інформацію, що дані надійшли до адресата без пошкодження та модифікації. Алгоритми для перевірки цілісності даних, які найчастіше використовуються – MD5 і SHA1. Наступним кроком, система здійснює перевірку на зміну даних у процесі руху мережею, з’ясовуючи чи це навмисно, чи помилково. Тобто, побудова VPN має на меті формування захищених від сторонніх очей доступу тунелів між кількома локальними мережами чи віддаленими користувачами [9].

Для формування VPN важливо мати програми шифрування вихідного та вхідного трафіків. При цьому, їх реалізація може бути як програмно так і апаратно-програмно, з будь-якими операційними системами, та не важливо, це комп’ютер чи мобільний пристрій. Тому важливо зробити висновок, що автентифікація та шифрування даних – є невід’ємними елементами захищеного з’єднання [9].

1.2 Протоколи VPN

Протокол VPN визначає, як саме система VPN взаємодіє зі всіма системами в мережі Інтернет та рівень захищеності трафіку. За умови використання внутрішнього інформаційного обміну, тоді взаємодія не є пріоритетною, але якщо навпаки, то власні протоколи не слід

використовувати. Тобто, протокол VPN впливає на рівень безпеки в цілому системи. Причиною є застосування шифрування між двома кінцевими вузлами. За умови незахищеності інформації, зловмисник може перехопити ключі та розшифрувати трафік [38].

Щоб сформувати VPN з використанням апаратного та програмного забезпечення (ПЗ) важливо дотримуватися стандартного механізму на базі протоколу Internet Protocol Security (IPSec). Саме він деталізує методи ідентифікації для ініціалізації тунелю, методів шифрування. Недоліками є орієнтація на використання IP-адреси [38].

Наступний протокол, який використовується для побудови VPN це – Point-to-Point Tunneling Protocol (PPTP), Layer-2 Forwarding (L2F) та Layer-2 Tunneling Protocol (L2TP), котрий об'єднує 2 вищеописаних протоколи. Але вони є не всеохоплюючі та не повнофункціональними [38].

Інший протокол Internet Key Exchange (IKE) забезпечує передачу інформації по тунелю, виключаючи втручання ззовні. Задачі, за які відповідає та які вирішує задля безпечного управління та обміну криптографічними ключами між віддаленими пристроями. IKE автоматизує процес передачі ключів, застосовуючи механізм шифрування через відкритий ключ. IKE змінює ключ для з'єднання, і надасть змогу підвищити конфіденційність переданої інформації. При цьому інкапсуляція – забезпечує мультиплексування кількох транспортних протоколів одним каналом [38].

Протокол Link Control Protocol (LCP) – Point-to-Point Protocol (PPP) вказує гнучкий LCP для встановлення, налаштування та перевірки каналу зв'язку. LCP узгоджує формат інкапсуляції, розміру пакета, параметру встановлення, розриву з'єднання та параметри автентифікації [38].

Протоколи управління мережею вказують певні специфічні конфігураційні параметри для певних транспортних протоколів [38].

Для створення тунелів VPN застосовуються протоколи PPTP, L2TP, IPsec, OpenVPN [38].

1.3 Функції та компоненти VPN

Безпечний віртуальний VPN – це одночасне застосування локальних мереж та комп'ютерів завдяки відкритому зовнішньому середовищі для передачі даних у єдиній віртуальній корпоративній мережі, котра гарантує захист даних, які циркулюють в організації [22].

У процесі підключення корпоративної локальної мережі до відкритої мережі є такі недоліки [22]:

– НСД до даних компанії, які передаються через відкриту мережу;

– НСД до внутрішніх ресурсів локальної мережі, які перехоплює зловмисник після НСД до мережі.

Захист інформації у процесі передачі відкритими канали фундаментується на функціях [22]:

– автентифікація взаємодіючих сторін;

– криптографічне шифрування даних, які передаються;

– перевірка правильності та цілісності переданої інформації.

Функції, які характеризуються зв'язком між собою. Реалізація ґрунтується на застосуванні методів КЗІ [22].

Для захисту КСМ від НСД із зовнішнього середовища застосовуються міжмережеві екрани для підтримки безпеки інформаційної взаємодії через фільтрацію повідомлень. Міжмережевий екран знаходиться на інтерфейсі між локальною та відкритою мережами. Для захисту конкретного комп'ютера, який під'єднаний до відкритої мережі, то встановлюється відповідне ПЗ міжмережевого екрану [22].

1.4 Мережі VPN та проблеми їх захисту

Сучасний системний адміністратор вважає за звичне налаштування VPN-каналів для співробітників, які працюють віддалено від мережі організації, як приклад, можна розглянути Рис. 1.1. VPN для двох офісних мереж, як приклад можна розглянути Рис. 1.2, де об'єднуються машини чи локальні мережі у віртуальну мережу, котра гарантує цілісність та

конфіденційність переданих даних [5].

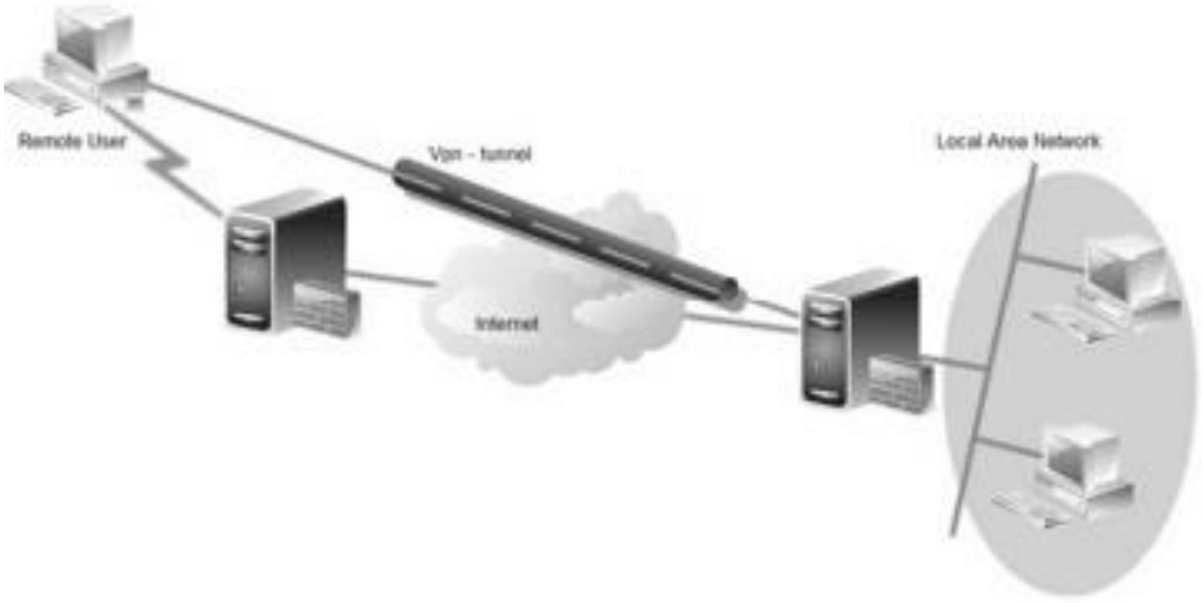


Рисунок 1.1 – VPN для віддалених користувачів

Рисунок 1.2 – VPN для двох офісних мереж

Застосування саме VPN має певний набір переваг порівнюючи інші сучасні методи дистанційного доступу. Тобто, користувач, який має доступ до Інтернету, може під’єднатися до мережі організації. Загальнодоступність даних не завжди дорівнює незахищеності. Система безпеки VPN – це можливість для захисту корпоративної інформації від НСД [5].

Інформація передається лише у зашифрованому виді. Зчитавши дані, їх власник підтверджує чинність та здійснює перевірку цілісності даних та ідентифікацію користувачів, які включають у VPN. Де, перша гарантує, що

дані надійшли до адресата у першочерговорму вигляді. Популярні алгоритми перевірки цілісності даних – MD5 і SHA1. Побудова VPN припускає формування захищених від НСД тунелів між кількома локальними мережами чи користувачами [5].

Для формування VPN з обох ліній зв'язку програми шифрування вихідного та розшифрованого вхідного трафіку. Які здійснюють роботу на спеціалізованих через ПЗ чи програмно-апаратне забезпечення та з будь-якими операційними системами [5].

VPN включають такі переваги: економічність, гнучкість та зручність застосування. Завдяки VPN мережі організації обмежують зростання кількості модемів, серверів доступу, комутаційних ліній та інших технічних засобів, котрі необхідно впроваджувати для забезпечення віддаленим користувачам доступ до своїх мереж [5].

Рівень безпеки та анонімності мереж VPN залежить від реалізації та налаштування. Високий рівень конфіденційності здійснюється завдяки ПЗ та правильної реалізації. Налаштування мереж VPN дозволяють користувачам досягти анонімності в віртуальному просторі [5].

Структура VPN містить два рівні [34]:

- Перший рівень називається «внутрішня мережа». Їх може бути кілька.
- Другий рівень – це «зовнішня мережа». Для з'єднання використовується інтернет, підключивши віддаленого користувача до віртуальної мережі через спеціальний сервер. Для підключення до VPN, комп'ютер здійснює пройти кілька етапів. Після успішного завершення процесу ідентифікації та автентифікації користувач здійснює процес авторизації. Авторизація, дозволяє отримати повний доступ до всієї мережі.

Споживча сутність VPN – віртуальний захищений тунель, чи шлях, завдяки якому можна здійснити віддалений захищений доступ відкритими каналами до серверів баз даних чи поштових серверів [34].

Фізична сутність технології VPN – здатність захисту трафіку

інформаційних систем, відеоконференцій , систем електронної комерції [34].

Захист інформації в мережах VPN – ґрунтується на кількох методах, які використовуються для реалізації заходів безпеки в інформаційних мережах [34]:

❖ Тунелювання – передача даних між двома точками, тобто для джерела та прийому даних є прихованою вся мережева інфраструктура, котра лежить між ними. Транспортне середовище тунелю ловить пакети застосованого мережного протоколу біля тунелю та без змін модифікацій доставляє їх до виходу. Побудова тунелю може з'єднати два мережевих вузли.

Окрім описаних переваг є ще і недоліки [34]:

o Інформація для передачі може бути перехоплена зловмисниками. Так як вона конфіденційна, то це є реальна загроза її компрометації.

o Зловмисники можуть модифікувати дані так, що отримувач не може перевірити їх достовірність.

Тоді варто зробити висновок, що тунель придатний для певних типів мережевих комп'ютерних ігор та не претендує на складніше застосування. Проблеми вирішуються сучасними засобами КЗІ. Для перешкоданню внесенню несанкціонованих змін до пакету з даними для проходженню тунелем, використовується кваліфікований електронний підпис (КЕП), де мета методу забезпечується додатковим блоком інформації, яка виготовляється завдяки асиметричного криптографічного алгоритму та унікального вмісту пакета та секретного ключа КЕП відправника. Даний блок інформації це КЕП пакету та надає здійснити автентифікацію даних отримувачем, якому відомий відкритий ключ КЕП відправника. Дані, які передаються тунелем захищається від НСД шляхом застосування сильних алгоритмів шифрування [34].

❖ Автентифікація – забезпечення безпеки VPN. Дані від комп'ютерів-клієнтів проходять від Internet до VPN-сервера. Сервер знаходитися на великій відстані від комп'ютера клієнту та дані на шляху до

мережі організації здійснюється через обладнання багатьох провайдерів. Для захисту даних від спотворення та НСД використовуючи різні методи автентифікації та шифрування [18].

Для автентифікації користувачів PPTP використовуються протоколи для PPP [18]:

- EAP (Extensible Authentication Protocol);
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security);
- MSCHAP (Microsoft Challenge Handshake Authentication Protocol), версії 1 і 2;
- CHAP (Challenge Handshake Authentication Protocol);
- SPAP (Shiva Password Authentication Protocol);
- PAP (Password Authentication Protocol).

Ефективні протоколи є MSCHAP версії 2 і EAP-TLS, так як забезпечують взаємну автентифікацію, де VPN сервер та VPN клієнт ідентифікують один одного. Тоді, як у всіх інших протоколах лише сервер здійснює автентифікацію клієнтів (через відритий тест, чи за схемою запит/відгук) [18].

Для відкритої автентифікації: клієнт посилає серверу пароль, який порівнюється з еталоном, і на основі цього здійснюється висновок про дозвіл чи заборону доступу. Такий вид автентифікації застосовується рідко [18].

Схема запит/відгук є більш розповсюдженіша, тоді клієнт надсилає серверу запит на автентифікацію, де сервер повертає випадковий відгук. Клієнт знімає зі свого пароля хеш, зашифровує ним відгук та передає його серверу. У свою чергу, сервер порівнює отриманий результат з відповіддю клієнта, за умови співпадіння автентифікація успішна [18].

Автентифікація клієнтів та серверів VPN, L2TP поверх IPSec застосовує локальні сертифікати, які отримуються служби сертифікації. Клієнт та сервер обмінюються сертифікатами та створюють захищене з’єднання ESP SA. Тоді, L2TP завершає процес автентифікації комп’ютера та

здійснює автентифікацію користувача, у такому випадку використовується будь-який протокол. Це є безпечно, і зашифровує всю сесію. Здійснення автентифікації користувача за допомогою MSCHAP, це застосовує різні ключі шифрування для автентифікації комп'ютера та користувача, зможе посилити захист [1].

❖ Шифрування – гарантує захист даних при пересиланні через Internet.

Наразі підтримуються методи шифрування [1]:

• Протокол шифрування MPPE (Microsoft Point-to-Point Encryption), сумісний тільки з MSCHAP (версії 1 і 2);

• Протокол EAP-TLS, автоматично обирає довжину ключа зашифрування при узгодженні параметрів між клієнтом та сервером.

MPPE підтримує роботу з ключами, які мають довжину 40, 56 чи 128 біт [1].

Застарілі версії ОС Windows підтримують шифрування лише з довжиною ключа 40 біт, тому у змішаному середовищі ОС Windows варто обрати мінімальну довжину ключа [1].

PPTP змінює значення ключа шифрування після кожного окремо прийнятого пакету. Протокол MMPE з початку був розроблений для каналів зв'язку точка-точка, у таких пакетах передаються послідовно та втрата даних низька. У такому випадку значення ключа для чергового пакету залежить від результатів розшифрування попереднього пакета. При побудові віртуальних мереж через мережі загального доступу таких умов дотримуватися складно, пакети можуть надходити у хаотичній послідовності, а PPTP застосовується для зміни ключа шифрування. Що дозволяє здійснити розшифрування незалежно від попередніх прийнятих пакетів [1].

Тому, послідовність «унелювання + автентифікація + зашифрування» дозволяє передати дані між двома точками через мережу загального користування, моделюючи роботу приватної мережі [1].

Також, VPN-з'єднання застосовує системи адресації, прийнятої у

локальній мережі [1].

Реалізація VPN представляється як у локальній обчислювальній мережі організації розміщується VPN сервер. Віддалений користувач із застосуванням клієнтського ПЗ, VPN ініціює процедуру зв'язку з сервером. Здійснюється автентифікація користувача, як вступна фаза – встановлення VPN-з'єднання. У випадку підтвердження повноважень настає наступна фаза – між клієнтом та сервером – погодження деталей забезпечення безпеки з'єднання. Далі здійснюється VPN-з'єднання, це забезпечує обмін інформацією між клієнтом та сервером у формі, тоді пакет з даними здійснюється через процедури зашифрування/розшифрування та перевірки цілісності автентифікації даних [7].

Глобальною проблемою мереж VPN є відсутність встановлених стандартів автентифікації та обміну зашифрованої інформації. Проблема тягне за собою сповільнення розповсюдження VPN, користуючись розробками різних виробників, і це ускладнений процес об'єднання мереж компаній-партнерів [7].

VPN розгортають на рівнях не вище мережевого. Застосуючи криптографію на таких рівнях надає застосовувати транспортні протоколи (TCP, UDP) [7].

Для створення віртуальної мережі застосовується інкапсуляція протоколу PPP в будь-який інший протокол. То даний спосіб використовує реалізацію PPTP чи Ethernet (PPPoE). Технологія VPN використовує не лише для формування приватних мереж, але надання виходу в Інтернет [7].

При належному рівні застосування одного ПЗ мережа VPN може забезпечити високий рівень шифрування переданої інформації. А за умови правильного налаштування та експлуатації всіх компонентів, технологія VPN забезпечує анонімність в мережі [7].

1.5 Висновки до першого розділу

У процесі підготовки першого розділу кваліфікаційної роботи було

проаналізовано загальні характеристики VPN, протоколи VPN, функції та компоненти VPN, а також визначено мережі VPN та проблеми їх захисту.

Протоколи, які наразі використовуються: IPSec, PPTP, L2F, L2TP, IKE, LCP, PPP, IPsec, OpenVPN, EAP, EAP-TLS, MSCHAP, CHAP, SPAP, PAP.

Структура VPN містить два рівні:

- Внутрішня мережа.
- Зовнішня мережа.

Захист інформації у мережі VPN ґрунтується на кількох методах, які використовуються для реалізації заходів безпеки в інформаційних мережах:

- ❖ Тунелювання.
- ❖ Автентифікація.
- ❖ Шифрування.

У ході аналізу проблем ІБ у локальних чи глобальних мережах, де є VPN, то варто робити висновки, що дані системи мають забезпечувати виявлення внутрішніх та зовнішніх загроз та вторгнень, фільтрація зовнішнього трафіку, контроль застосування корпоративних мережевих ресурсів та запобігання НСД. Вхідними даними є інформація щодо структури та характеристиках трафіку, це може надати можливість побудувати набір правил, котрі класифікують нормальні чи аномальні компоненти трафіку.

Тоді, можна отримати гарантований захист мереж завдяки швидкого реагування на набір відомих загроз та аномальні ситуації, за рахунок ідентифікації функціонуючих процесів та керування ними для забезпечення доступності інформаційних сервісів.

РОЗДІЛ 2 ДОПУСТИМІ КОНЦЕПЦІЇ ТА КОНФІГУРАЦІЇ ДЛЯ ПОБУДОВИ ЗАХИЩЕННОЇ МЕРЕЖІ VPN

2.1 Способи захисту каналів корпоративних мереж на базі VPN рішень

Корпоративна мережа (КМ) – сукупність мереж, служб передачі даних, котра призначена для надання одного захищеного мережного простору, який обмежується рамками організації певного кола користувачів [23].

КМ включає [23]:

1. Корпоративний сервер баз даних;
2. Електронний документообіг;
3. Доступ в мережу Інтернет;
4. Апаратний та програмний захист інформації;
5. Відеоконференцзв’язок;
6. Корпоративна електронна пошта;
7. Корпоративна IP-телефонія.

Особливостями КМ є [23]:

1. Застосування інструментарію для роботи при передачі даних загального користування.
2. Доступ до інформації надається певному колу осіб.
3. Циркуляція інформації трьох типів: офіційна, проектна/групова та неофіційна.
4. Наявність єдиної системи управління корпоративною мережею.

КМ надає можливість ефективно об’єднувати територіально виокремлені підрозділи компанії [23].

Єдина мережа надає перелік можливостей [23]:

- доступ до робочих місць у режимі online;
- віддалений доступ до сервісів КМ;
- доступ до мережі Інтернет;
- розсилання даних за адресами адресами.

Так КМ надає можливість отримувати доступ до Інтернету з єдиного

серверу та розподіляти канали у компанії, це може знизить витрати на Інтернет [23].

2.1.1 Класифікаційні ознаки корпоративних мереж

КМ властиві функціональні елементи [42]:

Робочі місця користувачів знаходяться:

- в одному приміщенні;
- у будь-якому місці.

Інформаційні сервери організації мають за мету зберігати, обробляти дані, і при цьому можуть знаходитися як в межах організації так і поза нею. Засоби телекомунікації, котрі взаємодіють між собою робочих станцій та між інформаційними серверами.

Засоби телекомунікації організації можуть бути [42]:

- виділеними;
- загального призначення.

Найчастіше зустрічаються останні.

Телеслужби [42].

У рамках організації інформаційний вплив реалізується в рамках однієї чи кількох служб, які забезпечуються засобами телекомунікації [42].

1. Система управління ефективністю функціонування КМ.

У залежності від реалізованого набору служб у КМ мають застосовуватися засоби керування мережею (засоби маршрутизації та комутації, засоби адміністрування). Управління елементами КМ виділяються:

- керовані в рамках корпорації функціональні елементи;
- некеровані в рамках корпорації функціональні елементи, що є приналежністю використовуваних корпорацією підмереж загального призначення.

2. Система управління безпекою функціонування КМ.

У КМ мають бути реалізовані необхідні мережні служби безпеки, які мають застосовуватися як відповідні засоби безпеки.

3. Система забезпечення надійності КМ.

Мають бути передбачені засоби забезпечення працездатності всієї мережі або її фрагментів при відмовах елементів КМ.

4. Система діагностики й контролю.

У КМ ають бути передбачені засоби контролю працездатності окремих функціональних елементів (система збору інформації про відмови й збої та надання її системам забезпечення живучості, керування ефективністю функціонування, керування безпекою). Для КМ мають бути розроблені засоби діагностики, реалізовані як у процесі функціонування мережі.

5. Система експлуатації.

КМ мають план процесу розвитку, котрі визначають функціональні можливості, котрі закладаються у ній.

Узагальнюючи КМ, отримаємо класифікацію:

- з набору функціональних елементів;
- з ієрархії керування;
- з набору поєднуваних у рамках КМ підмереж загального користування;
- з набору реалізованих у рамках КМ телеслужб.

Безпека КМ є надважливими для успіху будь-якої організації.

Великі організації фундаментуються на власних КМ для надання безпечного постійного доступу до інформації організації, застосуванням та електронній пошті [42].

Повний розв’язок для захисту КМ надає організації зберегти стабільність у роботі, стійкість до атак, захист конфіденційність даних компанії та забезпечить безперервний цілодобовий доступ до них [42].

Задача КМ організації у межах одного офісу досить просто вирішується. Але сучасна інфраструктура корпорацій найчастіше знаходиться в рамках не однієї будівлі, наприклад використовуються дата-центри, які можуть знаходитися географічно віддалено від організації, тому процес формування КМ досить складне завдання [42].

У зв’язку з розвитком Internet та колективним доступом до інформації у режимі реального часу, це стало поштовхом до розвитку КМ, користувачі отримали дешеві та доступні канали Internet. Організації мають застосовувати захищені канали для передачі критичної комерційної та управлінської інформації [42].

2.1.2 Функції й компоненти мережі VPN

Захищена віртуальна мережа VPN – об’єднання локальних мереж та окремих комп’ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну КМ, це забезпечить безпеку циркулюючих даних [11].

При підключенні локальної КМ до відкритої мережі виникають загрози безпеці двох основних типів [11]:

- НСД до корпоративних даних у процесі передачі відкритими каналами;
- НСД до внутрішніх ресурсів локальної КМ, який отриманий зловмисником в результаті НСД до мережі.

Сучасні КМ являють собою складні системи, котрі являють собою кілька компонентів. Компоненти виділяють різні комп’ютери, системне та прикладне ПЗ таких комп’ютерів, мережеві адаптери, комутатори, маршрутизатори та поєднання систем. Застосування Інтернету та ІТ призводить до змін в обчислювальних мереж. Раніше Інтернет застосувався як джерело передачі, тоді як наразі це засіб інтерактивної взаємодії людей та засіб ведення ділових операції організацій [11].

Популярність IP-технологій пояснюється перевагами [11]:

- Легкість принципів технології (відкритість, котра виражається вільним обговоренням, дослідженням та тестуванням нових протоколів стеку TCP/IP). Відкритість технології надає можливість забезпечити відносну легкість інтеграції у IP-мережі інших технологій, це значно збільшить область використання Інтернету.

- Масштабованість (продумана при розробці Інтернету). Ієрархічно організований стек TCP/IP надає можливість наростити мережу організації у досить великих межах.

Переваги надали поштовх для застосування IP-технологій, які призводять до успіху Інтернету, є перспективними для внутрішніх мереж організації – мереж інтранет (Intranet) [11].

КМ (інтранет) – це мережа, де використовуються програмні кошти, підставу на стеку протоколів TCP/IP [11].

Екстранет-мережа – інтранет-мережа, яка підключаєтеся до Інтернету, але доступ до її ресурсів певної категорії користувачів, котра наділяється відповідними повноваженнями [11].

Мережі являють собою локальні мережі, які підключені до Інтернету та використовують Web-технології, тому їх можна назвати КМ [11].

Особливостями КМ – глобальність зв'язків, масштабованість та гетерогенність – представляється як підвищена небезпека за виконанням функціональних завдань. Протоколи сімейства TCP/IP розробляються досить давно, тоді як проблеми не були настільки актуальними, так як вони розроблялися як функціональні, котрі допомагають поширюватись стеку TCP/IP на різних комп'ютерних платформах. При застосуванні Інтернету у розпорядженні зловмисників є засоби та методи для проникнення у КМ [27].

Зі зростанням кількості хостів, котрі підключені до мережі Інтернет, зі збільшенням компаній, застосовуються технології Інтернету для ведення власного бізнесу, кількість інцидентів збільшилося, які пов'язуються з інформаційною безпекою (ІБ). Дані CERT (Computer Emergency Response Team) виявляють вразливості та кількість зареєстрованих інцидентів, які постійно збільшуються [27].

Вразливості інформаційної системи – характеристики, які застосовуються порушниками для реалізації загрози. Загрози інформаційної системи – потенційно можливі події, дії, процеси чи явища, які викликають заподіяння шкоди ресурсів системи [27].

Види загроз – це параметри, котрі визначають направленість захисту інформації [27].

2.1.3 Методи реалізації VPN мереж

VPN ґрунтується на трьох методах реалізації [10]:

- Туннелювання.

Забезпечує передачу даних між двома точками. Транспортне середовище тунелю перехоплює пакети обраного мережевого протоколу біля входу в тунель та без модифікації доставляє їх до виходу. Побудови тунелю достатньо для поєднання двох мережевих вузла так, щоб з точки зору працюючого на них ПЗ вони виглядають підключеними до локальної мережі.

Варто пам’ятати, що дані, котрі проходять через проміжні вузли маршрутизаторів відкритої публічної мережі Даному стану притаманно дві проблеми. Тобто, для автентифікації користувачів використовуються протоколи MSCHAP версії 2 та EAP-TLS, так як вони забезпечують взаємну автентифікацію, а саме VPN сервер та клієнт ідентифікують один одного. У іншому випадку лише сервер здійснює автентифікацію клієнтів [10].

PPTP – забезпечує високий рівень безпеки, а L2TP – поверх IPSec надійніше, який забезпечує автентифікацію на рівнях «користувач» та «комп’ютер», окрім цього здійснює автентифікацію та шифрування даних.

- Автентифікація.

Реалізується чи відритим текстом чи за схемою запит/відгук. Відкрита автентифікація не є поширеною.

Схема запит/відгук досить розповсюджена, яка виглядає наступним чином [10]:

- клієнт посилає серверу запит на автентифікацію;
- сервер повертає випадковий відгук;
- клієнт знімає зі свого пароля хеш, шифрує їм відгук і передає його серверу;

- те ж саме проробляє і серверу та порівнює отриманий результат з відповіддю клієнта;
- якщо зашифрований відгук збігається, автентифікація вважається успішною.

В першу чергу, автентифікація клієнтів та серверів VPN, L2TP поверх IPSec застосовує локальні сертифікати, які одержуються від служби сертифікації. Клієнт та сервер обмінюються сертифікатами та формують захищене з'єднання ESP SA.

L2TP завершує процес автентифікації комп'ютеру, який здійснюється на рівні користувача. Варто використовувати будь-який протокол. Здійснення автентифікації користувача завдяки MSCHAP, це дає можливість застосовувати різні ключі шифрування для автентифікації комп'ютера та користувача, це надає змогу посилити захист.

- Шифрування.

Здійснюючи шифрування не можна отримати доступ до даних при пересиланні через Internet. Наразі використовуються два методи шифрування:

Протокол шифрування MPPE та TLS вміють автоматично обирати довжину ключа шифрування. Перший розробляється для каналів зв'язку точка-точка, де пакети передаються послідовно, але втрата даних низька. У даному випадку значення ключа для чергового пакета залежить від результатів розшифрування попереднього пакету. У віртуальних мереж через мережі загального доступу таких умов дотримуватися важко, пакети до отримувача можуть доходити у хаотичній послідовності. А PPTP застосовує для зміни ключа шифрування порядкові номери пакетів для розшифрування незалежно від раніше отриманих пакетів [10].

Тому, зв'язка «туннелювання+автентифікація+шифрування» дозволяють передавати дані між двома точками через мережу загального користування, моделюючи роботу локальної мережі. Таким чином, розглянуті засоби надають можливість побудувати віртуальну приватну

мережу.

Додатковим приємним ефектом VPN-з'єднання є можливість застосування системи адресації, прийнятої у локальній мережі Реалізація віртуальної приватної мережі на практиці являє собою як встановлення серверу VPN. Віддалений користувач із застосуванням клієнтського ПЗ VPN ініціює процедуру з'єднання з сервером [10].

Здійснюється автентифікація користувача – встановлення VPN-з'єднання, якщо успішно, то між клієнтом та сервером здійснюється погодження деталей забезпечення безпеки з'єднання. Далі, здійснюється VPN з'єднання, котре забезпечує обмін інформацією між клієнтом та сервером. У такому випадку, головна проблема – відсутність фіксованих стандартів автентифікації та обміну шифрованої інформації. Дані стандарти знаходяться процесі розробки, чи плануються для розробки. Така проблема може призвести до повільного застосування в організаціях VPN, так як це є не обов'язкове, а змусити організації до їх використання не можна [10].

2.2 Концепція побудови віртуальних захищених мереж VPN

У основі побудови VPN є ідея, де два вузли, які слід обміняти між ними, тоді будується віртуальний тунель для забезпечення конфіденційності та цілісності інформації, котрий передається відкритими мережами. Доступ варто ускладненими для всіх учасників та сторонніх осіб, які не є учасниками [29].

Перевагами для організації, які використовують дані віртуальні тунелі є економія фінансових коштів, так як немає потреби у побудові чи оренди виділених каналів зв'язку для формування власних intranet/extranet мереж та застосовуючи для цього дешеві Інтернет канали, надійність та швидкість передачі не втрачається. Економічна ефективність від інтеграції VPN технології стимулюють організації до активного їх впровадження [29].

2.2.1 Основні поняття і функції мережі VPN

Для під'єднання корпоративної локальної мережі до відкритої виникають загрози безпеки кількох типів [36]:

- НСД до внутрішніх ресурсів корпоративної локальної мережі, отримується шахраєм у результаті НСД до входу у мережу;
- НСД до корпоративних даних в процесі передачі відкритою мережею.

Забезпечення безпеки інформаційної взаємодії локальних мереж та окремих комп'ютерів відкритими каналами (у тому числі, Інтернет), може вирішити наступні задачі [36]:

- захист підключених до відкритих каналів зв'язку локальних мереж та окремих комп'ютерів від НСД;
- захист інформації у процесі передачі відкритими каналами зв'язку.

Для захисту локальних мереж та окремих комп'ютерів від НСД з боку зовнішнього середовища застосовується мережевий екран, котрі підтримують безпеку інформаційної взаємодії фільтруючи двосторонній потік повідомлень, здійснюючи функції посередництва при обміні інформації. Мережевий екран розташовується між локальною та відкритою мережею. Для захисту певного віддаленого комп'ютеру, підключеного до відкритої мережі встановлюється ПЗ мережевого екрану, саме він вважається персональним [36].

Захист інформації у процесі його передачі відкритими каналами ґрунтується на застосуванні віртуальних захищених мереж VPN. VPN – є об'єднанням локальних мереж та окремих комп'ютерів використовуючи відкрите зовнішнє середовище передачі інформації у єдину віртуальну корпоративну мережу, забезпечуючи безпеку циркулюючих даних. VPN будується на базі відкритих каналів зв'язку загальнодоступної мережі. Такі віртуальні захищені канали зв'язку є тунелями VPN. Мережа VPN дозволяє завдяки тунелів VPN поєднуючи центральний офіс, інші офіси, філії,

віддалені користувачі та передавати інформацію через Інтернет (Рис. 2.1) [36].

Тунель VPN поєднується завдяки проведенням через відкриту мережу, через яку передаються криптографічно захищені пакети даних віртуальної мережі. Захист інформації у процесі передачі тунелем VPN та ґрунтується [20]:

• на автентифікації взаємодіючих сторін;

• криптографічному закритті переданих даних;

• на перевірці достовірності та цілісності інформації, які доставляються.

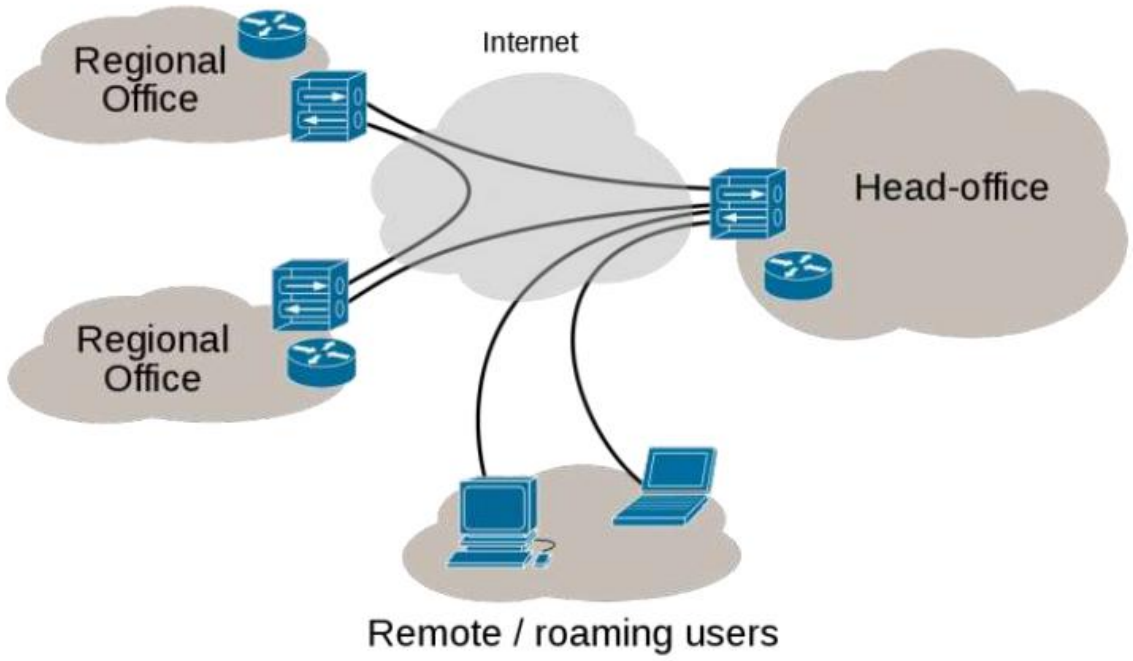


Рисунок 2.1 – Віртуальна захищена мережа VPN

Для даних функцій характеризується взаємозв’язок сторін. При реалізації застосовуються криптографічні методи захисту інформації. Ефективність для захисту здійснюється за рахунок спільного застосування симетричних та асиметричних криптографічних систем. Тунель, який формується облаштуваннями VPN, має певні властивості захищеної виділеної лінії, котра розгортається в рамках загальнодоступної мережі. Пристрої VPN мають певну роль VPN клієнта, VPN сервера чи шлюзу безпеки VPN [20].

VPN клієнт це програмний чи програмно-апаратний комплекс, котрий здійснюється на базі персонального комп'ютера. Мережеве ПЗ змінюється для виконання шифрування та автентифікації трафіку, даний пристрій обмінюється з іншими VPN клієнтами, VPN сервери чи шлюзи безпеки VPN. Реалізація VPN клієнта є програмне рішення, який доповнює стандартну ОС, – Windows 7/10 чи Unix [20].

VPN сервер може бути у вигляді ПЗ чи апаратно-програмного забезпечення, який встановлюється на комп'ютері, який здійснює функції сервера. VPN сервер здійснює захист серверів від НСД, організацію захищених з'єднань з окремими комп'ютерами та сегментами локальних мереж, які захищаються відповідними VPN продуктами. VPN сервер – функціональний аналог продукту VPN клієнт для серверних платформ. Відрізняється розширеними ресурсами для підтримки множинних з'єднань з VPN клієнтами. VPN сервер підтримується захищеними з'єднаннями з мобільними користувачами [20].

Шлюз безпеки VPN – цей мережевий пристрій, який має під'єднуватися до двох мереж та здійснити функції шифрування та автентифікації для численних хостів. Розміщується шлюз безпеки VPN для проходження трафіку, який призначається для внутрішньої корпоративної мережі. Адреса шлюзу безпеки VPN вказується як зовнішня адреса тунелює пакет, котрий входить, а внутрішня адреса пакету є адресою конкретного хосту позаду шлюзу. Шлюз безпеки VPN реалізується у вигляді окремого програмного рішення та апаратного пристрою, у вигляді маршрутизатора чи мережевого екрану, який наділений функціями VPN [20].

Відкрите зовнішнє середовище передачі інформації включає канали швидкісної передачі даних, котра застосовує мережу Інтернет, у якості яких застосовуються канали телефонної мережі. Ефективність VPN визначається мірою захищеності інформації, яка циркулює відкритими каналами зв'язку. Для безпечної передачі даних відкритими каналами зв'язку застосовується інкапсуляція та тунелювання. Завдяки методики тунелювання пакети даних

передаються загальнодоступною мережею. Між кожною парою «відправник – отримувач» встановлюється своєрідний тунель – логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого. Тунелювання інкапсулює, упаковує, передає порцію даних, разом зі службовими полями, у новий конверт. Пакет протоколу нижчого рівня розміщується у полі даних пакету протоколу більш високого чи такого ж рівня. Варто зауважити, що тунелювання як єдиний захист не є найкращим виходом з ситуації, тобто не захищає дані від НСД чи спотворення, але завдяки тунелюванню є можливість повного КЗІ (початкових пакетів), котрі інкапсулюються. Для забезпечення конфіденційності переданих даних, відправник зашифровує початкові пакети, пакує їх у зовнішній пакет з новим IP заголовком та надсилає транзитною мережею (Рис. 2.2) [29].

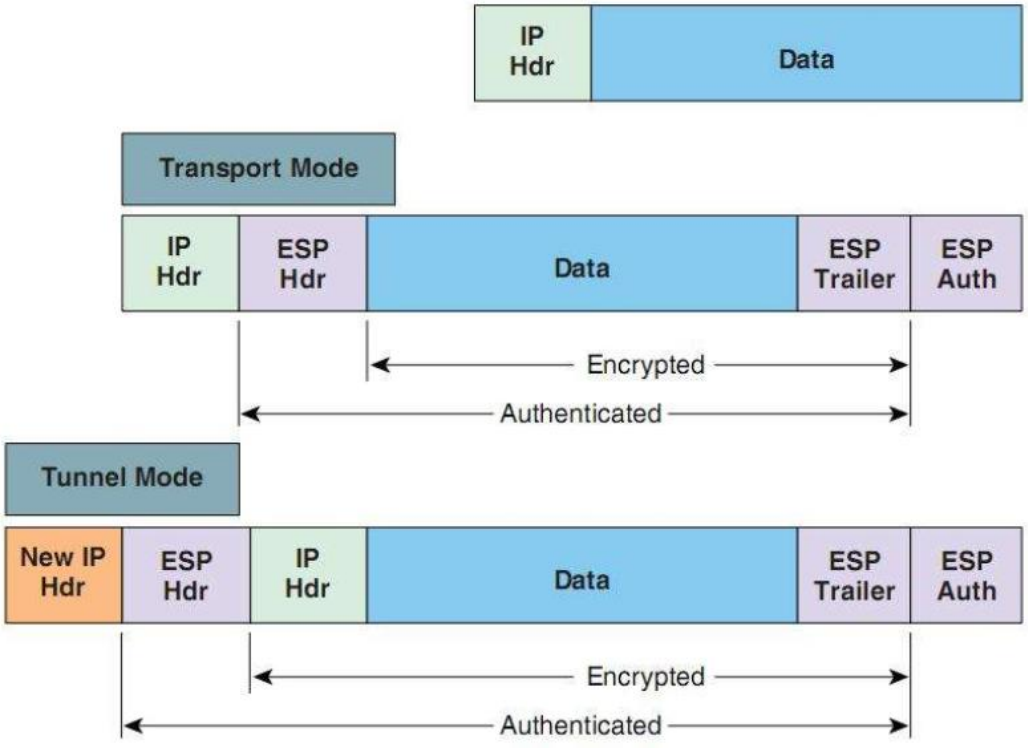


Рисунок 2.2 – Приклад пакету, підготовленого для тунелювання

Особливість технології тунелювання – дозволяє зашифровувати початковий пакет повністю, не лише поле даних. Деякі поля заголовка містять інформацію, котра потенційно може бути застосовано шахраєм. Із заголовку початкового пакету отримуються дані щодо внутрішньої структури мережі, інформація щодо кількості підмереж та вузлів, IP адреси. Зловмисник має використати дану інформацію при організації атак на КМ. Початковий

пакет із зашифрованим заголовком не застосовується для організації транспортування мережею [29].

Для захисту початкового пакету використовується інкапсуляція та тунелювання. Початковий пакет зашифровується повністю, далі зашифрований пакет розміщується у інший зовнішній пакет з відкритим заголовком. Для подальшого транспортування даних відкритою мережею застосовуються відкриті поля заголовку зовнішнього пакету [29].

Після доставки пакету витягається внутрішній початковий пакет, який розшифровується та використовується для відновлення та подальшої передачі внутрішньою мережею (Рис.2.3) [29].

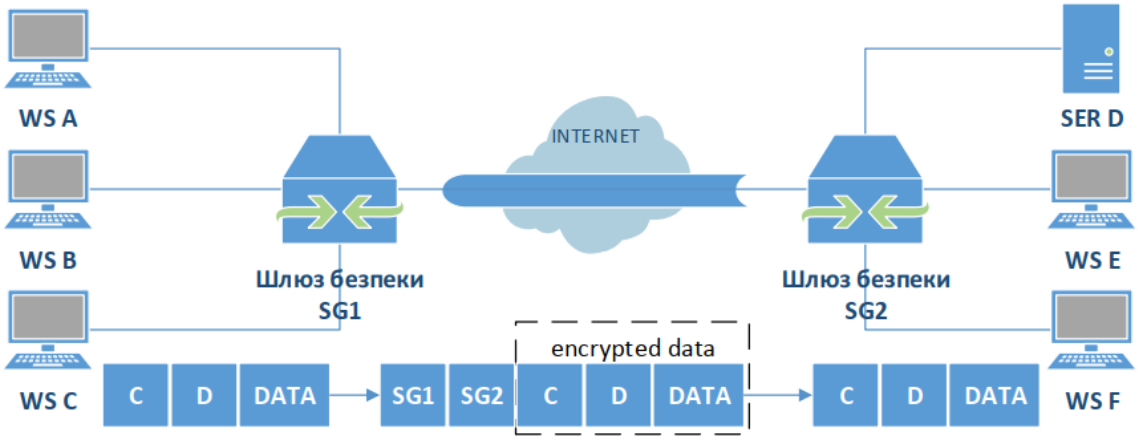


Рисунок 2.3 – Схема віртуального захищеного тунелю

Тунелювання застосовується для захисту конфіденційності, цілісності та автентичності даних пакету, при цьому КЕП розповсюджується на всі поля пакету. На останок до приховування мережевої структури між двома точками, тунелювання запобігає можливому конфлікту адрес між двома локальними мережами. При формуванні локальної мережі, не пов’язаної з Internet, компанія використовує будь-які IP адреси для своїх мережевих пристроїв та комп’ютерів. При об’єднанні раніше ізольованих мереж ці адреси можуть конфліктувати один з одним та з адресами, які вже використовують у мережі Internet [29].

Інкапсуляція пакетів вирішує проблему, так як дозволяє приховати первинні адреси та додати нові (унікальні), які далі можуть застосовувати для пересилки даних мережами, які розділяються. Також, варто налагодити IP

адреси та інші параметри для мобільних користувачів, які підключаються до локальної мережі [40].

Механізм тунелювання використовується у різних протоколах формування захищеного каналу. Тунель формується лише на ділянці відкритої мережі, де існує загроза порушення конфіденційності та цілісності даних, між точкою входу у відкритий Інтернет та точкою входу у КМ. При цьому для зовнішніх пакетів застосовуються адреси пограничних маршрутизаторів, встановлених у двох точках, внутрішні адреси кінцевих вузлів складаються у внутрішніх початкових пакетах у захищеному вигляді. Варто зауважити, що сам механізм тунелювання не залежить від способу застосування тунелювання. Тунелювання має використовуватися для забезпечення конфіденційності та цілісності переданої порції даних, організації переходу між мережами з різними протоколами [40].

Тунелювання може організувати передачу пакетів одного протоколу у логічному середовищі, який застосовує інший протокол. У результаті з’являється можливість вирішення проблеми взаємодії кількох різних мереж, починаючи із забезпечення цілісності та конфіденційності переданих даних та завершуючи подолання невідповідностей зовнішніх протоколів чи схем адресації. Реалізація механізму тунелювання представляється як результат роботи протоколів трьох типів: протокол «пасажиру», протоколу, який «несе» та протокол тунелювання [40].

Тунелі VPN формуються для різних типів кінцевих користувачів – це локальна мережа LAN з шлюзом безпеки, чи окремі комп’ютери видалених та мобільних користувачів. Для формування віртуальної приватної мережі великої організації слід застосовувати VPN шлюзи, VPN сервери та VPN клієнти. VPN шлюзи застосовують для захисту локальних мереж організації, VPN сервери та VPN клієнти застосовуються для організації захищених з’єднань видалених та мобільних користувачів з КМ через Інтернет [40].

2.2.2 Варіанти побудови віртуальних захищених каналів

Безпека інформаційного обміну забезпечується для об'єднання локальних мереж, у випадку доступу до локальних мереж видалених чи мобільних користувачів. При проектуванні VPN розподіляються на дві схеми віртуального захищеного каналу між [40]:

1) локальними мережами (канал ЛВСЛВС);

2) вузлом і локальною мережею (Рис. 2.4).

Схема 1 – надає можливість замінити дорогі виділені лінії між окремими організаціями та сформувати доступні захищені канали між ними. У такому випадку, шлюз безпеки служить інтерфейсом між тунелем та локальною мережею, тоді користувачі локальних мереж застосовують тунель для спілкування один з одним. Компанії застосовують вид VPN як заміну чи доповнення з'єднань глобальної мережі, як frame relay [40].

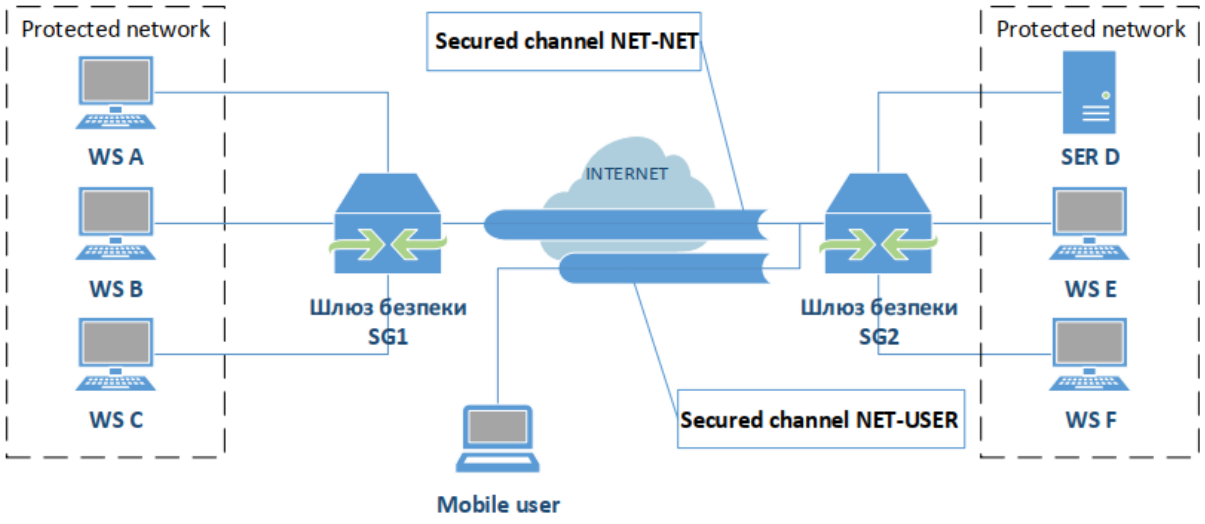


Рисунок 2.4 – Віртуальні захищені канали типу Мережа – Мережа, Клієнт – Клієнт

Схема 2 – захищені канали VPN призначаються для встановлення з'єднань з віддаленими чи мобільними користувачами. Формування тунелю ініціюється клієнтом. Для зв'язку з шлюзом, який захищає віддалену мережу, і саме він запускає на своєму комп'ютері спеціальне ПЗ для користувача.

Такий вид VPN замінює собою комутовані з'єднання та може застосовуватися разом з традиційними методами віддаленого доступу [40].

Варіанти схем віртуальних захищених каналів, де формується

віртуальний захищений канал, який належить кінцевій чи проміжній точці потоку повідомлень, які захищаються [40].

З боку забезпечення ІБ, то кращий варіант це тоді, коли кінцеві точки захищеного тунелю співпадають з кінцевими точками потоку повідомлень, які захищаються. Тоді забезпечується захищеність каналу впродовж шляху дотримання пакетів повідомлень. Варіант веде до децентралізації керування та надмірності ресурсних витрат. Варто встановити засоби формування VPN на кожному клієнтському комп'ютері локальної мережі. Це ускладнить централізоване керування доступом до комп'ютерних ресурсів та не завжди виправдано з боку фінансів. Адміністрування кожного клієнтського комп'ютера за для конфігурації засобів захисту, що може бути складним у великій мережі [40].

Всередині локальної мережі, котра входить у віртуальну мережу, не потребує захисту трафіку, і в цьому випадку у якості кінцевої точки захищеного тунелю обирається мережевий екран чи маршрутизатор даної локальної мережі. Потік повідомлень локальної мережі має бути захищений, у такому випадку, у якості кінцевої точки тунелю в має бути комп'ютер, котрий бере участь у захищеній взаємодії. При доступі до локальної мережі віддаленого користувача комп'ютер такого користувача буде кінцевою точкою віртуального захищеного каналу [40].

Часто зустрічається захищений тунель лише усередині відкритої мережі з комутацією пакетів. Він є зручним, але не дуже безпечним. Кінцевою точкою тунелю є провайдер Інтернету чи пограничні маршрутизатори локальної мережі. При об'єднанні локальних мереж тунель формується лише між пограничними провайдерами Інтернету, чи маршрутизаторами локальної мережі. При віддаленому доступі до локальної мережі тунель формується між сервером віддаленого доступу провайдера Інтернету, пограничним провайдером Інтернету чи маршрутизатором локальної мережі. Будуються віртуальні корпоративні мережі, які масштабуються та управляються. Сформовані захищені тунелі є прозорими

для клієнтських комп’ютерів та серверів локальної мережі, які входять у віртуальну мережу. ПЗ даних вузлів залишаються без змін, однак варіант характеризується досить низькою безпекою інформаційної взаємодії, так як частково трафік проходить відкритими каналами зв’язку у незахищеному виді. При створенні та експлуатації VPN, провайдером виступає ISP, у такому випадку VPN будується на шлюзах, але у такому випадку з’являються проблеми довіри до провайдера та постійної оплати його послуг [12].

Захищений тунель формується компонентами віртуальної мережі, які функціонують, де формується тунель, такі компоненти мають назву ініціатор та термінатор тунелю [12].

Ініціатор тунелю інкапсулює початковий пакет в новий пакет, який містить заголовок з інформацією щодо відправника та отримувача. Пакети, котрі інкапсулюються, можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, які не маршрутизуються. Всі пакети, які передаються тунелю, це є пакети IP. Маршрут між ініціатором та термінатором тунелю визначає звичайну мережу IP, які маршрутизуються, відмінною від Інтернету [12].

Ініціювати та розривати тунель мають право різні мережеві пристрої та ПЗ. Ініціатор може бути і маршрутизатор локальної мережі, який наділений відповідними функціональними можливостями. Тунель завершається комутатором мережі чи шлюзом провайдера послуг [12].

Термінатор тунелю здійснює процес, який є зворотний до інкапсуляції. Саме він видаляє нові заголовки та направляє окремо, кожен пакет отримувачу в локальній мережі [12].

Конфіденційність пакетів здійснюється шляхом шифрування, цілісність та достовірність здійснюється у процесі формування КЕП. Є безліч методів та алгоритмів КЗІ, ініціатор та термінатор тунелю погоджується один з одним та застосовує одні й ті ж методи та алгоритми захисту. Для забезпечення розшифрування даних та перевірки КЕП при прийомі ініціатору та термінатор тунелю має підтримувати функції безпечного обміну ключами.

Кінцеві сторони інформаційної взаємодії мають здійснити автентифікацію, для гарантії формування тунелів VPN лише між уповноваженими користувачами [12].

Існуюча мережева інфраструктура організації має бути підготовлена до застосування VPN завдяки апаратного та ПЗ.

2.2.3 Засоби забезпечення безпеки VPN

При побудові захищеної віртуальної мережі VPN в першу чергу є вирішення задачі – забезпечення ІБ. Відповідно визначенням, які вказуються у різних нормативно-правових актах, ІБ характеризується: конфіденційністю, цілісністю та доступністю. Що стосується задач VPN критерії безпеки даних визначаються як [15]:

• конфіденційність – інформація, яка передається доступна лише відправнику та отримувачу. Конфіденційність забезпечується за допомогою різних методів і алгоритмів симетричного і асиметричного шифрування.

• цілісність – інформація, яка має бути доставлена без модифікацій та пошкоджень. Цілісність переданих даних зазвичай досягається завдяки різних варіантів технології КЕП, які ґрунтуються на асиметричних методах шифрування та односторонніх функціях.

• доступність – інформація, має бути доступна лише легальним користувачам.

Автентифікація здійснюється на основі багаторазових та одноразових паролів, кваліфікованих сертифікатів, смарткарт, протоколів суворої автентифікації, який забезпечує встановлення VPN з’єднань лише між легальними користувачами та запобігає доступу до засобів VPN небажаних осіб [15].

Авторизація надає абонентам доступ лише тим, які довели свою автентичність. Авторизація та керування доступом реалізуються найчастіше одними й тими ж засобами [15].

Для забезпечення безпеки переданих даних віртуальними захищеними

мережами вирішуються наступними задачами [15]:

• взаємна автентифікація абонентів при встановленні з'єднання. Автентифікація абонентів здійснюється тоді, коли дозволяється вхід для легальних користувачів та запобігає доступу до мережі небажаних осіб.

• забезпечення конфіденційності, цілісності та автентичності переданої інформації. Завдання забезпечення конфіденційності інформації полягає в захисті переданих даних від НСД до читання та копіювання. Основний засіб забезпечення конфіденційності інформації є шифрування.

• авторизація та керування доступом. Компонент безпеки VPN це гарантія доступу до комп'ютерних сервісів для авторизованих користувачів, а для неавторизованих – ні.

При побудові програмних засобів авторизації застосовуються централізована (реалізує принцип єдиного входу) та децентралізована схема авторизації [15].

Часто зустрічається ролеве керування доступом, яке покращує керованість систем. Тобто, розподіляються між користувачами системі чи сервісів ролі, які наділені певними правами, у користувача може бути кілька ролей [15].

• безпека периметра мережі та виявлення вторгнень. Жорсткий контроль доступу до сервісів та ресурсів мережі, які захищаються, це є важливою функцією мережі. Застосування засобів безпеки, як мережевий екран, системи виявлення вторгнень та аудиту безпеки, антивіруси.

Важливим аспектом є мережевий екран, система виявлення вторгнень IDS (Intuasion Detection System) та системи аналізу захищеності.

• керування безпекою мережі. Мережі VPN інтегрують мережеві пристрої та сервіси управління безпекою та пропускною спроможністю. Для організацій важливим є цілісне управління даними пристроями та сервісами через інфраструктуру VPN, включаючи користувачів віддаленого доступу та засобів extranet. Система управління мережею включає набір засобів для управління політиками безпеки, пристроями та сервісами VPN будь-якого

масштабу.

2.3 Конфігурація VPN для безпечної передачі даних

Прогрес із застосування Інтернету для безпечної передачі даних і далі буде підвищуватися та покращуватися, так як буде збільшуватися кількість користувачів мережі, тому всі сфери людської діяльності змушують переосмислювати пріоритети в бізнесі, вимоги та потреби сучасного суспільства [30].

Рівень інформативності суспільства характеризується володіння певною інформацією чи знаннями. Захист інформації у процесі передачі відкритими каналами ґрунтується на основі здійснення функцій [30]:

- автентифікації взаємодіючих сторін;
- криптографічному закритті даних, що передаються;
- перевірці достовірності та цілісності доставленої інформації.

Для вищеописаних функцій характерний взаємозв’язок «один до одного», реалізація ґрунтується на використанні КЗІ, ефективність яких забезпечується за рахунок спільного застосування симетричних та асиметричних криптографічних систем [30].

Потреба у безпечній та дешевій передачі даних через засоби загального користування. Завдяки даним перевагам VPN є об’єктом підвищеного інтересу сфери ІТ. Ефективність VPN визначається ступенем захищеності інформації, що циркулює відкритими каналами зв’язку. Захист даних в процесі передачі ґрунтується на побудові захищених віртуальних каналів зв’язку це є тунелі VPN [30].

Тунелювання не захищає дані від НСД чи модифікації, але забезпечує можливість повного КЗІ, котрі інкапсулюються. Для забезпечення конфіденційності передачі даних, та надсилає відправнику зашифровані початкові пакети, запаковує їх у зовнішній пакет з новим IP заголовком та відправляє транзитною мережею. У кінці захищеного каналу із зовнішнього пакету вилучаються та розшифровуються внутрішні початкові пакети та

застосовують відновлений заголовок щодо подальшої передачі внутрішньою мережею. Тунелювання застосовується для забезпечення конфіденційності цілісності та автентичності, де можна застосувати КЕП, окрім цього, вирішуються проблеми переходів між мережами з різними протоколами [30].

Організовується взаємодія кількох різнотипних мереж, для забезпечення цілісності та конфіденційності даних, які передаються та завершують подолання невідповідностей зовнішніх протоколів чи схем адресації. Для тунелювання застосовуються протоколи канального рівня PPTP і L2TP, а також протокол мережевого рівня IPSec [30].

Безпека інформаційного обміну забезпечує об'єднання локальних мереж та доступ до локальних мереж виділених або мобільних користувачів. При проектуванні VPN розглядаються схеми [30]:

- «мережа-мережа». Заміна виділених ліній між офісами, які віддалені один від одного та сформувати захищені канали між ними. Де шлюз служить інтерфейсом між тунелем та локальною мережею; користувачі локальних мереж застосовують тунель для спілкування один з одним. Такий вид VPN застосовують організації як заміну чи доповнення до з'єднань глобальної мережі.
- «користувач-мережа». Встановлення з'єднань з віддаленими чи мобільними користувачами. Створення тунелю ініціює клієнт для зв'язку зі шлюзом, який захищає віддалену мережу, запускаючи спеціальне ПЗ користувача. Даний вид VPN замінює комутовані з'єднання та може застосовуватися разом з методами віддаленого доступу.

Для забезпечення безпеки даних, передаються у VPN, які вирішують задачі мережевої безпеки [14]:

- взаємна автентифікація користувачів при встановленні з'єднання;
- забезпечення конфіденційності, цілісності й автентичності інформації, що передається;
- авторизація та управління доступом.

У залежності від функцій мережі, VPN може будуватися із

застосуванням можливих рішень для забезпечення найкращого рівня ЗІ з найменшими затратами. Перед адміністрацією ІТ-підрозділів виникає проблема: вибір протоколів для оптимальної побудови такої мережі, так як підходи мають свої плюси та мінуси. У рамках дослідження аналіз дозволяє порівняти ряд протоколів, визначаючи їх переваги та недоліки та здійснити вибір оптимального рішення для побудови захищеної VPN мережі [14].

Порівняльний аналіз протоколів L2TP, IPSec та SSL, котрі претендують для розв'язку проблем, які стосуються безпеки в VPN мають певні результати [14]:

- переваги L2TP ґрунтуються на незалежності від транспортного рівня, який надає можливість застосовувати його в гетерогенних мережах;
- через «канальну природу» протоколу складно гарантувати, зможуть підтримувати мережі та проміжні маршрутизатори;
- IPSec забезпечує автентифікацію, перевірку цілісності та шифрування повідомлень на рівні кожного пакету;
- протокол має бути прозорим;
- робота між мережами з протоколами IPv4 та IPv6;
- важливе встановлення VPN клієнта на робочу станцію користувача та надсилання досить великого об'єму службової інформації знизить швидкість обміну даними на низькошвидкісних каналах зв'язку;
- SSL забезпечує захист даних між сервісними та транспортними протоколами, які у зашифрованому вигляді передаються із застосуванням асиметричних ключів для закодування/розкодування інформації;
- протокол здійснює «розпізнавання» серверу та клієнта;
- характеризується відсутністю завищеного навантаження на сервер;
- замість VPN-клієнта застосовується браузер.

2.4 Висновки до другого розділу

У ході підготовки другого розділу кваліфікаційного розділу було

проаналізовано способи захисту каналів КМ на базі VPN рішень, досліджено концепцію побудови віртуальних захищених мереж VPN та можливі конфігурації VPN для безпечної передачі даних.

Ідея побудови власних VPN є актуальною, за при поєднанні кількох локальних мереж у організаціях для формування власної мережі це є досить вартісним процесом та досить довгим, однак варто забезпечити захист переданих між сегментами мережі даних. Так як, далеко не завжди дозволено передавати дані загальнодоступними мережами у відкритому вигляді. Однак, захищати лише зв'язки між окремими комп'ютерами з різних сегментів, за умови того, що корпоративна політика організація вимагає забезпечення безпеки великої кількості інформації, то здійснювати захист кожного окремого каналу та комп'ютеру є досить складним процесом. При захисті окремих каналів інфраструктури КМ залишається прозорою для зовнішнього спостерігача. Для розв'язку проблем використовується архітектура VPN, а при застосуванні весь потік інформації, передається загальнодоступними мережами та шифрується.

Система управління ІБ мережі забезпечує наскрізну безпеку VPN. Для забезпечення високого рівня безпеки та управління VPN, також системи розподілу криптографічних ключів та сертифікатів, варто забезпечити централізоване скоординоване управління ІБ КМ, котра захищається.

IPSec зарекомендував себе як основний протокол, та здійснює безпеку передачі даних між двома пристроями та мережами, для гарантії ІБ на канальному та мережевому рівні варто вирішувати застсоування протоколу L2TP поверх IPSec. Тип доступу для користувачів VPN застосовується для постійного підключення до КМ та забезпечення високого рівня безпеки, між користувачем та співробітником при повному доступі до мережі. За умови швидкого розгортання VPN-мережі чи створення тимчасового підключення з середнім рівнем безпеки даних використовується SSL протокол. Підвищення рівня безпеки у такому випадку досягається комбінуванням SSL та IPSec протоколів.

Розділ 3 ЗАХИСТ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

3.1 Методи захисту інформації в мережах VPN

Пріоритетність захисту інформаційних ресурсів залежить і від безпеки даних, котрі належать підприємству та ефективності. Користувачі та організація можуть страждати унаслідок перехоплення інформації, отримання спаму чи блокуванні серверів [14].

Безліч продуктів та інструментів ПЗ надають можливість зберегти інформацію у мережі Інтернет від віртуальних атак зловмисників. Зручно та ефективно для здійснення забезпечення захисту інформації, тобто застосовування VPN [14].

Зі зростанням сучасних організацій зростають інформаційні потреби з обробки інформації. Так як кількість обладнання зростає з роками, то з'єднується мережею. Розвиток комп'ютерних мереж тягне за собою збільшення інформаційних ризиків. Загроза у такому випадку маніпулює трафіком у процесі передачі у мережі. Тоді, виникає потреба в розробці методів протидії даній загрозі [21].

У залежності від використання протоколів та призначень, VPN забезпечує з'єднання трьох видів [21]:

- вузол-вузол;
- вузол-мережу;
- мережу.

VPN складається з наступних частин [21]:

- «внутрішня» мережа (їх може бути кілька);
- «зовнішня» мережу (притаманна інкапсуляція).

Підключення до віртуальної мережі окремого комп'ютера здійснюється завдяки серверу доступу, підключається до внутрішньої та зовнішньої мережі. У випадку підключення віддаленого користувача сервер доступу вимагає проведення процесу ідентифікації та процесу автентифікації. Після успішного проходження обох процесів, віддалений користувач наділений

повноваженнями для роботи в мережі, здійснюється процес авторизації [21].

3.1.1 Програмні засоби захисту інформації

Використовувані наразі засоби захисту інформації [37]:

- Антивірусна програма – програма для виявлення комп'ютерних вірусів і лікування заражених файлів, для профілактики, щоб запобігти зараженню файлів чи ОС шкідливим кодом.
- Спеціалізовані програмні засоби захисту інформації від НСД володіють можливостями та характеристиками, а ніж вбудовані засоби. Програми зашифрування та криптографічних систем, існують інші доступні зовнішні засобів захисту інформації.
- Міжмережеві екрани – проміжні сервери, які аналізують та фільтрують трафік мережевого/транспортного рівнів, який проходить через них. Це дозволяє знизити загрози НСД ззовні у КМ, але не усуває цю небезпеку повністю. Більш захищений різновид методу – це спосіб маскування, коли трафік посилається від імені firewall сервера, приховуючи локальну мережу.
- Proxy-servers. Весь трафік мережевого/транспортного рівнів між локальної та глобальної мережами забороняється повністю, звернення з локальної до глобальної мережі здійснюється через спеціальні сервери-посередники. Звернення у такому випадку з глобальної у локальну мережу є неможливим. Даний метод не надає захист проти атак на високих рівнях.
- VPN надає можливість передати секретну інформацію через мережі, у такому випадку можливе прослуховування трафіку сторонніми особами (застосовуються технології: PPTP, PPPoE, IPSec).

3.1.2 Незахищеність мереж передачі даних

Загрози пов'язуються з недосконалістю протоколів, у тому числі стеку протоколів TCP/IP. Такі протоколи були розроблені тоді, коли проблема забезпечення безпеки даних не була повсякденною справою для системних

адміністраторів. Користувачі Інтернету являють собою обмежене коло осіб та не здійснює спроби порушення працездатності. Сформовані протоколи не містять механізм, які дозволяють протистояти можливим атакам зловмисників [37].

Підключенні до мережі вважається – підключенням комп'ютеру до зовнішнього середовища для спілкування з іншими ресурсами, за умови, якщо немає гарантій, що доступ мають лише користувачі комп'ютеру чи лише дозволені користувачі з мережі [37].

У випадку, якщо комп'ютер підключений до локальної мережі, то, є можливість підключення до даного комп'ютеру, і НСД до інформації можна отримати з локальної мережі [37].

Якщо комп'ютер під'єднати через провайдера до зовнішньої мережі, то комп'ютер та передані дані потенційно доступні зловмисникам у Інтернет. Через такий комп'ютер може існувати отримання доступу зловмисників та до ресурсів локальної мережі [37].

Для підключень використовуються засоби розмежування доступу ОС, чи спеціалізовані засоби захисту від НСД, чи криптографічні системи на рівні певних програм.

Дані заходи не гарантують необхідної безпеки при проведенні мережевих атак, у зв'язку з нижчеописаними причинами [37]:

- ОС відноситься до продуктів з високою складністю, формування яких здійснюється великою кількістю розробників. Аналіз даних систем здійснюється досить складно, тому точно обґрунтувати відсутність помилок чи недокументованих можливостей.

- У багатозадачій ОС, може бути одночасно застосовувати та працювати кілька ПЗ.

- У сучасних системах є велика кількість різноманітних механізмів віддаленого завантаження та запуску програм, контроль роботи яких досить складним.

3.1.3 Захищені канали передачі

Складним засобом захисту трафіку порівнюючи із захищеними каналами є VPN. Схожа мережа представляє собою «мережу в мережі», тобто сервіс, формує у користувачів існування приватної мережі у публічній мережі. Властивістю даної «приватної мережі» захищає трафік від атак користувачів публічної мережі. Мережа VPN доступна не лише здатністю імітації приватної мережі; користувачу надається можливість отримати власний адресний простір та забезпечується якість обслуговування, близьким до виділеного каналу [39].

VPN на основі шифрування визначається як сукупність захищених каналів, сформованих підприємством у відкритій публічній мережі для об'єднання своїх віддалених офісів. Для реалізації VPN застосовується техніка захищених каналів та використовується для інших масштабів, пов'язуючи будь-яку кількість клієнтських мереж [39].

Способи організації VPN наділені перевагами та недоліками [39]:

1) VPN на базі маршрутизаторів

Переваги:

- Функції підтримки мереж VPN вбудовані у маршрутизуючі пристрої, які не потребують додаткових витрат для купівлі засобів, які реалізують дані функції;

- Спрощується процес адміністрування VPN.

Недоліки:

- Функціонування VPN негативно впливає на інший трафік.

- Канал між отримувачем даних у локальній мережі та маршрутизатором може стати вразливою ланкою у системі захисту.

2) ПЗ VPN для брандмауерів

Переваги:

- Можливий контроль тунельованого трафіку;

- Висока ефективність адміністрування захищених віртуальних мереж;

- Забезпечується комплексний захисту інформації;

- Відсутня надмірність апаратних платформ для засобів мережевого захисту.

Недоліки:

- Процес шифрування інформації завантажує процесор та знижує продуктивність брандмауера;

- Канал між отримувачем інформації у локальній мережі та брандмауером є вразливою ланкою у системі захисту;

- Для зростання продуктивності серверних продуктів апаратне забезпечення модернізується.

3) VPN на базі спеціального ПЗ

Переваги:

- Можливість модернізації та оновлення версій;

- Оперативність ліквідації помилок;

- Немає необхідності у використанні спеціального апаратного засобу.

Недоліки:

- Адміністрування VPN вимагає окремного ПЗ та виділеного окремого каталогу;

- У майбутньому з’явиться необхідність оновлення апаратного забезпечення.

4) VPN на базі апаратних засобів

Переваги:

- Забезпечується більш висока продуктивність;

- Багатофункціональні апаратні пристрої полегшує конфігурацію та обслуговування;

- Однофункціональні апаратні пристрої використовують тонке налаштування для досягнення високої продуктивності.

Недоліки:

- У багатофункціональних блоках продуктивність однієї програми підвищується за рахунок завдання шкоди іншої;

- Однофункціональні пристрої вимагають окремих інструментів

адміністрування та каталогів;

- Вдосконалення для підвищення продуктивності може бути вартісним чи неможливим;

- Канал між отримувачем даних у локальній мережі та апаратним пристроєм шифрування трафіку є вразливим у системі захисту IPSec, та має право використовуватися у транспортному чи тунельному режимі.

IPSec зарекомендував себе як стандарт для надійної комунікації за IP, то використовується як розширення IPv4 та має бути невід'ємною складовою IPv6.

Типовими конфігураціями VPN є області використання стандарту IPSec, тобто динамічні з'єднання між хостами через Internet та захист внутрішнього трафіку в локальній мережі.

IPSec застосовується безпосередньо між взаємодіючими хостами без залучення додаткового обладнання, тобто формується з'єднання між хостами за протоколом IPSec з використанням транспортного режиму. У режимі кадру IPSec розміщується у вихідний пакет IP за заголовком IP. На супротив тунельного режиму жодні додаткові заголовки IP не мають додаватися. Таким рішенням вимагається реалізація підтримки IPSec у стеках IP на обох хостах [35].

Для того, щоб захищений трафік IP зміг здійснити прохід через міжмережеві екрани мереж партнерів, то адміністратори відкривається UDP-порт 500 для протоколів IKE та NAT Traversal. Інформаційний обмін за протоколом IPSec не перериватиме при проходженні через обладнання NAT [35].

Протокол NAT Traversal (NAT-T) інкапсулює трафік IPSec та одночасно формує пакети UDP, які NAT коректно пересилає. NAT-T поміщає додатковий заголовок UDP перед пакетом IPSec, для його обробки як звичайний пакет UDP та хост отримувача не здійснював жодних перевірок цілісності. Після надходження пакету за місцем призначення заголовок UDP видаляється, та здійснює власний шлях як інкапсульований пакет IPSec [35].

Протокол IPSec встановлює захищені комунікаційні канали у локальній мережі. Прозорість полегшує реалізацію, а у додатку не потрібно вносити значні виправлення [35].

IPSec вводиться у існуючі мережеві середовища. На перехідному етапі адміністратор має можливість надати можливість незахищені з'єднання з хостами, які не підтримуються IPSec. Для захисту трафіку локальної мережі віддалені користувачі не використовують IPSec-VPN для зв'язку з локальною мережею. Для використання служб, необхідна наявність ітераційної техніки тунелювання. При ітераційному тунелюванню кожен хост має дві чи більше асоціації безпеки, згідно яких здійснюється обмін даними з іншими хостами. Ітераційне туннелювання може бути невидимим для хосту [4].

Велика кількість сучасних підприємств, у випадку появи потреби у захищеному каналі зв'язку у локальній мережі чи між віддаленими офісами. Важливо акцентувати увагу на те, що слід пам'ятати, що дані рішення мають свої недоліки та абсолютний захист інформації забезпечується лише при розробці та впровадженні комплексу програмних, апаратних та організаційних заходів для конкретного об'єкта інформаційної діяльності [4].

SSL VPN – ґрунтується на використанні криптографічного протоколу для автентифікації, перевірки та шифрування переданих пакетів даних. Захист є надійним та безпечним, дешевшим та не вимагає постійних налаштувань. SSL першочергово розроблявся, як альтернативна технологія, але наразі це окремий пакет. Є сумісним з усіма ОС, для його застосування немає потреби встановлення додаткового ПЗ [4].

3.2 VPN від Avast

Використання VPN схожий на роботу під «прикриттям» використовується у мережі Інтернет. Варто звернути увагу на Політику щодо застосування VPN, а також збір яких саме даних відбувається у процесі застосування VPN-послуг [16].

Дані розглядаються всі як конфіденційні, варто розуміти процес

обробки, які саме нормативно-правові документи беруться за основу [16].

Збір та застосування персональних даних. Персональні дані вважаються ті дані, які стосуються ідентифікованої фізичної особи, чи фізичної особи, котра ідентифікується та включає відомості, які надає користувач у процесі застосування VPN-послуг від розробника [16].

До збору персональних даних входить [16]:

- Створення облікового запису та управління ним. При створенні облікового запису у системі, варто отримати відомості щодо користувача. Дані формуються та зберігаються для управління обліковим записом.
- Службові дані наших серверів VPN. При застосуванні VPN-послуги збирається та обробляється лише основна інформація, яка необхідна.

Дані зберігаються серверах упродовж 30 днів, далі видаляються. Дані не збираються у межах служби VPN.

Не збираються та не зберігаються жоден вид з таких даних [16]:

- Будь-яка вихідна IP-адреса.
- Будь-які запити DNS упродовж з’єднання.
- Будь-які журнали операцій.

Службові дані VPN-клієнтів. Для забезпечення необхідної роботи VPN-клієнтів та їх покращення необхідно знати, як користувачі взаємодіють із ними. Дані не можуть застосовуватися для виявлення та визначення мети використання VPN-послуги [16].

Сторонні послуги аналітики в VPN продукті. Використовуючи додаткове ПЗ даного розробника (що стосується аналізу подій програми вивчення роботи служб). Іноді варто використовувати сторонні інструменти, які мають на меті здійснювати певні задачі у спосіб, який не здатен повторити. Якщо необхідно, то продукт знеособлюється, маскується, обмежує розкриття інформації [16].

Сторонні інструменти мають дотримуватися політики конфіденційності при застосуванні. Варто ознайомитися з переліком інструментів, котра поширюється на всі продукти Avast [16].

Google Firebase Analytics для мобільних платформ (iOS та Android), надає можливість отримати інформацію, щодо взаємодії користувачів з аспектами програм. Firebase використовує Android Advertising ID чи iOS Identifier for Advertisers, що дозволяє використовувати ідентифікатори власної розробки для знеособлення. Тобто, не включається жодна інформація, котра може бути застосована для встановлення особи користувача. Але за необхідності, можна відмовитися від надання знеособлених даних для подальшої ефективності програми у налаштуваннях програми [16].

Google Fabric Crashlytics для мобільних платформ (iOS та Android), надає можливість покращити стабільність програми, для визначення елементів, які не працюють та підвищують ефективність надання послуг. У процесі застосування не використовується жодна інформація, котра застосовується для ідентифікації [16].

Firebase Analytics та Crashlytics підпадають під дію Політики конфіденційності Google [16].

AppsFlyer Analytics для мобільних платформ (iOS та Android), надає результати, щодо ефективності роботи маркетингового відділу, тобто як та звідки потрапив даний користувач до продукту. Від цієї послуги відмовитися не можна [16].

Deprecated Analytics – визначає актуальність оновленої чи застарілої версії [16].

- Facebook Analytics – для визначення кількості користувачів Facebook, які почали застосовувати послугу.
- HockeyApp – інструмент для поширення бета-версії програми.

3.3 VPN від Сайфер

Наразі є необхідність забезпечення конфіденційної та безпечної передачі даних мережею Інтернет для вже існуючих інформаційних систем вирішується завдяки технології VPN [33].

При побудові VPN рекомендується звернути увагу на [33]:

- Гнучкість та зручність управління ключами.
- Зручність експлуатації та інтеграції.
- Гнучкість та зручність налаштування мережі.
- Швидкість передачі даних.
- Перспективність.
- Орієнтація на хмарні технології.
- Широкий спектр підтримуваних апаратних платформ та ОС.

СКЗІ «Шифр-VPN» програмний чи програмно-апаратний комплекс, який базується на протоколі OpenVPN з підтримкою SSL/TLS протоколів, для забезпечення конфіденційності при передачі даних в комп'ютерних мережах [33].

СКЗІ «Шифр-VPN» надає можливість забезпечити конфіденційність між [33]:

- Мережа-Мережа (Сервер-Сервер). Надає можливість будувати VPN з'єднання між різними мережами, де весь трафік піддається захисту.
- Користувач-Мережа (Клієнт-Сервер). Надає можливість будувати VPN з'єднання між комп'ютером користувача та мережею, котра знаходиться за VPN Сервером.

Для забезпечення конфіденційності застосовуються криптографічні алгоритми реалізуються у бібліотеках власної розробки криптографічних примітивів «Шифр+» v 2.1.

СКЗІ «Шифр-VPN» ґрунтується навколо інфраструктури відкритих ключів [33]:

- Ключі видані КНЕДП/КНЕДП. Тоді для авторизації користувачів у захищеній мережі, можуть застосовуватися:
    - Перевірка статусу сертифікату за протоколом OCSP.
    - Ведення списку довірених ЦСК на сервері VPN.
    - Ведення списку дозволених користувачів на сервері VPN.
- Ключі видані внутрішнім ЦСК, використовується СКЗІ «Шифр-

X.509».

Можуть бути застосовані криптографічні алгоритми [33]:

- Національні криптографічні алгоритми: ДСТУ 4145:2002; ГОСТ 34.311-95, ДСТУ 7564:2014; ГОСТ 28147-89, ДСТУ 7624:2014.
- Міжнародні криптографічні алгоритми: RSA, ECDSA; SHA-1, SHA-2; AES, DEA, TDEA.

Ключі користувачів та серверів можуть використовуватись [33]:

- У вигляді файлу – файлового контейнеру.
  - PFX/PKCS#12 (КНЕДП Офіс Генерального прокурора, КНЕДП Україна, КНЕДП НДУ, КНЕДП Ощадбанк, АТ ІІТ та інші).
  - JKS (КНЕДП Приватбанк).
  - Key-6.dat (ЦСК побудовані на основі АТ ІІТ).
  - ZS2 (аналог PFX/PKCS#12 КНЕДП Україна, а також після конвертації в Key-6.dat).
- На захищеному носії:
  - В пасивному режимі: Aladdin/SafeNet/Gemalto eToken; Автор SecureToken-337; Авест AvestKey; Ефіт EfitKey.
  - В активному режимі: ІІТ Алмаз-1К; Автор SecureToken-337; Авест AvestKey; Ефіт EfitKey.

СКЗІ «Шифр-VPN» підтримує різні апаратні платформи та ОС [33]:

- Апаратні платформи: x86, x86-64; ARMv6, ARMv7, ARMv8.
- Операційні системи:
  - Сервер: Windows, Linux, FreeBSD.
  - Клієнт: Windows, Linux, MacOS.
  - Клієнт: Android, iOS.

Зручність використання СКЗІ «Шифр-VPN» забезпечується [33]:

- Управління Серверами VPN.
- Моніторинг Сервера VPN ґрунтується на базі агентів та розширень для Zabbix v3.0+.
- Налаштування сервера та клієнтів здійснюється за допомогою

підготовлених файлів налаштувань.

Що стосується інтеграції зі вже існуючими системами здійснюється з мінімальними змінами [33]:

- «Шифр-VPN» надає можливість балансування трафіку.
- «Шифр-VPN» надає можливість захищати мережеві підключення зі збільшеною пропускною здатністю.
- Агрегація трафіку може бути отримана завдяки паралельної роботи кількох Серверів VPN на одній обчислювальній машині.
- Застосовані в «Шифр-VPN» забезпечують ефективну можливість роботи на фізичному та віртуальному обладнані.

Варіанти побудови Сервера VPN [33]:

- Docker контейнер.
- Віртуальна машина.
- Архів з дистрибутивом для ручного встановлення.
- У захищеному апаратному виконанні.

СКЗІ «Шифр-VPN» будується захищений канал між двома мережами, де з обох боків розгорнутий Сервер VPN, який може [33]:

- Керуватися трафіком між мережами.
- Можливість проходження трафіку через брандмауери та HTTP-proxy.
- Шифрувати чи не шифрувати трафік.
- Агрегувати трафік з кількох мережевих інтерфейсів.
- Використовуються статичні ідентичні ключі у PKCS#12 контейнері.

СКЗІ «Шифр-VPN» здійснює та виконує задачі, які будують захищений канал між користувачем та мережею. Де розгортається Сервер VPN, а у користувача Клієнт VPN.

На стороні Сервера VPN [33]:

- Здійснюється управління трафіку між двома мережами.
- Проходження трафіку через брандмауер та HTTP-proxy.

- Шифрувати чи не шифрувати трафік.
- Агрегувати трафік з кількох мережевих інтерфейсів.
- Застосовуються ключі у PKCS#12 контейнері.
- Паралельна робота кількох Серверів VPN.
- Балансування підключень між пулом Серверів VPN.
- Автентифікація користувача за різними ознаками.
- Підтримка роботи з ЦСК за протоколами OCSP over HTTP, для перевірки статусу сертифікату.

На стороні Клієнта VPN [33]:

- Можливість застосування конфігураційних файлів для даного Сервера VPN.
- Можливість підключення до пулу Серверів VPN.
- Управління трафіком між мережами.
- Проходження трафіку через брандмауер та HTTP-proxy.
- Шифрувати чи не шифрувати трафік.
- Збереження ключа у файлових контейнерах чи на захищених носіях.
- Збереження паролю у пам’яті до захищеного носія, або введення його щоразу.
- Підтримка роботи з ЦСК за протоколами OCSP over HTTP, для перевірки статусу сертифікату.

Типовою задачею, яку може реалізовувати СКЗІ «Шифр-VPN», є побудова захищеного каналу між користувачем та мережею.

Сервер VPN розгортається на стороні серверу, тоді як Клієнт VPN розгортається у кожного клієнта окремо.

На стороні Сервера VPN здійснюється керування трафіком від клієнтських підключень між різними мережами.

Існує велика кількість підходів до побудови VPN, у залежності від рівня: Мережевий (IP/IPSec) та Транспортний (TCP/UDP).

Використовуючи такі методи, то вони можуть мати позитивні та

негативні сторони.

Виділяється протокол OpenVPN з підтримкою SSL/TLS, котрий дозволяє забезпечити [33]:

- Прозорість проходження Firewall, Proxy, NAT порівнюючи з LT2P/IPsec.
- Висока продуктивність використаних обчислювальних ресурсів у порівнянні з LT2P/IPsec.
- Підтримка протоколів транспортного рівня TCP та UDP.
- Стискання трафіку за допомогою алгоритмів LZO, ZIP.
- Гнучкість налаштування на стороні клієнтів розміщується на встановлених конфігураційних файлах.

3.4 VPN від Автор

«IP-шифратор» CryptoIP-459 назначений для КЗІ з обмеженим доступом та відкритої інформації, вимоги до яких встановлюється чинним законодавством [13].

«IP-шифратор» надає можливість крізного шифрування IP-трафіку, котрий передається між захищеними локальними мережами через IP-мережу загального користування. «IP-шифратор» є основою для формування VPN з шифруванням інформації [33].

У «IP-шифратор» реалізуються алгоритми КЗІ [33]:

- шифрування – ДСТУ ГОСТ 28147:2009;
- функція гешування – ГОСТ 34.311-95;
- КЕП – ДСТУ 4145-2002;
- створення сеансового ключа – ДСТУ ISO/IEC 15946-3:2006.

На базі пристроїв будуються криптографічні системи [33]:

- з відкритими ключами та підтримкою архітектури PKI;
- з відкритими ключами та ручним розподілом сертифікатів абонентів.

Пристрій підтримує два інтерфейси 10/100Base-T для підключення до

[33]:

- глобальної мережі;
- локальної мережі;
- ПЕОМ (завдяки попередньо налаштованої конфігурації).

Деталі, щодо особливостей «IP-шифратор» CryptoIP-459 відображені у табл. 3.1.

Таблиця 3.1 – Технічні характеристики

Швидкість шифрування	266 Мбіт/с
Сумарна пропускна спроможність	не менше, ніж 180 Мбіт/с
Пропускна спроможність в кожному напрямі	не менше, ніж 92 Мбіт/с
Кількість VPN-тунелів IP-шифратора	не більше, ніж 2047
Максимальна кількість шифраторів в одній мережі	8192
Носій ключових даних	змінний, SIM, CryptoCard-317
Період зміни ключових даних	3 роки
Аутентифікація СПО	локальна, дистанційна
Захист шифратора від НСД	криптографічний
Діапазон температур в умовах експлуатації	від +0°С до +45°С
Живлення пристрою	від мережі змінного струму напругою 85 – 265 В і номінальною частотою 50 або 60 Гц
Споживча потужність	не більше, ніж 10 Вт
Розміри IP-шифратора	204×157×37 мм

3.5 Висновки до третього розділу

У третьому розділі кваліфікаційної роботи було проаналізовано, які методи захисту інформації в мережах VPN. Розглянуто їх види, складові частини. Досліджено існуючі захист захисту інформації з їх особливостями, перевагами та недоліками, а саме: антивірусна програма, спеціалізовані програмні засоби захисту інформації від НСД, міжмережеві екрани, Proxy-servers.

Визначено, яким чином здійснюється передача секретної інформації за

допомогою VPN, також визначено способи організації VPN наділені певними перевагами та недоліками, а саме:

1) VPN на базі маршрутизаторів

2) ПЗ VPN для брандмауерів

3) VPN на базі спеціального ПЗ

4) VPN на базі апаратних засобів

Окремо, розглянуто та проаналізовано вже існуючі VPN, які мають експертні висновки в Україні

- VPN від Avast
- VPN від Сайфер
- VPN від Автор

Таким чином, досягнена мета захисту мереж від НСД із застосування технології VPN.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні **задачі**:

- Дослідження протоколів, функцій та проблеми VPN;
- Аналіз способів їх захисту каналів корпоративних мереж на базі VPN рішень та концепція побудови віртуальних захищених мереж VPN;
- Дослідження та аналіз сучасних VPN

У процесі підготовки першого розділу кваліфікаційної роботи було проаналізовано загальні характеристики VPN, протоколи VPN, функції та компоненти VPN, а також визначено мережі VPN та проблеми їх захисту.

Протоколи, які наразі використовуються: IPSec, PPTP, L2F, L2TP, IKE, LCP, PPP, IPsec, OpenVPN, EAP, EAP-TLS, MSCHAP, CHAP, SPAP, PAP.

Структура VPN містить два рівні:

- Внутрішня мережа.
- Зовнішня мережа.

Захист інформації у мережі VPN ґрунтується на кількох методах, які використовуються для реалізації заходів безпеки в інформаційних мережах:

- ❖ Тунелювання.
- ❖ Автентифікація.
- ❖ Шифрування.

У ході аналізу проблем ІБ у локальних чи глобальних мережах, де є VPN, то варто робити висновки, що дані системи мають забезпечувати виявлення внутрішніх та зовнішніх загроз та вторгнень, фільтрація зовнішнього трафіку, контроль застосування корпоративних мережевих ресурсів та запобігання НСД. Вхідними даними є інформація щодо структури та характеристиках трафіку, це може надати можливість побудувати набір правил, котрі класифікують нормальні чи аномальні компоненти трафіку.

Тоді, можна отримати гарантований захист мереж завдяки швидкого реагування на набір відомих загроз та аномальні ситуації, за рахунок ідентифікації функціонуючих процесів та керування ними для забезпечення

доступності інформаційних сервісів.

У ході підготовки другого розділу кваліфікаційного розділу було проаналізовано способи захисту каналів КМ на базі VPN рішень, досліджено концепцію побудови віртуальних захищених мереж VPN та можливі конфігурації VPN для безпечної передачі даних.

Ідея побудови власних VPN є актуальною, за при поєднанні кількох локальних мереж у організаціях для формування власної мережі це є досить вартісним процесом та досить довгим, однак варто забезпечити захист переданих між сегментами мережі даних. Так як, далеко не завжди дозволено передавати дані загальнодоступними мережами у відкритому вигляді. Однак, захищати лише зв'язки між окремими комп'ютерами з різних сегментів, за умови того, що корпоративна політика організація вимагає забезпечення безпеки великої кількості інформації, то здійснювати захист кожного окремого каналу та комп'ютеру є досить складним процесом. При захисті окремих каналів інфраструктури КМ залишається прозорою для зовнішнього спостерігача. Для розв'язку проблем використовується архітектура VPN, а при застосуванні весь потік інформації, передається загальнодоступними мережами та шифрується.

Система управління ІБ мережі забезпечує наскрізну безпеку VPN. Для забезпечення високого рівня безпеки та управління VPN, також системи розподілу криптографічних ключів та сертифікатів, варто забезпечити централізоване скоординоване управління ІБ КМ, котра захищається.

IPSec зарекомендував себе як основний протокол, та здійснює безпеку передачі даних між двома пристроями та мережами, для гарантії ІБ на канальному та мережевому рівні варто вирішувати застсоування протоколу L2TP поверх IPSec. Тип доступу для користувачів VPN застосовується для постійного підключення до КМ та забезпечення високого рівня безпеки, між користувачем та співробітником при повному доступі до мережі. За умови швидкого розгортання VPN-мережі чи створення тимчасового підключення з середнім рівнем безпеки даних використовується SSL протокол. Підвищення

рівня безпеки у такому випадку досягається комбінуванням SSL та IPSec протоколів.

У третьому розділі кваліфікаційної роботи було проаналізовано, які методи захисту інформації в мережах VPN. Розглянуто їх види, складові частини. Досліджено існуючі захист захисту інформації з їх особливостями, перевагами та недоліками, а саме: антивірусна програма, спеціалізовані програмні засоби захисту інформації від НСД, міжмережеві екрани, Proxy-servers.

Визначено, яким чином здійснюється передача секретної інформації за допомогою VPN, також визначено способи організації VPN наділені певними перевагами та недоліками, а саме:

1) VPN на базі маршрутизаторів

2) ПЗ VPN для брандмауерів

3) VPN на базі спеціального ПЗ

4) VPN на базі апаратних засобів

Окремо, розглянуто та проаналізовано вже існуючі VPN, які мають експертні висновки в Україні

- VPN від Avast
- VPN від Сайфер
- VPN від Автор

Таким чином, досягнена мета захисту мереж від НСД із застосування технології VPN.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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

2. Bollapragada V., Mohamed Kh., Wainner S. IPSec VPN Design. Cisco Press. (2005). 384 p.

3. 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/

4. Harsh Kupwade Patil. Wireless Sensor Network Security: The Internet of Things [Електронний ресурс] / Harsh Kupwade Patil, Thomas M.Chen // Computer and Information Security Handbook. – 2017. – Third Edition, Chapter 18. – P. 317-337. – Режим доступу: https://www.sciencedirect.com/science/article/pii/B9780128038437000181.

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

6. Mabrook Al-Rakhami. Saleh Almowuena Wireless Sensor Networks Security: State of the Art [Електронний ресурс] / Mabrook Al-Rakhami, Saleh Almowuena. – 2018. – Режим доступу: https://arxiv.org/abs/1808.05272.

7. Pure hardware VPNs uale high-availability tests [Електронний ресурс] – Режим доступу до ресурсу: https://web.archive.org/web/20070923013848/http://www.networkworld.com/reviews/2000/1211rev.html

8. Security of Cyber-Physical Systems from Concept to Complex Information Security System / V. Dudykevych, G. Mykytyn, T. Kret, A. Rebets // Advances in Cyber-Physical Systems. – Volume 1, Number 2 (2016). – C. 67-75.

9. Tebogo Kgogo. Software defined wireless sensor networks security challenges // Tebogo Kgogo, Bassey Isong, Adnan M. Abu-Mahfouz // IEEE AFRICON. – 2017. – P. 1508-1513.

10. Tomic I. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols / I. Tomić, J.A. McCann // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 6. – P. 1910-1923.

11. Virtual private network (VPN) [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Virtual_private_network

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

13. Waleed Al Shehri. A Survey On Security In Wireless Sensor Networks // International Journal of Network Security & Its Applications (IJNSA). – 2017. – Vol. 9, No. 1. – P. 25-32.

14. Wassim Itani. Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing / Wassim Itani, Ayman Kayssi, Ali Chehab // International Journal of Reliable and Quality E-Healthcare (IJRQEH). – 2016. – Vol. 5, Issue 2. – P. 1-30.

15. Wireless Sensor Network Security for Cyber-Physical Systems / Saqib Ali, Taiseera Al, BalushiZia, NadirOmar, Khadeer Hussain // Cyber Security for Cyber Physical Systems. Studies in Computational Intelligence. – 2018. – Vol. 768. – P. 35-63.

16. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / О.Г. Корченко, М.Б. Алєксандер, Р.С. Одарченко, А. Алі Наджі, О.Ю. Петренко // Захист інформації. – 6 – 2016. – Том 18. – № 1. – С. 48-56.

17. Базова реалізація бібліотек для роботи з IPsec для Unix-подібних систем [Електронний ресурс] – Режим доступу до ресурсу: http://ipsec-tools.sourceforge.net/99

18. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с

19. Василина А.В, Яловий М.М., Цибуляк Б.З. Захист кваліфікованих каналів зв’язку за допомогою систем віртуальних приватних мереж.

Міжнародна науково-практична конференція «Проблеми та перспективи забезпечення цивільного захисту». Збірник матеріалів. (Харків, 3-4 квітня 2013). Харків: Вид-во НУЦЗ України. (2013). С. 266- 268.

20. Волошко С.В. Інформаційна безпека в безпроводових сенсорних мережах [Електронний ресурс] / С.В. Волошко, Д.О. Курца // Новітні інформаційні системи і технології. – 2018. – Випуск 9. – Режим доступу: http://journals.pntu.edu.ua/mist/article/view/1039/869.

21. Галкін В.В., Пархоменко І.І. «Використання VPN-технологій для захисту інформації в каналах корпоративних мереж» // Проблема кібербезпеки інформаційно-телекомунікаційних систем: матеріали наук.-техніч. конф.,(КНУ, Київ, Україна, 10 – 11 березня 2016). – К.: КНУ, 2016. – С. 66

22. Дудикевич В.Б. Квінтесенція безпеки кіберфізичних систем / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець // Інформаційні системи і мережі. – 2018. – № 887. – С. 58-69.

23. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

24. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т «Харків. політехн. ін-т». – Харків: НТУ «ХПІ», 2014. – 251 с.

25. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації: НД ТЗІ 1.1-005-07. [Чинний від 2007.12.12]. К. : ДСТСЗІ СБУ, 2007. № 232. (Нормативний документ системи технічного захисту інформації).

26. Інформаційна безпека в середовищі безпроводових сенсорних мереж: монографія / М.Б. Александер, С.М. Балабан, М.П. Карпінський, С.А. Райба, В.М. Чиж. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 160 с.

27. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

28. Комплексні системи захисту інформації [Текст] : навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.] ; Вінницький національний технічний університет. − Вінниця : ВНТУ, 2018. − 118 с

29. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

30. Кулаков Ю.А., Луцкий Г.М. Локальные сети, - К.: Юниор, 2008. – 336с.

31. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие. – Киев: Издательство Интуит, 2010. − 608 с.

32. Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Медведев Н. Г., Пархоменко І.І., Галкін В.В., «Захист транзакцій в каналах корпоративних мереж за допомогою VPN технологій» // Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні: матеріали наук.-техніч. конф.,(НУБіП, Київ, Україна, 23 – 24 червня 2016). – К.: НУБіП, 2016. – С.47 – 48.

33. Політика безпеки для Internet. [Електронний ресурс]. – Режим доступу: https://lektsii.org/8-12435.html – Загол. з екрана. – Дата звернення 12.11.2019.

34. Постанова Кабінету міністрів України від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

35. Построение защищенного узла доступа в интернет с применением технологии VPN и тунеллирования [Електронний ресурс]. Режим доступу: http://www.opennet.ua/docs/UAS/vpn_solution/.

36. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. 1994. № 31. С. 286.

37. Проект Концепції інформаційної безпеки України. – [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf.

38. Райан Норманн Выбираем протокол VPN [Електронний ресурс] – Режим доступу до ресурсу: http://www.osp.ua/win2000/2001/07/175027/

39. Романов В.О. Вимоги до забезпечення функціональної та інформаційної безпеки бездротових сенсорних мереж / В.О. Романов, І.Б. Галелюка, В.О. Остапенко // Комп'ютерні засоби, мережі та системи. – 2017. – № 16. – С. 106-117.

40. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. [Чинний від 1999.04.28]. К.: ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

41. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: НД ТЗІ 3.6-001-2000. [Чинний від 2000.12.30]. К.: ДСТСЗІ СБУ, 2000. № 60. (Нормативний документ системи технічного захисту інформації).

42. Что такое SSL? [Електронний ресурс]. Режим доступу: http://www.ods.com.ua/win/uas/security/ssl.html.

ДОДАТОК А

Оформлення слайдів та роздаткового матеріалу

- Сучасні технології для обробки, передачі та збору інформації спряють для розвитку загроз, таких як можливість втрати, модифікації та розкриття даних, котрі направляються кінцевим користувачам. Забезпечення інформаційної безпеки (ІБ) комп'ютерних систем і мереж (КСМ) є одним з перспективних напрямків розвитку ІТ, а отже і актуальним.

Мета та задачі роботи

Метою є захист мереж від несанкціонованого доступу з використанням технології VPN.

У процесі підготовки кваліфікаційної роботи були поставлДослідження протоколів, функцій та проблеми VPN;

- Аналіз способів їх захисту каналів корпоративних мереж на базі VPN рішень та концепція побудови віртуальних захищених мереж VPN;
- Дослідження ені наступні задачі:
- та аналіз сучасних VPN

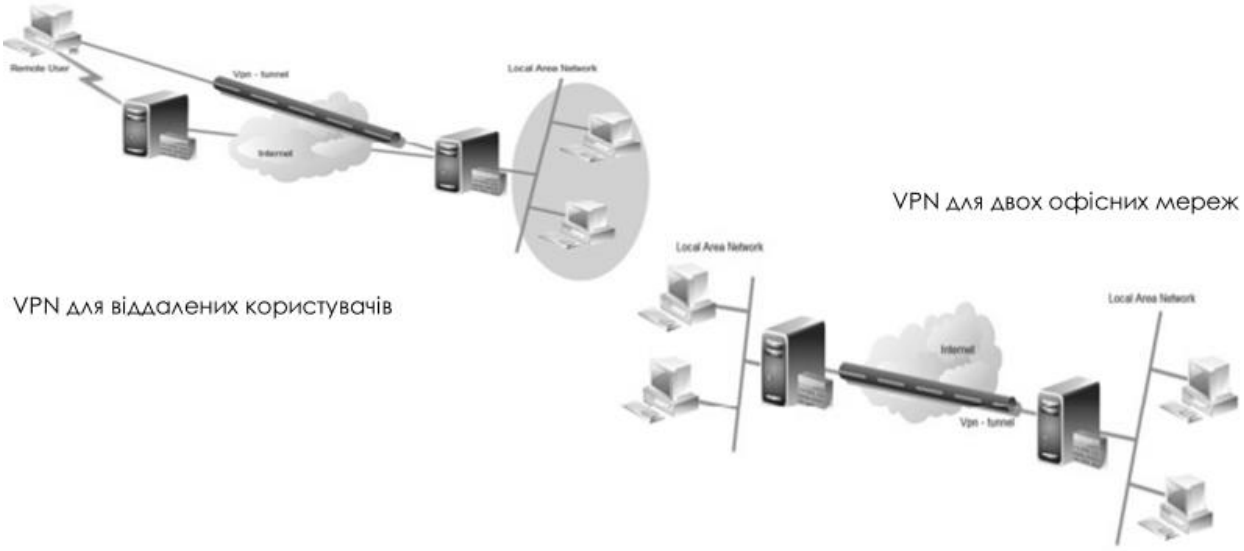
Об'єкт та предмет дослідження

- Об'єкт дослідження. Мережі.
- Предмет дослідження. Технології VPN.

Новизна та практична цінність

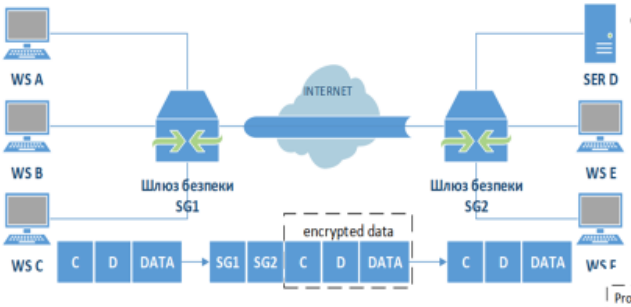
- Новизна роботи. Рекомендації щодо застосування технології VPN.
- Практична цінність. Аналіз, який проведено у роботі дозволить для організації підібрати найактуальніший VPN.

РОЗДІЛ 1 ЗНАЧЕННЯ ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ VPN

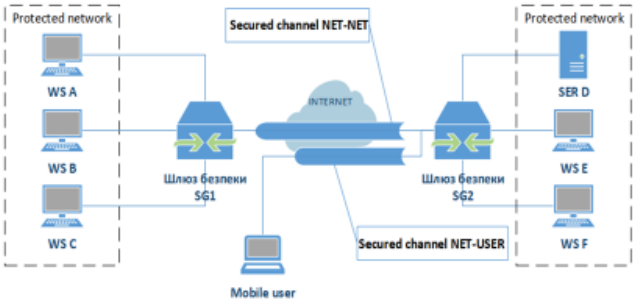


РОЗДІЛ 2 ДОПУСТИМІ КОНЦЕПЦІЇ ТА КОНФІГУРАЦІЇ ДЛЯ ПОБУДОВИ ЗАХИЩЕННОЇ МЕРЕЖІ VPN

Схема віртуального захищеного тунелю



Віртуальні захищені канали типу Мережа – Мережа, Клієнт – Клієнт



Розділ 3 ЗАХИСТ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

- VPN від Avast

Використання VPN схожий на роботу під «прикриттям» використовується у мережі Інтернет. Варто звернути увагу на Політику щодо застосування VPN, а також збір яких саме даних відбувається у процесі застосування VPN-послуг.

Розділ 3 ЗАХИСТ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

• VPN від Сайфер

СКЗІ «Шифр-VPN» забезпечує конфіденційність між:

- Мережа-Мережа (Сервер-Сервер). Надає можливість будувати VPN з'єднання між різними мережами, де весь трафік піддається захисту.
- Користувач-Мережа (Клієнт-Сервер). Надає можливість будувати VPN з'єднання між комп'ютером користувача та мережею, котра знаходиться за VPN Сервером.

Застосовуються криптографічні алгоритми:

- Національні криптографічні алгоритми: ДСТУ 4145:2002; ГОСТ 34.311-95, ДСТУ 7564:2014; ГОСТ 28147-89, ДСТУ 7624:2014.
- Міжнародні криптографічні алгоритми: RSA, ECDSA; SHA-1, SHA-2; AES, DEA, TDEA.

Розділ 3 ЗАХИСТ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

• VPN від Автор

«IP-шифратор» CryptoIP-459 назначений для КЗІ з обмеженим доступом та відкритої інформації, вимоги до яких встановлюється чинним законодавством [13].

У «IP-шифратор» реалізуються алгоритми КЗІ [33]:

- шифрування – ДСТУ ГОСТ 28147:2009;
- функція гешування – ГОСТ 34.311-95;
- КЕП – ДСТУ 4145-2002;
- створення сеансового ключа – ДСТУ ISO/IEC 15946-3:2006.

Висновки

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

- Дослідження протоколів, функцій та проблеми VPN;
- Аналіз способів їх захисту каналів корпоративних мереж на базі VPN рішень та концепція побудови віртуальних захищених мереж VPN;
- Дослідження та аналіз сучасних VPN

Проаналізовано, які методи захисту інформації в мережах VPN. Розглянуто їх види, складові частини. Досліджено існуючі захист захисту інформації з їх особливостями, перевагами та недоліками, а саме: антивірусна програма, спеціалізовані програмні засоби захисту інформації від НСД, міжмережеві екрани, Proxy-servers.

Висновки

Визначено, яким чином здійснюється передача секретної інформації за допомогою VPN, також визначено способи організації VPN наділені певними перевагами та недоліками, а саме:

1) VPN на базі маршрутизаторів

2) ПЗ VPN для брандмауерів

3) VPN на базі спеціального ПЗ

4) VPN на базі апаратних засобів

Проаналізовано вже існуючі VPN, які мають експертні висновки в Україні: VPN від Avast; VPN від Сайфер; VPN від Автор.

Таким чином, досягнена мета захисту мереж від НСД із застосування технології VPN.