Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: " Способи захисту інформаційно- телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Олійник Юрій Романович
підпис (прізвище та ініціали)

Керівник Оробчук О.Р.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Олійнику Юрію Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Способи захисту інформаційно-телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN

Керівник роботи Оробчук Олександра Романівна, доктор філософії, викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № *4/7 -112*

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз стану проблеми. 1.1. Постановка задачі. 1.2. Огляд вимог до захисту інформаційних систем. 1.3. Аналіз існуючих методів захисту. 1.4. Розгляд технологій та протоколів VPN. 1.5. Вибір оптимальної стратегії захисту. 2. Проектування систем захисту. 2.1. Визначення цілей та критеріїв безпеки. 2.2. Моделювання загроз та вразливостей. 2.3. Структурне проектування VPN-системи. 2.4. Вибір технологій реалізації VPN. 3. Практичне застосування. 3.1. Налаштування OpenVPN. 3.2. Аналіз впливу шифрування на канал зв'язку. 4. Безпека життєдіяльності. 4.1. Охорона праці. 4.2. Безпека в надзвичайних ситуаціях. 5. Перелік графічного матеріалу. 5.1. Сертифікат центру сертифікації. 5.2. Конфігурація сервера OpenVPN. 5.3. Тестування VPN-з'єднання. 5.4. Пропускна здатність з різними алгоритмами.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Успішне створення сертифікату центру сертифікації (CA), Конфігураційний файл сервера OpenVPN, Статус роботи OpenVPN-сервісу, Файл конфігурації клієнта OpenVPN, Команда запуску VPN-з'єднання, Процес налаштування конфігурації на Windows 10, Налаштування клієнтського конфігураційного файлу на Windows 10, Процес підключення до VPN-сервера, Середовище VirtualBox, Перевірка каналу VM Network без VPN, Пропускна здатність без VPN, Перевірка VPN-тунелю без шифрування, Пропускна здатність VPN без шифрування, Пропускна здатність VPN з DES-EDE, Пропускна здатність VPN з DES-EDE, Перевірка VPN-тунелю з шифруванням BF-CBC, Пропускна здатність VPN з BF-CBC, Перевірка VPN-тунелю з шифруванням AES-256, Пропускна здатність VPN з AES-256.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 23.09.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Підбір джерел з питань проектування систем захисту з використанням VPN	23.09 – 03.10	Виконано
3.	Опрацювання джерел з проектування та реалізації VPN-систем	04.10 – 12.10	Виконано
4.	Виконання дослідження щодо методів використання VPN для захисту інформаційних систем	12.10 – 20.10	Виконано
5.	Підготовка матеріалу	21.10-25.10	Виконано
6.	Підбір джерел з питань проектування систем захисту з використанням VPN	26.10 – 30.10	Виконано
7.	Оформлення розділу ≪Аналіз стану системи та вимог інформаційної безпеки	01.11 – 05.11	Виконано
8.	Оформлення розділу «Проектування систем захисту з використанням VPN»	06.11 – 11.11	Виконано
9.	Оформлення розділу «Практичне застосування технології OpenVPN»	12.11-20.11	Виконано
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи хорони праці	21.11 – 25.11	Виконано
11.	Нормоконтроль		
12.	Перевірка на плагіат	19.12	
13.	Попередній захист кваліфікаційної роботи		
14.	Захист кваліфікаційної роботи	26.12	
15.			

Студент _____ Олійник Ю.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Оробчук О.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Способи захисту інформаційно- телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN // ОР «Магістр» // Олійник Юрій Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 82, рис. – 18, табл. –, додат. –.

Ключові слова: VPN, захист інформаційних систем, IPSec, OpenVPN, безпека даних, телекомунікаційні мережі.

Робота присвячена дослідженню методів захисту інформаційно-телекомунікаційних систем із використанням технологій VPN. Особлива увага приділяється аналізу сучасних VPN-протоколів, таких як IPSec та OpenVPN, їх функціональних можливостей та ролі у забезпеченні безпеки даних. У ході дослідження виконано моделювання загроз та оцінку вразливостей VPN-систем, включаючи перевірку ефективності різних алгоритмів шифрування. Запропоновані рекомендації щодо впровадження OpenVPN у корпоративне середовище з метою мінімізації ризиків кіберзагроз і забезпечення стабільності з'єднань. Практичне значення роботи полягає у розробці підходів до інтеграції VPN-рішень із наявними системами, що дозволяє підвищити рівень захисту даних у телекомунікаційних мережах. Основна увага зосереджена на створенні універсальної моделі забезпечення кібербезпеки із використанням інноваційних VPN-технологій.

ABSTRACTS

Ways to protect information and telecommunication systems and networks from unauthorized access using VPN technology // Master's Degree Work // Oliinyk Yurii Romanovych // Ternopil National Technical University named after Ivan Puluj, Faculty of Computer and Information Systems and Software Engineering, Department of Cyber Security, SBm-61 Group // Ternopil, 2024 // P. 82, Fig.

Keywords: VPN, information systems protection, IPSec, OpenVPN, data security, telecommunication networks.

The paper is devoted to the study of methods of protecting information and telecommunication systems using VPN technologies. Particular attention is paid to the analysis of modern VPN protocols, such as IPSec and OpenVPN, their functionality and role in ensuring data security. The study includes threat modelling and vulnerability assessment of VPN systems, including testing the effectiveness of various encryption algorithms. Recommendations for the implementation of OpenVPN in the corporate environment to minimise the risks of cyber threats and ensure the stability of connections are proposed. The practical significance of the work lies in the development of approaches to the integration of VPN solutions with existing systems, which allows to increase the level of data protection in telecommunication networks. The main focus is on creating a universal model for ensuring cybersecurity using innovative VPN technologies.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN — Virtual Private Network

IPSec — Internet Protocol Security

SSL/TLS — Secure Sockets Layer/Transport Layer Security

L2TP — Layer 2 Tunneling Protocol

CLI — Command Line Interface

API — Application Programming Interface

NIST — National Institute of Standards and Technology

IETF — Internet Engineering Task Force

TCP/IP — Transmission Control Protocol/Internet Protocol

RFC — Request for Comments

PKI — Public Key Infrastructure

DNS — Domain Name System

SSH — Secure Shell

HTTP — Hypertext Transfer Protocol

HTTPS — Hypertext Transfer Protocol Secure

UDP — User Datagram Protocol

QoS — Quality of Service

AES — Advanced Encryption Standard

DES — Data Encryption Standard

RSA — Rivest–Shamir–Adleman

ВСТУП

У сучасному світі інформаційні та телекомунікаційні системи є ключовими складовими діяльності організацій різного масштабу та галузей. Вони забезпечують обробку, зберігання та передачу важливих даних, що робить їх захист пріоритетним завданням. Зростання обсягу даних та кількості пристроїв, які підключаються до мережі, супроводжується збільшенням ризиків кіберзагроз. Така загроза може поставити під ризик конфіденційність, цілісність та доступність інформації, що обумовлює необхідність впровадження сучасних технологій для її захисту. Одним із найбільш ефективних рішень цієї проблеми є використання віртуальних приватних мереж (VPN).

VPN дозволяє створювати захищені канали передачі даних через незахищені мережі, такі як Інтернет. Використання механізмів шифрування та аутентифікації мінімізує ризик перехоплення даних, роблячи технології VPN важливим елементом у сучасних стратегіях кібербезпеки. Вони забезпечують безпечний доступ до корпоративних ресурсів, підвищуючи мобільність співробітників та оптимізуючи витрати на інфраструктуру.

Метою цього дослідження є розробка комплексного підходу до захисту інформаційно-телекомунікаційних систем за допомогою VPN. Передбачено аналіз існуючих методів і VPN-протоколів, розробку моделі захисту, а також оцінку її ефективності через тестування. Дослідження обґрунтоване значним зростанням кількості кіберзагроз, що робить впровадження безпечних рішень нагальною потребою.

Структура роботи складається із чотирьох основних розділів. У першому розділі аналізуються поточний стан проблеми та вимоги до захисту інформації, включаючи сучасні методи безпеки з акцентом на VPN. Другий розділ присвячено проектуванню та вибору оптимальної системи VPN на основі моделювання загроз і розгляду відповідних технологій. У третьому розділі описуються процеси практичної реалізації VPN-рішень, зокрема технології OpenVPN, а також

аналізується ефективність їх впровадження. Четвертий розділ розглядає питання охорони праці та забезпечення безпеки в надзвичайних ситуаціях під час використання VPN.

Результати дослідження мають значне практичне значення для підвищення рівня безпеки інформаційно-телекомунікаційних систем. Запропонований підхід до використання технологій VPN дозволяє ефективно забезпечувати конфіденційність та цілісність даних, що передаються через незахищені мережі, такі як Інтернет. VPN допомагає мінімізувати ризики, пов’язані з перехопленням чи несанкціонованим доступом до інформації, що сприяє зменшенню кіберзагроз та підвищує довіру до комунікаційних мереж.

У роботі було проведено оцінку ефективності протоколів VPN, зокрема OpenVPN і WireGuard, які продемонстрували різні переваги. Протокол WireGuard виявив високу продуктивність, у той час як OpenVPN забезпечив більшу гнучкість у налаштуваннях. Це дозволило сформувати рекомендації щодо вибору та налаштування VPN-систем залежно від потреб конкретної організації. Враховуючи аспекти швидкості з'єднання, надійності шифрування та стійкості до кібератак, було визначено оптимальні технічні параметри для реалізації захисту мережевих ресурсів.

Розроблено стратегічні рекомендації щодо інтеграції VPN у загальні системи кібербезпеки. Серед додаткових заходів передбачено регулярне оновлення програмного забезпечення, застосування двофакторної автентифікації, моніторинг мережевої активності та коригування конфігурацій для запобігання типових уразливостей. Впровадження таких заходів гарантує підвищення безпеки корпоративних і приватних мереж у контексті сучасних кіберзагроз.

Практичне значення полягає у створенні ефективного механізму захисту інформаційно-телекомунікаційних систем, який може бути впроваджений у різних організаціях для забезпечення стабільного та безпечного функціонування мережевих інфраструктур. Застосування розроблених рекомендацій сприяє

підвищенню готовності до протидії кіберзагрозам та стійкості інформаційних систем у довгостроковій перспективі.

Це дослідження спрямоване на створення надійних рішень для захисту інформаційних систем, що дозволить підвищити рівень їх безпеки, зберігши стабільність функціонування організаційних мереж. В умовах постійного розвитку технологій та зростання складності кіберзагроз, інтеграція VPN у загальну стратегію кібербезпеки стає не лише бажаною, але й необхідною умовою для забезпечення стійкості та надійності інформаційних систем.

РОЗЛІЛ 1 АНАЛІЗ СТАНУ ПРОБЛЕМИ ТА ВИМОГ

1.1 Постановка задачі

У сучасному цифровому середовищі забезпечення безпеки інформаційно-телекомунікаційних систем стає одним з найважливіших пріоритетів для організацій будь-якого масштабу. Основною метою даної кваліфікаційної роботи є розробка й дослідження методів захисту інформаційних систем та мереж від несанкціонованого доступу, з акцентом на технології віртуальних приватних мереж (VPN). Використання VPN дозволяє створювати захищені канали зв'язку в загальнодоступних мережах, зберігаючи конфіденційність і цілісність переданих даних.

Перше завдання роботи полягає в аналізі сучасних кіберзагроз та уразливостей, що характерні для інформаційно-телекомунікаційних систем. Це дозволить ідентифікувати основні вимоги до безпеки та розробити відповідні стратегії захисту. Необхідно розглянути основні типи атак, які можуть загрожувати системам, а також методи їх виявлення та запобігання .

Друге завдання полягає в дослідженні існуючих VPN-технологій, таких як IPSec, SSL/TLS, і їх спроможності забезпечити захищений канал передачі даних. Це включає вивчення їх структурних особливостей, механізмів автентифікації, шифрування, а також можливостей інтеграції в сучасні мережі [1, 6].

Третє завдання передбачає розробку архітектури VPN-системи, яка може бути інтегрована в існуючі корпоративні мережі для забезпечення безпечного доступу до ресурсів організації. Важливим аспектом є забезпечення можливості масштабування системи, її адаптації до мінливих умов та вимог безпеки .

Четверте завдання полягає у тестуванні розробленої системи для оцінки її ефективності та стійкості до кіберзагроз. Це включає перевірку швидкості передачі даних, надійності шифрування, а також здатності системи протистояти різним

видам атак. Під час тестування будуть використовуватися різні сценарії для перевірки реальних умов експлуатації.

П'яте завдання полягає в оцінці економічної доцільності впровадження VPN-рішень, враховуючи витрати на реалізацію і обслуговування, а також потенційну вигоду від їх використання. Це допоможе визначити найбільш оптимальні рішення з точки зору ресурсів та безпеки для організації .

Дослідження є надзвичайно актуальним через постійне зростання кількості та складності кіберзагроз, які можуть порушити конфіденційність даних та стабільність роботи систем. Безпека інформаційних систем є критично важливою для збереження конкурентоспроможності та репутації організацій в умовах сучасної цифрової економіки.

Таким чином, постановка задачі полягає у створенні комплексної системи захисту інформаційних мереж за допомогою VPN, що дозволить організаціям забезпечити безпеку та збереження даних у сучасному цифровому світі. Це дослідження сприятиме підвищенню рівня безпеки інформаційних систем та підготовці спеціалістів, здатних ефективно протистояти кіберзагрозам .

1.2 Огляд вимог до захисту інформаційних систем від несанкціонованого доступу

1.2.1 Загальні вимоги до безпеки

Для забезпечення захисту інформаційних систем від несанкціонованого доступу необхідно дотримуватись низки загальних вимог безпеки. Одним із ключових аспектів є збереження конфіденційності даних. Це досягається за допомогою використання алгоритмів шифрування, таких як IPSec та SSL/TLS, які допомагають запобігти доступу неавторизованих осіб до чутливої інформації.

Ще однією важливою вимогою є забезпечення цілісності даних. Це гарантує, що інформація залишається незмінною під час передачі, завдяки застосуванню хеш-функцій та механізмів перевірки, наприклад, HMAC. Важливу роль також відіграє автентифікація користувачів. Процедури, такі як багатофакторна

автентифікація (MFA), додають додатковий рівень захисту, дозволяючи переконатися у достовірності особи, яка отримує доступ до системи.

Не менш важливим є забезпечення доступності системи, що потребує заходів для стабільного доступу до ресурсів. Це включає впровадження резервування та захисту від DoS-атак. Важливу увагу також приділяють контролю доступу, створюючи політики, які чітко визначають права користувачів та обмежують доступ до конфіденційних даних залежно від їхніх обов'язків.

Безперервний моніторинг та регулярні аудити є необхідними для відстеження активності та виявлення потенційних загроз безпеці. Крім того, управління вразливостями включає постійне оновлення програмного забезпечення та використання автоматизованих інструментів для своєчасного усунення критичних загроз.

Дотримання цих ключових вимог безпеки дає змогу забезпечити надійну роботу інформаційно-телекомунікаційних систем у динамічному цифровому середовищі, яке постійно змінюється [4].

1.2.2 Спеціальні вимоги до телекомунікаційних мереж

Для телекомунікаційних мереж існують спеціальні вимоги, які забезпечують їхню надійну роботу, продуктивність і захист. Однією з ключових умов є забезпечення високої пропускної здатності та якості обслуговування (QoS). Це дозволяє підтримувати стабільність з'єднань навіть при обробці великого обсягу трафіку. Сумісність протоколів є ще однією важливою вимогою. Телекомунікаційна мережа повинна безперешкодно інтегруватися з існуючими мережевими протоколами, такими як TCP/IP, для безпечної передачі даних між компонентами.

Масштабованість інфраструктури є критичною для підтримки зростаючої кількості користувачів і пристроїв. Розширення мережі не повинно знижувати її продуктивність і порушувати рівень безпеки. Також необхідно враховувати захист

від атак типу «людина посередині» (MitM). Для цього впроваджують надійні методи шифрування, які мінімізують ризик перехоплення або модифікації даних.

Рівномірний розподіл навантаження на мережу відіграє важливу роль у запобіганні перевантаженню трафіку. Крім того, механізми автоматичного відновлення з'єднань забезпечують безперервність процесів у разі збоїв у роботі мережі. Системи моніторингу дозволяють у реальному часі відслідковувати загрози та оперативно реагувати на аномальні ситуації.

Дотримуючись цих вимог, можна забезпечити стабільну, безпечну та ефективну роботу телекомунікаційних мереж навіть у динамічному цифровому середовищі [9, 12].

1.3 Аналіз існуючих методів захисту з використанням VPN

1.3.1 Традиційні методи захисту

Традиційні методи захисту інформаційно-телекомунікаційних систем становлять основу для забезпечення безпеки та впровадження сучасних технологій, таких як VPN. Одним із ключових елементів є межові фаєрволи, які контролюють трафік, запобігаючи несанкціонованому доступу та обмежуючи доступ до критично важливих ресурсів. Фаєрволи можуть бути реалізовані як у вигляді апаратних пристроїв, так і у формі програмного забезпечення.

Системи виявлення вторгнень (IDS) також відіграють важливу роль. Вони моніторять мережеву активність, дозволяючи виявляти та реагувати на підозрілі дії чи атаки через використання сигнатур або аналіз аномалій. Ще одним важливим компонентом є аутентифікація користувачів, яка підтверджує ідентифікацію за допомогою паролів, токенів чи біометричних даних, забезпечуючи доступ виключно авторизованим особам [3].

Шифрування даних є ще одним критично важливим елементом традиційного захисту. Використання криптографічних алгоритмів, наприклад AES, допомагає

захистити передані через незахищені мережі дані від перехоплення. У той же час фізичний захист гарантує контроль доступу до приміщень, серверного обладнання та мережевих пристроїв, запобігаючи несанкціонованим спробам отримання доступу до інформації.

Сегментація мережі також є важливою практикою. Розподіл мережі на підмережі дозволяє обмежити поширення загроз та посилює контроль над трафіком між сегментами. Застосування таких методів є важливим кроком для усунення ключових вразливостей та створює основу для подальшої інтеграції сучасних рішень, таких як VPN, що значно підвищує рівень безпеки інформаційних систем [7].

1.3.2 Сучасні підходи з акцентом на VPN

Сучасні підходи до захисту інформаційних систем із фокусом на VPN спрямовані на ефективну протидію кіберзагрозам. Інтеграція з Zero Trust архітектурою забезпечує постійну автентифікацію користувачів і пристроїв, мінімізуючи ризики довіри до мережі. Мультифакторна аутентифікація (MFA) додає додатковий рівень безпеки, зменшуючи ймовірність злому облікових записів.

Шифрування за стандартом AES-256 гарантує конфіденційність інформації, а динамічний контроль доступу адаптує політики залежно від контексту, наприклад, місцезнаходження чи типу пристрою. Автоматизоване управління вразливостями виявляє й усуває загрози, а моніторинг у реальному часі дозволяє оперативно реагувати на потенційні атаки.

Хмарні VPN вирізняються масштабованістю, гнучкістю та економністю, забезпечуючи швидке розгортання і надійний захист. Сукупність цих підходів робить VPN ефективним інструментом для захисту сучасних інформаційних систем [6].

1.4 Розгляд технологій та протоколів VPN

1.4.1 IPSec (Internet Protocol Security)

IPSec (Internet Protocol Security) є однією з ключових технологій для забезпечення захисту даних у VPN. Його головними особливостями є шифрування даних за допомогою AES і 3DES, що запобігає перехопленню та аналізу інформації. Протоколи безпеки, такі як AH, забезпечують автентифікацію та цілісність IP-пакетів, тоді як ESP додає шифрування для підвищення конфіденційності. Також IPSec використовує механізм тунелювання для безпечної передачі даних через незахищені мережі, створюючи віртуальні тунелі.

IPSec активно застосовується в корпоративних мережах для захисту комунікацій і забезпечення безпечного доступу віддаленим працівникам. У міжмережевих з'єднаннях воно створює надійний зв'язок між офісами через загальнодоступну інфраструктуру. Крім того, урядові установи використовують IPSec для захисту чутливої інформації відповідно до стандартів високого рівня безпеки.

Ця технологія має низку переваг. Вона універсальна та підтримується більшістю обладнання й операційних систем. IPSec легко інтегрується з іншими VPN-протоколами, утворюючи багатошаровий захист, а також демонструє високу стійкість до атак, запобігаючи підміні або модифікації даних і протидіючи кіберзлочинам. Завдяки цим характеристикам IPSec залишається критично важливим елементом для забезпечення шифрування, автентифікації та цілісності даних у сучасних інформаційних системах [8, 10].

1.4.2 OpenVPN

OpenVPN — це гнучкий і потужний VPN-протокол, розроблений для безпечного обміну даними в інформаційно-телекомунікаційних системах. Його доступність як відкритого програмного забезпечення дає змогу налаштовувати його

відповідно до особливостей будь-якого мережевого середовища. OpenVPN використовує бібліотеки OpenSSL, застосовуючи передові алгоритми шифрування, такі як AES, RSA та SHA, що забезпечують високий рівень конфіденційності та цілісності даних. Завдяки підтримці TCP і UDP OpenVPN дозволяє вибирати оптимальний режим передачі для досягнення балансу між продуктивністю і безпекою. Для автентифікації реалізовано багатофакторний підхід, який використовує сертифікати X.509, ключі безпеки та облікові дані.

Цей протокол широко застосовується для забезпечення безпеки корпоративних мереж, зокрема для захищеного доступу віддалених співробітників до внутрішніх ресурсів компанії. OpenVPN ефективно об'єднує офісні мережі через загальнодоступний інтернет, створюючи цілісні та захищені міжмережеві канали. Крім того, протокол використовують урядові структури для захисту конфіденційної інформації, відповідаючи високим стандартам безпеки.

Основними перевагами OpenVPN є прозорість завдяки відкритому коду, який регулярно проходить аудит безпеки, а також підтримка різних платформ, включаючи Windows, macOS, Linux, Android та iOS. Потужні криптографічні методи забезпечують високу стійкість до кіберзагроз, роблячи OpenVPN надійним вибором для захисту мереж. Постійно вдосконалюючись, цей протокол залишається актуальним інструментом для боротьби з кіберзагрозами в сучасному цифровому світі [1, 14].

1.4.3 L2TP/IPSec (Layer 2 Tunneling Protocol over Internet Protocol Security)

L2TP/IPSec (Layer 2 Tunneling Protocol over Internet Protocol Security) є технологією, яка забезпечує додатковий рівень безпеки при передачі даних. Поєднання протоколу L2TP, що створює тунелі, з IPSec, який виконує шифрування, забезпечує подвійний захист інформації. Застосовуючи алгоритми шифрування AES і 3DES, L2TP/IPSec гарантує, що дані залишаться конфіденційними та

захищеними від несанкціонованого доступу. Для автентифікації використовується протокол IKE, що забезпечує надійний обмін ключами між сторонами.

L2TP/IPSec широко використовується в корпоративних мережах для надання безпечного віддаленого доступу співробітникам до внутрішніх ресурсів компанії.

Також ця технологія дозволяє створювати захищені міжмережеві з'єднання між офісами через загальнодоступний Інтернет. Крім того, її активно впроваджують державні установи для передачі конфіденційних даних, дотримуючись високих стандартів безпеки.

До переваг L2TP/IPSec належить сумісність із більшістю сучасних мережевих пристроїв і операційних систем, що робить її легкою у впровадженні. Завдяки двошаровому захисту цей протокол забезпечує високий рівень безпеки, захищаючи від перехоплення, модифікації або підміни даних. Гнучкість налаштувань дозволяє адаптувати методи шифрування до конкретних потреб користувача. Завдяки таким характеристикам L2TP/IPSec залишається універсальним і надійним рішенням для захисту даних у різних середовищах, зокрема корпоративних і державних мережах [15].

1.4.4 PPTP (Point-to-Point Tunneling Protocol)

PPTP (Point-to-Point Tunneling Protocol) — це простий і швидкий VPN-протокол, відомий своєю легкістю налаштування та широкою сумісністю. Завдяки підтримці операційних систем, таких як Windows, macOS, Linux, iOS та Android, PPTP зручний для користувачів із базовими технічними знаннями. Простота методів шифрування забезпечує високу швидкість з'єднання, що є його ключовою перевагою.

Раніше PPTP активно використовувався в корпоративних мережах для підключення віддалених офісів та працівників. У сучасності його застосування звелося до особистих мереж, де він забезпечує базовий захист з'єднань у публічних

Wi-Fi мережах. Його перевагою також є мінімальні вимоги до обладнання, що робить PPTP доступним для інтеграції з наявними мережами.

Водночас PPTP має значні обмеження. Відомі вразливості у шифруванні та механізмах автентифікації ставлять під сумнів його надійність у середовищах із високими вимогами до безпеки. З появою сучасніших протоколів, як-от OpenVPN і L2TP/IPSec, PPTP значно втратив популярність та актуальність для складних корпоративних завдань. Через це, хоча PPTP і зберіг свою простоту та швидкість, його роль значно обмежилась [11].

1.4.5 SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL/TLS (Secure Sockets Layer / Transport Layer Security) — це важлива технологія, яка забезпечує захист переданих даних в мережах. Шифрування з використанням симетричних алгоритмів, таких як AES (Advanced Encryption Standard) або ChaCha20, гарантує конфіденційність інформації, запобігаючи її доступу стороннім. Симетричні алгоритми забезпечують високошвидкісну передачу даних без втрати безпеки, що робить їх незамінними для передачі великих обсягів інформації в стислі строки. Крім того, цифрові сертифікати, засновані на інфраструктурі відкритих ключів (PKI), забезпечують автентифікацію клієнтів і серверів, підтверджуючи їхню особу та довіру до них. Популярні центри сертифікації, такі як DigiCert і Let's Encrypt, гарантують надійну видачу таких сертифікатів.

Для збереження цілісності даних застосовуються хеш-функції, наприклад, SHA-256 або SHA-3, які створюють унікальний хеш-код для будь-якої інформації. В результаті зміна хоча б одного символу в даних призводить до повної невідповідності хеш-коду, що дозволяє виявити ймовірні модифікації під час передачі. Такий підхід захищає інформацію від атак типу "людина посередині" та збоїв, які можуть виникнути в процесі її транспортування.

Цей протокол широко підтримується веб-браузерами, такими як Google Chrome, Mozilla Firefox, та серверами, наприклад, Apache і NGINX, а також більшістю мережевих протоколів, таких як HTTPS. Це робить його універсальним рішенням для захисту цифрових комунікацій. SSL/TLS легко інтегрується в існуючі інфраструктури через сучасні API та готові бібліотеки, як-от OpenSSL, що зменшує витрати на впровадження і забезпечує високий рівень безпеки. Завдяки шифруванню та автентифікації мінімізується ризик несанкціонованого доступу до приватної інформації, включаючи фінансові дані, логіни та паролі.

Технологія активно використовується в корпоративних мережах для захисту внутрішніх комунікацій, як-от електронної пошти (Microsoft Exchange), доступу до баз даних і VPN-з'єднань, які гарантують безпечний віддалений доступ до корпоративних ресурсів. Це зводить ризик витоку конфіденційної інформації, важливої для бізнесу, до мінімуму. В області інтернету SSL/TLS є основою для HTTPS, що гарантує безпеку онлайн-транзакцій, таких як оплата на платформах Amazon або PayPal, захищаючи дані покупців від шахраїв. Крім того, ця технологія є обов’язковою для веб-сайтів, оскільки пошукові системи, як-от Google, віддають пріоритет сайтам з HTTPS у пошуковій видачі, сприяючи покращенню довіри користувачів.

Урядові установи також активно застосовують цей протокол для захищеної передачі інформації між державними відомствами. Наприклад, шифрування та автентифікація використовуються в електронному документообігу, державних порталах надання послуг та обміні персональних даних громадян. SSL/TLS забезпечує відповідність сучасним стандартам кібербезпеки, в тому числі нормативам ISO/IEC 27001 і GDPR, створюючи надійні умови для захищених комунікацій.

У підсумку, SSL/TLS залишається ключовим інструментом для створення надійних і безпечних з'єднань, відповідаючи актуальним вимогам цифрового середовища. Впровадження цієї технології є критично важливим як для приватного

сектору, так і для урядових структур, забезпечуючи захист даних, просунутий рівень автентифікації та запобігання кіберзагрозам.

1.4.6 IKEv2 (Internet Key Exchange version 2)

IKEv2 (Internet Key Exchange version 2) — це сучасний протокол, що забезпечує швидкість, надійність і високу безпеку передачі даних. Завдяки підтримці технології MOBIKE, IKEv2 гарантує стабільність з’єднань навіть у разі зміни IP-адрес, що робить його ідеальним рішенням для мобільних середовищ. Протокол використовує передові алгоритми шифрування, такі як AES, а також підтримує автентифікацію на основі сертифікатів або попередньо узгоджених ключів. Його сумісність із IPsec підтверджує універсальність і дозволяє легко впроваджувати це рішення як у корпоративних, так і в урядових мережах.

IKEv2 відзначається ефективністю, забезпечуючи швидке встановлення з'єднань із мінімальними затримками, що є критичним для мобільних пристроїв. Крім того, він гарантує безперебійність зв'язку навіть у динамічних умовах, зберігаючи стабільність підключення. Гнучкість протоколу дозволяє адаптувати його до різних алгоритмів шифрування та автентифікації залежно від вимог користувача.

Протокол активно використовується в корпоративних мережах, де він забезпечує безпечний доступ мобільних працівників до ресурсів компанії. Він також надійно захищає передавання конфіденційних даних, що відповідає високим стандартам безпеки, необхідним державним установам.

Технічний аспект IKEv2 включає двофазний процес встановлення з'єднання, який забезпечує автентифікацію користувачів і обмін ключами для створення надійного зв’язку. Підтримка EAP (Extensible Authentication Protocol) дозволяє додатково інтегрувати цей протокол із системами управління доступом для посилення контролю.

Завдяки своїй ефективності, мобільності та високому рівню безпеки, IKEv2 є універсальним і надійним VPN-рішенням для сучасних мобільних і фіксованих мереж [15].

1.5 Вибір оптимальної стратегії захисту з використанням VPN

Вибір оптимальної стратегії захисту з використанням VPN полягає в ретельному аналізі потреб і можливостей. По-перше, важливо врахувати безпекові вимоги, оцінюючи потенційні загрози, такі як атаки "людина посередині" (MITM), перехоплення даних або спуфінг IP-адрес. Для захисту даних слід використовувати сучасні протоколи, як-от IPSec, що забезпечує шифрування на рівні мережі, або OpenVPN, який має відкритий вихідний код і підтримує шифрування з використанням SSL/TLS. Ці протоколи гарантують конфіденційність і цілісність переданої інформації навіть у нестабільних мережевих умовах. Окрім цього, такі протоколи, як WireGuard, пропонують сучасніший підхід із фокусом на швидкість і простоту налаштування, що є особливо важливим для малого і середнього бізнесу.

Інфраструктура відіграє ключову роль у забезпеченні ефективності VPN-рішень. Важливо, щоб обране рішення було сумісним із наявним обладнанням, зокрема маршрутизаторами, брандмауерами та пристроями кінцевих користувачів. Наприклад, багато сучасних VPN-рішень підтримують кросплатформеність для Windows, macOS, iOS і Android, що дозволяє інтегрувати їх у різні робочі середовища. Також важливо враховувати можливість масштабування, щоб VPN-інфраструктура могла адаптуватися до зростання компанії, наприклад, додавання нових офісів або збільшення кількості віддалених користувачів. Для організаційних потреб протоколи на зразок IKEv2 забезпечують стабільність підключення навіть за умови зміни мережі, що робить їх ідеальними для мобільних працівників.

Вибір протоколу залежить від балансу між безпекою та продуктивністю. Наприклад, OpenVPN є ефективним рішенням для захисту глобальних мереж і використовується багатьма корпораціями через високий рівень безпеки та гнучкість

у налаштуванні. PPTP, хоча і швидкий, використовує застарілі алгоритми шифрування, тому підходить тільки для задач із мінімальними вимогами до безпеки. Завдання об’єднання високої продуктивності та безпеки можуть бути вирішені за допомогою WireGuard, який демонструє низьку затримку з'єднання при збереженні високого рівня захисту.

Додаткові заходи значно посилюють ефективність стратегії із впровадження VPN. Використання багатофакторної аутентифікації (MFA), наприклад, застосування паролів у поєднанні з біометричними даними або одноразовими паролями (OTP), додає додатковий рівень захисту навіть у разі компрометації доступу. Моделі Zero Trust гарантують доступ лише авторизованим користувачам і пристроям, що суттєво знижує ризик внутрішніх і зовнішніх загроз. Моніторинг у реальному часі, наприклад через платформи SIEM (Security Information and Event Management), дозволяє оперативно виявляти підозрілу активність, включаючи спроби несанкціонованого доступу або вразливостей у мережі.

Фінансовий аспект вибору VPN-стратегії включає витрати на обладнання, програмне забезпечення та навчання персоналу. Апаратні VPN-шлюзи потребують значних інвестицій, забезпечуючи високу продуктивність, тоді як хмарні рішення коштують дешевше та включають автоматичну підтримку. Головна мета — знайти баланс між витратами й рівнем безпеки.

У підсумку, вибір оптимальної стратегії захисту з використанням VPN включає всебічний підхід до аналізу потреб організації. Врахування вимог безпеки, відповідність інфраструктурі, правильний вибір протоколу та впровадження додаткових заходів забезпечують високий рівень захищеності та продуктивності. Фінансова оцінка гарантує ефективне використання ресурсів, створюючи надійну основу для безпечних комунікацій у будь-якому масштабі.

РОЗДІЛ 2 ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ З ВИКОРИСТАННЯМ VPN

2.1 Визначення цілей та критеріїв безпеки

2.1.1 Конфіденційність даних

Визначення цілей та критеріїв безпеки є основою для забезпечення конфіденційності даних, яка є критично важливим аспектом захисту інформаційно-телекомунікаційних систем від несанкціонованого доступу, особливо в контексті використання технологій VPN. В епоху цифрових комунікацій забезпечення конфіденційності інформації стає пріоритетним завданням для організацій, оскільки порушення конфіденційності може призвести до значних фінансових втрат та шкоди репутації [1].

Одним із ключових методів забезпечення конфіденційності даних у VPN є шифрувальні протоколи для забезпечення конфіденційності, такі як IPSec та SSL/TLS. IPSec забезпечує конфіденційність і цілісність даних на мережевому рівні, використовуючи криптографічні методи для захисту даних під час передачі через мережу. Це включає в себе аутентифікацію, шифрування та управління ключами, що разом гарантують захищене з'єднання. З іншого боку, SSL/TLS забезпечує конфіденційність даних на транспортному рівні, створюючи захищене з'єднання між клієнтом і сервером. Це широко використовується для захисту веб-трафіку, гарантує автентичність сторін та шифрує дані, що передаються.

Криптографія відіграє ключову роль у підтримці конфіденційності даних у VPN-системах. Симетричне шифрування, яке використовує один ключ для шифрування та дешифрування, є ефективним для захисту великих обсягів даних завдяки своїй швидкості. Асиметричне шифрування, що базується на парі ключів (публічний та приватний), забезпечує високий рівень безпеки при обміні ключами між сторонами.

Для збереження конфіденційності даних важливо враховувати виклики та стратегії забезпечення конфіденційності, зокрема постійно оновлювати криптографічні алгоритми та ключі з метою протистояння новим загрозам і атакам. Це вимагає регулярного моніторингу безпекових політик, проведення аудитів та впровадження нових технологій. Наприклад, впровадження мультифакторної аутентифікації (MFA) може додатково захистити дані від несанкціонованого доступу [19].

Таким чином, забезпечення конфіденційності даних у VPN є багатогранним процесом, що вимагає інтеграції сучасних технологій та методів для ефективного захисту інформації, що передається через мережі, від несанкціонованого доступу. Це має важливе значення для захисту чутливої інформації в умовах зростаючих кіберзагроз.

2.1.2 Цілісність даних

Цілісність даних гарантує, що інформація залишається незмінною під час передачі та захищеною від несанкціонованих змін. Її порушення може призвести до втрати довіри, фальсифікації даних чи фінансових збитків.

Ключовим протоколом забезпечення цілісності в VPN є IPSec, який використовує Authentication Header (AH) та Encapsulating Security Payload (ESP). Хеш-функції, як-от SHA-256, створюють унікальні цифрові підписи, а MAC (Message Authentication Code) захищає дані за допомогою секретних ключів.

Основні виклики включають управління криптографічними ключами, оновлення алгоритмів та протидію новим загрозам. Регулярний моніторинг, аудит та інструменти, такі як цифрові підписи або багатофакторна аутентифікація (MFA), допомагають зберігати високий рівень безпеки.

Таким чином, надійний захист даних базується на сучасних криптографічних методах і активному моніторингу. Експерти, як-от Stallings (2019) і Schneier (2015), наголошують на важливості адаптивності та постійного вдосконалення систем [16].

2.1.3 Особливості підтримки стабільності з’єднань в OpenVPN

Стабільність VPN-з’єднань у OpenVPN залежить від належних налаштувань, які зменшують ризик розривів зв’язку та забезпечують автоматичне відновлення.

IKEv2 забезпечує швидке відновлення з’єднання після втрати сигналу, що є критично важливим для користувачів, які перемикаються між мережами (наприклад, Wi-Fi і мобільний інтернет). Завдяки функції MOBIKE VPN-з’єднання зберігається навіть при зміні IP-адреси.

OpenVPN використовує функцію keepalive для моніторингу і контролю активності з’єднання. У разі відсутності відповіді від сервера клієнт автоматично намагається відновити зв’язок.

Протоколи TCP і UDP мають свої переваги. TCP гарантує доставку даних у мережах із високою завадністю, тоді як UDP забезпечує швидкість у стабільніших умовах.

Правильні налаштування тайм-аутів, такі як оптимізація тайм-аутів і налаштування DNS, наприклад, параметру --reconnect-timeout, забезпечують оперативне перепідключення. Опція --block-outside-dns допомагає уникнути витоку DNS-запитів за межі тунелю.

Різні профілі конфігурації, що забезпечують багатопрофільність для адаптації, дозволяють оптимізувати роботу OpenVPN під конкретні умови. Наприклад, один профіль можна використовувати для TCP у мережах із низькою якістю зв’язку, а інший — для UDP у стабільних мережах.

Таким чином, правильно налаштований OpenVPN забезпечує стабільні з’єднання навіть за несприятливих умов. Ключову роль у цьому відіграють функції моніторингу, адаптивні налаштування та підтримка багатопрофільності [1].

2.1.4 Відповідність стандартам безпеки

Дотримання стандартів безпеки є важливим для захисту інформаційних систем і мереж, включаючи VPN. Це забезпечує структуру для управління ризиками, захисту даних і моніторингу безпеки, зменшуючи фінансові втрати та зберігаючи довіру [2].

Основні стандарти, такі як міжнародний стандарт ISO/IEC 27001, призначені для управління інформаційною безпекою (ISMS), який включає розробку політик безпеки, управління ризиками та постійне вдосконалення системи безпеки.

Рекомендації NIST SP 800-77, як важливі нормативні засади, містять детальні вказівки щодо захисту інформаційних систем за допомогою IPsec VPN, забезпечуючи відповідність федеральним стандартам США та підвищуючи рівень безпеки.

Деякі сфери, наприклад фінансова та медична, враховують роль галузевих регулювань, що вимагають спеціальних заходів безпеки для захисту чутливих даних. Відповідність таким регулюванням є необхідною для уникнення штрафів і підтримання довіри клієнтів.

Для відповідності організаціям слід інтегрувати стандарти безпеки у свої системи через впровадження у VPN, політики шифрування, автентифікацію та моніторинг. Регулярні аудити та використання автоматизованих рішень сприяють підтримці актуальності заходів безпеки [12].

Організації, впроваджуючи ISO/IEC 27001, створюють команди безпеки, проводять навчання персоналу та аудити систем. Це допомагає знизити ризики і забезпечити відповідність стандартам.

2.2 Моделювання загроз та вразливостей

2.2.1 Ідентифікація активів та загроз

Ідентифікація активів є важливим кроком для оцінки, які елементи системи потребують захисту. Активи включають апаратне й програмне забезпечення, дані та мережеві ресурси. Розуміння їх взаємодії дозволяє ефективно визначити критичні елементи для забезпечення безпеки системи [5].

Використання систем управління активами та методів інвентаризації активів для створення реєстру всіх компонентів організації.

Автоматизовані рішення дозволяють відстежувати стан активів, оновлення та потенційні ризики, як-от застаріле програмне забезпечення.

Ідентифікація загроз показує, що загрози можуть бути внутрішніми (помилки персоналу) або зовнішніми (атаки зловмисників). Різновиди загроз включають технічні збої, природні катастрофи та навмисні дії, спрямовані на порушення роботи системи.

Методи аналізу загроз включають моделювання загроз, яке допомагає виявляти можливі вектори атак і слабкі місця. Аналіз ризиків оцінює ймовірність виникнення загроз і їхній потенційний вплив, дозволяючи визначати пріоритети у впровадженні заходів безпеки.

Ідентифікація активів і загроз забезпечує основну базу для стратегій управління ризиками. Це дозволяє організаціям впроваджувати цільові заходи, як-от шифрування, автентифікацію, моніторинг і VPN-технології, знижуючи вплив загроз до прийнятного рівня.

Впровадження стратегій безпеки базується на отриманій інформації про активи та загрози, яка використовується для розробки політик доступу, впровадження захисних технологій, навчання персоналу, регулярного моніторингу й аудитів. Це підвищує стійкість системи до кіберзагроз і захищає цінні активи.

2.2.2 Аналіз вразливостей у VPN-системах

Аналіз вразливостей у VPN-системах показує, що вони схильні до низки типових проблем, які можуть знижувати ефективність захисту. До таких вразливостей належать слабкості протоколів, викликані недостатньою криптографічною стійкістю чи відсутністю належного шифрування. Також часто трапляються проблеми з неправильним налаштуванням, відкритими портами або помилками маршрутизації. Крім того, слабкі паролі, відсутність двофакторної автентифікації та низька обізнаність користувачів про безпекові практики стають значними ризиками [10].

До потенційних загроз у таких системах входить перехоплення даних через слабке шифрування, несанкціонований доступ до мережевих ресурсів, а також витік інформації. Зловмисники можуть використовувати уразливі VPN для створення ботнетів або інших шкідливих дій.

Щоб знизити ці ризики, необхідно застосовувати ефективні методи захисту. Регулярні аудити допомагають ідентифікувати та усувати вразливості у VPN-системах. Оновлення програмного забезпечення та встановлення патчів надають захист від відомих загроз. Важливим аспектом є навчання користувачів, що охоплює створення сильних паролів, використання двофакторної автентифікації та розпізнавання фішингових атак.

Застосування цих заходів дозволяє своєчасно виявляти ризики й мінімізувати їхній вплив, забезпечуючи захист даних та стійкість систем до атак [4].

2.2.3 Оцінка вразливостей шифрування та тунелювання в OpenVPN

Захист даних у OpenVPN забезпечується криптографічними алгоритмами і налаштуваннями тунелювання, які за певних обставин можуть бути уразливими.

Основні ризики.

Перехоплення даних (MITM-атаки). Зловмисники можуть отримати доступ до трафіку між клієнтом і сервером. Для зменшення загроз необхідно впроваджувати TLS-автентифікацію та регулярно оновлювати ключі шифрування.

Застарілі шифрувальні алгоритми. Використання RC4 чи DES знижує безпеку. Рекомендується застосовувати AES-256 або AES-128 як найефективніші сучасні алгоритми.

Неправильне налаштування може призвести до витоку даних. Наприклад, використання опцій --redirect-gateway та --block-outside-dns захищає від витоків трафіку поза VPN-каналом.

Рекомендації з безпеки:

- Регулярно оновлювати OpenVPN.
- Використовувати сильне шифрування (AES-256 або AES-128).
- Впроваджувати TLS-auth для додаткового захисту.
- Налаштовувати багатофакторну автентифікацію (MFA) для підвищеної надійності.

Впровадження сучасних алгоритмів шифрування та регулярний огляд конфігурацій допомагають мінімізувати ризики та забезпечити захист даних в OpenVPN [16].

2.2.4 Стратегії пом’якшення загроз

Стратегії пом’якшення загроз є ключовим елементом у захисті інформаційно-телекомунікаційних систем від несанкціонованого доступу, особливо при використанні технологій VPN. Ці стратегії допомагають зменшити ризики та покращити безпеку, забезпечуючи надійну захищеність даних .

Шифрування є однією з найефективніших стратегій захисту даних у VPN. Використання сильних криптографічних алгоритмів забезпечує конфіденційність даних, що передаються через мережу. Це унеможливлює їхнє перехоплення та

несанкціоноване прочитання. Протоколи, такі як IPsec та OpenVPN, широко застосовуються для забезпечення надійного шифрування .

Контроль доступу є ще однією важливою стратегією пом'якшення загроз, яка включає в себе встановлення чітких політик та процедур управління доступом до системи. Це може включати використання двофакторної автентифікації або біометричних даних для доступу до VPN [12]. Такі заходи дозволяють переконатися, що доступ до критично важливих ресурсів мають лише авторизовані користувачі.

Постійний моніторинг мережі дозволяє виявляти та реагувати на підозрілу активність у режимі реального часу. Встановлення систем виявлення та запобігання вторгнень (IDS/IPS) допомагає виявляти спроби несанкціонованого доступу та інші загрози, що можуть вплинути на безпеку VPN . Це дозволяє своєчасно реагувати на інциденти безпеки та запобігати потенційним збиткам.

Забезпечення актуальності програмного забезпечення через регулярні оновлення та встановлення патчів є критично важливим для закриття відомих вразливостей у системах VPN. Це знижує ризик експлуатації цих вразливостей зловмисниками і підвищує загальний рівень безпеки .

Підвищення обізнаності користувачів щодо основ кібербезпеки та безпечних практик використання VPN є важливим аспектом захисту. Навчання персоналу правильному використанню системи допомагає зменшити ризик людських помилок, які можуть призвести до безпекових інцидентів [20].

2.3 Структурне проектування VPN-системи захисту

2.3.1 Архітектурні рішення для VPN

Архітектурні рішення для впровадження VPN є критично важливими для захисту інформаційно-телекомунікаційних систем від несанкціонованого доступу.

Існує кілька основних типів архітектур, кожна з яких має свої переваги та виклики в контексті безпеки мережі [1].

Site-to-site VPN з'єднує цілі мережі через Інтернет, забезпечуючи безпечний канал між офісами компанії. Це рішення ідеально підходить для великих організацій з декількома віддаленими офісами.

Висока ефективність та централізоване управління є основними перевагами. Висока ефективність забезпечує безпечний обмін даними між офісами без необхідності індивідуального налаштування на кінцевих пристроях .

Централізоване управління полегшує контроль над мережею, оскільки всі з'єднання проходять через централізований шлюз.

Однак, site-to-site VPN може бути складним у налаштуванні та управлінні, особливо якщо мережа складається з багатьох вузлів .

Remote Access VPN забезпечує індивідуальним користувачам безпечний доступ до корпоративної мережі з будь-якого місця. Це рішення ідеально підходить для мобільних працівників або тих, хто працює з дому.

Переваги включають можливість користувачів підключатися до мережі з будь-якого пристрою і місця, що забезпечує високу мобільність, а також підвищену продуктивність, яка дозволяє співробітникам працювати з корпоративними ресурсами без фізичної присутності в офісі.

Серед викликів — необхідність забезпечення безпеки на кожному кінцевому пристрої та управління великою кількістю різних з'єднань.

Hybrid VPN поєднує елементи site-to-site і remote access VPN, забезпечуючи гнучкість і універсальність. Цей підхід дозволяє великим організаціям задовольняти різноманітні потреби своїх користувачів.

Основні переваги включають комбіновану функціональність, яка підтримує як віддалені офіси, так і мобільних користувачів, забезпечуючи безперебійну роботу, а також оптимізацію ресурсів, що дозволяє ефективніше використовувати мережеві ресурси та знижувати витрати на інфраструктуру [7].

Складність налаштування та управління може бути значною, оскільки вимагає інтеграції різних технологій і протоколів.

2.3.2 Вибір протоколів та технологій

Вибір протоколів та технологій для реалізації VPN є ключовим аспектом захисту інформаційно-телекомунікаційних систем від несанкціонованого доступу. При ухваленні рішення щодо відповідних протоколів слід враховувати такі критерії, як безпека, продуктивність та сумісність.

Протоколи повинні забезпечувати надійний захист даних, включаючи шифрування та аутентифікацію, щоб запобігти несанкціонованому доступу. Важливо вибирати протоколи, які забезпечують стійкість до відомих атак та відповідають сучасним стандартам безпеки.

Обрані протоколи не повинні значно впливати на швидкість передачі даних. Продуктивність VPN може варіюватися в залежності від складності шифрування і типу протоколу.

Протоколи повинні бути сумісними з існуючою інфраструктурою мережі та різноманітними операційними системами, що використовуються в організації [17].

Порівняння популярних протоколів.

IPsec (Internet Protocol Security) є одним з найбільш використовуваних протоколів для забезпечення безпеки VPN-з'єднань. Він підтримує режим тунелювання та режим транспорту, що дозволяє шифрувати окремі пакети. IPsec забезпечує високу безпеку завдяки використанню сильних алгоритмів аутентифікації та шифрування. Проте, він може вимагати складної конфігурації та значних ресурсів.

OpenVPN є одним з найбільш гнучких і безпечних варіантів для VPN. Цей протокол підтримує різні методи шифрування, включаючи SSL/TLS, що робить його стійким до багатьох типів атак. Він є відкритим і може бути налаштований на

різних платформах, однак може вимагати значних обчислювальних ресурсів, що може вплинути на продуктивність.

L2TP (Layer 2 Tunneling Protocol) часто використовується в поєднанні з IPsec для забезпечення безпеки. L2TP сам по собі не забезпечує шифрування, але у поєднанні з IPsec стає надійним рішенням [15]. Цей протокол простий у налаштуванні та добре підтримується багатьма операційними системами. Однак, його ефективність може бути нижчою у порівнянні з іншими протоколами через подвійне тунелювання .

2.3.3 Інтеграція з існуючими системами

Інтеграція VPN з існуючими інформаційними системами є важливим аспектом забезпечення захисту даних і безперебійності роботи мережі. Цей процес може бути складним через необхідність врахування різних факторів, таких як сумісність, масштабованість і безпека.

Одним з основних викликів є забезпечення сумісності VPN з існуючими мережевими протоколами та інфраструктурою. Це може вимагати адаптації конфігурацій та налаштувань, щоб забезпечити коректну роботу всіх компонентів системи [5].

Інтеграція VPN повинна враховувати можливість легкого збільшення чи зменшення обсягу мережевих ресурсів у відповідь на зміну потреб організації. Масштабованість є критично важливою для організацій, що планують розширення або скорочення своєї діяльності.

Забезпечення додаткового рівня безпеки при інтеграції з існуючими системами є необхідністю. Це включає в себе управління доступом, шифрування даних та захист від можливих вразливостей, які можуть бути використані зловмисниками.

Оцінка системних вимог: Перед початком інтеграції важливо провести детальний аналіз існуючої інфраструктури, щоб визначити специфічні вимоги та можливі проблеми, які можуть виникнути в процесі інтеграції.

Використання стандартизованих протоколів: Обрання широко підтримуваних і стандартизованих протоколів, таких як IPsec або OpenVPN, полегшує інтеграцію завдяки їх сумісності з багатьма мережевими пристроями і операційними системами.

Впровадження процесу тестування на всіх етапах інтеграції допомагає виявити та усунути можливі проблеми на ранньому етапі. Постійний моніторинг після впровадження також є важливим для забезпечення стабільності та безпеки.

Регулярні оновлення та підтримка: Забезпечення актуальності системи через регулярні оновлення програмного забезпечення та патчі допомагає зберігати високий рівень безпеки і продуктивності [20].

2.3.4 Підходи до налаштування режимів передачі даних (TCP та UDP) в OpenVPN

Протоколи TCP і UDP мають суттєвий вплив на стабільність, швидкість і енергоефективність з'єднання в OpenVPN.

TCP

Переваги:

- Забезпечує стабільне з'єднання навіть в умовах мереж із затримками та втратою пакетів.
- Гарантує доставку даних завдяки механізму підтвердження.

Недоліки:

- Низька швидкість передачі через часті підтвердження.
- Підвищене споживання енергії, що є проблемою для мобільних пристроїв.

UDP.

Переваги:

- Вища швидкість передачі даних завдяки відсутності підтвердження.

– Менше навантаження на ресурси пристроїв, що робить його зручнішим для мобільного використання.

Недоліки:

– Часті втрати пакетів через відсутність гарантії доставки.
– Нестабільність у мережах із високим рівнем перешкод.

Рекомендації

– Використовувати UDP для високошвидкісних програм реального часу (стрімінг, відеодзвінки).
– Обрати TCP, якщо важлива надійність у нестабільних мережах.
– Враховувати специфіку мобільного користування, балансучи між швидкістю та стабільністю.

Гнучкі налаштування OpenVPN дозволяють легко змінювати протоколи, забезпечуючи адаптацію під конкретні умови роботи[19].

2.4 Вибір засобів та технологій реалізації VPN

2.4.1 Огляд доступних VPN-рішень

В сучасному світі захист інформаційно-телекомунікаційних систем від несанкціонованого доступу є пріоритетом для багатьох організацій. VPN (віртуальні приватні мережі) пропонують ефективні рішення для забезпечення безпеки даних. Розглянемо декілька популярних VPN-рішень, їхні особливості, переваги та обмеження.

IPsec є одним з найпоширеніших рішень для захисту даних на рівні мережевого протоколу. Він забезпечує шифрування і аутентифікацію даних, що передаються, підтримуючи високу безпеку з'єднань. Серед переваг IPsec є його сумісність з багатьма мережевими пристроями і операційними системами. Однак, складність налаштування може бути значним обмеженням для організацій з обмеженими ресурсами IT [6].

OpenVPN є відкритим протоколом, відомим своєю гнучкістю і надійністю. Він використовує SSL/TLS для захисту з'єднань, що забезпечує стійкість до багатьох типів атак. OpenVPN підтримує безліч конфігурацій та сумісний з різними платформами, що робить його універсальним рішенням для багатьох організацій. Проте, його використання може вимагати значних обчислювальних ресурсів, що може вплинути на продуктивність.

Комерційні VPN-сервіси, такі як NordVPN, ExpressVPN, і CyberGhost, пропонують прості у використанні рішення для захисту даних користувачів. Ці сервіси часто забезпечують високий рівень шифрування, а також додаткові функції, такі як блокування реклами і захист від витоків DNS [14]. Основними перевагами цих рішень є легкість в налаштуванні та використанні. Водночас, їхньою найбільшою вадою може стати залежність від сторонніх провайдерів, що може викликати занепокоєння щодо конфіденційності даних.

2.4.2 Порівняння комерційних та відкритих рішень

У сучасному світі організації стикаються з вибором між комерційними та відкритими рішеннями для впровадження VPN. Обидва типи мають свої переваги та недоліки, які слід враховувати при ухваленні рішення.

Комерційні VPN-рішення, такі як NordVPN та ExpressVPN, зазвичай пропонують користувачам готові продукти з високим рівнем підтримки та додатковими функціями.

Комерційні рішення, як правило, вимагають регулярних підписок або ліцензійних платежів, що може стати значним фінансовим навантаженням для організації [9]. Однак ці витрати можуть бути виправданими завдяки широкому спектру функцій і підтримці.

Ці рішення часто забезпечують високий рівень шифрування і безпеки даних, хоча користувачі повинні довіряти постачальнику щодо обробки їхніх даних.

Комерційні VPN-рішення зазвичай прості в установці та використанні, що знижує потребу в глибоких технічних знаннях серед користувачів. Проте, вони можуть бути менш гнучкими в налаштуванні під специфічні потреби організації

Відкриті рішення, такі як OpenVPN, надають більшу свободу в налаштуванні і можуть бути адаптовані під специфічні вимоги організації.

Однією з головних переваг відкритих рішень є їх безкоштовність, хоча організаціям може знадобитися інвестувати в технічну підтримку та налаштування.

Відкриті рішення дозволяють користувачам перевіряти та модифікувати код, що може підвищити довіру до безпеки системи. Проте, це також вимагає наявності висококваліфікованих IT-фахівців для налаштування і підтримки.

OpenVPN та інші відкриті рішення пропонують високу гнучкість в налаштуванні, що дозволяє підлаштовувати їх під специфічні бізнес-процеси [11]. Це може бути великим плюсом для організацій з унікальними вимогами.

2.4.3 Вибір апаратних та програмних засобів

Вибір відповідних апаратних та програмних засобів є критично важливим етапом у впровадженні VPN для захисту інформаційно-телекомунікаційних систем від несанкціонованого доступу. Врахування аспектів продуктивності, безпеки та витрат допомагає оптимізувати рішення для специфічних потреб організації.

Спеціалізовані VPN-апарати призначені для обробки VPN-трафіку і зазвичай пропонують високу продуктивність та безпеку. Вони можуть обробляти великі обсяги даних з низькою затримкою, що є важливою перевагою для великих підприємств. Однак, такі рішення можуть бути дорогими та вимагати фахової підтримки.

Використання загального серверного обладнання для VPN дозволяє знизити витрати і забезпечити більшу гнучкість у налаштуванні [7]. Проте, це може призвести до зниження продуктивності при високих навантаженнях або обмежити можливості безпеки без відповідного програмного забезпечення.

OpenVPN є яскравим прикладом програмного забезпечення з відкритим кодом, яке забезпечує високий рівень налаштування і безпеки. Використання таких рішень дозволяє організаціям контролювати і модифікувати код, що підвищує довіру до безпеки, але може вимагати значних технічних ресурсів.

Комерційні програмні рішення зазвичай забезпечують велику підтримку і простоту в налаштуванні. Вони можуть бути привабливими для організацій з обмеженими технічними ресурсами, проте часто вимагають постійних ліцензійних витрат.

Вибір апаратних та програмних засобів має забезпечити високу швидкість та надійність VPN-з'єднань, особливо для великих підприємств або мереж з важливими даними [16].

Рішення повинні відповідати сучасним стандартам безпеки, забезпечуючи шифрування та захист від несанкціонованого доступу. Важливо враховувати можливості адаптації до нових загроз .

Врахування початкових витрат на придбання, а також довгострокових витрат на підтримку та обслуговування є важливим для оптимізації бюджету.

2.4.4 Оцінка продуктивності та впливу різних алгоритмів шифрування в OpenVPN

Алгоритми шифрування відіграють ключову роль у забезпеченні безпеки VPN-з’єднань, при цьому суттєво впливаючи на швидкість роботи та використання системних ресурсів.

AES-256 забезпечує максимальний рівень безпеки завдяки великій довжині ключа, що робить його практично незламним. Однак його використання може знижувати швидкість передачі даних і збільшувати споживання енергії, що менш зручно для мобільних пристроїв або систем із обмеженими ресурсами.

AES-128 пропонує компроміс між швидкістю, енергоефективністю та безпекою. Цей алгоритм забезпечує вищу пропускну здатність і менше

навантаження на систему, зберігаючи при цьому доволі високий рівень стійкості до атак, чого достатньо для більшості сценаріїв[18].

Рекомендації.

Використовувати AES-256 для захисту критичних даних, де безпека є пріоритетом.

Вибирати AES-128 для користувачів із потребами в швидкодії, особливо на мобільних пристроях або в умовах обмежених ресурсів.

Ці опції дозволяють адаптувати OpenVPN до різних умов і завдань, забезпечуючи баланс між продуктивністю та безпекою.

РОЗДІЛ 3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ OPEN VPN

3.1 Алгоритм налаштування параметрів OpenVPN

OpenVPN є ключовим інструментом захисту в сучасних мережах, забезпечуючи конфіденційність і цілісність даних через передові технології шифрування та сертифіковану аутентифікацію. Ця технологія забезпечує високий рівень захисту від кібератак, таких як "людина посередині", що робить її незамінною для корпоративних мереж і віддаленого доступу. Дотримання сучасних практик, включаючи налаштування брандмауера, шифрування та мережевий форвардинг, є важливими для створення безпечного й стабільного VPN-з'єднання[16].

Етапи налаштування і встановлення з'єднання OpenVPN:

Встановлення OpenVPN та Easy-RSA є основним кроком для забезпечення захищеного VPN-з'єднання. Для початку необхідно оновити список пакетів командою `sudo apt-get update` .

Це гарантує завантаження останніх оновлень та виправлень безпеки. Далі потрібно встановити OpenVPN та Easy-RSA для створення VPN-з'єднання та генерації сертифікатів `sudo apt-get install openvpn easy-rsa` .

OpenVPN забезпечує платформу для з'єднань, а Easy-RSA дозволяє створювати центр сертифікації для захисту даних[16]. Правильна установка цих двох утиліт формує основу для подальшого налаштування безпечної та стабільної

Центр сертифікації (CA) забезпечує довіру між сервером і клієнтами, генеруючи сертифікати та ключі для захисту даних. Для створення директорії виконуються наступні команди:

```
mkdir -p ~/easy-rsa
cp -r /usr/share/easy-rsa/
~/easy-rsa/ cd ~/easy-rsa
```

Ці команди створюють структуру файлів Easy-RSA у вашій домашній директорії, включаючи налаштування та скрипти для роботи з сертифікатами [14]. Створення власного CA дозволяє контролювати процес сертифікації, що підвищує безпеку та незалежність VPN-з'єднання.

Налаштування змінних центру сертифікації

Налаштування змінних для центру сертифікації (CA) є важливим кроком, який забезпечує персоналізацію сертифікатів і підвищує їх безпеку. Цей процес визначає унікальні параметри сертифікатів, що відповідають конкретній організації. Для виконання цього завдання необхідно відредагувати файл vars, використовуючи текстовий редактор `nano vars` .

В цьому файлі зазначаються ключові змінні, які характеризують організацію. Змінивши стандартні значення на власні, створюються сертифікати, які несуть унікальну інформацію про вашу організацію.

```
set_var EASYRSA_REQ_COUNTRY "UA"
set_var EASYRSA_REQ_PROVINCE "Kyiv"
set_var EASYRSA_REQ_CITY "Kyiv"
set_var EASYRSA_REQ_ORG "YourOrganization"
set_var EASYRSA_REQ_EMAIL "admin@example.com"
set_var EASYRSA_REQ_OU "YourUnit"
```

Ці змінні включають назву країни, регіону, міста, а також назву організації, підрозділу та адресу електронної пошти. Встановлення цих значень гарантує, що сертифікати є персоналізованими для вашої конкретної інфраструктури [10].

Персоналізація сертифікатів забезпечує кілька важливих переваг. По-перше, це створює унікальні криптографічні ключі, що значно ускладнює їх підробку. По-друге, сертифікати, які містять інформацію про організацію, підвищують довіру до мережі серед клієнтів чи партнерів, які підключаються до VPN .

Значимість цього етапу полягає також у тому, що коректно налаштовані змінні гарантують автентичність всіх підключень. Наприклад, якщо клієнт отримує сертифікат з неправильними або фальшивими параметрами, сервер має змогу

відхилити це підключення, оскільки воно не підтверджується активованим центром сертифікації. Це забезпечує більш високий рівень контролю доступу до мережі.

Встановлення грамотних і достовірних параметрів сертифікації є основоположною практикою інформаційної безпеки. Це створює міцну базу для роботи OpenVPN, забезпечуючи максимальний рівень автентичності й захисту даних.

Таким чином, цей етап є не лише технічною вимогою, але й практикою забезпечення довіри та високого рівня безпеки для всіх майбутніх VPN-з'єднань.

Центр сертифікації (CA) є основним компонентом у структурі безпеки OpenVPN, оскільки він виконує функцію авторизації та зберігання сертифікатів, які забезпечують захищене з'єднання між сервером і клієнтами. Для ініціалізації PKI (Public Key Infrastructure) та створення CA виконуються наступні команди:

```
./easyrsa init-pki
./easyrsa build-ca
```

Перша команда init-pki створює інфраструктуру публічних ключів (PKI), яка буде використовуватися для зберігання всіх генерованих сертифікатів і ключів. Це крок є критично важливим для забезпечення централізованого управління безпекою даних.

Друга команда `build-ca` генерує приватний ключ і записує інформацію сертифікату для центру сертифікації. Програма попросить вас ввести пароль для захисту приватного ключа CA. Це запобіжний захід, що захищає ключ CA від несанкціонованого доступу та зменшує ризик компрометації.

Крім того, створення власного CA дозволяє адміністратору контролювати кожен етап сертифікації, включаючи налаштування терміну дії сертифікатів, що унеможливлює довготривале використання застарілих або скомпрометованих сертифікатів. CA також забезпечує створення сертифікатів для серверів і клієнтів, які використовують стандарти безпечного шифрування для захисту передаваних даних в OpenVPN [14].

Успішне виконання команди `./easyrsa build-ca` відображає інформацію про створення сертифікату разом із підтвердженням збереження приватного ключа. Запропоноване зображення процесу може виглядати так (див. рисунок 3.1).

Рисунок 3.1. Успішне створення сертифікату центру сертифікації (CA)

Примітка: Це місце зарезервоване для зображення вашого виводу терміналу після виконання цієї команди.

Цей етап гарантує, що всі майбутні сертифікати, видані вашим CA, будуть надійними та підвищать захищеність мережі відповідно до сучасних стандартів.

Таким чином, створення центру сертифікації (CA) є фундаментальною частиною налаштування VPN, яка забезпечує контроль доступу до інфраструктури та сильне шифрування даних [18].

Створення сертифіката, ключа і файлів шифрування для сервера

На цьому етапі налаштування OpenVPN створюються необхідні серверні ключі та сертифікати, які є основними елементами для забезпечення безпечного з’єднання. Виконання цих дій гарантує, що сервер буде використовувати надійні криптографічні механізми.

Спочатку потрібно згенерувати запит на створення сертифіката сервера

```
./easyrsa gen-req server nopass.
```

Ця команда генерує приватний ключ сервера та файл запиту на підпис сертифіката (CSR). Використання прапора `nopass` означає, що приватний ключ не буде захищений паролем, що полегшує автоматизацію процесу. Однак це може бути менш безпечно для деяких середовищ .

Для підписання запиту та створення сертифіката для сервера використовується наступна команда `/easyrsa sign-req server server.`

На цьому етапі CA (центр сертифікації) перевіряє та підписує запит. Результатом є повноцінний сертифікат сервера, який дозволяє OpenVPN ідентифікувати сервер як авторизовану сторону.

OpenVPN використовує параметри Діффі-Геллмана для встановлення спільного секрету між сторонами. Генерація цих параметрів здійснюється так

```
./easyrsa gen-dh.
```

Параметри Діффі-Геллмана додають додатковий рівень захисту процесу обміну ключами, зменшуючи ризик компрометації з'єднання, [13]. Це особливо важливо для забезпечення надійності шифрування, оскільки вони забезпечують ідеальну пряму секретність.

Для ще більшого посилення безпеки OpenVPN рекомендується згенерувати HMAC-ключ

```
openvpn --genkey --secret ta.key.
```

Цей ключ використовується для TLS-аутентифікації, що запобігає DoS-атакам і небажаним з'єднанням, які можуть бути націлені на сервер. HMAC-ключ забезпечує, що сервер і клієнт можуть перевіряти автентичність трафіку, дозволяючи лише авторизованим з'єднанням.

Для коректної роботи OpenVPN необхідно перемістити всі згенеровані файли

```
в конфігураційну директорію
sudo cp pki/ca.crt pki/issued/server.crt pki/private/server.key
pki/dh.pem ta.key /etc/openvpn/.
```

Дані файли включають:

- `ca.crt` — сертифікат центру сертифікації.
- `server.crt` — сертифікат сервера.
- `server.key` — приватний ключ сервера.
- `dh.pem` — параметри Діффі-Геллмана.
- `ta.key` — HMAC-ключ.

Цей крок гарантує, що серверна конфігурація матиме доступ до всіх необхідних файлів для налаштування захищеного з’єднання.

Виконання команди для створення приватного ключа та запиту на підпис сертифіката (CSR): `./easyrsa gen-req client1 nopass.`
Ключ без пароля (`nopass`) забезпечує простішу автоматизацію.
Підписання запиту сертифікатом центру сертифікації (CA)
`./easyrsa sign-req client client1.`
Це підтверджує автентичність клієнта, дозволяючи захищений доступ [14].

Для підготовки клієнта необхідно перенести файли, такі як client1.crt, client1.key, `ta.key` та `ca.crt`, до каталогу `client-configs`
`cp pki/issued/client1.crt pki/private/client1.key ta.key pki/ca.crt ~/client-configs/.`

Необхідні файли містять сертифікат клієнта, приватний ключ, HMAC-ключ для TLS-аутентифікації та сертифікат CA.

Сертифікати забезпечують автентифікацію, шифрування та захист клієнтських з’єднань з сервером OpenVPN [7].

Налаштування сервісу OpenVPN є важливим етапом для забезпечення стабільного з'єднання та високого рівня безпеки. Після створення сертифікатів і ключів необхідно налаштувати конфігураційний файл для сервера OpenVPN(див. рисунок 3.2).

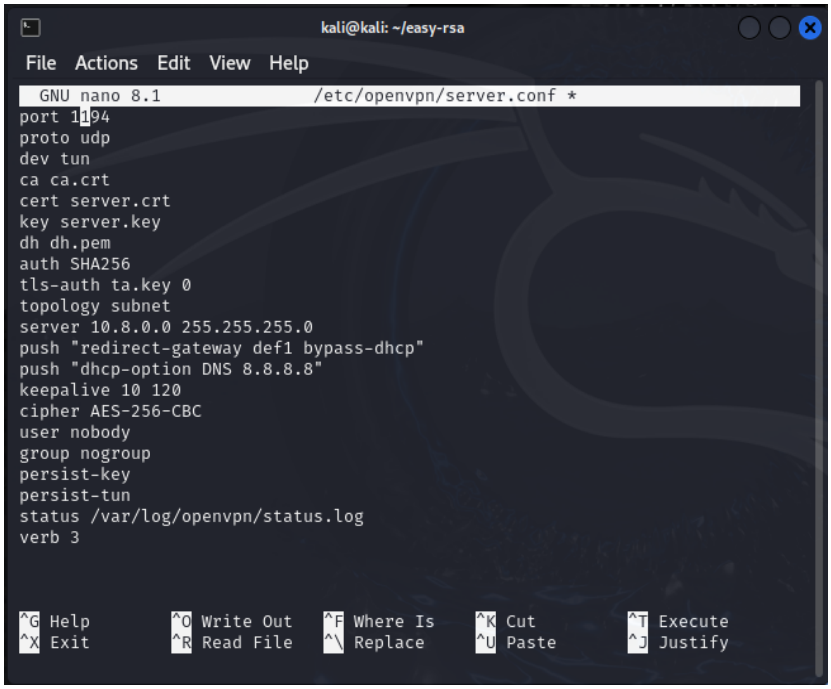

Рисунок 3.2. Конфігураційний файл сервера OpenVPN

У конфігураційному файлі задаються наступні параметри.

Параметр `port 1194` — відкриває порт для прослуховування сервером OpenVPN. Використання стандартного порту 1194 полегшує сумісність із клієнтами.

Параметр `proto udp` — вибір UDP як протоколу транспортування. Це знижує затримки порівняно із TCP, але, за необхідності, можна переключитися на TCP для збільшення стабільності.

Параметри `dev tun` — налаштовують сервер для використання тунельного інтерфейсу (TUN), що створює віртуальний IP-тунель між клієнтом і сервером.

Параметри `ca, cert, key, dh` — прив’язка сертифікатів і ключів до відповідних файлів, створених на етапі сертифікації. Ці компоненти забезпечують аутентифікацію та шифрування даних [12].

Параметр `auth SHA256` — механізм аутентифікації забезпечує захист трафіку за допомогою хешування за алгоритмом SHA-256.

Параметри `tls-auth` та `ta.key 0` — використовують HMAC-ключ для додаткового рівня захисту від DoS-атак і запобігання спуфінгу .

Параметр `cipher AES-256-CBC` — алгоритм шифрування AES-256-CBC гарантує високий рівень захисту переданих даних.

Параметр `server 10.8.0.0 255.255.255.0` — задає IP-адресу та маску підмережі, яку використовуватимуть клієнти VPN.

Параметри `push "redirect-gateway, def1 bypass-dhcp"` — перенаправляють весь трафік користувачів через VPN для захисту їхніх даних у незахищених мережах.

Параметр push "dhcp-option `DNS 8.8.8.8`" — встановлює DNS-сервер (наприклад, Google DNS), які будуть використовувати клієнти для безпечного доступу до Інтернету.

Параметри `persist-key` та `persist-tun` — забезпечують збереження ключів і тунелю після перезапуску OpenVPN, що мінімізує час простою.

Параметр verb 3 — задає рівень ведення журналів для діагностики роботи сервера.

Ці дії дозволяють серверу OpenVPN забезпечувати стабільне з'єднання з високим рівнем безпеки.

Налаштування мережевої конфігурації сервера

Після створення конфігураційного файлу необхідно налаштувати мережеве середовище для маршрутизації трафіку через VPN.

IP-форвардинг потрібен для передачі даних між клієнтами VPN і зовнішніми мережами. Його включення здійснюється за допомогою редагування файлу `sudo nano /etc/sysctl.conf`.

Потрібно додати або змінити рядок `net.ipv4.ip_forward = 1`.

Для застосування змін, виконується команда `sudo sysctl -p`.

Цей етап дозволяє передавати дані через маршрути VPN, забезпечуючи зв'язок між клієнтами та сервером [11].

Для належної роботи VPN потрібно розширити правила брандмауера. Це налаштовується командою

`sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE.`

Це правило дозволяє NAT (трансляція мережевих адрес) для вихідного трафіку з підмережі VPN на зовнішній інтерфейс eth0. Для збереження змін, використовується `sudo iptables-save > /etc/iptables/rules.v4.`

Цей крок гарантує, що трафік VPN може проходити через сервер і досягати зовнішніх мереж, залишаючи безпечним з'єднання між клієнтом і сервером.

Включення сервісу OpenVPN — це ключовий етап, який дозволяє серверу приймати підключення від клієнтів. Правильне налаштування та запуск сервісу гарантують стабільність його роботи та безпеку з’єднань.

Для запуску OpenVPN, виконується команда

`sudo systemctl start openvpn@server.`

Ця команда активує службу OpenVPN із зазначеним файлом конфігурації (server.conf). Після її виконання сервер буде готовий до обробки запитів на підключення клієнтів. Відсутність помилок під час запуску вказує на правильно сформовану конфігурацію.

Щоб автоматизувати запуск OpenVPN після перезавантаження системи, використовується `sudo systemctl enable openvpn@server.`

Це налаштування гарантує, що сервер завжди буде готовим обслуговувати клієнтів, навіть після випадкових збоїв або перезавантажень. Використання автоматичного запуску є найкращою практикою для забезпечення доступності VPN Перевірити поточний стан сервісу можна за допомогою sudo systemctl status openvpn@server.

У результаті виконується моніторинг роботи OpenVPN, включаючи можливі помилки або збої. Ця інформація допомагає швидко реагувати та усувати проблеми. Регулярний контроль стану сервісу забезпечує стабільність роботи VPN, зменшуючи ризик перебоїв(див. рисунок 3.3).

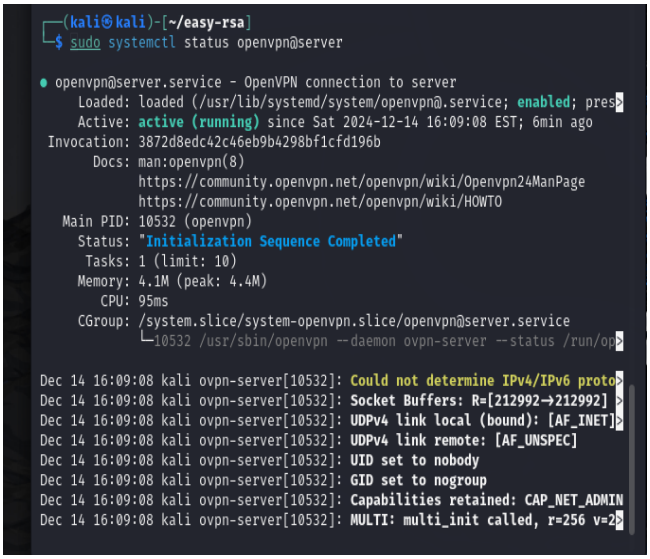

Рисунок 3.3. Статус роботи OpenVPN-сервісу

Активуючи OpenVPN та перевіряючи його стан, адміністратори отримують наступні переваги:

– Забезпечення постійної готовності серверу до роботи.
– Виявлення можливих помилок у конфігурації або підключенні.
– Відсутність необхідності вручну запускати сервер після кожного вимкнення або оновлення системи.
– Підвищення загальної стабільності та надійності послуг [13], [16].

Налаштування конфігураційного файлу для клієнта дозволяє створити необхідні умови для встановлення захищеного з'єднання з сервером. Виконання цього етапу гарантує, що клієнт отримає доступ до VPN із необхідними рівнями шифрування та аутентифікації.

Для кожного користувача створюється спеціалізований конфігураційний файл, наприклад client1.ovpn. Використовується наступна команда для його створення `nano ~/client-configs/client1.ovpn .`

Використання цієї команди відкриває текстовий редактор, де можна заповнити файл необхідною інформацією для клієнта (див. рисунок 3.4).

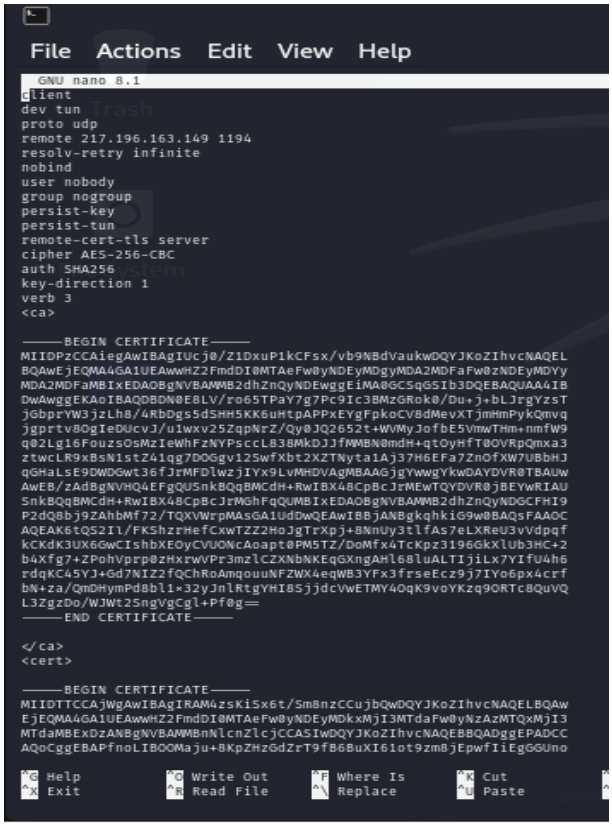

Рисунок 3.4. Файл конфігурації клієнта OpenVPN

Необхідно заповнити файл client1.ovpn наступними параметрами.

Параметр `client` — вказує, що це конфігурація клієнта.

Параметр `dev tun` — визначає використання тунельного інтерфейсу, що сприяє безпечній передачі даних.

Параметр `proto udp` — встановлює протокол UDP, який мінімізує затримки. При необхідності стабільності можна використати TCP.

Параметр `remote YOUR_SERVER_IP 1194` — вказує IP-адресу сервера OpenVPN і порт для підключення. Замініть YOUR_SERVER_IP на фактичну IP-адресу сервера.

Параметр `cipher AES-256-CBC` — забезпечує надійне шифрування переданих даних за допомогою алгоритму AES-256 [14].

Ці налаштування гарантують, що клієнт буде відповідати стандартам безпеки серверу і підтримуватиме високопродуктивний зв'язок.

Після створення основних налаштувань, у файл вставляються сертифікати клієнта, ключі та CA. Це забезпечує справжність клієнта й підтвердження справжності сервера під час підключення.

Ці сертифікати забезпечують довіру між клієнтом і сервером .

Після створення конфігураційного файлу, передаємо його клієнту. Це можна зробити за допомогою захищених методів передачі, таких як SCP або USB-накопичувач.

Для встановлення підключення здійнюється виконання команди на пристрої клієнта `sudo openvpn --config client1.ovpn`.

Ця команда запускає VPN-клієнт із використанням створеного конфігураційного файлу. Успішне підключення підтверджує правильність усіх зроблених налаштувань (див. рисунок 3.5).

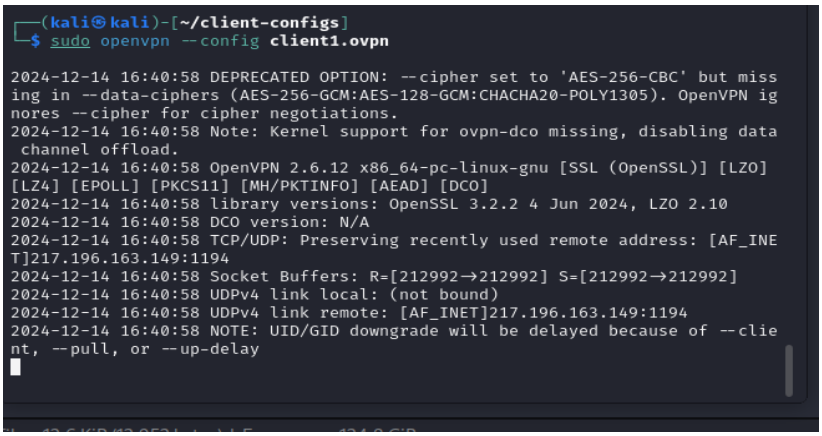

Рисунок 3.5. Команда запуску VPN-з’єднання

Завдяки використанню унікальних сертифікатів і ключів для кожного клієнта гарантується конфіденційність і захист від несанкціонованих підключень.

Організація конфігураційного файлу спрощує процес налаштування та підключення клієнтів.

Налаштування з використанням протоколу UDP і шифрування AES-256 гарантує високу швидкість з'єднання при збереженні високого рівня безпеки [17].

Налаштування клієнтського конфігураційного файлу на Windows 10 (див. рисунок 3.6) .

Рисунок 3.6. Процес налаштування конфігурації на Windows 10

Підключення клієнта до VPN-сервера (див. рисунок 3.7) .

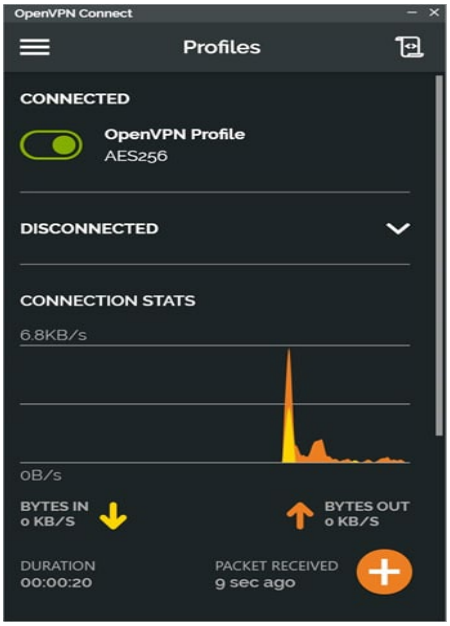

Рисунок 3.7 Процес підключення до VPN-сервера

3.2 Аналіз впливу шифрування на канал зв’язку у технології OpenVPN

Для оцінки впливу шифрування на пропускну здатність каналу зв’язку провели аналіз у віртуальному середовищі VirtualBox (див. рисунок 3.8).

У мережі 216.196.153.1/24 між віртуальною машиною на Ubuntu (VPN-сервер) та хост-машиною на Windows 10 (VPN-клієнт) було налаштовано з’єднання. Для тестування використано Iperf 3.1.3 як генератор трафіку. На одній машині Iperf працював у режимі передачі даних (клієнт), а на іншій — у режимі прийому (сервер).

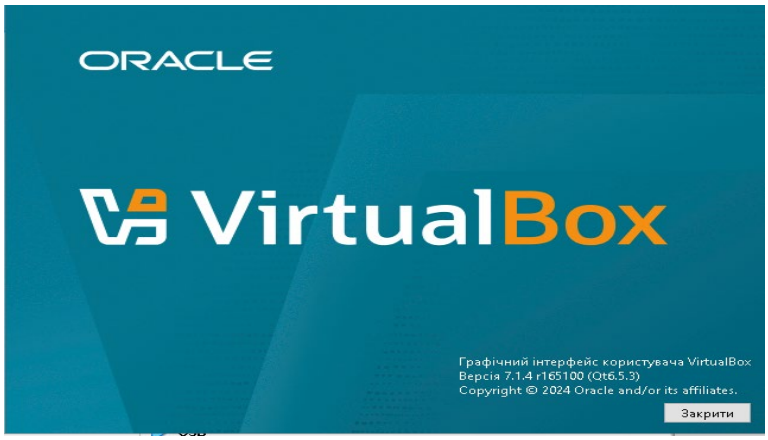

Рисунок 3.8. Середовище VirtualBox

Використання такого середовища дозволило точно оцінити показники пропускної здатності каналу при різних алгоритмах шифрування, враховуючи криптографічні накладні [14]

Перевірка каналу VM Network без VPN (див. рисунок 3.9).

```
C:\iperf-3.1.3-win64>iperf3.exe -c 217.196.163.149
Connecting to host 217.196.163.149, port 1194
[  4] local 217.196.163.179 port 53744 connected to 217.196.163.149 port 1194
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec   520 MBytes  4.37 Gbits/sec
[  4]   1.00-2.00   sec   538 MBytes  4.52 Gbits/sec
[  4]   2.00-3.00   sec   538 MBytes  4.51 Gbits/sec
[  4]   3.00-4.00   sec   500 MBytes  4.19 Gbits/sec
[  4]   4.00-5.00   sec   526 MBytes  4.42 Gbits/sec
[  4]   5.00-6.00   sec   514 MBytes  4.31 Gbits/sec
[  4]   6.00-7.00   sec   521 MBytes  4.37 Gbits/sec
[  4]   7.00-8.00   sec   533 MBytes  4.47 Gbits/sec
[  4]   8.00-9.00   sec   511 MBytes  4.29 Gbits/sec
[  4]   9.00-10.00  sec   524 MBytes  4.40 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  5.10 GBytes  4.38 Gbits/sec                  sender
[  4]   0.00-10.00  sec  5.10 GBytes  4.38 Gbits/sec                  receiver

iperf Done.

C:\iperf-3.1.3-win64>
```

Рисунок 3.9 Пропускна здатність без VPN

Перевірка VPN-тунелю без шифрування (див. рисунок 3.10).

```
C:\iperf-3.1.3-win64>
C:\iperf-3.1.3-win64>iperf3.exe -c 10.0.2.15
Connecting to host 10.0.2.15, port 1194
[  4] local 10.0.2.24 port 53769 connected to 10.0.2.15 port 1194
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  19.4 MBytes   162 Mbits/sec
[  4]   1.00-2.00   sec  28.1 MBytes   236 Mbits/sec
[  4]   2.00-3.00   sec  28.8 MBytes   241 Mbits/sec
[  4]   3.00-4.00   sec  29.0 MBytes   243 Mbits/sec
[  4]   4.00-5.00   sec  28.1 MBytes   236 Mbits/sec
[  4]   5.00-6.00   sec  29.1 MBytes   244 Mbits/sec
[  4]   6.00-7.00   sec  28.6 MBytes   240 Mbits/sec
[  4]   7.00-8.00   sec  27.8 MBytes   233 Mbits/sec
[  4]   8.00-9.00   sec  28.5 MBytes   239 Mbits/sec
[  4]   9.00-10.00  sec  28.4 MBytes   238 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec   276 MBytes   231 Mbits/sec
 sender
[  4]   0.00-10.00  sec   276 MBytes   231 Mbits/sec
 receiver
```

Рисунок 3.10 Пропускна здатність VPN без шифрування

Перевірка VPN-тунелю з шифруванням DES-EDE (див. рисунок 3.11).

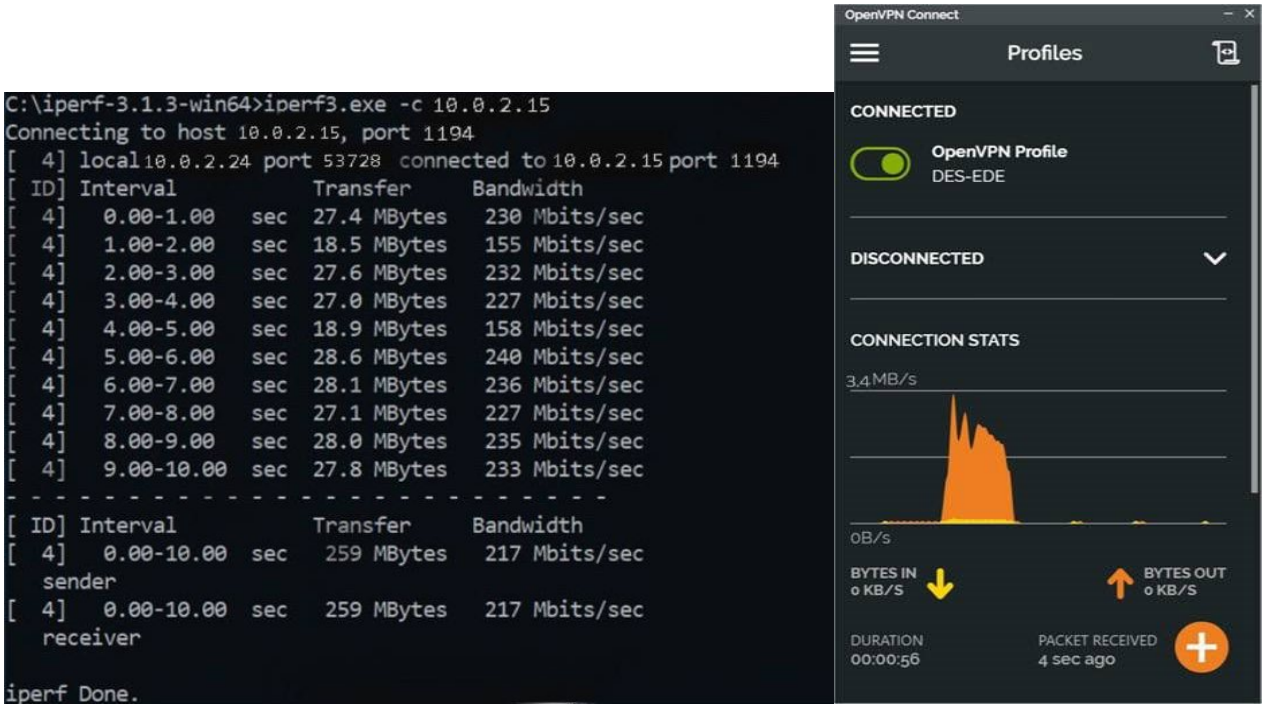

Рисунок 3.11 Пропускна здатність VPN з DES-EDE

Перевірка VPN-тунелю з шифруванням BF-CBC (див. рисунок 3.12).

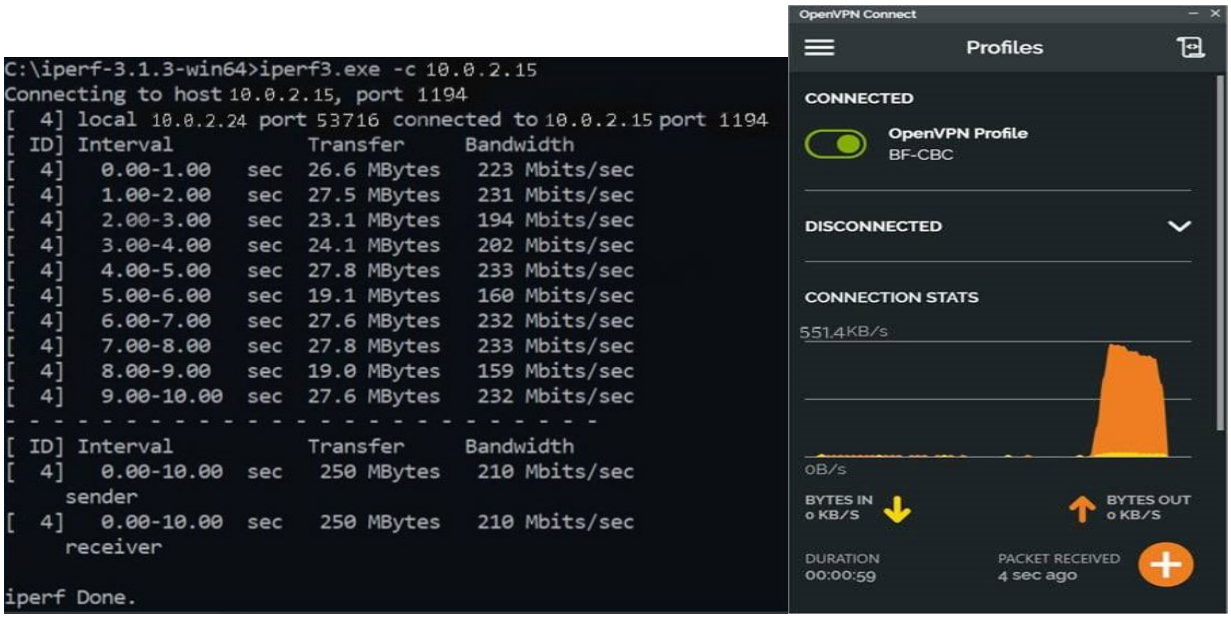

Рисунок 3.12 Пропускна здатність VPN з BF-CBC

Перевірка VPN-тунелю з шифруванням AES-256 (див. рисунок 3.13).

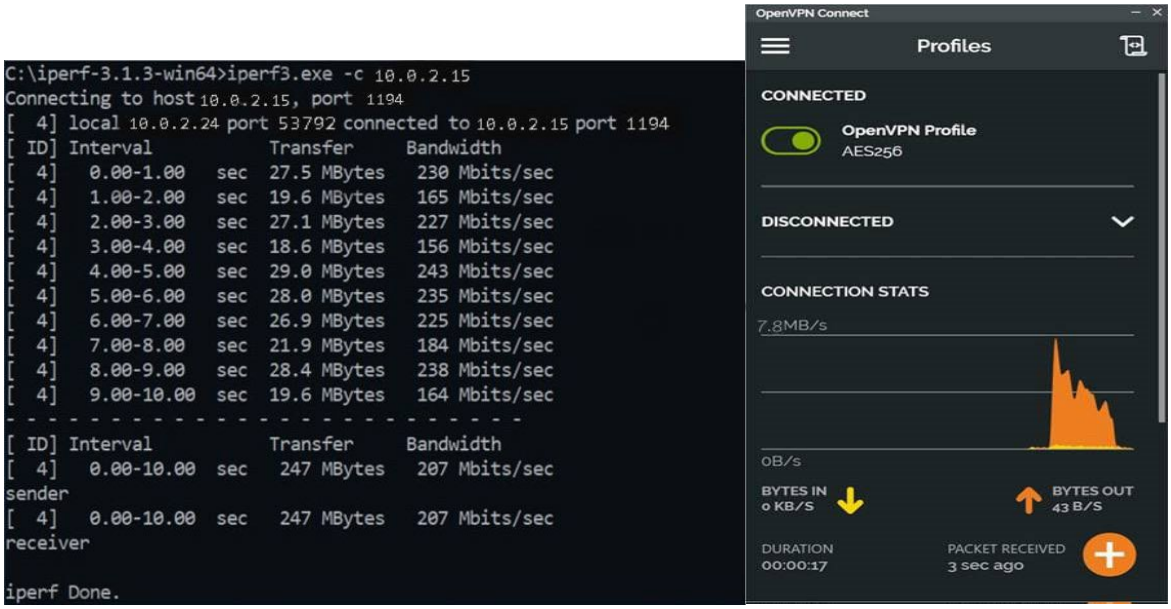

Рисунок 3.13 Пропускна здатність VPN з AES-256

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Виконуючи магістерську кваліфікаційну роботу, було забезпечено дотримання необхідних стандартів для приміщень, де застосовуються візуальні дисплейні термінали (ВДТ) та персональні електронні обчислювальні машини (ПЕОМ). Також було виконано вимоги щодо санітарних норм і умов праці, включаючи такі показники як мікроклімат, освітлення, рівень шуму та організація робочих зон.

1. Вимоги до приміщень для роботи з ВДТ, ЕОМ та ПЕОМ

1) Площа на одне робоче місце — не менше 6,0 м², об’єм — мінімум 20,0 м³ (ДБН В.2.2-9:2018, ДСТУ Б В.2.2-28:2010).

2). Приміщення для роботи з ВДТ повинні бути обладнані природним і штучним освітленням, відповідно до вимог ДБН В.2.5-28:2018, що забезпечує зручність роботи та знижує зорове навантаження.

3). Природне освітлення повинно забезпечуватись через світлові прорізи, орієнтовані переважно на північ чи північний схід, що сприяє рівномірному розподілу світла протягом дня. КПО має бути не нижче 1,5%, згідно з методикою, визначеною у ДБН В.2.5-28:2018, для захисту зору та зниження навантаження.

4). Звукоізоляція огороджувальних конструкцій приміщень з ВДТ повинна відповідати параметрам шуму, визначеним ДСН 3.3.6.037-99, для створення комфортних умов роботи та зниження впливу шуму на персонал.

5). Приміщення з ВДТ повинні бути оснащені системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією відповідно до ДБН В.2.5-67:2013. Нормовані параметри мікроклімату, включаючи температуру, вологість, іонний склад повітря та рівень шкідливих речовин, мають строго відповідати вимогам ДБН В.2.5-67:2013 «Опалення, вентиляція та

кондиціонування» та ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Це забезпечує комфортні та безпечні умови для персоналу.

6.) Віконні прорізи приміщень для роботи з ВДТ повинні бути згідно з ДБН В.2.5-28:2018 обладнані регульованими пристроями, такими як жалюзі, завіски або зовнішні козирки, що дозволяють ефективно контролювати рівень освітлення та забезпечувати комфорт працівникам.

7).У приміщеннях з ВДТ слід щоденно проводити вологе прибирання для підтримання чистоти, гігієни та створення комфортних умов праці, що сприяє зниженню рівня пилу і забезпеченню здорової робочої атмосфери бо це вимагає вимогам ДСанПіН 3.3.2.007-98.

8) Приміщення з ВДТ повинні бути оснащені аптечками першої допомоги відповідно до Наказу МОЗ України № 164 від 05.03.2003, щоб забезпечити безпеку працівників і швидке реагування у разі нещасних випадків.

9) При приміщеннях з ВДТ повинні бути обладнані побутові приміщення для відпочинку під час роботи і кімната психологічного розвантаження. У кімнаті психологічного розвантаження слід передбачити пристрої для приготування та роздачі тонізуючих напоїв, а також місця для занять фізичною культурою, відповідно до вимог ДБН В.2.2-9:2018 та ДСТУ Б В.2.2-28:2010. Це сприяє підтриманню здоров'я та ефективності працівників.

2. Гігієнічні вимоги до робочого середовища.

Мікроклімат

1) На робочих місцях з ВДТ у виробничих приміщеннях повинні забезпечуватись оптимальні параметри мікроклімату, такі як температура, відносна вологість і рухливість повітря, відповідно до вимог ДСН 3.3.6.042-99.

2) Параметри мікроклімату повинні підтримуватися в межах, що забезпечують комфортні та безпечні умови праці відповідно до ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» та з урахуванням специфіки виробничого процесу (за наявності).

Освітлення

1) Вимоги до природного освітлення наведені в пунктах 1.2 та 1.3 цих Правил.
2) Освітлення в приміщеннях з ВДТ, ЕОМ і ПЕОМ повинно бути загальним рівномірним. У приміщеннях для роботи з документами допускається комбіноване освітлення – загальне та місцеве, згідно з вимогами ДБН В.2.5-28:2018.
3) Згідно з вимогами ДБН В.2.5-28:2018 Освітленість робочого столу для документів має бути 300-500 лк. Якщо це неможливо забезпечити загальним освітленням, дозволяється використовувати місцеве освітлення, уникаючи відблисків на екрані, де освітленість не повинна перевищувати 300 лк.
4)Для штучного освітлення рекомендовано люмінесцентні лампи типу ЛБ. У приміщеннях із відбитим освітленням дозволено галогенні лампи до 250 Вт, а лампи розжарювання – лише у світильниках місцевого освітлення, відповідно до ДБН В.2.5-28:2018.
5) Система загального освітлення по вимогам ДБН В.2.5-28:2018 повинна складатися з суцільних або переривчастих ліній світильників, розташованих збоку від робочих місць, переважно зліва, паралельно лінії зору працівників.

Шум і вібрація

1) Рівні звукового тиску, рівні звуку та еквівалентні рівні звуку на робочих місцях з ВДТ, ЕОМ і ПЕОМ повинні відповідати вимогам ДСН 3.3.6.037-99.
2.) Устаткування, що створює шум (наприклад, АЦП, принтери), слід встановлювати за межами приміщень, призначених для роботи з ВДТ, ЕОМ і ПЕОМ.
3) Для досягнення допустимих рівнів шуму на робочих місцях необхідно використовувати засоби звукопоглинання, вибір яких має базуватися на спеціальних інженерно-акустичних розрахунках це згідно вимог ДСН 3.3.6.037-99.
4) Під час роботи з ВДТ, ЕОМ і ПЕОМ у виробничих приміщеннях рівні вібрації на робочих місцях мають відповідати нормам ДСН 3.3.6.039-99.

3. Гігієнічні вимоги до організації і обладнання робочих місць з ВДТ ЕОМ і ПЕОМ:

1). Обладнання та організація робочих місць із ВДТ, ЕОМ і ПЕОМ повинні відповідати ергономічним вимогам, враховуючи особливості роботи, згідно з ДСТУ EN ISO 9241-5:2019, ДСТУ ISO 6385:2018.

2) Конструкція робочого місця користувача ЕОМ і ПЕОМ із ВДТ повинна забезпечувати підтримання оптимальної робочої пози тобто мають відповідати вимогам ДСТУ EN ISO 9241-5:2019; ДСТУ ISO 6385:2018.

3) Робочі місця з ВДТ потрібно розташовувати так, щоб природнє світло надходило збоку, переважно зліва як вимагає стандарт ДСТУ EN ISO 9241-5:2019.

4) Робочі столи з ВДТ мають по стандарту ДСТУ EN ISO 9241-5:2019 розташовувати так, щоб відстань між бічними поверхнями ВДТ становила 1,2 м, а відстань від тильної поверхні одного ВДТ до екрана іншого – 2,5 м.

5) Висота робочої поверхні столу з ВДТ повинна регулюватися в межах 680-800 мм, а ширина (600-1400 мм) і глибина (800-1000 мм) мають забезпечувати виконання операцій у зоні досяжності моторного поля як вимагає ДСТУ EN ISO 9241-5:2019.

6) По вимозі ДСТУ EN ISO 9241-5:2019 робочий стіл повинен мати простір для ніг заввишки не менше 600 мм, завширшки не менше 500 мм, завглибшки на рівні колін — не менше 450 мм, на рівні простягнутої ноги — не менше 650 мм.

7) Висота поверхні сидіння повинна регулюватися в межах 400-500 мм, ширина і глибина мають бути не менше 400 мм, а кут нахилу сидіння — до 15° вперед і до 5° назад це вимагає стандарт ДСТУ EN ISO 9241-5:2019.

8) Екран ВДТ повинен розташовуватися на відстані 600-700 мм від очей користувача, але не ближче ніж 600 мм, з урахуванням розміру літеро-цифрових знаків і символів згідно з стандарту ДСТУ EN ISO 9241-5:2019.

9) Екран ВДТ ДСТУ EN ISO 9241-5:2019 має бути розташований так, щоб забезпечувати зручність зорового спостереження у вертикальній площині під кутом +30° до нормальної лінії погляду працюючого це по вимогам ДСТУ EN ISO 9241-5:2019.

4.2. Безпека в надзвичайних ситуаціях

Державна система моніторингу довкілля є важливою складовою національної інформаційної інфраструктури, яка виконує стратегічну функцію збору, обробки та обміну даними про стан довкілля. Ці дані дозволяють здійснювати моніторинг екосистем, підтримувати їхній баланс та створювати ефективні механізми для розв’язання глобальних екологічних проблем . Завдяки зосередженню на сучасних технологіях, таких як VPN, національні системи можуть відповідати суворим міжнародним стандартам безпеки. Інтеграція таких систем із міжнародними інформаційними платформами не лише підвищує рівень співпраці у сфері охорони довкілля, а й забезпечує надійний захист даних, які передаються між країнами. У цьому контексті забезпечення безпеки інформаційно-телекомунікаційних систем є одним із найбільш важливих пріоритетів, а VPN, які гарантують безпечний і конфіденційний обмін інформацією, стають ключовим рішенням для підтримки стійкості цих систем на глобальному рівні.

Системи моніторингу довкілля покликані збирати та зберігати критично важливі для екології дані, серед яких — заміри якості повітря, води, рівень токсичних викидів і зміни клімату. Ці дані можуть мати значний вплив на прийняття екологічної політики та реагування на надзвичайні ситуації, тому їх безпека має першорядне значення. Надзвичайно важливим є забезпечення захисту цих даних, зокрема їх надійної передачі міжнародним організаціям, як-от ВООЗ чи GEMS, при цьому мінімізуючи ризики перехоплення чи підроблення. VPN стають ключовим інструментом захисту, забезпечуючи шифрування між кінцевими точками та використання таких стандартів безпеки, як IPsec і SSL/TLS. Ці протоколи створюють надійний фундамент для збереження конфіденційності навіть у середовищах із публічним доступом,. Наприклад, сучасні рішення дозволяють дослідникам використовувати шифрування VPN для передачі екологічних даних між країнами, гарантуючи відсутність ризиків кіберзагроз і несанкціонованого втручання у процес зв'язку. Завдяки цьому забезпечується не лише безпека

інформації, але й її цілісність, яка є необхідною для глобальних ініціатив зі збереження довкілля.

Для функціонування національних систем моніторингу в умовах глобальної інтеграції критичною є їхня сумісність із міжнародними платформами. Віртуальні приватні мережі забезпечують створення єдиного безпечного простору для комунікації між різними національними екологічними системами, спираючись на стандартизацію протоколів та архітектур. Наприклад, у Постанові №391 Кабінету Міністрів України передбачено використання структурованих методів передачі даних в рамках інтеграції національної системи з міжнародними екологічними ініціативами. VPN відіграють важливу роль у цьому процесі, підтримуючи швидкість передачі даних, а також захищаючи інформацію від несанкціонованого доступу завдяки передовим протоколам, таким як IPsec. Висока швидкість доступу до екологічних даних у реальному часі, що забезпечується VPN, дозволяє ефективно реагувати на екологічні ситуації та приймати стратегічні рішення в рамках міжнародної співпраці . Це робить VPN ключовим інструментом у створенні стійких інформаційних мереж для глобального моніторингу довкілля.

Одним із ключових аспектів, на який орієнтуються системи моніторингу довкілля, є збереження цілісності й конфіденційності переданих даних. VPN активно використовуються для захисту від атак «людина посередині», які в іншому разі могли б призвести до модифікації або втрати екологічних даних, . Наприклад, у режимах реального часу сенсорні системи контролю стану забруднення вод і атмосфери передають інформацію, що стає критичною основою для прийняття оперативних управлінських рішень. За допомогою алгоритмів шифрування, таких як AES, та багаторівневої автентифікації VPN гарантують, що екологічні дані залишаються недоторканими навіть у складних мережевих середовищах. Це особливо важливо в ситуаціях, коли дані передаються через публічні або незахищені мережі, оскільки VPN не лише запобігають несанкціонованому доступу, а й забезпечують високу швидкість передачі інформації. Зрештою, технології VPN створюють надійну інфраструктуру для обробки екологічних

даних, від чого залежить ефективність регіональних та міжнародних екологічних програм.

Серед міжнародних ініціатив із забезпечення безпеки екологічних даних особливо вирізняється платформа SEIS, яка встановлює суворі стандарти конфіденційності та правильного управління інформацією. Використання VPN у таких системах сприяє зниженню ризиків витоку даних, гарантуючи доступ лише авторизованим користувачам через багаторівневу автентифікацію та шифрування. Завдяки впровадженню протоколів IPsec і SSL/TLS підвищується безпека передачі даних, що є ключовим для міжнародних екологічних програм . Як зазначено у звіті NIST, технології VPN забезпечують захищеність великих обсягів даних навіть під час складного міжмережевого обміну, особливо між країнами з різною технічною інфраструктурою [41]. Це дозволяє не лише уникнути втрати або компрометації інформації, а й створити надійні умови для інтеграції та обробки даних у реальному часі, сприяючи оперативному реагуванню на глобальні екологічні виклики.

Забезпечення масштабованості систем моніторингу є ще одним важливим викликом сучасності. VPN технології дозволяють об'єднувати національні й локальні екологічні платформи в єдину інфраструктуру, яка зберігає відповідність міжнародним стандартам безпеки. Зокрема, адаптовані VPN-рішення із застосуванням протоколів, таких як IPsec і OpenVPN, забезпечують передачу даних великих обсягів навіть у країнах із неоднорідними технічними можливостями. Наприклад, практичні випробування показали, що використання VPN дозволяє знизити ризики втрати даних під час передачі інформації про якість повітря або води між різними географічними регіонами. Це також сприяє міжнародному обміну даними в режимі реального часу завдяки високій пропускній здатності VPN-мереж та гнучкості їхньої конфігурації. У результаті створюється надійна та масштабована інфраструктура, яка підтримує злагоджену роботу систем моніторингу на глобальному рівні.

Інноваційний підхід до використання Інтернету речей (IoT) в екологічному моніторингу створює нові можливості для інтеграції з VPN-мережами. Сенсори

IoT, що фіксують дані, такі як рівень викидів парникових газів або забруднення атмосфери, можуть передавати інформацію в централізовані системи через надійно зашифровані VPN-канали. Це забезпечує не лише високий рівень безпеки, але й мінімізує ризик порушення цілісності даних. Крім того, ці системи активно підтримують автоматичне оновлення алгоритмів безпеки, таких як AES-шифрування, яке знижує необхідність у постійному ручному втручанні . Подібна інтеграція дозволяє обробляти великі обсяги даних у реальному часі, створюючи базу для швидкого реагування на екологічні проблеми. Завдяки гнучкості VPN такі платформи можуть адаптуватися до специфічних регіональних умов, сприяючи міжнародній співпраці та обміну даними між різними країнами. Це важливо для глобальних ініціатив у сфері екології, де IoT та VPN працюють разом, забезпечуючи надійність і безпеку інформаційних процесів.

Впровадження VPN у системи моніторингу довкілля створює надзвичайно стійку інфраструктуру захисту, яка сприяє ефективній міжнародній співпраці. Використання цих технологій допомагає об'єднати розрізнені локальні та національні екологічні платформи у глобальну мережу, забезпечуючи збереження конфіденційності та точності переданих даних . Завдяки масштабованості VPN, що підтримує передачу великих обсягів інформації, екологічні дані, такі як рівень забруднення повітря чи стан водних ресурсів, можуть бути оперативно передані в міжнародні центри аналізу. Це дозволяє не лише швидко реагувати на кризи, але й приймати стратегічні рішення для запобігання майбутнім проблемам.

Крім того, VPN уможливлюють створення єдиного захищеного середовища для обміну даними між різними державами, навіть за умов неоднакової технічної розвиненості їхніх систем [43]. Завдяки шифруванню даних і автентифікації доступу, технології VPN знижують ризики втрати чи викрадення інформації.

Таким чином, сучасні інформаційні технології стають важливим інструментом у вирішенні глобальних екологічних проблем, дозволяючи забезпечити постійну інтеграцію на локальному, регіональному та міжнародному рівнях, що є фундаментом сталого розвитку.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було розглянуто сучасні проблеми та вимоги до захисту інформаційно-телекомунікаційних систем, що дозволило визначити ключові загрози та вразливості. Проведений аналіз актуальних методів забезпечення безпеки, зокрема технологій VPN, підтвердив їхню ефективність у створенні надійного рівня захисту даних.

Проектування VPN-систем виконувалося з акцентом на моделюванні загроз, виборі відповідних протоколів та технологій. У результаті було обрано оптимальні рішення для забезпечення конфіденційності, стабільності та швидкодії. Розроблені моделі відповідають сучасним стандартам кібербезпеки, забезпечуючи високу надійність та захист інформаційних ресурсів організацій.

Практичне застосування технології OpenVPN дало змогу оцінити вплив параметрів шифрування на продуктивність систем. Тестування підтвердило, що правильний вибір алгоритмів шифрування та налаштувань забезпечує баланс між безпекою та продуктивністю мережі, що є критично важливим для бізнес-процесів.

Дослідження аспектів охорони праці та безпеки в надзвичайних ситуаціях показало, що впровадження VPN-технологій не лише знижує кіберризики, а й сприяє формуванню безпечного робочого середовища. Рекомендації щодо налаштування інфраструктури враховують як технічні, так і організаційні аспекти, забезпечуючи комплексний підхід до управління ризиками.

Загалом, результати дослідження підтверджують, що впровадження VPN є одним із найефективніших рішень для підвищення рівня кібербезпеки в організаціях. Обрані протоколи, розроблені системи та практичні рекомендації забезпечують надійний захист даних, сприяють економічній доцільності рішень та підвищують стійкість інформаційних систем до сучасних загроз. Таким чином, ця робота робить значний внесок у оптимізацію стратегій захисту інформаційних ресурсів в умовах постійного зростання кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings, W. (2019). Network Security Essentials: Applications and Standards. Pearson Education.

2. Kaufman, C., Perlman, R., & Speciner, M. (2016). Network Security: Private Communication in a Public World. Prentice Hall.

3. Ferguson, N., & Schneier, B. (2003). Practical Cryptography. Wiley Publishing.

4. Lupenko, S., Orobchuk, O., Pasichnyk, V., Kunanets, N., & Xu, M. (2018). The axiomatic-deductive strategy of knowledge organization in onto-based e-learning systems for Chinese Image Medicine. In CEUR Workshop Proceedings (pp. 126-134).

5. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170.

6. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach. Pearson.

7. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193.

8. Lupenko, S. A., Orobchuk, O., & Kateryniuk, I. (2020, November). Mathematical Modeling of Diagnosis and Diagnostic Information Space of Chinese Image Medicine for their Unified Representation in Information Systems for Integrative Scientific Medicine. In IDDM (pp. 370-376).

9. Journal of Network and Computer Applications. (2021). Evaluating the Performance of VPNs in Modern Information Systems.

10. Cisco Systems. (2022). VPN Security: Best Practices and Implementation Guide. Cisco White Paper.

11. Rouse, M. (2021). Understanding VPNs and Their Role in Secure Networking. TechTarget.

12. Lupenko, S. A., Orobchuk, O. R., & Zahorodna, N. V. (2017, December). Formation of the onto-oriented electronic educational environment as a direction the formation of integrated medicine using the example of CIM. In Actual scientific research in the modern world: Collection of scientific papers of the XXIII International scientific conference (Vol. 12, No. 32, pp. 56-61).

13. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

14. Gibson, D. (2021). CompTIA Security+ Guide to Network Security Fundamentals. Cengage Learning.

15. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

16. OpenVPN Technologies, Inc. (2022). OpenVPN: Implementation and Management. OpenVPN Technical Documentation.

17. RFC 4301. (2005). Security Architecture for the Internet Protocol. Internet Engineering Task Force (IETF).

18. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

19. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

20. Lupenko, S., Orobchuk, O., & Xu, M. (2020). The ontology as the core of integrated information environment of Chinese Image Medicine. In Advances in Computer Science for Engineering and Education II (pp. 471-481).

21. Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.

22. Lupenko, S., Orobchuk, O., & Xu, M. (2019, September). Logical-structural models of verbal, formal and machine-interpreted knowledge representation in Integrative scientific medicine. In Conference on Computer Science and Information Technologies (pp. 139-153).

23. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. Prentice Hall.

24. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

25. Harkins, D. (2020). IPsec VPN Design. Cisco Press.

26. Kent, S., & Atkinson, R. (1998). Security Architecture for the Internet Protocol. RFC 2401.

27. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології "Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

28. Zwicky, E. D., Cooper, S., & Chapman, B. (2000). Building Internet Firewalls. O'Reilly Media.

29. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

30. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

31. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

32. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

33. Stuart Davidson та інші. (2021). A Performance Comparison of WireGuard and OpenVPN. ACM Digital Library.

34. Kent, S., & Atkinson, R. (1998). Security Architecture for the Internet Protocol. RFC 2401. Internet Engineering Task Force.

35. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

36. Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.

37. Fryz, M., Mlynko, B., Mul, O., & Zagorodna, N. (2010). Conditional Linear Periodical Random Process as a Mathematical Model of Photoplethysmographic Signal. Rigas Tehniskas Universitates Zinatniskie Raksti, 45, 82.

38. Palamar, A., Stadnyk, M., & Palamar, M. (2022). Adaptive pid regulation method of uninterruptible power supply battery charge current based on artificial neural network. Вісник Тернопільського національного технічного університету, 107(3), 5-13.

39. Kharchenko, O., Raichev, I., Bodnarchuk, I., & Zagorodna, N. (2018, February). Optimization of software architecture selection for the system under design and reengineering. In 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (pp. 1245-1248). IEEE.

40. OpenVPN Technologies, Inc. (2022). OpenVPN: Implementation and Management. Офіційна документація OpenVPN із детальними інструкціями з налаштування. OpenVPN.

41. Kali Linux Documentation. Повний путівник із налаштування та використання Kali Linux, включаючи безпечне застосування інструментів для аудиту мереж.

42. OpenVPN Community Resources. Ресурси та керівництва для спільноти OpenVPN, доступні для налаштування VPN у різних середовищах.

ДОДАТОК А - Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ,
СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ

2024

УДК 001

М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професо**р.**

Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.

Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.

Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.

Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної

інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,

тел. (0352) 52-41-33, факс (0352) 25-49-83.

E-mail: conffis2024@gmail.com

Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.056.55

Ю.Р. Олійник, студент, Ph.D Олександра Оробчук.

(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

Y. Oliynyk, student, Ph.D Oleksandra Orobchuk.

METHODS OF PROTECTING INFORMATION AND TELECOMMUNICATION SYSTEMS AND NETWORKS FROM UNAUTHORIZED ACCESS USING VPN TECHNOLOGY

У сучасному цифровому світі питання захисту інформації стає дедалі важливішим. Інформаційно-телекомунікаційні системи є вразливими до кіберзагроз, що можуть спричиняти витік даних чи несанкціонований доступ. Одним із ефективних рішень є використання VPN, який створює захищені з'єднання навіть через публічні мережі. Це дозволяє забезпечити конфіденційність та цілісність даних, що передаються, знижуючи ризики для користувачів.

Розвиток кібератак, таких як "людина посередині" (MITM), вимагає застосування складних технологій безпеки. VPN забезпечує шифрування даних і мінімізує ризик їх перехоплення, що є важливим як для корпоративних систем, так і для приватних осіб. Це підвищує загальний рівень довіри до мережевих комунікацій.

У роботі проведено дослідження ефективності VPN-протоколів, таких як OpenVPN та WireGuard. Аналіз включав тестування продуктивності під час різного навантаження та вивчення стійкості до кібератак. Такий підхід дозволив визначити оптимальні технічні параметри для захисту мережевих ресурсів. Додатково, було розглянуто вплив різних конфігурацій на швидкість з'єднання та загальну безпеку системи.

WireGuard показав вищу продуктивність, тоді як OpenVPN забезпечив більшу гнучкість налаштувань. Надійність шифрування залежить від довжини ключів і обраних алгоритмів. Розроблено рекомендації для налаштування VPN-систем у контексті запобігання типових уразливостей. Важливо також враховувати специфічні потреби організації для оптимізації безпеки та ефективності мережі.

VPN є ключовим інструментом для захисту інформаційно-телекомунікаційних систем. Однак для максимального ефекту потрібно інтегрувати VPN у загальну стратегію кібербезпеки, забезпечуючи регулярні оновлення та оптимізацію налаштувань. Це включає впровадження додаткових заходів безпеки, таких як двофакторна автентифікація та моніторинг мережевої активності.

Література

1. RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2).
2. Jason A. Donenfeld. WireGuard Cryptokey Routing Protocol.
3. OpenVPN Community. OpenVPN Protocol Documentation.

ДОДАТОК Б. ПОСІБНИКИ З АРХІТЕКТУРИ OPENVPN

1. НАСТАНОВА ДЛЯ ПОЧАТКІВЦІВ

   Посібник *"OpenVPN for Beginners"*, що пропонує просте пояснення початкового налаштування архітектури OpenVPN.

2. РОЗШИРЕНИЙ ПОСІБНИК З НАЛАШТУВАННЯ

   Керівництво *"Advanced OpenVPN Configuration Guide"*, яке розглядає оптимізацію роботи архітектури OpenVPN.

3. ПОСІБНИК ПОКРОКОВОГО РОЗГОРТАННЯ

   "Deploying OpenVPN Step-by-Step" — покрокова інструкція з налаштування OpenVPN на різних платформах.

4. ТУТОРІАЛ ІЗ НАЛАШТУВАННЯ СЕРВЕРА OpenVPN

   "Setting Up an OpenVPN Server" — відеокурс із детальним роз'ясненням створення серверу OpenVPN.

5. ТУТОРІАЛ ІЗ ДОПОВНЕННЯМ TLS

   "OpenVPN with TLS Authentication Tutorial" — покроковий аналіз налаштування OpenVPN із додатковими рівнями безпеки.

6. БАЗОВІ ІНСТРУКЦІЇ

   Офіційний ресурс Керівництва на OpenVPN.net із докладними рекомендаціями для налаштування архітектури OpenVPN.

ДОДАТОК В. АЛГОРИТМ НАЛАШТУВАННЯ ПАРАМЕТРІВ OPENVPN

1. КРОКИ НАЛАШТУВАННЯ VPN
    - Покрокова інструкція для встановлення і налаштування серверу та клієнтів за допомогою OpenVPN.
    - Конфігураційні файли OpenVPN для різних середовищ (Windows, Linux).
2. СКРІНШОТИ КОНФІГУРАЦІЇ
    - Ілюстрація графічного інтерфейсу (GUI) налаштувань.
    - Приклади командної лінії для генерації сертифікатів SSL/TLS.

ДОДАТОК Г. ДОДАТКОВА ІНФОРМАЦІЯ ЩОДО ПРОТОКОЛІВ VPN

1. ПОГЛИБЛЕНИЙ АНАЛІЗ ПОПУЛЯРНИХ ПРОТОКОЛІВ VPN
    - Порівняння IPSec, OpenVPN, SSL/TLS і L2TP/IPSec за показниками швидкості, безпеки та сумісності.
    - Особливості виконання криптографічних операцій.
2. ФРАГМЕНТИ RFC, ЩО СТОСУЮТЬСЯ VPN
    - Витяги з RFC-документів для протоколів IPSec (RFC 4301) та OpenVPN.

ДОДАТОК Д. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА

1. ПЛАНИ ЕВАКУАЦІЇ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ
    - Маршрут евакуації для IT-персоналу в умовах небезпеки.
    - Алгоритм дій у разі виявлення кібератаки.
2. ДОКУМЕНТАЦІЯ З ПРОТИДІЇ КІБЕРЗАГРОЗАМ
    - Інструкції з управління ризиками для захисту OpenVPN під час екстрених ситуацій.

ДОДАТОК Е. РОЗШИРЕНИЙ ГЛОСАРІЙ

1. СЛОВНИК ТЕХНІЧНИХ ТЕРМІНІВ
    - Розширений перелік термінів, використаних у роботі, з поясненнями.
    - Включення акценту на специфічні VPN-протоколи і технології.
2. ПЕРЕЛІК СКОРОЧЕНЬ
    - Всі абревіатури, використані в роботі, з їхніми повними розшифровками.

ДОДАТОК Є. ТЕХНІЧНА ДОКУМЕНТАЦІЯ

1. СПЕЦИФІКАЦІЇ ТА РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕКИ OPENVPN
    - Технічні рекомендації з документації OpenVPN для забезпечення стабільності та конфіденційності.
2. ОСОБЛИВОСТІ ПРОДУКТИВНОСТІ СИСТЕМІЙ VPN
    - Опис методів оптимізації продуктивності VPN-рішень на різних платформах.