ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ VPN»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Денис КОСТЕНКО

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
КОСТЕНКО Денис
(ПРІЗВИЩЕ, Ім'я)
Керівник: БОРСУКОВСЬКИЙ Юрій
к.т.н., доцент (ПРІЗВИЩЕ, Ім'я)
Рецензент: ТУРОВСЬКИЙ Олександр
д.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Костенко Денису Вікторовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN»
керівник кваліфікаційної роботи: БОРСУКОВСЬКИЙ Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
технологія організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж.
2. Методи та засоби управління мережевим доступом організацій.
3. Розроблення варіанта технології організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми управління привілеями в інформаційній системі організації	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж	27.10. 2023р.	
4.	Методи та засоби управління мережевим доступом організацій	03.11.2023 р.	
5.	Розроблення варіанта Технологія організації захищеного обміну даними віддалених користувачів на базі VPN	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Денис КОСТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Костенко Д.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***КОСТЕНКО Денис*** обрав тему роботи, метою якої було дослідити зміст технології контролю доступу до мережі організацій. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***КОСТЕНКО Денис*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КОСТЕНКО Дениса*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Борсуковський Ю.В.
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***КОСТЕНКО Денис***. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ пина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача Костенко Дениса

на тему: «Технологія організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN».

Актуальність:

Розробка технології організації захищеного обміну даними віддалених користувачів на базі VPN є вкрай актуальною, враховуючи зростаючу потребу в безпечних рішеннях для дистанційної роботи та обміну інформацією. Умови постійних кіберзагроз, необхідність конфіденційності та дотримання регуляторних вимог роблять впровадження VPN технологій ключовим для забезпечення безпеки, ефективності та відповідності стандартам у сучасному інформаційному середовищі. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На підставі проведеного аналізу роботи виявлено суть проблеми забезпечення контролю над доступом до мережі організації.
2. Досліджено різноманітні методи та інструменти управління доступом до мережі в організаційному контексті.
3. Запропоновано варіант технології організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN.
4. Текст представлений досить вмотивовано та логічно, використовуючи грамотну мову. Висновки чіткі та важливі. Графічний матеріал виглядає якісно. Список використаної літератури свідчить про вміння дослідника користуватись науковими та технічними ресурсами відповідно до теми магістерської роботи..

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально описати різні системи VPN та їх відмінності.
2. Запропонований варіант технології управління доступом до мережі організації на базі VPN доцільно було б показати на конкретному прикладі або підприємстві.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **КОСТЕНКО Денис** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ Олександр ТУРОВСЬКИЙ

підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра: 74 сторінок, 9 рисунків, 41 джерело.

Об'єкт дослідження – Мережі.

Предмет дослідження – Технології VPN.

Мета роботи – захист мереж від несанкціонованого доступу з використанням технології VPN.

Методи дослідження – 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

В роботі проведено аналіз проблеми сучасних технологій обробки, передачі та збору інформації, які призводять до нових загроз, пов'язаних з втратою, модифікацією та розкриттям даних, що направляються користувачам.

Досліджено протоколи, функції та проблеми VPN.

Запропоновано варіант технологію організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі розроблено варіант технології організації захищеного обміну даними віддалених користувачів інформаційної системи організації на базі VPN.

Галузь використання – кібербезпека корпоративної мережі.

VPN, МЕТОДИ ЗАХИСТ ІНФОРМАЦІЇ, ПРОТОКОЛИ VPN, МЕРЕЖІ VPN, КОНФІГУРАЦІЯ VPN.

ABSTRACT

Text part of the qualifying work for the master's degree: 74 pages, 9 figures, 41 sources.

Research Object – Networks.

Research Subject – VPN Technologies.

The aim of the work is to secure networks from unauthorized access using VPN technology.

Research Methods – Study of protocols, functions, and issues of VPN;

Analysis of ways to protect corporate network channels based on VPN solutions and the concept of building virtual secure VPN networks;

Study and analysis of modern VPNs.

The work includes an analysis of the problem of modern information processing, transmission, and collection technologies, leading to new threats related to data loss, modification, and disclosure sent to users.

Protocols, functions, and issues of VPN were studied.

A proposed variant of technology for organizing secure data exchange for remote users of the organization's information system based on VPN. The purpose, main functions, and components of this technology were determined.

Based on the conducted research, the work developed a variant of the technology for organizing secure data exchange for remote users of the organization's information system based on VPN.

Field of application – cybersecurity of a corporate network.

VPN, Information Security Methods, VPN Protocols, VPN Networks, VPN Configuration.

Зміст

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

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

ВСТУП

Віртуальна Приватна Мережа, або VPN, - це технологія, що дозволяє створити забезпечений тунель для обміну даними між двома вузлами (або комп'ютерами) через незабезпечені або менш довірені мережі, такі як Інтернет. За допомогою VPN користувач може отримати доступ до ресурсів внутрішньої мережі, таких як веб-сайти, бази даних, друкери та інші послуги, навіть якщо він або вона перебуває поза цією мережею. Ця технологія забезпечує зашифрований канал для безпечної передачі інформації через публічні мережі, тим самим захищаючи дані від сторонніх осіб. VPN дозволяє об'єднати різні мережі в єдину систему, використовуючи ненадійні канали для зв'язку. Багато постачальники пропонують свої VPN-послуги для побудови власних VPN-мереж, які часто розглядаються як клієнт-серверні системи.

Сучасні технології обробки, передачі та збору інформації призводять до нових загроз, пов'язаних з втратою, модифікацією та розкриттям даних, що направляються користувачам. Забезпечення інформаційної безпеки комп'ютерних систем і мереж є важливим аспектом розвитку інформаційних технологій. Інформація завжди була цінним ресурсом, що можна продавати, обмінювати та захищати. Вартість інформації завжди перевищує вартість самої техніки та обслуговування комп'ютерних систем.

Забезпечення інформаційної безпеки комп'ютерних систем передбачає заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також їх компонентів і ресурсів. При розробці таких систем важливо враховувати можливі наслідки поломок та розробляти методи їхньої ліквідації. Тому комп'ютерна безпека має надзвичайно важливе значення, і ця тематика є дуже актуальною.

Загалом, заходи забезпечення безпеки мають включати технічні, організаційні та правові аспекти. Вони спрямовані на захист інформаційних систем від незаконного доступу та атак, які можуть завдати шкоди користувачам або власникам інформації. Такі заходи повинні гарантувати конфіденційність, цілісність та доступність даних та ресурсів, і вони повинні відповідати вартості та

важливості інформації, яку вони захищають. Останні роки відзначають стрімке зростання підприємств, які стають дедалі більш розподіленими та розташованими на різних територіях. Це стало актуальним як після спалаху пандемії, так і внаслідок повномасштабного вторгнення країни-агресора. Як результат, багато організацій перейшли до політики віддаленої роботи, яка залишається актуальною і надалі. У зв'язку з цим, працівники потребують безпечного віддаленого доступу до систем та ресурсів компанії через надійні мережі. Часто в компаніях є відокремлені офіси і хмарна інфраструктура, що призводить до необхідності безпечного з'єднання цих різних територіально розподілених мереж.

Безпека мережі асоціюється з великими корпоративними мережами, в яких тисячі комп'ютерів спільно використовують ресурси. Однак навіть невелика кількість комп'ютерів, підключених до домашнього роутера, також формують мережу. Забезпечення безпеки в домашньому середовищі не менш важливе, оскільки воно стосується особистих даних.

Один з важливих аспектів - у внутрішній мережі всі користувачі користуються однією і тією ж мережею, що забезпечує доступ до спільних ресурсів та забезпечує безпеку компанії. Віддалені працівники, які не можуть фізично бути в офісі, потребують можливості віддаленого доступу з використанням VPN.

Віртуальні приватні мережі (VPN) стають популярним вибором для вирішення цих викликів. VPN із віддаленим доступом створює зашифрований тунель між комп'ютером користувача та кінцевою точкою VPN, дозволяючи віддаленим працівникам отримувати доступ до ресурсів компанії з будь-якого місця, де є Інтернет. Це забезпечує доступ до всіх ресурсів компанії, але забезпечує безпеку даних, навіть коли використовується громадська Wi-Fi мережа.

Ростуть сценарії віддаленої роботи, що робить VPN основним об'єктом інтересу для кіберзлочинців. Зловмисники спритно атакують домашні та корпоративні мережі з метою особистої вигоди. Це може включати крадіжку особистих даних, таких як номери банківських рахунків, а також шифрування файлів комп'ютера з вимогою викупу. Отже, безпека мережі має вирішальне

значення для запобігання витоку конфіденційної інформації. Правильна настройка політик безпеки важлива для захисту команди від потенційно шкідливих дій.

Метою даної роботи є захист мереж від несанкціонованого доступу за допомогою технології VPN.

У процесі підготовки кваліфікаційної роботи вирішувалися такі завдання:

- дослідження протоколів
- функцій та проблем VPN
- аналіз методів захисту каналів мереж з використанням рішень VPN
- розробка концепції віртуальних захищених мереж VPN

Об’єкт дослідження: Мережі.

Предмет дослідження: Технології VPN.

Новизна роботи: Рекомендації щодо застосування та розроблення технології VPN.

РОЗДІЛ 1: ЗНАЧЕННЯ ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ VPN

1.1 Загальні характеристики VPN

Віртуальна приватна мережа (VPN) - це технологічний засіб, який дозволяє безпечно і конфіденційно об'єднати різні види вузлів або мереж на мережі Інтернет. VPN розвивається для забезпечення захисту даних та безпечного обміну інформацією через глобальну мережу, і вона може використовуватися для різних цілей, включаючи з'єднання віддалених користувачів з внутрішніми мережами та об'єднання декількох локальних мереж в єдину систему [25].

Існують різні види VPN-з'єднань, такі як вузол-вузол (користувач-користувач), вузол-мережа (користувач-мережа) та мережа-мережа. Вузли VPN-проходять через різні точки глобальної мережі та використовують захищені протоколи для створення зашифрованих "тунелів" для обміну даними.

Технологія VPN включає в себе ряд важливих компонентів, таких як маршрутизатори, які визначають шляхи для передачі даних, і захищені протоколи для шифрування інформації під час передачі [25].

Важливим аспектом технології VPN є захист даних. Перед передачею через мережу Інтернет дані шифруються, і це забезпечує їх конфіденційність та безпеку від несанкціонованого доступу. Таким чином, інформація стає невидимою для інших користувачів Інтернету, і вона може безпечно подорожувати в зашифрованому "тунелі" [25].

Одним з важливих аспектів безпеки VPN є протоколи шифрування та протоколи автентифікації. Вибір правильних протоколів грає важливу роль у забезпеченні надійного захисту даних та у запобіганні несанкціонованого доступу.

Зараз VPN використовується в різних сферах, включаючи віддалену роботу та з'єднання великої кількості організацій. Особливо важливим стало використання VPN під час карантинних обмежень, коли багато організацій перейшли на віддалену роботу. VPN допомагає захищати дані, що надсилаються через мережу Інтернет, та надає безпечний доступ до важливих сервісів і ресурсів [25].

В технології віртуальних приватних мереж (VPN) протоколи шифрування використовуються в залежності від протоколу тунелювання, який використовується в конкретному VPN-рішенні. Один з важливих аспектів безпеки в VPN - це автентифікація, тобто підтвердження правильності підключення користувача до мережі [25].

У багатьох VPN-рішеннях використовується стандарт X.509, який є найбільш розповсюдженим стандартом для автентифікації. Цей стандарт використовує сертифікати для підтвердження ідентичності користувачів та забезпечення безпеки під час обміну інформацією. За допомогою правильної конфігурації протоколів автентифікації в VPN можна гарантувати захист від несанкціонованого доступу до мережі [25].

Зараз використання технології VPN набуло великої популярності, і воно стало важливою складовою системи захисту інформації (КСЗІ). Ця технологія необхідна для роботи у різних організаціях, як державних, так і приватних, а також поза межами організацій, особливо у зв'язку з переходом багатьох компаній на віддалену роботу під час карантинних обмежень [25].

VPN мають певні переваги порівняно з іншими методами підключення до мереж. Вони дозволяють користувачам підключатися до офісної мережі через Інтернет, не створюючи окремих комутованих з'єднань і не потребуючи виділених ліній [25].

Однак важливо зауважити, що хоча дані відправляються через мережу Інтернет, це зовсім не означає, що вони не захищені. VPN забезпечують безпеку корпоративної інформації від несанкціонованого доступу, оскільки дані передаються у зашифрованому вигляді і доступ до них має лише правомірний власник. Один з алгоритмів шифрування, який часто використовується, - це Triple DES, який використовує трійний шифрувальний ключ для забезпечення високого рівня безпеки даних [9].

Достовірність у технології віртуальних приватних мереж (VPN) досягається за допомогою двох важливих аспектів: перевірки цілісності даних і ідентифікації

користувачів, які приєднані до VPN. Це гарантує, що дані, які надсилаються через VPN, дійшли до свого призначення без змін та пошкоджень [9].

Для перевірки цілісності даних ідентифікації користувачів використовуються певні алгоритми, які дозволяють виявити будь-які спроби модифікації даних під час їх передачі. Два найпоширеніших алгоритми для цього - MD5 і SHA1. Вони допомагають впевнитися, що дані лишаються недоторканими протягом всього процесу передачі [9].

Окрім цього, VPN використовує перевірку на зміну даних під час їх переміщення через мережу. Це важливо, оскільки це допомагає виявити будь-які навмисні або випадкові зміни в даних, які можуть виникнути в процесі передачі [9].

Мета побудови VPN полягає в створенні безпечних "тунелів" для обміну даними між різними локальними мережами або віддаленими користувачами. Для реалізації цього підходу важливо мати програми, які здатні шифрувати вихідний і вхідний трафік в VPN. Це може бути реалізовано як на рівні програмного забезпечення, так і на рівні апаратно-програмного комплексу, і це може працювати на різних операційних системах, незалежно від того, чи це комп'ютер, чи мобільний пристрій. Важливо зазначити, що автентифікація та шифрування даних є обов'язковими компонентами для забезпечення безпеки в VPN [9].

1.2 Протоколи VPN

Протокол VPN (віртуальної приватної мережі) визначає спосіб взаємодії між системою VPN та іншими системами в Інтернеті, а також рівень захисту трафіку. Використання внутрішнього обміну інформацією не завжди вимагає високого рівня взаємодії, але в таких випадках власні протоколи не обов'язкові. Однак у випадку незахищеної інформації зловмисник може перехопити ключі та розшифрувати трафік [38].

Для створення VPN використовуються різні протоколи. Один із них - Internet Protocol Security (IPSec), який надає деталізовану інформацію про ідентифікацію та методи шифрування для ініціалізації тунелю. Протокол IPSec може використовувати IP-адреси для своєї роботи [38].

Іншими протоколами, які використовуються для VPN, є Point-to-Point Tunneling Protocol (PPTP), Layer-2 Forwarding (L2F) та Layer-2 Tunneling Protocol (L2TP). Ці протоколи об'єднують два першопрохідні протоколи, але вони можуть бути менш функціональними та не охоплювати всі вимоги [38].

Ще одним важливим протоколом є Internet Key Exchange (IKE), який забезпечує передачу інформації через тунель без зовнішніх втручань. Він відповідає за безпечний обмін криптографічними ключами між віддаленими пристроями та автоматизує цей процес за допомогою механізмів шифрування з відкритим ключем.

Link Control Protocol (LCP) - Point-to-Point Protocol (PPP) використовується для налаштування та перевірки каналу зв'язку. LCP визначає параметри інкапсуляції, розміру пакета, параметри з'єднання та автентифікації [38].

Крім того, існують протоколи управління мережею, які встановлюють специфічні конфігураційні параметри для різних транспортних протоколів [38].

Отже, для створення VPN використовуються різні протоколи, такі як PPTP, L2TP, IPSec, OpenVPN, які визначають рівень безпеки та взаємодії між системами VPN та мережею Інтернет [38].

1.3 Функції та компоненти VPN

Безпечний віртуальний VPN - це підхід, який дозволяє поєднати локальні мережі та комп'ютери, використовуючи відкрите зовнішнє середовище для передачі даних в єдиній віртуальній корпоративній мережі. Головною метою цього підходу є забезпечення безпеки даних, які передаються в організації [22].

Під час підключення корпоративної локальної мережі до відкритої мережі виникають деякі недоліки, зокрема [22]:

1. Несанкціонований доступ до даних компанії, які передаються через відкриту мережу.
2. Несанкціонований доступ до внутрішніх ресурсів локальної мережі, який може здійснити зловмисник після отримання доступу до мережі.

Для забезпечення безпеки інформаційної взаємодії використовуються такі функції [22]:

1. Автентифікація взаємодіючих сторін, що дозволяє визначити легітимність користувачів та пристроїв.
2. Криптографічне шифрування даних, що передаються, забезпечуючи їх конфіденційність та недоступність для сторонніх осіб.
3. Перевірка правильності та цілісності переданої інформації, щоб упевнитися, що дані не були під час передачі незаконно модифіковані.

Ці функції базуються на методах комп'ютерної захисту і виконуються з використанням різних засобів і технологій. Для захисту комп'ютерних систем від несанкціонованого доступу з зовнішнього середовища часто використовуються міжмережеві екрани, які контролюють і фільтрують повідомлення, що пересилаються між локальною та відкритою мережами. Для окремих комп'ютерів, які підключені до відкритої мережі, встановлюється відповідне програмне забезпечення міжмережевого екрану [22].

1.4 Мережі VPN та проблеми їх захисту

Сучасний системний адміністратор вважає за рутину налаштовувати VPN-канали для співробітників, які працюють віддалено поза мережею організації. VPN, що означає "віртуальна приватна мережа," використовується для з'єднання двох або більше локальних мереж або комп'ютерів у віртуальну мережу, яка гарантує цілісність та конфіденційність переданих даних [5].

Застосування VPN має свої переваги в порівнянні з іншими методами дистанційного доступу. Наприклад, користувач, який має доступ до Інтернету, може підключитися до мережі своєї організації, не вимагаючи фізичного з'єднання з офісною мережею. Проте загальнодоступність даних не завжди означає їх незахищеність. VPN створює систему безпеки, яка захищає корпоративну інформацію від несанкціонованого доступу. Інформація передається тільки в зашифрованому вигляді, що забезпечує конфіденційність та невідомість для сторонніх осіб [5].

Перевірка цілісності даних та ідентифікація користувачів гарантує, що дані надійшли до адресата без пошкодження і підтверджує легітимність користувачів,

які беруть участь у VPN. Популярні алгоритми для перевірки цілісності даних включають MD5 і SHA1 [5].

Побудова VPN передбачає створення захищених тунелів між локальними мережами чи користувачами для забезпечення цілісності та конфіденційності переданих даних. Для створення VPN з двох кінців зв'язку використовуються програми шифрування для обробки вихідного та вхідного трафіку. Це може бути реалізовано як за допомогою спеціалізованого програмного забезпечення, так і апаратно-програмного комплексу, і підтримується різними операційними системами [5].

VPN мають декілька переваг, таких як економічність, гнучкість і зручність використання. Вони дозволяють організаціям обмежити витрати на обладнання, такі як модеми, сервери доступу та комутаційні лінії, необхідні для надання віддаленим користувачам доступу до їхніх мереж. Рівень безпеки та анонімності в мережах VPN залежить від належної реалізації та налаштувань. Правильне налаштування VPN може забезпечити високий рівень конфіденційності та анонімності віртуальному просторі [5].

Структура VPN включає два рівні [34]:

1. Перший рівень називається "внутрішня мережа," і в організації може бути декілька таких мереж.
2. Другий рівень це "зовнішня мережа," і для з'єднання використовується Інтернет, щоб підключити віддаленого користувача до віртуальної мережі через спеціальний VPN-сервер.

Для підключення до VPN, комп'ютер користувача повинен пройти кілька етапів, включаючи ідентифікацію, автентифікацію і авторизацію. Після успішного завершення цих процесів користувач отримує повний доступ до всієї мережі організації [34].

Сама сутність VPN полягає в створенні віртуального захищеного "тунелю" або шляху, який дозволяє віддаленому користувачеві безпечно підключатися до серверів баз даних, поштових серверів та інших ресурсів через відкриті канали [34].

В технології VPN важливу роль відіграє захист інформації, і цей захист базується на декількох методах, включаючи [34]:

- Тунелювання, що передбачає передачу даних між двома точками зі збереженням конфіденційності щодо всієї мережевої інфраструктури між ними.

За допомогою тунелю можуть бути об'єднані два мережевих вузли. Важливо відзначити, що тунелювання має деякі переваги, але і недоліки, такі як можливість перехоплення інформації та модифікації даних зловмисниками [34].

Зокрема, щоб запобігти таким загрозам, застосовують сучасні методи криптографічного захисту інформації, включаючи використання кваліфікованих електронних підписів (КЕП) і сильних алгоритмів шифрування [34].

Автентифікація грає важливу роль в забезпеченні безпеки в VPN. В процесі передачі даних від клієнтських комп'ютерів до VPN-сервера через Інтернет та інші мережеві пристрої, зокрема, обладнання різних постачальників, важливо застосовувати різні методи автентифікації та шифрування для захисту даних від спотворення та несанкціонованого доступу [34].

Для автентифікації користувачів в мережах PPTP (Point-to-Point Tunneling Protocol) використовуються протоколи для PPP (Point-to-Point Protocol) [34]:

1. EAP (Extensible Authentication Protocol) - розширюваний протокол автентифікації.
2. EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) - розширюваний протокол автентифікації з використанням Transport Layer Security.

3. MSCHAP (Microsoft Challenge Handshake Authentication Protocol), версії 1 і 2 - протокол автентифікації, розроблений Microsoft.
4. CHAP (Challenge Handshake Authentication Protocol) - протокол викликуваної рукостискавшії автентифікації.
5. SPAP (Shiva Password Authentication Protocol) - протокол автентифікації з використанням паролю.
6. PAP (Password Authentication Protocol) - протокол автентифікації за допомогою паролю.

Зазвичай, вважаються найбільш ефективними протоколи MSCHAP версії 2 і EAP-TLS, оскільки вони забезпечують взаємну автентифікацію, де як VPN-сервер і VPN-клієнт ідентифікують один одного. В інших протоколах автентифікації клієнти виконують автентифікацію лише сервера [34].

Автентифікація клієнтів та серверів VPN у випадку L2TP (Layer 2 Tunneling Protocol) над IPSec (Internet Protocol Security) базується на локальних сертифікатах, які видані службою сертифікації. Клієнт і сервер обмінюються сертифікатами та створюють захищене з'єднання ESP SA (Encapsulating Security Payload Security Association). Потім L2TP завершує процес автентифікації комп'ютера і користувача, застосовуючи будь-який протокол. Цей підхід досить безпечний, оскільки шифрує всю сесію. Автентифікація користувачів за допомогою MSCHAP застосовує різні ключі шифрування для автентифікації комп'ютера і користувача, що підвищує рівень захисту [18].

Автентифікація грає ключову роль у забезпеченні безпеки в VPN (віртуальних приватних мережах). У процесі передачі даних від клієнтських комп'ютерів до VPN-сервера через Інтернет і інші мережеві пристрої, що можуть бути частиною різних постачальників, важливо застосовувати різні методи автентифікації та шифрування для захисту даних від спотворення та несанкціонованого доступу [18].

У мережах PPTP (Point-to-Point Tunneling Protocol) для автентифікації користувачів використовують різні протоколи, які базуються на PPP (Point-to-Point Protocol) [18]:

1. EAP (Extensible Authentication Protocol) - розширюваний протокол автентифікації.
2. EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) - розширюваний протокол автентифікації з використанням Transport Layer Security.
3. MSCHAP (Microsoft Challenge Handshake Authentication Protocol), версії 1 і 2 - протокол автентифікації, розроблений Microsoft.
4. CHAP (Challenge Handshake Authentication Protocol) - протокол викликуваної рукостискавшії автентифікації.
5. SPAP (Shiva Password Authentication Protocol) - протокол автентифікації з використанням паролю.
6. PAP (Password Authentication Protocol) - протокол автентифікації за допомогою паролю.

Зазвичай найбільш ефективними вважаються протоколи MSCHAP версії 2 і EAP-TLS, оскільки вони дозволяють взаємну автентифікацію, де і VPN-сервер, і VPN-клієнт ідентифікують один одного. У інших протоколах автентифікації клієнти лише підтверджують свою ідентифікацію перед сервером [18].

У випадку L2TP (Layer 2 Tunneling Protocol) над IPSec (Internet Protocol Security), автентифікація користувачів та серверів VPN базується на локальних сертифікатах, які видані службою сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють захищене з'єднання ESP SA (Encapsulating Security Payload Security Association). Після цього L2TP завершує процес автентифікації комп'ютера і користувача, застосовуючи будь-який протокол. Цей підхід досить безпечний, оскільки шифрує всю сесію. Автентифікація користувачів за допомогою MSCHAP включає в себе використання різних ключів шифрування для автентифікації як комп'ютера, так і користувача, що підвищує рівень захисту [18].

Шифрування грає важливу роль в забезпеченні безпеки при передачі даних через Інтернет. Наразі існують різні методи шифрування [18]:

1. Протокол шифрування MPPE (Microsoft Point-to-Point Encryption) - цей метод сумісний тільки з MSCHAP (версії 1 і 2) і підтримує роботу з ключами довжиною 40, 56 або 128 біт.
2. Протокол EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) - використовує автоматичне вибір довжини ключа шифрування під час узгодження параметрів між клієнтом та сервером.

Протокол MPPE змінює значення ключа шифрування після кожного окремого прийнятого пакету, що дозволяє розшифровувати дані навіть в умовах, коли пакети надходять в хаотичній послідовності. Ця можливість особливо важлива при побудові віртуальних мереж через мережі загального доступу [1].

У загальному, послідовність "тунелювання + автентифікація + шифрування" дозволяє передавати дані між двома точками через мережу загального користування, створюючи враження роботи приватної мережі [1].

Також важливим аспектом в VPN-з'єднаннях є використання системи адресації, аналогічної тій, яка використовується в локальних мережах [1].

Для розгортання VPN створюється VPN сервер в межах організації. Віддалений користувач, використовуючи спеціальне клієнтське програмне забезпечення, ініціює процедуру зв'язку з сервером. Після автентифікації користувача та узгодження параметрів забезпечення безпеки, встановлюється VPN-з'єднання. Це забезпечує захищену передачу даних між клієнтом і сервером за допомогою шифрування та перевірки цілісності даних [1].

Однак однією з глобальних проблем мереж VPN є відсутність стандартів для автентифікації та обміну зашифрованою інформацією. Ця проблема ускладнює процес об'єднання мереж компаній-партнерів та сповільнює розповсюдження VPN [7].

VPN зазвичай розгортають на мережевому рівні і можуть застосовувати транспортні протоколи, такі як TCP і UDP [7].

Для створення віртуальних мереж часто використовують інкапсуляцію протоколу PPP в інший протокол, такий як PPTP чи Ethernet (PPPoE). VPN можуть використовуватися для створення приватних мереж, а також для надання доступу до Інтернету [7].

Правильна настройка та використання VPN може забезпечити високий рівень шифрування та анонімність в мережі [7].

РОЗДІЛ 2: ДОПУСТИМІ КОНЦЕПЦІЇ ТА КОНФІГУРАЦІЇ ДЛЯ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ VPN

2.1 Способи захисту каналів корпоративних мереж на базі VPN

Корпоративна мережа (КМ) представляє собою систему мереж та сервісів передачі даних, призначених для створення безпечного мережевого простору, обмеженого в межах конкретної організації та призначеного для використання обмеженого 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. Відеоконференційний зв’язок;
6. Корпоративна електронна пошта;
7. Корпоративна IP-телефонія.

Особливостями КМ є [23]:

Застосування інструментарію для роботи при передачі даних

1. загального користування.
2. Доступ до інформації надається певному колу осіб.
3. Циркуляція інформації трьох типів: офіційна, проектна/групова та
4. неофіційна.
5. 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.

Елементи, які входять до складу корпоративної мережі, охоплюють корпоративний сервер баз даних, електронний документообіг, доступ до мережі Інтернет, апаратний та програмний захист інформації, відеоконференцзв'язок, корпоративну електронну пошту та корпоративну IP-телефонію [41].

Основні риси корпоративної мережі включають застосування інструментів для передачі даних загального користування, обмежений доступ до інформації для конкретного кола осіб, циркуляцію інформації різних типів (офіційна, проектна/групова, неофіційна) та наявність єдиної системи управління корпоративною мережею [41].

Корпоративна мережа надає можливість ефективно об'єднувати територіально розташовані підрозділи компанії, що в свою чергу дозволяє здійснювати роботу в режимі онлайн, забезпечувати віддалений доступ до сервісів КМ, використовувати мережу Інтернет та розсилати дані за адресами. Однією з переваг є можливість зниження витрат на Інтернет, оскільки доступ до Інтернету здійснюється через єдиний сервер, а канали розподіляються в межах компанії [41].

Функціональні елементи корпоративної мережі (КМ) включають робочі місця користувачів, які можуть знаходитися або в одному приміщенні, або в будь-якому іншому місці. Інформаційні сервери організації призначені для зберігання та обробки даних і можуть розташовуватися як всередині, так і поза організацією. Засоби телекомунікації взаємодіють між робочими станціями та інформаційними серверами [41].

Засоби телекомунікації організації можуть бути виділеними або загального призначення, причому загального призначення є найпоширенішими. Телеслужби в межах організації реалізують інформаційний вплив через служби телекомунікації [41].

Корпоративна мережа має систему управління ефективністю, яка включає керовані та некеровані функціональні елементи, систему управління безпекою, систему забезпечення надійності, систему діагностики та контролю та систему експлуатації. Класифікація КМ може відбуватися за набором функціональних

елементів, ієрархією керування, поєднанням підмереж загального користування та реалізованих телеслужб [41].

Безпека КМ є надзвичайно важливою для успіху будь-якої організації, забезпечуючи захист конфіденційності даних, стійкість до атак та безперервний доступ до інформації. Вирішення завдань, пов'язаних з КМ, стає більш складним у випадках великих корпорацій з географічно розташованими підрозділами та датацентрами, що вимагає дбайливого планування та розвитку [41].

З розвитком Інтернету та загальнодоступного доступу до інформації в реальному часі виникла потреба в розвитку корпоративних мереж (КМ). Користувачі мали можливість використовувати доступні та вигідні Інтернет-канали. Організації, у зв'язку з цим, повинні використовувати безпечні канали для передачі важливої комерційної та управлінської інформації [11].

Захищена віртуальна мережа (VPN) – це об'єднання локальних мереж та окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, сприяючи безпеці обміну даними [11].

При підключенні локальної корпоративної мережі до відкритої мережі виникають дві основні загрози безпеці [11]:

1. Несанкціонований доступ до корпоративних даних під час їх передачі через відкриті канали.
2. Несанкціонований доступ до внутрішніх ресурсів локальної корпоративної мережі, отриманий зловмисником через порушення безпеки мережі.

Сучасні корпоративні мережі складаються з різних компонентів, таких як комп'ютери, системне та прикладне програмне забезпечення, мережеві адаптери, комутатори, маршрутизатори та їх взаємодіючі системи. Використання Інтернету та інформаційних технологій призводить до змін у сфері обчислювальних мереж, де Інтернет тепер виступає не лише як засіб передачі, але і як засіб для взаємодії та ведення ділових операцій організацій [11].

Популярність IP-технологій пояснюється декількома перевагами. По-перше, легкість принципів технології, виражена в їхній відкритості, що сприяє вільному обговоренню, дослідженню та тестуванню нових протоколів стеку TCP/IP. Ця

відкритість дозволяє легко інтегрувати інші технології у IP-мережі, що значно розширює область використання Інтернету. По-друге, масштабованість, продумана при розробці Інтернету, дозволяє наростити мережу організації у великих масштабах [11].

Переваги цих технологій стали основою для успіху Інтернету і визначають їхню перспективність для внутрішніх мереж організацій, таких як інтранети. Інтранет - це мережа, яка використовує програмне забезпечення, побудоване на стеку протоколів TCP/IP [11].

Екстранет-мережа - це інтранет-мережа, яка підключена до Інтернету, але має обмежений доступ до своїх ресурсів для конкретної категорії користувачів з відповідними повноваженнями [11].

Особливості корпоративних мереж (КМ), також відомих як інтранети, включають глобальність зв'язків, масштабованість та гетерогенність, що призводить до підвищеної небезпеки виконання функціональних завдань. Протоколи сімейства TCP/IP, хоча розроблені досить давно, сталкиваються з актуальними проблемами, такими як безпека, оскільки вони були розроблені як функціональні засоби для розширення стеку TCP/IP на різних комп'ютерних платформах. Застосування Інтернету створює можливості для зловмисників проникати в корпоративні мережі [27].

Зі зростанням кількості хостів, підключених до мережі Інтернет, та розширенням компаній, які використовують технології Інтернету, збільшується кількість інцидентів, пов'язаних із інформаційною безпекою (ІБ). CERT (Computer Emergency Response Team) реєструє вразливості та збільшення кількості інцидентів [27].

Вразливості інформаційних систем - це характеристики, які використовуються зловмисниками для реалізації загроз. Загрози інформаційних систем - це потенційно можливі події, дії, процеси чи явища, які можуть завдати шкоди ресурсам системи. Види загроз визначають параметри, які направлені на захист інформації [27].

Важливим ефектом VPN-з’єднання є можливість використання системи адресації, аналогічної тій, що використовується в локальній мережі. Реалізація віртуальної приватної мережі на практиці включає в себе встановлення VPN-серверу. При цьому віддалений користувач ініціює процедуру з’єднання з сервером, використовуючи клієнтське програмне забезпечення VPN [10].

Процес включає в себе автентифікацію користувача, встановлення VPN-з’єднання та погодження деталей забезпечення безпеки. Після успішної автентифікації між клієнтом та сервером встановлюється VPN-з’єднання, що дозволяє обмінюватися інформацією. Однак головною проблемою може бути відсутність фіксованих стандартів для автентифікації та обміну шифрованою інформацією. Зазначено, що стандарти знаходяться в процесі розробки або плануються до розробки, що може призвести до повільного прийняття VPN в організаціях, оскільки це не є обов'язковим, і впровадження їх не може бути примусовим [10].

2.2 Концепція побудови віртуальних захищених мереж VPN

Основна ідея, яка лежить в основі побудови віртуальної приватної мережі (VPN), полягає в тому, що два вузли, які потрібно обміняти між собою, встановлюють віртуальний тунель. Цей тунель призначений для забезпечення конфіденційності та цілісності інформації, яка передається через відкриті мережі. Доступ до цього тунелю робиться складним для всіх учасників, захищаючи від сторонніх осіб, які не є учасниками цього обміну [29].

Організації, що використовують такі віртуальні тунелі, відзначають ряд переваг, зокрема, економію фінансових ресурсів. Це досягається завдяки відсутності необхідності у побудові або оренді виділених каналів зв'язку для створення власних інтранет / екстранет мереж. Замість цього вони використовують доступні та економічні канали Інтернету. Такий підхід забезпечує надійність та швидкість передачі інформації, не втрачаючи ефективності. Економічна вигода від впровадження технології VPN служить стимулом для активного застосування її в організаціях [29].

Для з'єднання корпоративної локальної мережі з відкритою мережею, такою як Інтернет, виникають різні загрози безпеки. До них відносяться [36]:

1. **Несанкціонований доступ до внутрішніх ресурсів корпоративної локальної мережі**: Атаки, які спрямовані на отримання несанкціонованого доступу до внутрішніх ресурсів шляхом вторгнення в мережу.
2. **Несанкціонований доступ до корпоративних даних у процесі передачі через відкриту мережу**: Ризик несанкціонованого доступу до конфіденційної інформації, яка передається відкритими каналами зв'язку.

Для забезпечення безпеки інформаційної взаємодії локальних мереж і окремих комп'ютерів через відкриті канали зв'язку, можна використовувати різні заходи [36]:

1. **Мережевий екран**: Встановлення мережевого екрану між локальною та відкритою мережею. Цей елемент фільтрує двосторонній потік повідомлень, виконуючи функції посередництва при обміні інформацією. Мережевий екран розташовується між цими мережами.
2. **Віртуальні приватні мережі (VPN)**: Захист інформації у процесі передачі здійснюється за допомогою віртуальних захищених мереж VPN. VPN є об'єднанням локальних мереж та окремих комп'ютерів через відкрите середовище, створюючи безпечний тунель для циркуляції даних. Такі віртуальні захищені канали зв'язку відомі як тунелі VPN, і вони дозволяють об'єднувати різні мережі та передавати інформацію через Інтернет.

Такі заходи допомагають захистити локальні мережі та окремі комп'ютери від потенційних загроз з боку зовнішнього середовища [20].

Тунель VPN виникає шляхом проведення криптографічно захищених пакетів даних через відкриту мережу, створюючи віртуальну приватну мережу. Захист інформації під час передачі через VPN-тунель базується на декількох принципах [20]:

1. **Автентифікація взаємодіючих сторін**: Перевірка і підтвердження ідентичності сторін, які здійснюють з'єднання через тунель VPN. Це важливий етап для

забезпечення того, що тільки легітимні користувачі мають доступ до віртуальної мережі.

2. **Криптографічне закриття переданих даних**: Використання криптографічних методів для шифрування даних, які передаються через тунель. Це забезпечує конфіденційність і непроникність інформації в процесі передачі.
3. **Перевірка достовірності та цілісності інформації**: Засоби для визначення, чи були дані змінені або пошкоджені під час передачі. Це гарантує, що інформація, яка надходить, є вірною та не була піддана несанкціонованій модифікації.

Такий підхід забезпечує повністю захищений канал для обміну даними між точками, які використовують VPN-тунель, забезпечуючи високий рівень безпеки та конфіденційності інформації [20].

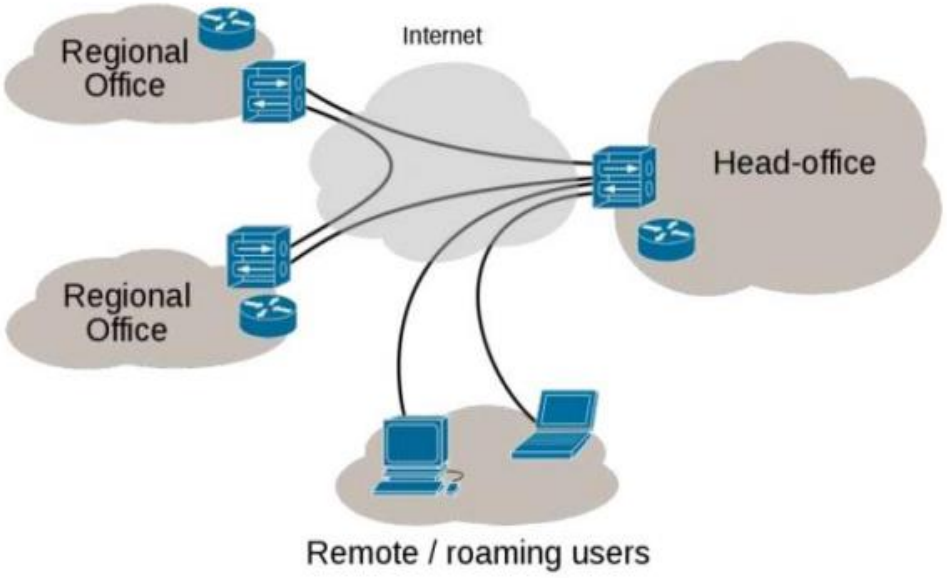

Рисунок 2.1 – Віртуальна захищена мережа VPN

Для реалізації функцій VPN взаємодія між сторонами характеризується. У виконанні цих функцій застосовуються криптографічні методи для захисту інформації. Забезпечення ефективності відбувається завдяки використанню симетричних та асиметричних криптографічних систем. Тунель, створений VPN, представляє собою безпечний канал, який розгортається в межах відкритої мережі [20].

Ролі в облаштуваннях VPN виконують VPN клієнт, VPN сервер та шлюз безпеки VPN [20].

1. **VPN клієнт**: Це програмний або програмно-апаратний комплекс, розгорнутий на персональному комп'ютері. Він модифікує мережеве програмне забезпечення для шифрування та автентифікації трафіку. VPN клієнт взаємодіє з іншими VPN клієнтами, серверами та шлюзами безпеки VPN. Реалізація VPN клієнта може бути програмним рішенням, яке доповнює стандартну операційну систему, таку як Windows 7/10 чи Unix.
2. **VPN сервер**: Це програмне або апаратно-програмне забезпечення, встановлене на сервері, яке виконує функції сервера. VPN сервер захищає сервери від НСД, організує захищені з'єднання з окремими комп'ютерами та сегментами локальних мереж. Він є функціональним аналогом VPN клієнта для серверних платформ та має розширені ресурси для підтримки багатьох з'єднань з VPN клієнтами. VPN сервер підтримує захищені з'єднання з мобільними користувачами.
3. **Шлюз безпеки VPN**: Це мережевий пристрій, який з'єднується з двома мережами та здійснює функції шифрування та автентифікації для численних хостів. Він розміщується для проходження трафіку, який призначений для внутрішньої корпоративної мережі. Шлюз безпеки VPN може бути реалізований як окреме програмне рішення або апаратний пристрій, такий як маршрутизатор чи мережевий екран, з функціями VPN.

Відкрите зовнішнє середовище передачі інформації охоплює різноманітні шляхи для швидкого обміну даними, такі як канали Інтернету та телефонні мережі. Ефективність віртуальної приватної мережі (VPN) визначається рівнем захищеності інформації, яка передається через відкриті канали зв’язку. Для забезпечення безпечної передачі даних через ці канали використовується метод інкапсуляції та тунелювання [29].

Механізм тунелювання дозволяє передавати пакети даних через загальнодоступну мережу. Для кожної пари "відправник-отримувач" встановлюється індивідуальний тунель, що представляє собою логічне з'єднання [29].

Це дозволяє інкапсулювати дані одного протоколу в пакети іншого. Процес тунелювання полягає в упаковці певної кількості даних, разом із службовими

полями, у новий "конверт". Пакет протоколу більш низького рівня розміщується у полі даних пакету протоколу більш високого або такого ж рівня [29].

Важливо зауважити, що тунелювання, хоча і є ефективним засобом захисту, не є панацеєю. Воно не забезпечує повноцінний захист від несанкціонованого доступу чи спотворення даних. Однак завдяки тунелюванню можна досягти повного конфіденційності початкових пакетів, які інкапсулюються. Для забезпечення конфіденційності переданих даних, відправник шифрує початкові пакети, упаковує їх у зовнішній пакет із новим IP-заголовком, а потім відсилає через транзитну мережую (Рис. 2.2) [29].

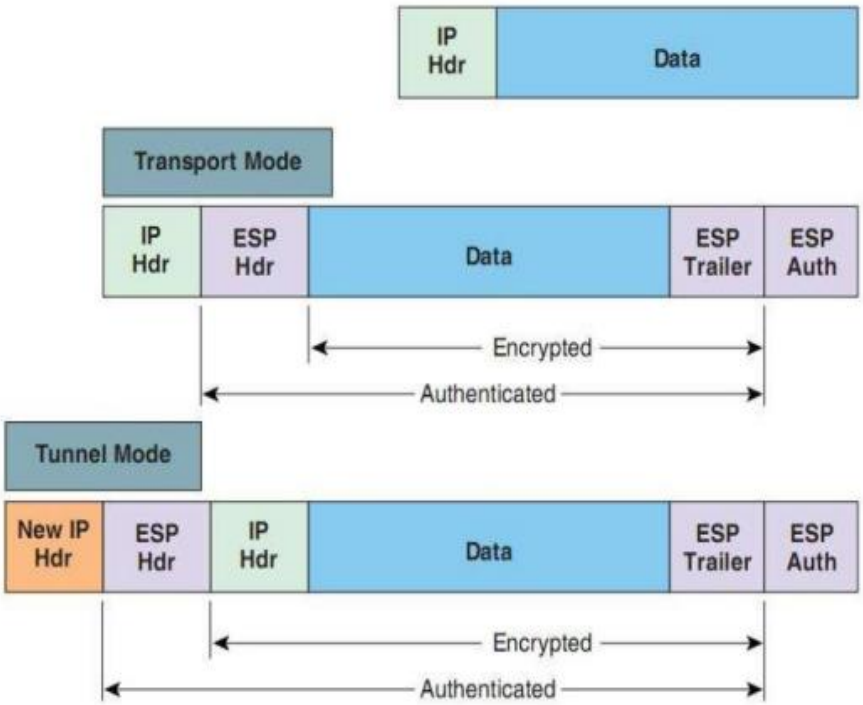

Рисунок 2.2 – Приклад пакету, підготовленого для тунелювання

Технологія тунелювання має особливість - здатність повністю зашифровувати початковий пакет, включаючи не лише поле даних, але і поля заголовка. Деякі з цих заголовкових полів містять конфіденційну інформацію, яка може бути використана для атаки, якщо потрапить у руки зловмисника. Ця інформація може включати в себе деталі внутрішньої структури мережі, інформацію про кількість підмереж та вузлів, а також IP-адреси. Зашифрований заголовок початкового пакету не використовується для маршрутизації через мережу, що дозволяє уникнути витоку конфіденційної інформації [29].

Для захисту початкового пакету використовується процес інкапсуляції та тунелювання. Початковий пакет повністю шифрується, а потім цей зашифрований пакет упаковується у новий зовнішній пакет з відкритим заголовком. Для передачі даних через відкриту мережу використовуються відкриті поля заголовка зовнішнього пакету [29].

Після того, як пакет доставлений, внутрішній початковий пакет витягується, розшифровується і використовується для відновлення та подальшої передачі в межах внутрішньої мережі. Такий підхід дозволяє забезпечити конфіденційність та цілісність даних, які передаються через відкриті мережі (Рис.2.3) [29].

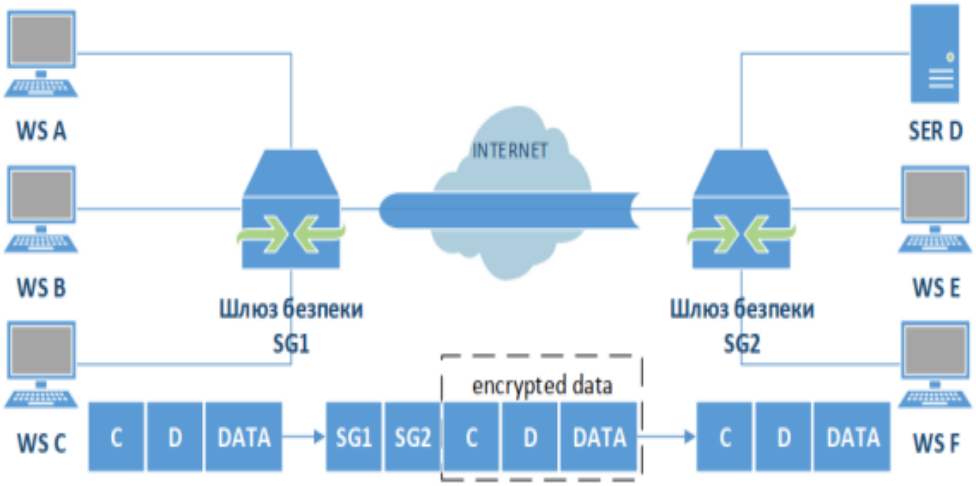

Рисунок 2.3 – Схема віртуального захищеного тунелю

Тунелювання застосовується з метою забезпечення конфіденційності, цілісності та автентичності даних пакету, розповсюджуючи КЕП (ключ-еквівалентні параметри) на всі поля пакету. Окрім того, цей процес дозволяє приховати мережеву структуру між двома точками та уникнути можливих конфліктів адрес між двома локальними мережами [40].

Коли компанія формує локальну мережу, яка не має прямого зв'язку з Інтернетом, вона може використовувати будь-які IP-адреси для своїх мережевих пристроїв та комп'ютерів. Проте при об'єднанні раніше ізольованих мереж може виникнути конфлікт адрес між ними та з адресами, які вже використовуються в Інтернеті. Тунелювання розв'язує цю проблему шляхом інкапсуляції пакетів, яка приховує первинні адреси та додає нові (унікальні). Ці нові адреси можуть

використовуватися для подальшої передачі даних між розділеними мережами. Також, тунелювання дозволяє встановлювати IP-адреси та інші параметри для мобільних користувачів, які приєднуються до локальної мережі [40].

Отже, тунелювання вирішує проблеми конфліктів адрес та забезпечує безпечну та ефективну передачу даних через мережі [40].

Механізм тунелювання використовується у різних протоколах для формування захищеного каналу. Цей тунель утворюється лише на ділянці відкритої мережі, де існує загроза порушення конфіденційності та цілісності даних, а саме між точкою входу у відкритий Інтернет та точкою входу у корпоративну мережу (КМ). Зовнішні пакети отримують адреси пограничних маршрутизаторів, встановлених у двох точках, тоді як внутрішні адреси кінцевих вузлів формуються у внутрішніх початкових пакетах у захищеному вигляді [40].

Під час створення безпечної віртуальної мережі VPN головною метою є забезпечення інформаційної безпеки (ІБ). Згідно з різними нормативно-правовими актами, ІБ характеризується трьома основними аспектами: конфіденційністю, цілісністю та доступністю. У контексті завдань VPN критерії безпеки даних розглядаються наступним чином [40]:

- **Конфіденційність:** Інформація, що передається, повинна бути доступна лише відправнику та отримувачу. Забезпечення конфіденційності використовує різні методи і алгоритми симетричного і асиметричного шифрування.
- **Цілісність:** Інформація має бути доставлена без модифікацій та пошкоджень. Забезпечення цілісності переданих даних зазвичай використовує технології КЕП, які базуються на асиметричних методах шифрування та односторонніх функціях.
- **Доступність:** Інформація повинна бути доступною лише легальним користувачам.

Автентифікація здійснюється за допомогою багаторазових та одноразових паролів, кваліфікованих сертифікатів, смарт-карт, а також протоколів суворої автентифікації, що дозволяє встановлювати VPN-з'єднання лише для легальних користувачів та запобігає доступу небажаним особам [40].

Авторизація надає доступ абонентам лише після підтвердження їхньої автентичності. Авторизація та управління доступом часто реалізуються за допомогою тих самих засобів [40].

Для забезпечення безпеки передачі даних у віртуальних захищених мережах вирішуються наступні завдання [15]:

1. **Взаємна автентифікація абонентів при встановленні з'єднання:** Абоненти проходять взаємну автентифікацію при встановленні з'єднання. Це забезпечує вхід лише легальним користувачам та має на меті запобігти доступу небажаних осіб до мережі.
2. **Забезпечення конфіденційності, цілісності та автентичності інформації:**

- **Конфіденційність:** Інформацію шифрують для захисту від несанкціонованого читання та копіювання.
- **Цілісність:** Гарантує, що передані дані не модифікувалися.
- **Автентичність:** Забезпечує, що інформація має правильного відправника та отримувача.

3. **Авторизація та керування доступом:** Компонент безпеки VPN гарантує доступ до комп'ютерних сервісів лише для авторизованих користувачів. Це може бути реалізовано через централізовану або децентралізовану схему авторизації. Ролеве керування доступом також використовується для покращення керованості системи, розподіляючи ролі з певними правами між користувачами чи сервісами.
4. **Безпека периметра мережі та виявлення вторгнень:** Застосовуються жорсткий контроль доступу до сервісів та ресурсів мережі, використовуються засоби безпеки, такі як мережевий екран, системи виявлення вторгнень (IDS), системи аналізу захищеності, та антивіруси. Важливою є функція мережевого екрану, IDS та систем аналізу захищеності.
5. **Керування безпекою мережі:** Управління безпекою мережі включає інтеграцію мережевих пристроїв та сервісів для контролю над безпекою та пропускною здатністю. Для організацій важливим є всебічне управління пристроями та сервісами через інфраструктуру VPN, що охоплює користувачів віддаленого доступу та ресурси extranet. Система управління мережею об'єднує різноманітні

інструменти для керування політиками безпеки, пристроями та сервісами VPN будь-якого розміру [15].

2.3 Конфігурація VPN для безпечної передачі даних

Прогрес у використанні Інтернету для безпечної передачі даних продовжує розвиватися і вдосконалюватися, оскільки зростає кількість користувачів мережі. Це примушує всі галузі людської діяльності переосмислювати пріоритети в бізнесі та враховувати вимоги та потреби сучасного суспільства [30].

Рівень інформативності суспільства визначається рівнем володіння конкретною інформацією чи знаннями. Забезпечення безпеки інформації під час передачі через відкриті канали базується на виконанні таких функцій [30]:

- Автентифікація взаємодіючих сторін.
- Криптографічне зашифрування передаваних даних.
- Перевірка достовірності та цілісності доставленої інформації.

Для цих функцій характерний взаємозв'язок "один до одного", їх реалізація базується на використанні засобів криптографічного захисту інформації, ефективність яких забезпечується за рахунок комбінації симетричних та асиметричних криптографічних систем [30].

Постійна потреба в безпеці та економічно вигідній передачі даних через загальнодоступні засоби є об'єктом збільшеного інтересу у сфері IT. Ефективність VPN визначається ступенем захищеності інформації, що передається відкритими каналами зв'язку. Захист даних під час передачі ґрунтується на створенні захищених віртуальних каналів зв'язку, які представляють собою VPN-тунелі [30].

Тунелювання не забезпечує безпеку від НСД чи модифікації даних, проте надає можливість повного криптографічного захисту інформації, яка інкапсулюється. З метою забезпечення конфіденційності передачі даних, тунель шифрує початкові пакети та впаковує їх у новий пакет з іншим IP-заголовком для відправки через транзитну мережу. На кінці захищеного каналу внутрішні початкові пакети вилучаються та розшифровуються зовнішньою оболонкою, і відновлений заголовок застосовується для подальшої передачі внутрішньою мережею [30].

Тунелювання застосовується для забезпечення конфіденційності, цілісності та автентичності даних, використовуючи КЕП. Крім того, вирішуються проблеми переходів між мережами з різними протоколами. Цей процес організовує взаємодію кількох різнотипних мереж з метою забезпечення цілісності та конфіденційності передаваних даних, а також подолання невідповідностей зовнішніх протоколів чи схем адресації. Для тунелювання використовуються протоколи канального рівня, такі як PPTP і L2TP, а також протокол мережевого рівня IPSec [30].

Безпека обміну інформацією вирішує завдання об'єднання локальних мереж та надання доступу до них для виділених або мобільних користувачів. При проектуванні віртуальної приватної мережі (VPN) розглядаються дві основні схеми [30].

1. **Мережа-мережа**: Ця схема використовується для заміни виділених ліній між віддаленими офісами. Замість того, щоб з'єднувати офіси безпосередньо, створюються захищені канали (тунелі) між ними. Шлюз служить інтерфейсом між тунелем та локальною мережею, і користувачі використовують тунель для спілкування між собою. Цей тип VPN може слугувати альтернативою або доповненням до глобальних мережевих з'єднань.
2. **Користувач-мережа**: Ця схема застосовується для створення з'єднань із віддаленими чи мобільними користувачами. Клієнт ініціює створення тунелю до шлюзу, який захищає віддалену мережу. Даний тип VPN замінює комутовані з'єднання та може використовуватися разом з методами віддаленого доступу.

Для забезпечення безпеки передачі даних у VPN вирішуються завдання мережевої безпеки, такі як взаємна автентифікація користувачів, забезпечення конфіденційності, цілісності та автентичності переданої інформації, а також авторизація та управління доступом. Існують різні підходи до побудови VPN, і вибір протоколів визначається функціональністю мережі та бюджетними обмеженнями. Адміністраторам IT-підрозділів доводиться вирішувати проблему вибору оптимальних рішень для побудови захищеної VPN мережі, порівнюючи переваги та недоліки різних протоколів [14].

Порівняльний аналіз протоколів L2TP, IPSec та SSL, які претендують на вирішення проблем безпеки в VPN, приводить до наступних висновків [14]:

1. **L2TP (Layer 2 Tunneling Protocol)**:

   Переваги: Незалежність від транспортного рівня, що дозволяє використовувати його в гетерогенних мережах.

   Недоліки: Складно гарантувати підтримку мереж та маршрутизаторів через "канальну природу" протоколу.

2. **IPSec (Internet Protocol Security)**:

   Переваги: Забезпечує автентифікацію, перевірку цілісності та шифрування повідомлень на рівні кожного пакету. Прозорий протокол, працює між мережами з IPv4 та IPv6.

   Недоліки: Встановлення VPN-клієнта на робочу станцію може знизити швидкість обміну даними на низькошвидкісних каналах.

3. **SSL (Secure Sockets Layer)**:

   Переваги: Забезпечує захист даних між сервісними та транспортними протоколами за допомогою асиметричних ключів для шифрування/розшифрування інформації. Розпізнає сервер та клієнта, має високу ефективність та не навантажує сервер вище міри.

   Недоліки: Використовується через браузер, а не окремий VPN-клієнт.

   Кожен протокол має свої сильні та слабкі сторони, і вибір між ними залежить від конкретних потреб та умов використання.

РОЗДІЛ 3: ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ ОБМІНУ ДАНИМИ ВІДАЛЕНИХ КОРИСТУВАЧІВ НА БАЗІ VPN

3.1 Розробка VPN мережі

У вигляді спроектованої віртуальної мережі входять декілька ключових компонентів, включаючи шлюзи кодування, програму контролю цілісності та модулі генерації та розподілу ключів, а також реєстрації та підготовки електронних ключів для мобільних клієнтів [14].

Шлюз виступає основним модулем VPN і виконує кілька важливих функцій, включаючи маршрутизацію, фільтрацію та кодування пакетів. Кожен шлюз призначений для захисту конкретної групи локальних мереж. На комп'ютері-шлюзі встановлюється модуль, що відповідає за кодування та декодування, а також програма аутентифікації [14].

Ці елементи спільно працюють для створення безпечного та ефективного з'єднання в мережі. Шлюзи відповідають за забезпечення безпеки та обміну даними між різними локальними мережами, забезпечуючи маршрутизацію і фільтрацію трафіку. Модулі генерації та розподілу ключів відповідають за забезпечення безпеки ключів, які використовуються для кодування та декодування даних. Програма контролю цілісності відповідає за перевірку цілісності даних під час їх передачі через мережу [21].

Усі ці компоненти працюють у взаємодії, щоб забезпечити високий рівень безпеки та функціональності віртуальної мережі [21].

Функції шлюзу включають кілька ключових завдань, які спрямовані на забезпечення безпеки та ефективності віртуальної мережі [21]:

1. **Фільтрація трафіка:** Шлюз відповідає за визначення та обробку трафіку, що проходить через мережу, фільтруючи його відповідно до зазначених правил та параметрів.
2. **Кодування трафіка:** Ця функція полягає в захисті конфіденційності даних шляхом їх кодування перед передачею через мережу, забезпечуючи таким чином захист від несанкціонованого доступу.

3. **Взаємодія з іншими шлюзами:** Шлюз взаємодіє з іншими аналогічними вузлами в мережі, сприяючи обміну інформацією та координації для забезпечення єдиної системи безпеки.
4. **Реєстрація подій у центрі моніторингу:** Шлюз фіксує події та інциденти, пов'язані з безпекою, та передає цю інформацію в центр моніторингу для подальшого аналізу та реагування.
5. **Забезпечення власного захисту:** Ця функція передбачає заходи для захисту самого шлюзу від можливих загроз та атак, забезпечуючи стійкість та безпеку його функціонування.

Модуль розподілу ключів відповідає за керування периметром безпеки та виконує такі завдання [21]:

1. **Одержання відкритих ключів шлюзів:** Модуль отримує відкриті ключі шлюзів з визначеного джерела.
2. **Розсилання повідомлень про зміни структури мережі:** Модуль інформує інші шлюзи про будь-які зміни в структурі захищеної мережі.
3. **Виконання процедури зміни сеансових ключів:** Модуль забезпечує безпечну зміну сеансових ключів для підтримки неперервного захисту.
4. **Збереження інформації про структуру мережі:** Модуль зберігає важливу інформацію щодо структури мережі для ефективного управління безпекою.

Модуль генерації ключів включає в себе кілька етапів:

1. **Генерація пар ключів:** Створення пар відкритого і секретного ключів для кодуючих модулів.
2. **Генерація ключів для сертифікації:** Створення пар ключів для процедури сертифікації відкритих ключів кодуючих модулів.
3. **Генерація сертифікатів відкритих ключів:** Створення сертифікатів відкритих ключів, які підписуються секретним ключем сертифікації.
4. **Розміщення та збереження сертифікатів:** Розміщення підписаних сертифікатів відкритих ключів на змінні носії та збереження еталонних копій в архіві.

Засоби формування та перевірки контрольних сум файлів у VPN представлені програмою контролю цілісності. Ця програма призначена для виявлення,

повідомлення та реагування на будь-які зміни, додавання або видалення файлів у системі, забезпечуючи контроль за їх цілісністю та безпекою [37].

Функції кодування інформаційних потоків між мережами в межах VPN виконуються спеціальними протоколами. Кожна мережа, яка входить до складу VPN, захищена власним кодуючим модулем, розташованим в точці її з'єднання з зовнішніми мережами. Захищена інформація кодується перед відправленням на передавальному модулі і розкодовується на приймальному, тобто передається у відкритому вигляді в межах локальних мереж і у кодованому за їхніми межами [37].

VPN створює периметр безпеки, що об'єднує IP-адреси всіх абонентів, які мають доступ до віртуальної захищеної мережі. Абонентами VPN можуть бути цілі мережі, їх підмережі та окремі робочі станції [37].

Периметр безпеки формується для розділення трафіку на трафік, який кодується, та той, який не кодується. Кодуючий модуль VPN визначає пакети, які потрібно кодувати, на підставі IP-адрес відправника та одержувача пакета, а також інтерфейсу, через який проходить пакет. Кодування даних виконується за допомогою сеансових ключів, які автоматично генеруються за допомогою довгострокових ключів і мають обмежений термін дії [37].

VPN виконує необхідні кроки з управління ключами, такі як генерація та розподіл довгострокових ключів, створення сеансових ключів, сертифікація відкритих ключів та планова зміна ключів кодування [37].

Протоколи VPN також відповідають за збір та збереження статистичної та службової інформації щодо всіх подій, пов'язаних з аутентифікацією вузлів, передачею кодованої інформації та обмеженням доступу абонентів в локальній обчислювальній мережі. Засоби моніторингу здійснюють збір і аналіз протоколів реєстрації від усіх модулів комплексу по кодованому каналу [37].

3.2 Локальна мережа головного корпусу

Локальна комп'ютерна мережа побудована на основі технології Fast Ethernet і забезпечує швидкість передачі даних на рівні 100 Мбіт/с. Фізично використовується специфікація 100 Base-TX, яка використовує UTP-кабель 5-ї категорії. Мережа працює під управлінням операційної системи Windows NT 2000,

використовуючи стек телекомунікаційних протоколів TCP/IP та налічує 50 комп'ютерів [39].

З прикладного програмного забезпечення використовується текстовий редактор Word, редактор електронних таблиць Excel, поштова програма Outlook та система управління базами даних Oracle. У мережу включені різні сервери, такі як маршрутизатор для доступу в Інтернет, сервер VPN, сервер DNS, сервер SMTP, сервер FTP/HTTP та міжмережевий екран [39].

Вхідний маршрутизатор відокремлює мережу Інтернет-провайдера від корпоративної мережі. Основна фільтрація трафіку відбувається на цьому маршрутизаторі, який допускає в мережу тільки дозволений TCP або UDP трафік від вузлів з допустимими IP-адресами. Це дозволяє відкидати трафік з небажаних напрямків або від неавторизованих сервісів [39].

Міжмережевий екран (брандмауер) виконує фільтрацію та аналіз TCP-сесій, що проходять через нього. Він може мати кілька сегментів, відомих як "демілітаризовані зони" (DMZ), наприклад, для серверів, що відкриті для публічного доступу (Web, FTP), або для підключення серверів VPN. DMZ обмежує не тільки трафік за IP-адресами і TCP-портами, але і його напрямок, запобігаючи можливості завантажити на скомпрометований сервер додаткові атаки та не дозволяючи хакерам переключати деякі сесії під час атак [39].

У системі загальної безпеки відіграє ключову роль сервер DNS, який має обмежити небажаному користувачеві доступ до вивчення мережі. Для цього він встановлює заборону на міжзональні пересилання (zone transfers) для всіх вузлів, за винятком авторизованих вторинних серверів DNS. Сервер SMTP також відіграє важливу роль, проводячи перевірку електронних повідомлень, які користувачі відправляють, та блокуючи віруси, які можуть потрапляти во внутрішню мережу. Міжмережевий екран також фільтрує SMTP-повідомлення, пропускаючи тільки необхідні команди для поштового сервера [39].

Внутрішній маршрутизатор виконує функції розподілу IP-адрес та маршрутизації між сегментами Інтернету та корпоративною мережею. Цей пристрій виступає в ролі маршрутизатора і не проводить фільтрацію вхідного

трафіку. Власне кажучи, він є межею між внутрішньою мережею та зовнішнім середовищем.

Концентратор VPN забезпечує безпечне підключення віддалених користувачів до корпоративної мережі. Перед наданням користувачеві доступу до мережі, концентратор VPN встановлює сесію зв'язку із сервером контролю доступу у внутрішній мережі. Цей сервер, за допомогою системи одноразових паролів, проводить аутентифікацію користувача, забезпечуючи високий рівень захисту.

Після концентратора VPN трафік надходить на міжмережевий екран. Існують різні конфігурації включення міжмережевого екрана та VPN шлюзу, і розглянемо основні [35]:

1. **Шлюз VPN на брандмауері:**

- *Перевага:*
- Є лише одна точка керування інформаційною безпекою, що спрощує налаштування.
- *Недолік:*
- Неправильне налаштування брандмауера може допустити Інтернет-трафіку у внутрішню мережу через адреси VPN.

2. **Шлюз VPN попереду брандмауера:**

- *Переваги:*
- VPN трафік не проходить через брандмауер, що дозволяє уникнути змін у його конфігурації для підтримки пакетів VPN.
- Легка масштабованість мережі.
- *Недолік:*
- VPN-сервер прямо пов'язаний з Інтернетом.

3. **Шлюз VPN позаду брандмауера:**

- *Перевага:*
- VPN повністю захищена від Інтернету брандмауером.
- *Недоліки:*
- Весь потік інформаційного обміну мережі VPN повинен пройти через брандмауер, збільшуючи час затримки.
- Брандмауер не може перевірити зашифрований потік.

Кожен з варіантів має свої переваги та недоліки, і вибір між ними може залежати від конкретних вимог та умов конфігурації мережі [35].

У спроектованій мережі використовується конфігурація, де міжмережевий екран розташований перед брандмауером, що дозволяє блокувати атаки на брандмауері за допомогою системи виявлення вторгнень [35].

Для підмережі обирається адреса з діапазону Intranet, яка становить 192.168.16.0/24. Це означає, що доступні IP-адреси розпочинаються з 192.168.16.1 і закінчуються 192.168.16.254. Перша адреса (192.168.16.0) є адресою мережі і не може використовуватися для ідентифікації конкретних мережевих вузлів. Остання адреса діапазону (192.168.16.254) є широкомовною адресою і також не може бути використана для ідентифікації конкретних вузлів [35].

Для ідентифікації інтерфейсу маршрутизатора, що з'єднує нашу мережу з Інтернетом, використовується адреса 192.168.16.1/24. Решта IP-адрес розподіляється між різними пристроями в мережі, такими як VPN комутатор (192.168.16.2/24), WWW і FTP сервер, розташовані на одному комп'ютері (192.168.16.3/24), E-mail сервер (192.168.16.5/24) та зовнішній інтерфейс брандмауера (192.168.16.4/24). Кожен з цих пристроїв отримує унікальну IP-адресу для ідентифікації в мережі. Інші IP-адреси присвоюємо робочим станціям мережі (Рис. 3.1) [35].

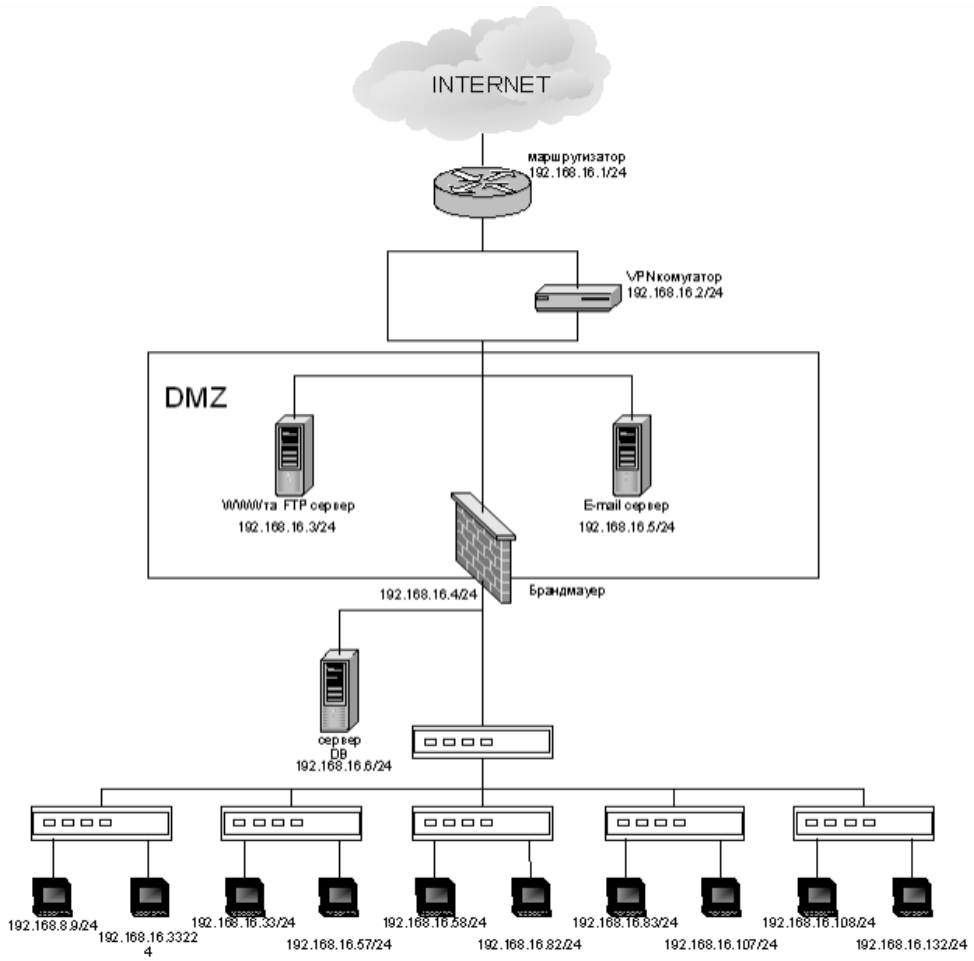

Рисунок 3.1 – Структура локальної мережі Головного корпусу

Мережу можна умовно розділити на три частини, починаючи від інтерфейсу маршрутизатора провайдера, який з'єднує нас з Інтернетом. На ближній до нас стороні цього маршрутизатора розташована зона DMZ (Demilitarized Zone). DMZ є свого роду буфером, що відокремлює нашу внутрішню мережу від простору Інтернету. Вона включає різні ресурси під нашим контролем, такі як WWW сервер, FTP сервер та E-mail сервер. Зона DMZ закінчується на зовнішньому інтерфейсі брандмауера [4].

За внутрішнім інтерфейсом брандмауера розпочинається внутрішня мережа, яка включає в себе всі наші комп'ютери та інші пристрої, що об'єднані в єдину систему. Така структура дозволяє ефективно використовувати брандмауер як захисний шар для відокремлення зовнішніх ризиків, таких як атаки з Інтернету, від внутрішньої мережі, забезпечуючи високий рівень безпеки [4].

В будь-якому з'єднанні між брандмауерами та відкритими мережами важливо використовувати механізми шифрованих віртуальних приватних мереж (VPN) для

забезпечення конфіденційності та цілісності передачі даних через глобальні мережі. VPN надає засоби для створення безпечного тунелю між різними мережевими пристроями, який шифрує дані та забезпечує їх безпечний обмін [4].

Крім того, важливо впроваджувати ефективні механізми розподілу і адміністрування ключів шифрування перед використанням VPN. Ключі шифрування є основним елементом безпеки в VPN і використовуються для захисту інформації від несанкціонованого доступу [4].

У контексті VPN також враховується використання засобів формування й перевірки контрольних сум файлів. Ці засоби призначені для виявлення змін, додавання або видалення файлів, що можуть виникнути внаслідок несанкціонованої діяльності або інших подій. Адміністратор безпеки отримує повідомлення про такі зміни, що дозволяє ефективно реагувати на можливі загрози і забезпечувати стабільність системи [4].

В системі віртуальної приватної мережі (VPN) кожна підмережа має свій власний кодуючий модуль, який встановлений у точці її з'єднання з зовнішніми мережами. Цей модуль виконує дві ключові функції: кодує інформацію на передавальному етапі, щоб забезпечити безпеку під час передачі, і декодує її на етапі приймання, щоб знову зробити її доступною у відкритому вигляді в межах локальних мереж [4].

Необхідно визначити периметр безпеки, який об'єднує IP-адреси всіх абонентів, що мають доступ до цієї віртуальної захищеної мережі. Це створює ізольоване середовище, в якому інформація може безпечно обмінюватися між учасниками VPN [16].

Протоколи VPN відповідають за збір і збереження різноманітної інформації. Це включає в себе статистичні та службові дані про події, що виникають під час аутентифікації вузлів, передачі кодованої інформації та обмеження доступу абонентів в локальній обчислювальній мережі. Засоби моніторингу використовуються для збору і аналізу протоколів реєстрації від усіх модулів комплексу через зашифрований канал. Це дозволяє відслідковувати та реагувати на всі події, що стосуються безпеки мережі VPN [16].

Кожен відокремлений структурний підрозділ має власну унікальну адресу електронної пошти, щоб забезпечити конфіденційність комерційної інформації та уникнути її розкриття. З метою безпеки і доступу до електронної пошти використовується віртуальна приватна мережа (VPN) – Інтранет [16].

Кожна філія має свій власний POP-сервер для отримання електронної пошти. Це дозволяє філіям працювати автономно, знижуючи залежність від зовнішніх служб. Система використовує SMTP-сервер для отримання пошти, який потім перевіряється на легітимність і направляється через VPN-шлюз на відповідний POP-сервер [16].

Всі адміністративні операції і доступ здійснюються через управляючі функції VPN, що забезпечує безпечний та конфіденційний обмін інформацією між відокремленими структурними підрозділами. VPN використовується як безпечний тунель для забезпечення захищеного з'єднання та обміну даними через Інтернет [16].

3.4 Захист інформаційної взаємодії

Протокол SSL (Secure Sockets Layer) розроблений для вирішення ряду основних завдань, пов'язаних із забезпеченням безпеки інформаційного обміну, зокрема в середовищі клієнт/сервер. Відомості щодо його функцій можна розглядати наступним чином [33]:

1. **Перевірка Ідентичності Сервера:**
   Під час підключення користувача до сервера важливо, щоб користувач мав впевненість, що він взаємодіє саме з тим сервером, який він очікує. SSL здійснює аутентифікацію сервера, використовуючи цифрові сертифікати, які підтверджують його ідентичність.
2. **Шифрування Даних:**
   Після встановлення з'єднання між сервером і клієнтом, SSL застосовує шифрування для захисту всього інформаційного потоку між ними від несанкціонованого доступу. Це забезпечує конфіденційність даних під час їх передачі.
3. **Цілісність Даних:**

У процесі обміну інформацією між сторонами SSL також гарантує, що дані не піддаються випадковим або навмисним змінам під час передачі. Це досягається за допомогою методів контролю цілісності, таких як хеш-функції [33].

Отже, SSL створений для забезпечення довіри, конфіденційності та цілісності при обміні інформацією між клієнтом і сервером в мережевому середовищі [33].

Протокол SSL (Secure Sockets Layer) використовується для забезпечення безпеки взаємодії між сервером і клієнтом під час передачі інформації через мережу. Його функції можна розглядати докладніше [33]:

1. **Автентифікація:**

   Перед тим, як почати обмін інформацією, сервер і клієнт взаємно підтверджують свою ідентичність. Це важливо для того, щоб упевнитися, що обидві сторони взаємодіють із вірними системами, а не імітаціями або підставними пристроями.

2. **Узгодження Алгоритмів Шифрування:**

   SSL дозволяє серверу та клієнту домовитися про використання конкретного алгоритму шифрування для захисту даних під час їхньої передачі. Це включає в себе вибір методу шифрування та інших параметрів, які забезпечують безпеку обміну інформацією.

3. **Формування Криптографічних Ключів:**

   За допомогою криптосистем, таких як RSA (алгоритм з двома ключами), SSL дозволяє сторонам створювати загальні криптографічні ключі. Один ключ використовується для шифрування даних перед їхньою передачею, а інший ключ використовується для розшифрування отриманої інформації.

Таким чином, протокол SSL забезпечує безпеку інформаційної взаємодії, здійснюючи процес автентифікації, узгодження алгоритмів шифрування та створення криптографічних ключів для захисту конфіденційності інформації [33].

Процес забезпечення конфіденційності інформації, що передається через захищене з'єднання, включає в себе кілька етапів та використання криптографічних методів. Давайте розглянемо цей процес докладніше [33]:

1. **Шифрування потоку даних:**

Конфіденційність даних забезпечується за допомогою симетричних криптографічних алгоритмів, основним із яких є RC4. Шифрування виконується в режимі CFB (Cipher Feedback Mode), який є одним із режимів потокового шифрування. Процес використовує загальний ключ, який був створений попередньо між сервером і клієнтом.

2. **Генерація Послідовності Ключів:**

   Для шифрування використовується таблиця станів шифратора S, яка містить 256 восьмирозрядних слів. Початкове формування цієї таблиці виконується на етапі ініціалізації ключем К. Таблиця S заповнюється послідовністю чисел, а ключ К розбивається на групи по 8 розрядів і розміщується в таблиці К довжиною 255 байт. Якщо довжина ключа менше 255 байт, виконується циклічне заповнення таблиці К вихідною послідовністю символів ключа.

3. **Хешування для Контролю Цілісності:**

   Для забезпечення контролю цілісності переданих блоків даних використовуються коди автентифікації повідомлень, що обчислюються за допомогою хеш-функцій, таких як MD5. Це дозволяє сторонам перевіряти, чи була змінена передана інформація під час її передачі.

4. **Криптостійкість Алгоритму:**

   RC4, як симетричний алгоритм шифрування, має високий рівень криптостійкості. Його безпека базується на складній структурі і механізмах генерації ключів. Навіть кількість станів таблиці S у RC4 (близько 10^1700) робить його дуже міцним шифром [13].

Отже, цей процес забезпечення конфіденційності використовує симетричний шифр RC4, режим потокового шифрування CFB, генерацію послідовності ключів та хеш-функції для контролю цілісності, що разом створює високий рівень безпеки для переданих даних [13].

Протокол SSL включає два ключові етапи взаємодії між сторонами, які встановлюють безпечне з'єднання [13]:

1. Установлення SSL-сесії (Процедура "Рукостискання"):

На цьому етапі сторони, які хочуть встановити безпечне з'єднання, проводять аутентифікацію. Це означає, що як сервер, так і клієнт перевіряють свою взаємну ідентичність. Після цього сторони домовляються про використання криптографічних алгоритмів, які будуть використовуватись для шифрування даних. Також сторони формують загальний "секрет", на основі якого генеруються унікальні сеансові ключі. Ці ключі використовуються для захисту подальших комунікацій. Цей етап також відомий як процедура "рукостискання".

2. Захист Потоку Даних:

На другому етапі відбувається захист потоку даних. Інформаційні повідомлення розбиваються на блоки, для кожного з яких обчислюється код аутентифікації повідомлення (MAC - Message Authentication Code). Потім дані шифруються за допомогою сеансових ключів і відправляються приймальній стороні. На стороні отримувача виконуються зворотні дії, такі як дешифрування, перевірка коду аутентифікації повідомлення, складання повідомлень, і передача їх на рівень застосунків.

Таким чином, SSL визначає процеси аутентифікації, взаємодії щодо криптографічних алгоритмів і ключів, а також захист потоку даних для забезпечення безпеки під час передачі інформації через мережу [13].

SSL (Secure Sockets Layer) має декілька переваг, серед яких важливо відзначити його незалежність від прикладного протоколу. Це означає, що протоколи, такі як HTTP, FTP, TELNET і інші, можуть працювати поверх SSL без будь-яких змін у своєму функціоналі. SSL може встановлювати угоду щодо алгоритму шифрування та сесійного ключа, а також аутентифікувати сервер навіть до того, як буде переданий або прийнятий перший байт даних [13].

Основними характеристиками безпечного каналу, який надає протокол SSL, є:

1. Приватність каналу:

Шифрування застосовується до всіх повідомлень після простого діалогу, під час якого визначається спільний секретний ключ. Це робить канал приватним, оскільки тільки авторизовані сторони можуть розшифрувати та зрозуміти передані дані.

2. Аутентифікація каналу:

Протокол SSL надає можливість аутентифікації сервера, що означає, що клієнт може перевірити, що він спілкується саме з тим сервером, який він очікує. Це зменшує ризик атак типу "man-in-the-middle" (людина посередині).

3. Надійність каналу:

Крім того, передача повідомлень через канал SSL містить в собі перевірку цілісності. Це означає, що приймальна сторона може впевнитися, що дані не були змінені або пошкоджені під час транспортування.

Отже, SSL надає безпечний канал, який забезпечує конфіденційність, аутентифікацію та надійність при передачі інформації між сторонами [13].

У протоколі SSL всі дані передаються у вигляді рекордів, що є об'єктами, складеними з заголовка та поля даних. Кожен заголовок рекорду має два або три байти коду довжини. Якщо старший біт у першому байті коду довжини рекорду рівний 1, то цей рекорд не має заповнювача, і загальна довжина заголовка становить 2 байти. У протилежному випадку, якщо рекорд має заповнювач, то загальна довжина заголовка становить 3 байти. Кожен обмін даними завжди розпочинається з передачі заголовка [13].

Довжина рекорда обчислюється вказаним чином: RECORD-LENGTH=((byte[0]&0*x*3*F*)≪8)|byte[1]

Де:

- \text{byte}[0] та \text{byte}[1] представляють перші два байти запису.
- \text{IS-ESCAPE} визначається як byte[0]&040≠0, що вказує на наявність "escape" біта.
- \text{PADDING} представляє третій байт запису, який визначає кількість байтів заповнювача.

Заголовок рекорда визначається значенням \text{PADDING}, яке вказує на кількість байтів, які додаються відправником до вихідного рекорда. Отримавши "заповнений" рекорд, відправник додає заповнювач після наявних даних і потім шифрує весь запис. Зміст заповнювача не має значення, оскільки обсяг переданих даних відомий. Таким чином, заголовок повідомлення може бути коректно сформований з урахуванням обсягу підполя PADDING. Одержувач рекорда, після

дешифрування усіх полів даних, обчислює фактичне значення \text{RECORD-LENGTH}, виключаючи заповнювач із поля "дані".

Дані рекорду SSL складаються з трьох компонентів [13]:

1. **MAC-DATA** *MAC−SIZE*: Це код аутентифікації повідомлення (Message Authentication Code), який визначається за допомогою хеш-функції. Розмір цього коду визначається значенням MAC-SIZE.
2. **ACTUAL-DATA** *N*: Представляє собою реальні передані дані.
3. **PADDING-DATA** *PADDING*: Це дані заповнювача, використовувані при використанні блокового коду шифрування.

Коли рекорди SSL передаються відкритим текстом (не зашифровані), не використовуються шифри, тому довжина PADDING-DATA і обсяг MAC-DATA будуть нульовими. При використанні шифрування PADDING-DATA стає функцією розміру блоку шифру. Значення MAC-DATA залежить від вибору шифру (CIPHER-CHOICE).

Обчислення MAC-DATA включає в себе хешування за допомогою хеш-функції, яка приймає SECRET (переданий хеш-функції першим), ACTUAL-DATA, PADDING-DATA та SEQUENCE-NUMBER. Порядковий номер (SEQUENCE-NUMBER) є 32-бітним кодом, який передається хеш-функції у форматі 4 байт. Порядковий номер передається у мережний порядок передачі (big endian), починаючи зі старшого байта.

MAC-SIZE - це розмір коду аутентифікації повідомлення (Message Authentication Code), і його значення залежить від алгоритму, який використовується для обчислення дайджесту [13].

SECRET - це значення, яке визначається залежно від того, хто є відправником або одержувачем повідомлення. Якщо клієнт відправляє повідомлення, SECRET дорівнює CLIENT-WRITE-KEY (сервер використовує SERVER-READ-KEY для верифікації MAC). Якщо клієнт отримує повідомлення, SECRET дорівнює CLIENT-READ-KEY (сервер використовує SERVER-WRITE-KEY для генерації MAC).

SEQUENCE-NUMBER - це лічильник, який інкрементується як для відправника, так і для одержувача. Для кожного напрямку передачі використовуються пари лічильників (один для відправника, інший для одержувача). Порядкові номери - це 32-бітні беззнакові цілі числа, які анулюються при переповненні [13].

Одержувач повідомлення використовує очікуване значення порядкового номера для передачі хеш-функції MAC. Обчислена MAC-DATA повинна збігатися з переданою MAC-DATA. Якщо порівняння не пройшло, рекорд вважається пошкодженим, і це розглядається як випадок "I/O Error" [32].

Остаточна перевірка відповідності виконується, коли використовується блоковий шифр і відповідний протокол шифрування. Розмір даних у рекорді (RECORD-LENGTH) повинен бути кратним розміру блоку шифру. Якщо отриманий рекорд не є кратним розміру шифру, він вважається пошкодженим, і це розглядається як помилка "I/O Error", що може призвести до розриву з'єднання [32].

Рівень рекордів SSL використовується для всіх комунікацій SSL, включаючи повідомлення діалогу та інформаційний обмін, і використовується як клієнтом, так і сервером [32].

Для двобайтового заголовка протоколу SSL, максимальна довжина рекорду може складати до 32767 байтів, а для трибайтового заголовка - до 16383 байтів. Повідомлення протоколу діалогу SSL повинні відповідати одиночним рекордам протоколу SSL (Record Protocol). Однак повідомлення прикладного протоколу можуть бути розділені на кілька рекордів SSL для передачі [32].

Перед відправленням першого рекорду SSL всі порядкові номери встановлюються на нуль. При передачі повідомлення порядковий номер інкрементується, починаючи з повідомлень CLIENT-HELLO і SERVER-HELLO [32].

Протокол діалогу SSL проймає дві основні фази. Перша фаза використовується для встановлення конфіденційного каналу комунікації, під час якої визначаються параметри шифрування і генеруються сеансові ключі. Друга фаза

включає аутентифікацію клієнта, де клієнт підтверджує свою ідентичність перед сервером, що дозволяє забезпечити безпеку і довіру взаємодії [32].

Перша фаза

SSL - це етап ініціалізації з'єднання, коли обидва партнери по обміну повідомленнями "HELLO" для встановлення зв'язку. Процес розпочинається з того, що клієнт ініціює діалог, надсилаючи повідомлення CLIENT-HELLO. Сервер, отримавши це повідомлення, обробляє його і видає відповідь у вигляді повідомлення SERVER-HELLO [32].

На цій стадії обидва партнери вже мають достатньо інформації, щоб визначити, чи потрібно встановити новий головний ключ. Якщо так, SERVER-HELLO містить необхідні дані, такі як підписаний сертифікат сервера, список базових шифрів і ідентифікатор з’єднання (який представляє собою випадкове число, створене сервером для використання протягом сесії) [32].

Якщо новий головний ключ не потрібен, обидва партнери негайно переходять до фази 2. У випадку, коли необхідний новий головний ключ, клієнт генерує його і висилає повідомлення CLIENT-MASTER-KEY. Як альтернативу, якщо інформація від сервера свідчить про неможливість узгодження базового шифру, клієнт висилає повідомлення ERROR [32].

Кожна закінчена точка SSL використовує пари шифрів для кожного з’єднання, що загалом дає 4 шифри для кожного кінця з'єднання. У кожній точці, будь то клієнт або сервер, існують два ключі для шифрування та розшифрування даних. Один ключ використовується для вихідних комунікацій (відправка даних), а інший - для вхідних (приймання даних) [32].

При генерації ключа сесії клієнт або сервер створюють два основні ключі: SERVER-READ-KEY (іноді відомий як CLIENT-WRITE-KEY) та SERVER-WRITE-KEY (іноді відомий як CLIENT-READ-KEY). Ці ключі використовуються для забезпечення шифрування та розшифрування даних, які передаються між клієнтом і сервером під час сесії [32].

Після визначення головного ключа сервер надсилає клієнту повідомлення SERVER-VERIFY. Цей крок важливий для аутентифікації сервера, оскільки тільки

сервер, який володіє відповідним загальнодоступним ключем, може знати головний ключ [32].

Друга фаза

Процес SSL є фазою аутентифікації, де сервер, який вже пройшов аутентифікацію клієнтом на першій фазі, тепер аутентифікує самого клієнта. У типовому сценарії сервер висилає запит клієнту, і клієнт відповідає позитивно, якщо має необхідну інформацію, або повідомлення про помилку у випадку відсутності необхідної інформації. Коли один з партнерів успішно аутентифікує іншого, він висилає повідомлення "finished". У випадку клієнта це повідомлення, CLIENT-FINISHED, містить зашифрований ідентифікатор CONNECTION-ID, який сервер повинен перевірити. Якщо перевірка не вдається, сервер висилає повідомлення ERROR [32].

Якщо партнер відправив повідомлення "finished", він повинен продовжувати приймати повідомлення, доки не отримає відповідне повідомлення "finished" від партнера. Коли обидва партнери надіслали та отримали повідомлення "finished", протокол діалогу SSL завершує свою роботу, і з цього моменту починає діяти прикладний протокол [32].

3.5 Налаштування VPN мережі

Оскільки VPN-шлюзи працюють під управлінням операційної системи Linux, налаштування буде виконано за допомогою команд Linux.

Перший крок - створення користувача, який буде відповідальний за запуск команд VPN на обох кінцях з'єднання. Назвемо цього користувача "sslvpn".

```
root # groupadd sslvpn
root # useradd –m –d /opt ssl –vpn –c “SSL VPN User” –g sslvpn sslvpn
```

Робочу станцію, що ініціює процес з'єднання з віддаленим абонентом, називаємо VPN-клієнтом, а віддаленого абонента - VPN-сервером.

Далі, для забезпечення аутентифікації обох кінців SSL-з'єднання і переконанняся у легітимності цих кінцевих точок, необхідно створити ключі та сертифікати як для клієнта, так і для сервера. VPN-сервер повинен вимагати сертифікат для обох кінців. Для цієї мети використовуються самопідписні

сертифікати. Генерація ключів та сертифікатів виконується за допомогою конфігураційного файлу OpenSSL з ім'ям sslvpn.conf.

Створені ключі та сертифікати слід розмістити в спеціальних каталогах Stunnel. Для можливості створення декількох VPN із різними сертифікатами та ключами, для кожного VPN-з'єднання створюється окремий каталог із іменем /opt/ssl-vpn/etc/ім'я_VPN/. Наприклад, vpn1, vpn2, vpn3, і так далі.

Далі виконується створення та підпис ключа на серверній машині.

```
vpn-server$ cd/opt/ssl-vpn/etc/vpn1
vpn-server$ openssl reg -new -x509 -days 365 \
-config/opt/ssl-vpn/etc/sslvpn.cnf\
-out server.pem -keyout server.pem
```

Підпис ключа на клієнтській машині:

```
client$ cd /opt/ssl-vpn/etc/vpn1
client$ openssl reg -new -x509 -days 365\
-config/opt/ssl-vpn/etc/sslvpn.cnf\
-out server.pem -keyout server.pem
```

Команда виглядає наступним чином: openssl req -new -x509 -days 365 -config /шлях_до/файл_конфігурації_openssl.conf -out файл_сертифіката.pem -keyout файл_приватного_ключа.pem

Тут аргументи означають:

- **-new**: створити новий сертифікат;
- **-x509**: використовувати формат X.509;
- **-days 365**: сертифікат діє протягом 365 днів;
- **-config /шлях_до /файл_конфігурації_openssl.conf**: шлях до конфігураційного файлу OpenSSL;
- **-out файл_сертифіката.pem**: файл для запису сертифіката;
- **-keyout файл_приватного_ключа.pem**: файл для запису приватного ключа.

Отже, команда створює ключ і сертифікат, які зберігаються в файлах server.pem і client.pem. Далі, сертифікат сервера копіюється на клієнтську машину (і навпаки) для подальшого використання у перевірці.

Після цього виконується налаштування таблиці маршрутизації.

sslvpn@client$ sudo route add -net 192.168.1.2/24 gw

123.45.67.82

sslvpn@server$ sudo route add -net 192.168.1.1/24 gw

125.51.67.82

Створення конфігураційних файлів для програм vpn-server та vpn-client є частиною процесу налаштування VPN-з'єднань. Кожен VPN скрипт отримує конфігураційні змінні з відповідного файлу, таким чином, якщо, наприклад, ми маємо VPN з ім'ям "vpn1", ми повинні створити файл /opt/ssl-vpn/etc/vpn1/config.
В цьому конфігураційному файлі кожна змінна починається з "server_" або "client_", що вказує на можливість використання одного файлу для обох систем.
Отже, створення конфігураційного файлу виглядатиме приблизно так:

 # Параметри сервера

server_address=192.168.1.1

server_port=5000

server_protocol=tcp

 # Параметри клієнта

client_address=192.168.1.2

client_port=5000

client_protocol=tcp

У цьому прикладі "server_" вказує на параметри сервера, а "client_" - на параметри клієнта. Кожен параметр визначає адресу, порт і протокол для відповідної сторони VPN-з'єднання. Ви можете додати інші необхідні параметри, такі як шифрування, ключі, тощо, в залежності від ваших вимог.

Цей конфігураційний файл буде використовуватися обома програмами vpn-server і vpn-client для встановлення та налаштування VPN-з'єднань.

Вот який виглядає конфігураційний файл:

Визначення мережі клієнта і сервера

client_network=192.168.1.2/24

server_network=192.168.1.1/24

```
# Включення режиму налагодження для клієнта і сервера
client_debug="yes"
server_debug="yes"
# Вибір IP-адрес для обох сторін VPN
server_ppp_ip=125.51.67.82
client_ppp_ip=123.45.67.82
# Налаштування PAP та CHAP аутентифікації
client_require_pap="no"
server_require_pap="no"
client_require_chap="yes"
server_require_chap="yes"
# Нестандартні аргументи для pppd
client_pppd_args="usepeerdns"
server_pppd_args="proxyarp"
```

Цей конфігураційний файл визначає параметри мережі для клієнта і сервера, активує режим налагодження для обох сторін, визначає IP-адреси для підключення та конфігурує параметри аутентифікації за допомогою PAP та CHAP. Також містить коментарі для налаштування нестандартних аргументів для pppd, які можуть бути включені за необхідності.

Цей конфігураційний файл буде використовуватися для налаштування VPN з'єднання з ім'ям "vpn1".

Опис змінних, які використовуються в конфігураційному файлі:

- **client_network**: Визначає мережу на VPN-клієнті. VPN-сервер використовує це значення для встановлення маршруту до віддаленої мережі за допомогою команди **route add**. Якщо значення не встановлено, клієнт розглядається як хост, а не шлюз, і маршрути не встановлюються.
- **server_network**: Визначає мережу на VPN-сервері. Використовується VPN-клієнтом для встановлення маршруту до віддаленої мережі за допомогою команди **route add**.

- **server_ppp_ip**: IP-адреса кінця PPP-з’єднання, на якому розташований VPN-сервер.
- **client_ppp_ip**: IP-адреса кінця PPP-з'єднання, на якому розташований VPN-клієнт.
- **client_debug**: Додає опцію **debug** до аргументів **pppd**; додає опцію **D7** до аргументів Stunnel і запускає **set -x** для покрокового виводу крипта VPN-клієнта.
- **server_debug**: Аналогічно до попереднього, але для сервера.
- **client_stunnel_args**: Додаткові аргументи Stunnel для клієнта.
- **server_stunel_args**: Додаткові аргументи Stunnel для сервера.
- **client_pppd_args**: Додаткові аргументи командної стрічки **pppd**, які специфічні для даної VPN.
- **server_pppd_args**: Додаткові аргументи командної стрічки **pppd**, які специфічні для даної VPN.
- **client_require_pap**: Вказує, чи клієнт VPN вимагатиме PAP-аутентифікацію сервера. Усі значення, крім "yes", еквівалентні "no".
- **server_require_pap**: Вказує, чи сервер VPN вимагатиме PAP-аутентифікацію клієнта. Усі значення, крім "yes", еквівалентні "no".

Щодо запуску та зупинки VPN, на клієнтській машині виконують команду:
/etc/init.d/vpn1 start

На сервері використовують ту ж саму команду для запуску VPN. Для зупинки VPN виконують команду:
/etc/init.d/vpn1 stop

Таким чином, ці команди використовуються для управління процесом запуску та зупинки VPN на обох сторонах - клієнті та сервері.

3.3 Тестування продуктивності VPN мережі

Для тестування VPN-шлюзів використовувалася програма SmartFlow, яка генерує TCP та UDP-пакети. Під час тестування виявлено, що пропускна здатність використовуваних шлюзів складає 152 Мбіт/с. Передача пакетів різних розмірів (128, 512 та 1400 байт) не показала залежності втрат пакетів від їх розмірів, а втрати склали 1%.

Оцінка продуктивності VPN мережі проводилася за допомогою програми NetIQ Chariot. Виконано порівняльний аналіз продуктивності VPN при створенні різної кількості тунелів. Спочатку був створений криптозахисний тунель (1-2), та заміряна його продуктивність. Отримані показники використовуються для побудови графіку, який відображає ефективність VPN залежно від кількості створених тунелів (Рис. 3.2).

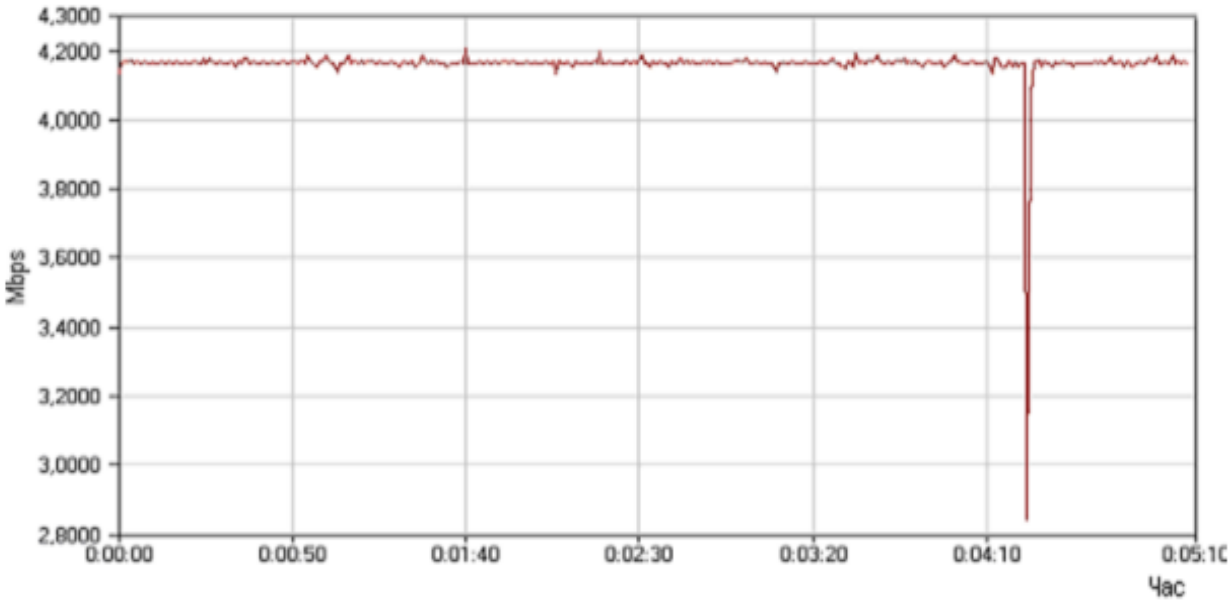

Рисунок 3.2 – Графік продуктивності криптотунелю

Середня швидкість передачі даних складає 4.159 Мбіт/с. Під час проведення тестування виявлено, що середня продуктивність першого VPN-тунелю (1-2) становить 2.907 Мбіт/с, а другого - 2.604 Мбіт/с.

Далі, для отримання додаткових даних, було створено два криптозахисних тунелі (1-2 та 1-3), і їх продуктивність було виміряно одночасно (Рис. 3.3).

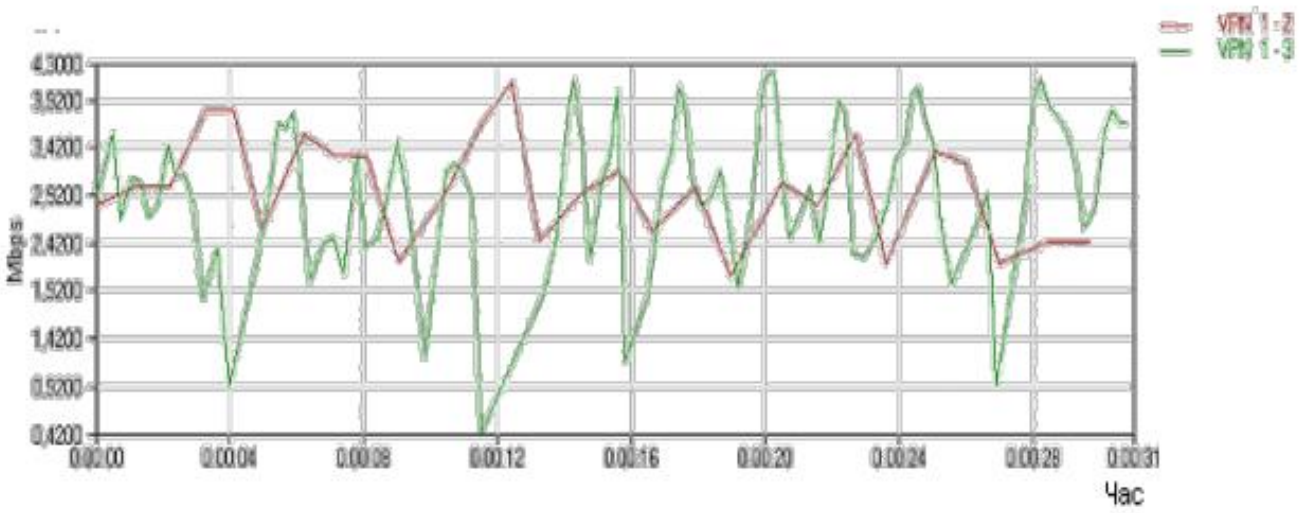

Рисунок 3.3 – Порівняння продуктивності VPN тунелів (1-2)

Сумарну продуктивність між двома VPN тунелями на діаграмі (Рис . 3.3).

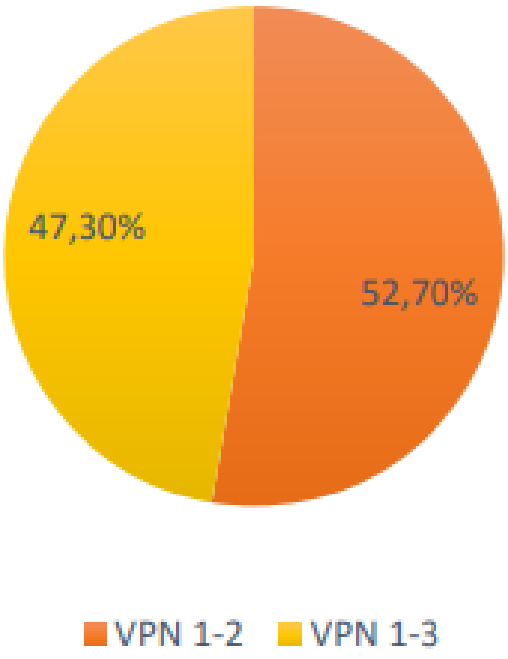

Рисунок 3.4 – Сумарна продуктивність між двома VPN тунелями

Далі, додавши ще один тунель (1-4), були отримані результати, які відображено на графіку на рисунку 3.5.

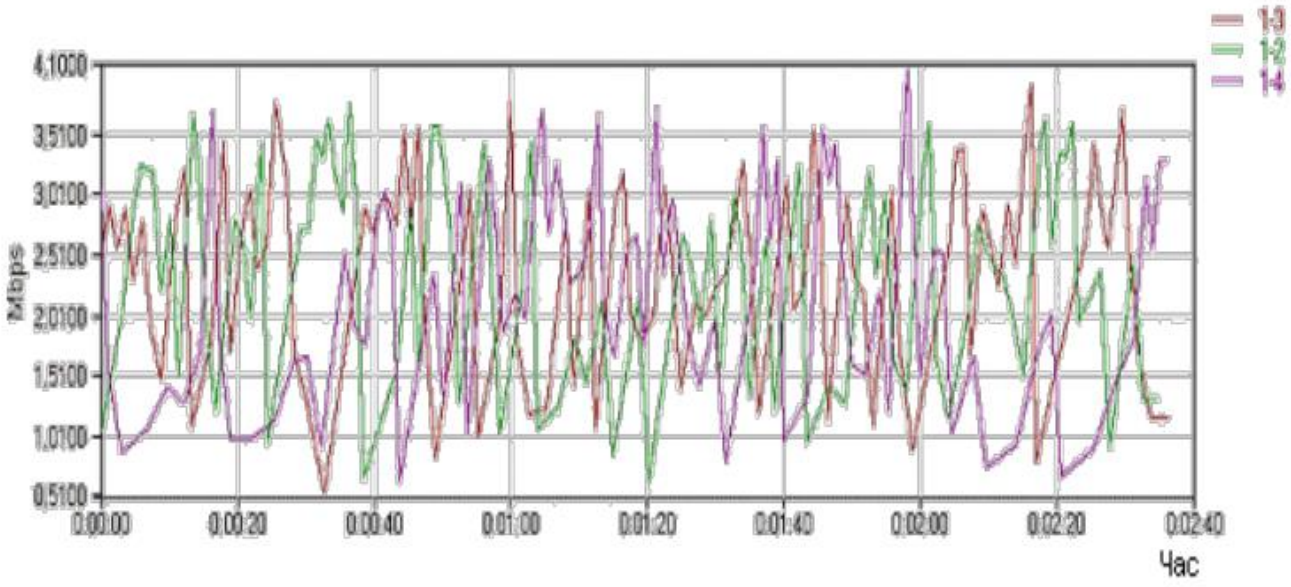

Рисунок 3.5 – Порівняння продуктивності VPN тунелів (1-4)

Середня продуктивність тунелю 1-2 становила 1.963 Mbps, для тунелю 1-3 ця величина дорівнювала 2.048 Mbps, а для тунелю 1-4 — 1.743 Mbps. Сумарна середня продуктивність між трьома VPN-тунелями склала 5.754 Mbps. Ці результати відображені на діаграмі, яку можна побачити на рисунку 3.6.

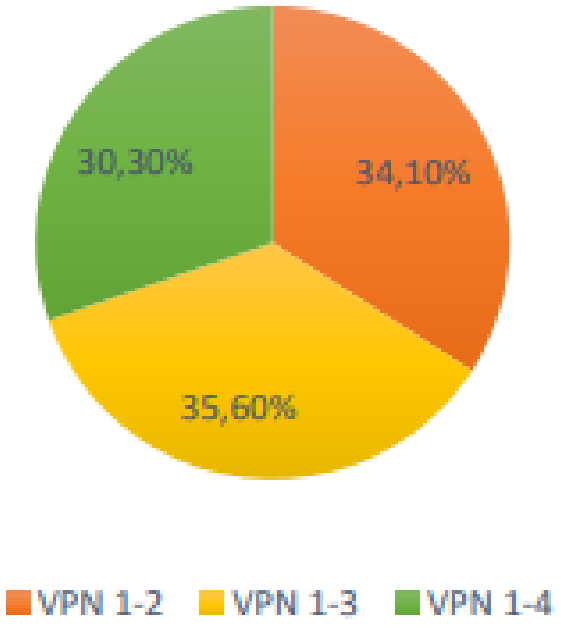

Рисунок 3.6 – Сумарна продуктивність між трьома VPN тунелями

Можна зазначити, що VPN мережа успішно впоралася із завданою навантаження та продемонструвала високі швидкісні характеристики, що робить її ефективною для використання на Інтернет-каналах.

3.3 Аналіз стійкості до атак

У цьому розділі розглядаються певні атаки, які можна виконати проти VPN мережі, побудованої на основі протоколу SSL.

Розкриття шифрів: Атаки на комунікаційні сесії можуть бути виконані шляхом запису сесії, а потім, витрачаючи значну кількість обчислювального часу, проводиться спроба підібрати ключ сесії або ключ RSA. У випадку успіху відкривається можливість читати передану інформацію. SSL робить вартість таких атак вищою, ніж можливі вигоди від успішної атаки, зробивши це невигідним і неефективним заходом.

Атака відкритого тексту: Атака відкритого тексту відбувається тим способом, що атакуючий має уявлення про тип повідомлень, які передаються зашифровано. Атакуючий може створювати базу даних, де ключами є зашифровані фрагменти відомого тексту і, використовуючи апаратні або програмні засоби, визначати ключ сесії.

SSL намагається протистояти цим атакам, використовуючи великі ключі сесії. Клієнт генерує ключ, що є довшим, ніж допускають обмеження експорту, і відправляє частину його відкритим текстом серверу. Це дозволяє об'єднати відкриту частину ключа із секретною для отримання достатньо довгого ключа.

Атака відгуку: Атака відгуку відбувається, коли зловмисник записує комунікаційну сесію між клієнтом і сервером, а потім встановлює з'єднання із сервером для відтворення записаних повідомлень клієнта. SSL протистоїть цій атакі за допомогою спеціального коду "nonce" (ідентифікатор з'єднання), який є унікальним.

Теоретично зловмисник не може вгадати цей код заздалегідь через його базування на наборі випадкових подій, недоступних для зловмисника. Зловмисник, маючи значні ресурси, може записати багато сесій між клієнтом і сервером і намагатися відтворити "правильну" сесію, використовуючи код nonce. Однак

довжина кодів nonce SSL є принаймні 128 біт, і, таким чином, зловмисник повинен записати приблизно 2^64 кодів nonce, щоб мати лише 50% ймовірність вгадування. Це значення достатньо велике, щоб зробити такий вид атаки малоефективним.

Людина посередині: Атака посередника включає участь трьох суб'єктів: клієнта, сервера і посередник-зловмисника, розташованого між ними. Зловмисник може перехоплювати всі повідомлення, що йдуть у обидві сторони і підмінювати їх.

SSL робить таку атаку неможливою завдяки використанню сервером сертифікатів. Під час встановлення безпечного з'єднання сервер повинен надати сертифікат, підписаний сертифікаційним центром, що містить загальнодоступний ключ сервера, його ім'я та ім'я емітента сертифіката. Клієнт перевіряє підпис сертифіката і перевіряє ім'я емітента.

Якщо посередник намагається представити підроблений сертифікат, він не пройде перевірку підпису, оскільки зловмисник не знає секретного ключа сервера.

ВИСНОВКИ

В сучасних комп'ютерних мережах використовуються різноманітні протоколи для реалізації віртуальних приватних мереж (VPN). Деякі з них включають IPSec, PPTP, L2F, L2TP, IKE, LCP, PPP, IPsec, OpenVPN, EAP, EAP-TLS, MSCHAP, CHAP, SPAP, та PAP.

Архітектура VPN включає два рівні: внутрішню мережу і зовнішню мережу. Захист інформації у VPN базується на кількох методах безпеки:

1. Тунелювання: Цей метод дозволяє створювати зашифрований "тунель" між двома точками в мережі, що гарантує конфіденційність переданих даних.
2. Аутентифікація: Процес перевірки ідентичності користувачів або пристроїв, який забезпечує визначення, що лише вповноважені особи мають доступ до мережі.
3. Шифрування: Процес перетворення інформації в нерозбірливий вигляд, який може бути розшифрований лише за допомогою вірного ключа.

Під час аналізу проблем інформаційної безпеки в мережах з використанням VPN, важливо враховувати виявлення внутрішніх і зовнішніх загроз, фільтрацію зовнішнього трафіку, контроль застосування мережевих ресурсів та запобігання інцидентам інформаційної безпеки.

Побудова власних VPN може бути актуальною для об'єднання кількох локальних мереж в одну велику мережу. Це забезпечує захист переданих даних між сегментами мережі, зокрема за допомогою шифрування. VPN також використовуються для вирішення проблем, пов'язаних із захистом окремих каналів та комп'ютерів у мережі.

IPSec часто використовується як основний протокол для забезпечення безпеки передачі даних, а L2TP поверх IPSec використовується для забезпечення безпеки на канальному та мережевому рівні. SSL протокол застосовується для швидкого розгортання VPN та тимчасового підключення з середнім рівнем безпеки даних.

Загалом, використання різних комбінацій протоколів дозволяє підвищити рівень безпеки в VPN-мережах і забезпечити ефективний захист інформації.

Було проведено детальне вивчення та аналіз теоретичних аспектів, що стосуються комп'ютерних мереж загалом та методів їх захисту. Далі була розроблена та налаштована віртуальна приватна мережа (VPN), яка використовує протокол SSL. Цей протокол надає можливість серверу та клієнту аутентифікувати один одного, узгоджувати алгоритми шифрування та створювати спільні криптографічні ключі перед початком обміну інформацією.

Проведене тестування продуктивності віртуальної корпоративної мережі підтвердило, що VPN мережа відмінно впоралася із завданою навантаження та показала високу швидкість роботи. Отримані результати свідчать про ефективність використання VPN на Інтернет-каналах та підтверджують її здатність до швидкого та надійного обміну даними.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Framework for IP Based Virtual Private Networks [Електронний ресурс] – Режим доступу до ресурсу:

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-differencechoose/ 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/B9780128038437 01. 5. IPSec – протокол захисту мережевого трафіку на IP-рівні. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ixbt.com/comm/ipsecure.shtm

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://ipsectools.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.

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.

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).