МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

Кафедра Комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Аліна САВЧЕНКО

«_____»_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ДИПЛОМНА РОБОТА, ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

"МАГІСТРА"

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ "ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ"

Тема: «Інформаційна мережа передачі даних навчального закладу»

Виконав: Тимочко Христина Ігорівна

Керівник: к.т.н., доцент кафедри КІТ Колісник Олена Василівна

Нормоконтролер Ігор РАЙЧЕВ

Київ – 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет *Комп'ютерних наук та технологій*

Кафедра *Комп'ютерних інформаційних технологій*

Галузь знань, спеціальність, освітньо-професійна програма: 12 "Інформаційні технології", 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології"

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____Аліна САВЧЕНКО

"___"_____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи студента

Тимочко Христини Ігорівни

(прізвище, ім'я, по батькові)

1.Тема роботи: «Інформаційна мережа передачі даних навчального закладу», затверджена наказом ректора від "29" вересня 2023 р. за № 1976/ст.

2. Термін виконання роботи: : з 02 жовтня 2023 р. по 31 грудня 2023 р.

3. Вихідні дані до роботи: методи та засоби проектування та реалізації інформаційної мережі передачі даних навчального закладу.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці): загальна характеристика, призначення і аналіз вимог до інформаційної мережі навчального закладу; вибір мережевого обладнання, розробка схеми адресації та проектування мережі; налаштування, тестування та перевірка функціональності інформаційної мережі навчального закладу.

5. Перелік обов'язкового графічного матеріалу: інформативні рисунки, графічні скріншоти роботи системи, слайди презентації в MS PowerPoint.

6. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Пошук і дослідження наукових джерел.	02.10.2023 – 08.10.2023	
2.	Розроблення та затвердження календарного плану виконання дипломної роботи.	09.10.2023 – 10.10.2023	
3.	Проведення консультацій з науковим керівником.	11.10.2023 – 13.10.2023	
4.	Написання Розділу 1. Аналіз предметної області та постановка задачі.	14.10.2023 –27.10.2023	
5.	Написання Розділу 2. Проектування інформаційної мережі навчального закладу.	28.10.2023 – 16.11.2023	
6.	Написання Розділу 3. Налаштування та тестування мережі.	17.11.2023 – 30.11.2023	
7.	Оформлення пояснювальної записки дипломної роботи.	01.12.2023 – 04.12.2023	
8.	Написання, друк та підписання Рецензії у рецензента та Відгуку керівника у встановленому порядку.	05.12.2023 – 10.12.2023	
9.	Створення Презентації та доповіді.	11.12.2023 – 12.12.2023	
10.	Підготовка до захисту та попередній захист дипломної роботи на випусковій кафедрі.	13.12.2023 – 17.12.2023	

7. Дата видачі завдання: «02» жовтня 2023 р.

Керівник дипломної роботи _____ Олена КОЛІСНИК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Христина ТИМОЧКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Інформаційна мережа передачі даних навчального закладу» викладена на 72 сторінках і містить 47 рисунків, 6 таблиць та один додаток. Список бібліографічних посилань складається з 9 найменувань.

Ключові слова: ІНФОРМАЦІЙНА МЕРЕЖА, НАВЧАЛЬНИЙ ЗАКЛАД, ТРАФІК, ПРОЕКТУВАННЯ, ПРОПУСКНА ЗДАТНІСТЬ, ІНТЕРФЕЙС, ТЕСТУВАННЯ.

Об'єкт дослідження – процес створення інформаційної мережі даних навчального закладу.

Предмет дослідження – особливості побудови і функціонування інформаційної мережі навчального закладу.

Мета роботи. Проектування оптимальної інформаційної мережі для конкретного навчального закладу з урахуванням його потреб та вимог.

Актуальність дипломної роботи полягає в необхідності створення більш надійної, точної та ефективної інформаційної мережі передачі даних навчального закладу, оскільки в їхніх мережах циркулює велика кількість конфіденційної інформації – персональні дані учнів та викладачів, навчальні матеріали, внутрішня документація тощо.

У роботі висвітлено:

- аналіз вимог до інформаційної мережі навчального закладу;
- вибір раціональної топології та архітектури мережі;
- підбір необхідного обладнання та розробка схеми IP-адресації;
- проектування логічної та фізичної структури мережі;
- моделювання роботи спроектованої мережі.

Результати тестування безпеки були підтверджені звітами, які включали детальний аналіз виявлених вразливостей, відповідь системи на різні види атак та рекомендації щодо поліпшення безпеки мережі. Це дало нам змогу вдосконалити нашу мережу та забезпечити високий рівень безпеки для захисту від потенційних кіберзагроз.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

SSID	Service Set Identifier
SQL	Structured Query Language
LMS	Learning management system
IDS	Intrusion Detection System
PoE	Power over Ethernet
WAN	Wide Area Network
LAN	Local Area Network
VLAN	Virtual Local Area Network
SSID	Service Set Identifier
AD	Active Directory

ЗМІСТ

ВСТУП

Актуальність теми. В умовах стрімкого розвитку інформаційних технологій все більшого значення набуває побудова надійних і захищених мереж передачі даних. Особливо гостро це питання стоїть для навчальних закладів, адже в їхніх мережах циркулює велика кількість конфіденційної інформації - персональні дані учнів та викладачів, навчальні матеріали, внутрішня документація тощо.

Дані, що передаються по незахищених мережах, можуть стати доступними зловмисникам. Це може призвести до витоку персональних даних, крадіжки інтелектуальної власності, пошкодження чи викрадення важливої інформації. Тому питання захисту даних при їх передачі є надзвичайно актуальним для інформаційних мереж навчальних закладів.

Мета і завдання роботи. Метою даної роботи є проектування оптимальної інформаційної мережі для конкретного навчального закладу з урахуванням його потреб та вимог.

Основні завдання:

- аналіз вимог до інформаційної мережі навчального закладу;
- вибір раціональної топології та архітектури мережі;
- підбір необхідного обладнання;
- розробка схеми IP-адресації;
- проектування логічної та фізичної структури мережі;
- моделювання роботи спроектованої мережі.

Об’єкт дослідження – інформаційна мережа навчального закладу.

Предмет дослідження – особливості побудови і функціонування інформаційної мережі навчального закладу.

Методи дослідження – аналіз вимог до мережі, порівняння топологій та архітектур мереж, моделювання.

- аналіз вимог до інформаційної мережі навчального закладу – дослідження потреб користувачів мережі, визначення необхідної кількості підключень, пропускної здатності каналів, вимог до надійності та захищеності передачі даних;

– порівняльний аналіз топологій та архітектур мереж – розгляд переваг і недоліків різних топологій (зірка, шина, кільце тощо) та архітектур (клієнт-сервер, однорангова мережа тощо) для вибору оптимальної для конкретного випадку;

– моделювання роботи спроектованої мережі – побудова логічної моделі мережі та її налагодження за допомогою спеціалізованих програмних засобів (Packet Tracer та ін.) з метою перевірки працездатності та відповідності вимогам;

– тестування мережі в лабораторних умовах – практична перевірка основних параметрів спроектованої мережі (швидкість передачі даних, якість з'єднання, надійність тощо).

Практичне значення даного дослідження полягає в наступному: розроблена в роботі модель інформаційної мережі навчального закладу може бути використана як основа для створення реальної комп'ютерної мережі. Запропоновані технічні рішення з побудови мережі, вибору обладнання, налаштування політик безпеки можуть застосовуватися на практиці при розгортанні мережі в навчальному закладі. Результати дослідження топологій і архітектур мереж можуть слугувати основою для вибору оптимальної мережевої структури. Запропонована схема IP-адресації та принципи побудови мережевих сегментів можуть бути використані на практиці. Розроблені рекомендації з налаштування мережевих пристроїв, сервісів, політик безпеки можуть застосовуватися фахівцями з комп'ютерних мереж. Методики моделювання та тестування мережі можуть використовуватися для перевірки працездатності реальних мереж на етапі впровадження. Таким чином, проведене дослідження має значний прикладний потенціал та може стати основою для створення реальної мережі навчального закладу.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновку та списку використаних джерел.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1. Загальна характеристика і призначення інформаційної мережі навчального закладу

Інформаційна мережа є важливою складовою інфраструктури будь-якого сучасного навчального закладу. Вона призначена для об'єднання комп'ютерів, інших цифрових пристроїв та користувачів в єдине інформаційне середовище з метою спільного використання ресурсів та обміну даними.

Основними компонентами мережі є (рис. 1.1):

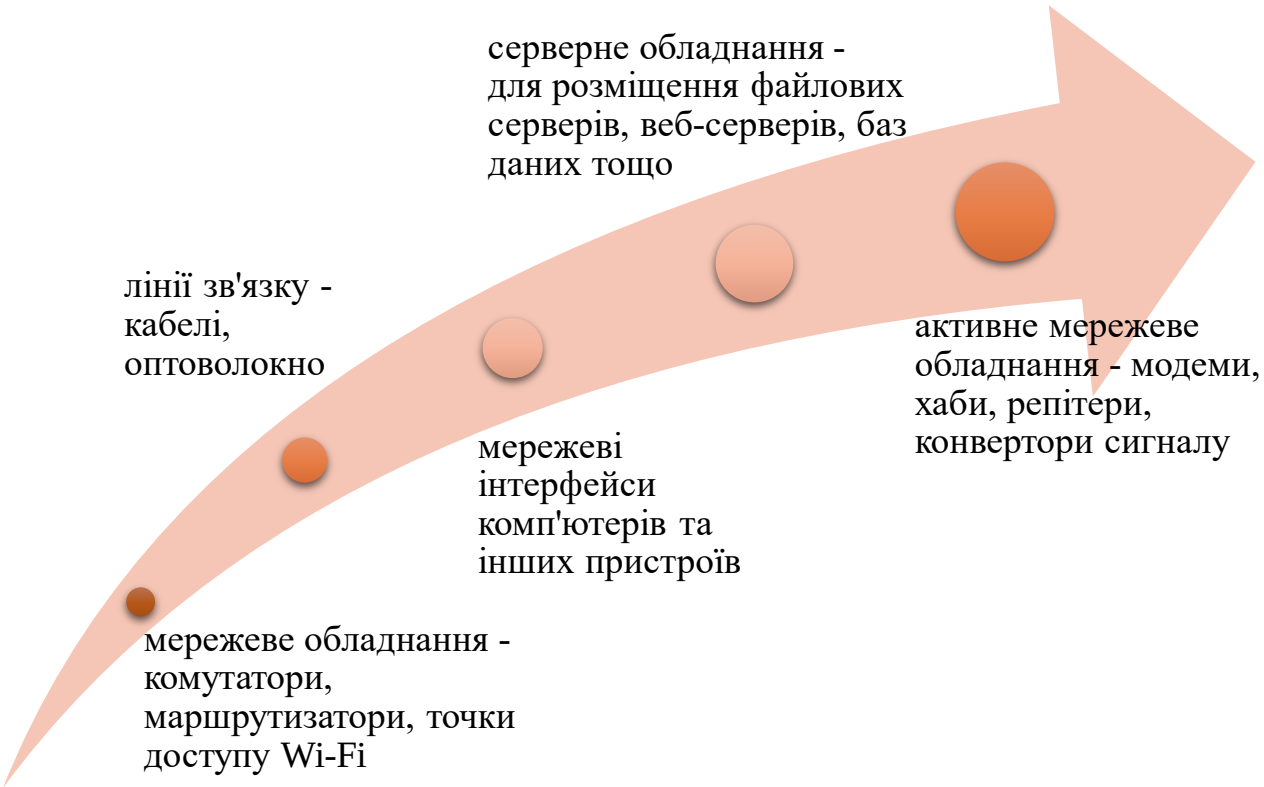

Рис. 1.1. Основні компоненти інформаційної мережі

Основними компонентами будь-якої сучасної комп'ютерної мережі є мережеве обладнання, таке як комутатори, які відповідають за комутацію пакетів даних в мережі на рівні дата-лінків моделі OSI та допомагають оптимізувати трафік, маршрутизатори, які забезпечують маршрутизацію пакетів між різними мережами, а також точки доступу Wi-Fi, які є бездротовими інтерфейсами, що дозволяють пристроям під'єднуватися до мережі.

Центральне місце в мережевій структурі також займають лінії зв'язку: кабелі різних типів, таких як коаксіальний, вита пара чи категорійний, для передачі сигналу в провідних мережах, і оптоволокно, яке гарантує високошвидкісну передачу на великі відстані. До мережі під'єднуються за допомогою мережевих інтерфейсів, які можуть бути вбудовані в пристрої або зовнішніми. Серверне обладнання, таке як спеціалізовані комп'ютери або системи зберігання, використовуються для розміщення файлових серверів, веб-серверів і баз даних. Активне мережеве обладнання включає модеми, які модулюють аналоговий сигнал, хаби, що передають інформацію всім пристроям в мережі, репітери для посилення сигналу та конвертори сигналу, які адаптують один тип мережевого сигналу до іншого.

Завдяки такому багатогранному підходу до побудови, сучасні мережі забезпечують стабільність, швидкість та надійність для задоволення потреб користувачів і бізнесу.

Загальна характеристика інформаційної мережі передбачає розгляд кількох ключових аспектів.

По-перше, з точки зору топології та архітектури, на типовому рівні така мережа в основному формується з центрального сервера чи кількох серверів, доповнених комутаційним обладнанням. До цього також додаються бездротові точки доступу та різноманітні кінцеві пристрої, серед яких зокрема можна виокремити комп'ютери, планшети та смартфони.

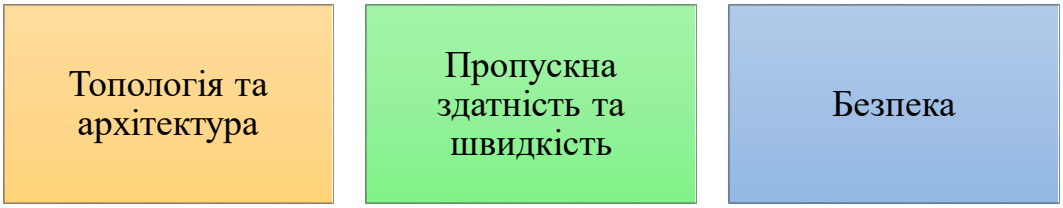

Рис. 1.2. Головні аспекти інформаційної мережі

По-друге, велику роль відіграє пропускна здатність та швидкість мережі. В сучасних умовах, коли завданням стає передача великих об'ємів інформації, висока швидкість є критично важливою, особливо для активів, як-от онлайн-лекції, відеоконференції, а також для завантаження густих навчальних матеріалів.

По-третє, безпека інформаційної мережі займає особливе місце у загальній характеристиці. Враховуючи, що така мережа зберігає значну кількість персональних та конфіденційних даних, впровадження систем безпеки, таких як файерволи, антивірусні програми та системи виявлення вторгнень, стає не просто бажаним, а вкрай необхідним кроком.

Мережа навчального закладу виконує такі функції:

- надає доступ користувачам до локальних і глобальних мережевих ресурсів;
- забезпечує обмін даними між комп'ютерами;
- надає колективний доступ до периферійних пристроїв;
- слугує основою для впровадження хмарних технологій;
- забезпечує інформаційну підтримку навчального процесу та управління закладом.

Рис. 1.3. Призначення інформаційної мережі навчального закладу

Призначення інформаційної мережі навчального закладу має ряд важливих аспектів, серед яких слід виокремити наступне.

По-перше, однією з ключових функцій мережі є забезпечення доступу до Інтернету, що включає в себе не лише загальний доступ до інтернет-ресурсів, але й конкретно до тих, що використовуються для навчання, дослідницької роботи та різноманітних комунікацій.

По-друге, електронна бібліотека та бази даних служать місцем централізованого зберігання навчальних матеріалів, наукових робіт, публікацій, забезпечуючи легкий доступ до них.

По-третє, в сучасних умовах актуальність електронного навчання зростає, отже платформи для онлайн-лекцій, семінарів, вебінарів та інших форм дистанційного навчання стають невід'ємною частиною освітнього процесу.

Адміністраційні функції в мережі допомагають автоматизувати численні процеси управління навчальним закладом: від ведення журналів до планування розкладу. Інструменти для спілкування та співпраці в мережі забезпечують ефективну комунікацію між усіма учасниками навчального процесу і сприяють командній роботі над проектами.

На завершення, важливо підкреслити можливість інтеграції інформаційної мережі з іншими програмами і платформами, як-от CRM-системи або системи управління навчанням (LMS), що розширює функціонал та можливості для користувачів.

1.2. Аналіз вимог до інформаційної мережі конкретного навчального закладу

При плануванні інформаційної мережі для навчального закладу важливо враховувати конкретні потреби і особливості цього закладу. Вимоги до мережі можуть змінюватися залежно від типу, розміру, кількості студентів, специфіки навчального процесу, доступних ресурсів та інших параметрів (рис. 1.4).

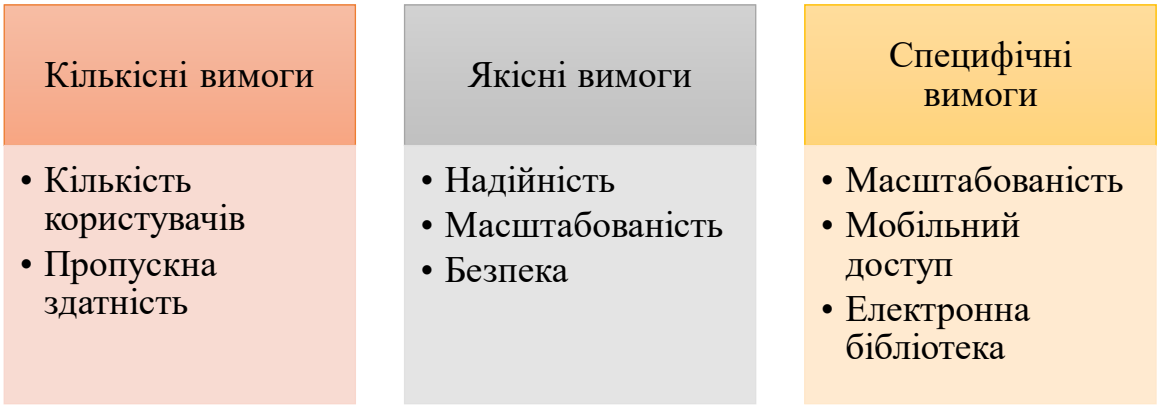

Рис. 1.4. Вимоги до інформаційної мережі конкретного навчального закладу

Основою успішного планування та розгортання інформаційної мережі є коректне розуміння та визначення кількісних вимог. Ці вимоги стосуються числових характеристик, які визначають робочу навантаження мережі і відповідно, необхідні ресурси.

Центральним параметром є визначення потенційної кількості осіб, які будуть одночасно використовувати мережеві ресурси. Особливо важливо розуміти максимальну кількість користувачів під час пікових навантажень. Наприклад, під час онлайн-лекцій, екзаменів або інших важливих подій. Враховуючи різноманітний склад осіб – від студентів до викладачів, і аж до адміністративного персоналу, ця кількість стає ключовим фактором для забезпечення стабільності роботи мережі.

Ще одним критичним параметром є визначення необхідної пропускної здатності мережі. Це стосується швидкості передачі даних, яка необхідна для комфортного доступу до Інтернету та інших внутрішніх ресурсів. Враховуючи ростучу потребу в високошвидкісному доступі до мультимедійного контенту, великих об'ємів наукових даних або ресурсів для онлайн-навчання, правильно обрана пропускна здатність вирішує проблему затримок і забезпечує високу продуктивність користувача.

Отже, при плануванні інформаційної мережі необхідно ретельно аналізувати ці кількісні характеристики, щоб забезпечити її ефективність та надійність для всіх користувачів.

Якість роботи інформаційної мережі може істотно впливати на здатність навчального закладу забезпечувати високоякісне навчання та взаємодію між учасниками освітнього процесу. Тому при проектуванні такої мережі важливо враховувати ряд ключових якісних характеристик.

У сучасному освітньому середовищі, де багато процесів відбувається онлайн, надійність мережі є критично важливою. Це означає, що мережа повинна забезпечувати стабільний доступ до ресурсів без перебоїв, автоматично відновлюючись після можливих збоїв. Можливі технічні проблеми та відмови обладнання повинні мінімізуватися шляхом використання якісного та перевіреного обладнання, а також запровадженням систем моніторингу.

Охорона конфіденційності, цілісності та доступності інформації є важливим аспектом будь-якої інформаційної мережі. Навчальні заклади часто стають мішенями для кіберзлочинців через велику кількість даних, які вони зберігають. Тому важливо застосовувати передові методи захисту, включаючи регулярні оновлення ПЗ, резервне копіювання даних та системи аварійного відновлення, щоб у випадку втрати даних швидко відновити роботу.

З урахуванням швидкого розвитку технологій та зростання потреб користувачів, інформаційна мережа повинна бути готова до масштабування. Це означає здатність додавати нові пристрої, сервіси або користувачів без необхідності значного переоснащення або перебудови існуючої інфраструктури. Мережа повинна бути гнучкою, щоб адаптуватися до змінюваних потреб та обставин навчального закладу.

Сучасні навчальні заклади стикаються із завданням інтеграції різноманітних технологічних рішень, що значущо впливає на якість освітнього процесу. Ці специфічні потреби вимагають особливої уваги при проектуванні та налаштуванні інформаційних мереж.

В сучасному навчальному процесі велику роль відіграють специфічні програми та платформи. Це можуть бути системи управління навчанням (LMS), які дозволяють автоматизувати процес навчання, відстежувати успіхи студентів, проводити онлайн-тестування та інше. Також це можуть бути віртуальні лабораторії, які дозволяють

студентам експериментувати в цифровому середовищі. Враховуючи це, мережа повинна забезпечувати високу пропускну здатність, стабільність та сумісність із цими додатками.

Сучасні студенти та викладачі все частіше використовують мобільні пристрої для доступу до навчальних матеріалів та ресурсів. Отже, забезпечення стабільного Wi-Fi покриття в усіх приміщеннях закладу, включаючи аудиторії, коридори, бібліотеку та інші загальнодоступні зони, є ключовим. Також важливо забезпечити оптимальну швидкість та безперебійність з'єднання для мобільних пристроїв, незалежно від їх кількості.

В епоху цифровізації традиційні бібліотечні ресурси все частіше доповнюються або замінюються електронними аналогами. Електронні книги, наукові журнали, дослідницькі роботи та інші матеріали можуть бути доступні онлайн через спеціалізовані платформи. Мережа повинна забезпечувати швидкий та надійний доступ до цих ресурсів, гарантуючи комфорт користувачам при їх вивченні.

Отже, проаналізувавши вимоги до інформаційної мережі навчального закладу, можемо зробити кілька ключових висновків. По-перше, сучасний навчальний заклад вимагає високопродуктивної, стабільної та безпечної мережі, яка здатна задовольнити потреби великої кількості користувачів одночасно. Це включає не лише забезпечення доступу до Інтернету, але й підтримку специфічних додатків, віртуальних лабораторій, систем управління навчанням та інших цифрових ресурсів. По-друге, безпека даних є пріоритетом. Оскільки мережі навчальних закладів зберігають чимало конфіденційних даних, їхнє захищене зберігання та передача є критично важливими. По-третє, мережа повинна бути масштабованою і гнучкою для адаптації до змінюваних освітніх потреб та технологічних нововведень у майбутньому. З урахуванням вищезгаданих аспектів, при проектуванні та розгортанні мережі важливо враховувати як кількісні, так і якісні характеристики, а також специфічні потреби закладу. Тільки інтегрований підхід до визначення вимог може забезпечити створення ефективної, надійної та безпечної інформаційної мережі для навчального закладу.

1.3. Огляд програмних засобів для захисту інформації

Основні програмні засоби захисту інформації, що застосовуються в комп'ютерних системах:

1. ***Антивіруси.*** Це програмні засоби, що надають захист від шкідливого програмного забезпечення, такого як віруси, трояни, черви, шпигунське програмне забезпечення та інше. Вони виконують пошук, виявлення, блокування і видалення шкідливого програмного забезпечення.

2. ***Файрволи.*** Це програмні засоби, що контролюють мережевий трафік, блокуючи небажані або небезпечні пакети даних. Файрволи використовуються для встановлення правил мережевого доступу і захисту від зовнішніх атак.

3. ***Шифрування.*** Це процес перетворення інформації в нерозбірливий формат для захисту від несанкціонованого доступу. Шифрована інформація може бути розшифрована тільки за допомогою відповідного ключа.

4. ***Системи керування доступом.*** Ці програмні засоби дозволяють контролювати, хто має доступ до певної інформації або системи, та що вони можуть робити з цією інформацією.

5. ***Системи обнаруження вторгнень (IDS).*** Це програмні засоби, які виявляють підозрілу активність в системі, що може свідчити про спробу несанкціонованого доступу або атаки.

6. ***Системи запобігання вторгнень (IPS).*** Це програмні засоби, які, крім виявлення підозрілої активності, також здатні блокувати таку активність.

Вибір конкретного програмного засобу захисту інформації залежить від конкретних вимог до захисту інформації, а також від технологічного середовища, в якому він буде використовуватися.

При аналізі сучасних програмних засобів для захисту інформації варто відзначити, що багато компаній пропонують комплексні рішення, які включають різні методи захисту. До таких компаній відносяться:

Рішення Symantec (Norton) для захисту інформації включають антивіруси, файрволи, системи обнаруження вторгнень (IDS), системи запобігання вторгнень (IPS), а також технології шифрування.

Рис. 1.5. Логотип компанії Symantec (Norton)

Основними особливостями продуктів Symantec є їх багатофункціональність і зручність використання. Завдяки інтеграції різних методів захисту в одну систему (антивірус, файрвол, системи IDS/IPS, шифрування), користувач отримує комплексний захист від різних видів загроз. Ефективність цих рішень висока, але їхня вартість може бути досить високою для невеликих організацій або індивідуальних користувачів.

Kaspersky Lab пропонує комплексні антивірусні рішення, які включають захист від вірусів, шпигунського програмного забезпечення, троянців, файрволі та інших методів захисту.

Рис. 1.6. Логотип компанії Kaspersky Lab

Продукти Kaspersky відомі своєю високою ефективністю проти вірусів та інших шкідливих програм. Особливістю є гнучкі налаштування захисту, що дозволяє користувачам адаптувати систему захисту до своїх специфічних потреб. Крім того, Kaspersky Lab постійно оновлює свої бази даних з відомими загрозами, що дозволяє надавати актуальний захист.

McAfee – інша популярна компанія, яка пропонує комплексні рішення для захисту інформації. Вони пропонують широкий спектр програмних засобів, включаючи антивіруси, файрволи, шифрування, системи IDS/IPS та ін.

Рис. 1.7. Логотип компанії McAfee

Основна перевага продуктів McAfee - це їхня спроможність працювати на велику кількість різних платформ та операційних систем. Ефективність захисту McAfee аналогічна Norton та Kaspersky, але залежить від конкретного продукту та його налаштувань.

Cisco пропонує широкий спектр рішень для захисту інформації, включаючи файрволи, системи IDS/IPS, шифрування, а також рішення для безпечного віддаленого доступу.

Рис. 1.8. Логотип компанії Cisco

Cisco відома своїми рішеннями для корпоративного сектору, включаючи файрволи та системи IDS/IPS. Особливістю їх продуктів є висока масштабованість та

зручність управління, що робить їх ідеальним вибором для великих мереж.

Bitdefender пропонує комплексні антивірусні рішення, які включають захист від вірусів, шпигунського програмного забезпечення, файрволі та ін.

Рис. 1.9. Логотип компанії Bitdefender

Продукти Bitdefender відрізняються високою ефективністю при боротьбі з вірусами та шкідливим ПЗ. Вони включають найновіші технології захисту, такі як штучний інтелект та машинне навчання, для більш точного виявлення та видалення загроз.

Рішення з відкритим кодом, такі як OpenSSL для шифрування, pfSense як файрвол та Snort як IDS/IPS.

Рис. 1.10. Логотип програмного роутера pfSense

Ці відкриті програмні засоби відрізняються доступністю та гнучкістю. OpenSSL є стандартом для шифрування в Інтернеті. pfSense є потужним файрволом, який можна налаштувати для вирішення різних задач захисту. Snort є однією з найбільш

популярних систем IDS/IPS, яка поєднує в собі потужність і гнучкість.

Greenbone Security Manager (GSM) – це відкрите програмне забезпечення для сканування вразливостей мережі та керування безпекою. В рамках даного проекту Greenbone можна використовувати для забезпечення додаткового рівня безпеки і детального аналізу вразливостей мережі.

Рис. 1.11. Логотип системи оцінки вразливостей OpenVAS

З використанням Greenbone Security Manager можна виконати наступні дії:

1. ***Сканування вразливостей.*** Greenbone дозволяє провести сканування мережі з метою виявлення потенційних вразливостей в системі. Це включає в себе сканування портів, перевірку наявності вразливих версій програмного забезпечення, аналіз конфігураційних помилок та інші типи сканування.

2. ***Аналіз результатів.*** Greenbone надає детальну інформацію про виявлені вразливості, включаючи опис проблеми, рекомендації щодо виправлення та рівень серйозності кожної вразливості. Це допомагає зрозуміти потенційні ризики та прийняти відповідні заходи щодо їх усунення.

3. ***Управління вразливостями.*** Greenbone дозволяє стежити за статусом виявлених вразливостей та керувати процесом виправлення. Ви можете створювати та відстежувати тікети для вразливостей, а також налаштовувати автоматичні процеси виправлення.

4. ***Звітність.*** Greenbone надає можливість генерувати детальні звіти про стан безпеки мережі, включаючи виявлені вразливості, рекомендації щодо виправлення та статистику сканування. Це допомагає зберігати документацію про виконані заходи забезпечення безпеки та дотримання внутрішніх та зовнішніх вимог щодо безпеки.

У контексті даного проекту Greenbone може бути використаний як допоміжний інструмент для сканування та виявлення вразливостей мережі, доповнюючи функціональність pfSense і Snort. Використання Greenbone дозволить отримати більш детальний аналіз стану безпеки мережі, забезпечити виявлення вразливостей та прийняття відповідних заходів щодо їх усунення. Комбінація Greenbone, pfSense і Snort створить потужну систему захисту інформації з мережевим фаєрволом, системою виявлення вторгнень та скануванням вразливостей.

1.4. Формулювання задачі проектування інформаційної мережі

На підставі проведеного аналізу вимог до інформаційної мережі навчального закладу формулюємо основні задачі, які повинен вирішувати проект інформаційної мережі:

1. ***Створення ефективної та масштабованої структури мережі***. Проектована мережа повинна враховувати поточні та майбутні потреби закладу. Це означає можливість додавання нових пристроїв, підтримки нових додатків без необхідності перебудови основної структури мережі.

2. ***Забезпечення високої пропускної здатності та надійності***. Мережа повинна забезпечувати стабільний доступ до ресурсів інтернету та внутрішніх сервісів для усіх користувачів одночасно.

3. ***Розробка системи безпеки***. Наявність захисних механізмів від зовнішніх і внутрішніх загроз, включаючи файерволи, системи виявлення вторгнень, антивірусне програмне забезпечення, а також регулярне резервне копіювання даних.

4. ***Інтеграція специфічних додатків та сервісів***. Підтримка систем управління навчанням (LMS), віртуальних лабораторій, електронних бібліотек, а також інших специфічних для освітнього процесу програм і платформ.

5. ***Мобільний доступ***. Гарантування якісного бездротового зв'язку у всіх приміщеннях навчального закладу та оптимізація мережі для роботи з мобільними пристроями.

6. ***Гнучкість та масштабованість***. Можливість швидко адаптуватися до змін у технологічному ландшафті, додавання нових пристроїв та сервісів без великих витрат.

7. ***Оптимізація витрат***. Проектування мережі таким чином, щоб вона була економічно ефективною, враховуючи інвестиції у обладнання, підтримку та експлуатацію.

У підсумку, основна мета проектування – створити інформаційну мережу, яка буде відповідати всім потребам навчального закладу, забезпечуючи якісний доступ до ресурсів і, одночасно, буде надійною, безпечною та масштабованою.

В рамках формулювання задач проектування інформаційної мережі навчального закладу, особлива увага приділяється інтеграції нової мережі з уже існуючими системами та технологіями. Це означає, що мережева інфраструктура повинна бути спроектована таким чином, аби забезпечити легку сумісність та інтеграцію з різноманітними операційними системами, базами даних та додатковими програмами, які вже використовуються в освітньому процесі. Також важливою є можливість швидко та ефективно впроваджувати новітні технології та сервіси, що виникають у результаті технологічного розвитку та змін у навчальному процесі. Проект має передбачати створення такої мережевої структури, яка буде не тільки відповідати поточним потребам навчального закладу, але й матиме достатню гнучкість для адаптації до майбутніх вимог.

Крім технічних аспектів, важливу роль відіграє і економічна складова проекту. Ефективне використання бюджетних коштів, планування витрат на обслуговування та підтримку мережі, а також розробка стратегії щодо мінімізації витрат на майбутнє розширення та модернізацію є ключовими для створення стабільної та економічно вигідної мережевої інфраструктури.

Зазначимо, що основна мета проектування – створити інформаційну мережу, яка буде відповідати всім потребам навчального закладу, забезпечуючи якісний доступ до ресурсів і, одночасно, буде надійною, безпечною та масштабованою.

У підсумку, головна мета проекту полягає у створенні такої інформаційної мережі, яка забезпечить високу якість доступу до ресурсів, безпеку даних та здатність до масштабування, водночас враховуючи потреби освітнього процесу та особливості навчального закладу. Створення мережі, яка буде відповідати цим критеріям, гарантуватиме не лише ефективне функціонування навчального процесу в сучасних умовах, але й забезпечить основу для подальшого розвитку та інновацій в навчальному закладі.

РОЗДІЛ 2
ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ

2.1. Вибір мережевої топології та обґрунтування мережевої архітектури

Виходячи з аналізу існуючих методів та програмних засобів захисту інформації, поставлено задачу розробки системи захисту інформації на основі відкритого програмного забезпечення. Для цього буде використано pfSense як базову платформу мережевого фаєрволу та Snort як систему виявлення вторгнень (IDS).

Специфічні завдання постановки задачі включають:

1. Вивчення та аналіз основних можливостей та функцій pfSense та Snort;
2. Розробка схеми мережі, в якій pfSense та Snort будуть ефективно використовуватися для захисту інформації;
3. Розробка та впровадження процедур налаштування pfSense та Snort, включаючи налаштування правил фаєрволу, IDS та інших параметрів безпеки;
4. Тестування та оцінка ефективності запропонованого рішення за допомогою симулювання атак і витоку інформації;
5. Підготовка документації, що описує процедури налаштування, управління та моніторингу розробленої системи захисту;

Додатково, поставлено завдання розробки програми для сканування диску на предмет наявності .bat файлів. Для цього, специфічні завдання включають:

6. Аналіз та вивчення вимог до програми для сканування диску на предмет наявності .bat файлів;
7. Обґрунтування вибору мови програмування та технологій, які будуть використані для розробки цієї програми;
8. Розробка алгоритму та програмного коду для сканування диску;
9. Тестування розробленої програми на коректність роботи та ефективність;

10. Впровадження та налаштування програми в середовищі користувача.

Метою цієї розробки є створення ефективного, гнучкого та доступного рішення для захисту інформації від витоку через інформаційні канали. Планується, що ця система буде в змозі адаптуватися до змінюваних умов загрози та забезпечить високий рівень захисту для різноманітних мережевих середовищ.

Перед розробкою потрібно поставити вимоги до розроблюваного проекту. Вимоги допоможуть більш детально зрозуміти, яким повинен бути проект.

Розробка й впровадження захисних засобів для боротьби з витоком інформації через інформаційні канали є важливим завданням в сучасному цифровому світі. Вимоги до таких систем можуть суттєво відрізнятися залежно від конкретного застосування, але є декілька загальних вимог, які повинні бути виконані:

1. **Надійність**. Засоби захисту інформації повинні бути надійними, щоб забезпечити неперервний моніторинг й захист від можливих загроз. Вони повинні витримувати невеликі сбої без значних перебоїв в роботі.

2. **Масштабованість**. Розмір і складність мереж можуть варіюватися, тому важливо, щоб системи захисту могли масштабуватися, щоб задовольнити потреби різних організацій.

3. **Простота впровадження й управління**. Засоби захисту інформації повинні бути легкими для встановлення й управління. Інтерфейси повинні бути інтуїтивно зрозумілими, а процеси конфігурації - максимально простими.

4. **Швидкодія**. Захисні засоби повинні бути достатньо швидкими, щоб впоратися з великим обсягом даних, який може проходити через мережу. Затримки в обробці можуть призвести до пропуску потенційних загроз.

5. **Відповідність стандартам і нормативам**. Важливо, щоб захисні засоби відповідали вимогам законодавства, стандартам безпеки і галузевим нормативам.

6. **Гнучкість**. Системи захисту повинні бути гнучкими, щоб підтримувати різноманітні протоколи, додатки і платформи.

7. **Спроможність до інтеграції**. Засоби захисту інформації повинні бути в стані інтегруватися з іншими системами управління безпекою, зокрема, з системами

аудиту, системами ідентифікації та аутентифікації користувачів, системами контролю доступу тощо.

У контексті даної роботи, враховуючи використання PfSense і Snort, вимоги до засобів захисту повинні включати здатність до глибокого аналізу пакетів (Deep Packet Inspection, DPI), спроможність визначення аномалій та здатність до адаптації під нові загрози через оновлення бази даних сигнатур та правил.

Задача сканування диску відіграє важливу роль в системі захисту інформації. Програма для сканування диску повинна виявляти потенційні загрози інформаційній безпеці, такі як наявність .bat файлів, які можуть використовуватись для автоматичного виконання потенційно шкідливих операцій.

Аналізуючи вимоги до такої програми, можна виділити наступні основні аспекти:

1. Швидкість сканування: програма повинна мати здатність швидко сканувати великі об'єми даних, що знаходяться на диску. Така здатність забезпечить максимально швидке виявлення потенційних загроз інформаційної безпеки.
2. Точність виявлення: програма повинна мати високий рівень точності при виявленні .bat файлів, мінімізуючи кількість помилкових спрацювань та пропусків.
3. Безпека використання: програма повинна бути безпечною для використання, не вносити змін до файлів на диску під час сканування і не містити шкідливого коду.
4. Простота використання: програма повинна мати зручний інтерфейс та бути легкою у встановленні та налаштуванні.
5. Автоматичний режим роботи: програма повинна мати можливість працювати в автоматичному режимі, виконуючи сканування на заданих інтервалах часу або за подіями, такими як завантаження системи.
6. Ведення логів: програма повинна вести детальні логи своєї роботи, що дає можливість прослідкувати хід сканування і виявлені загрози.

Ці вимоги дозволять створити ефективний інструмент для сканування диску, який допоможе виявляти потенційні загрози інформаційній безпеці, а також забезпечити безпеку інформації від витоку через інформаційні канали.

В ході розгляду завдання розробки засобів захисту інформації були визначені основні вимоги до подібних систем. Це включає надійність, масштабованість, простоту впровадження та управління, високу швидкість обробки, відповідність стандартам та нормативам, гнучкість та спроможність до інтеграції з іншими системами безпеки.

В контексті даної роботи, виходячи з необхідності використання PfSense і Snort, до вимог також було додано глибокий аналіз пакетів, виявлення аномалій і здатність адаптуватися до нових загроз через оновлення бази даних сигнатур та правил.

Сформульовані вимоги стануть основою для детального проектування та розробки системи захисту від витоку інформації в інформаційному каналі.

Додатково, було проведено аналіз вимог до програми для сканування диску, яка є інтегральною частиною комплексної системи захисту. Серед ключових вимог вказано швидкість та точність сканування, безпеку використання, простоту інтерфейсу, автоматичну роботу. Врахування цих вимог дозволить створити ефективний інструмент для виявлення потенційних загроз інформаційній безпеці.

Виконане визначення вимог допоможе забезпечити здатність розробленої системи захисту ефективно виявляти і блокувати потенційні витоки інформації через інформаційні канали.

При виборі методів і засобів розробки засобів захисту від витоку інформаційного каналу було взято до уваги декілька критеріїв.

Перш за все, було необхідно забезпечити найвищий рівень безпеки. В контексті цього завдання, найефективнішими методами є методи глибокого аналізу пакетів і виявлення аномалій. Вони дозволяють виявляти небезпечні активності, які можуть бути приховані в звичайному трафіку, і визначати нові загрози, для яких ще не було розроблено сигнатур.

При виборі засобів розробки було вибрано PfSense і Snort. PfSense було обрано через його широкі можливості як межового маршрутизатора, а також через високу надійність та здатність обробляти великі обсяги трафіку.

Snort було обрано через його високу ефективність у виявленні аномалій та інтрузій на основі глибокого аналізу пакетів. Також важливою є підтримка спільноти

та регулярні оновлення бази даних сигнатур та правил, що дозволяє Snort залишатися актуальним у виявленні нових загроз.

Таким чином, вибір PfSense і Snort обґрунтований їх високою ефективністю, надійністю, широкими можливостями, активною підтримкою спільноти та спроможністю адаптуватися до нових загроз.

Проходження трафіку відображено на схемі (рис 2.1)

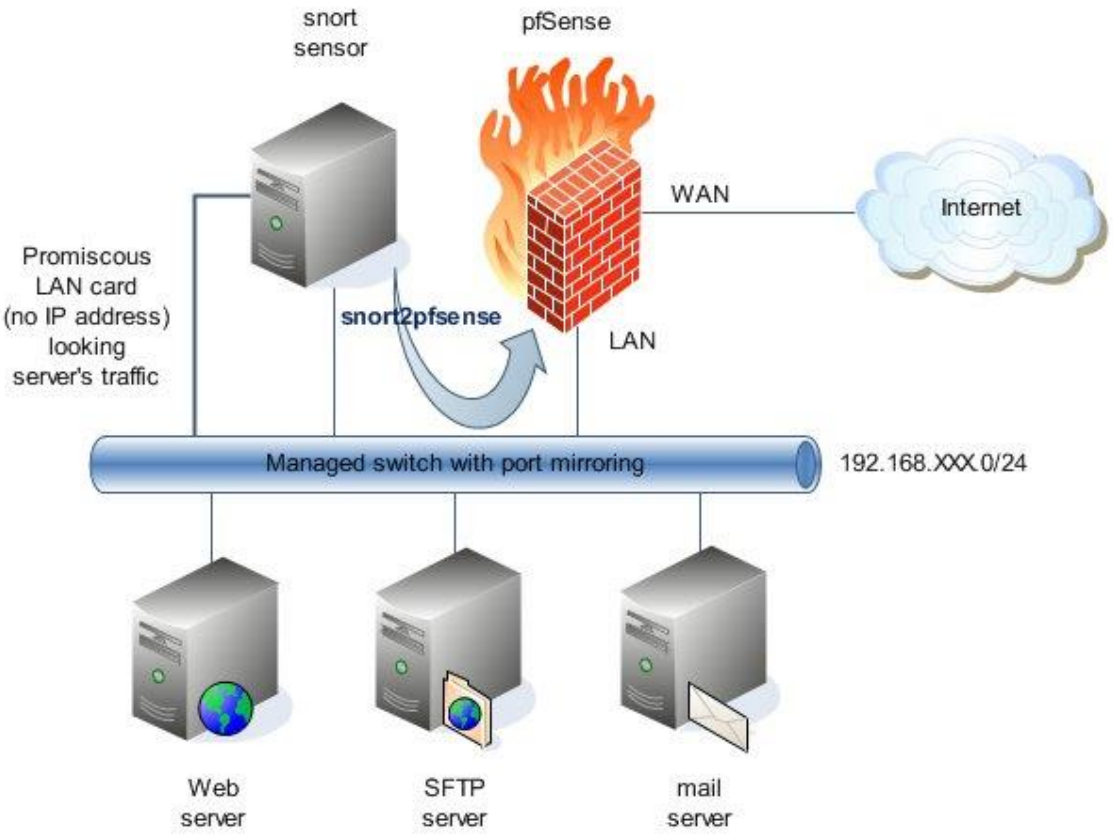

Рис. 2.1. Схема проходження трафіку Pfsense + Snort

Для обґрунтованого вибору засобів тестування на вразливості було враховано декілька ключових параметрів, таких як доступність, деталізація результатів, підтримка спільноти та можливість інтеграції з іншими системами.

На основі цих критеріїв було вибрано GreenBone OpenVAS. OpenVAS стоїть на передовій захисту від витоку інформації, оскільки ця система постійно оновлює свою базу даних вразливостей, що дозволяє швидко виявляти нові потенційні загрози. Крім

того, OpenVAS надає глибокий аналіз результатів сканування, що дозволяє не тільки виявити вразливості, але й розуміти їх природу та вплив на систему.

Також важливим аспектом є відкритий код OpenVAS. Це забезпечує високу гнучкість та адаптивність системи, дозволяючи вносити власні зміни для вдосконалення процесу сканування. Широка підтримка спільноти та регулярні оновлення також є ключовими перевагами OpenVAS.

І, нарешті, OpenVAS може легко інтегруватися з PfSense і Snort, що дозволяє створити єдину систему захисту від витоку інформації.

Таким чином, обрано GreenBone OpenVAS як основний інструмент тестування на вразливості через його високу ефективність, глибоку деталізацію результатів, активну підтримку спільноти та можливість інтеграції з обраними програмними засобами розробки.

При виборі технологій для розробки програми слід враховувати декілька ключових факторів, включаючи вимоги до проекту, доступні ресурси, та досвід команди. Для даної програми, що сканує диск на наявність файлів певного формату і пропонує видалити їх, було вирішено використовувати Python як основну технологію.

Python був обраний з декількох причин. По-перше, Python має багатий набір стандартних бібліотек, які підтримують широкий спектр завдань, включаючи взаємодію з файловою системою. Зокрема, модуль **os** надає ряд корисних функцій для роботи з файлами та директоріями, які були використані у цій програмі.

По-друге, Python відомий своєю простотою і читабельністю, що сприяє швидкому розробуванню та легкому супроводу програми. Код Python легко розуміти, навіть для людей, які не є експертами в Python, що робить його відмінним вибором для невеликих до середніх проектів, таких як цей.

По-третє, Python є крос-платформеною мовою програмування, що означає, що програма, написана на Python, може бути запущена на різних операційних системах без внесення значних змін до коду. Це забезпечує гнучкість при розгортанні програми.

Додатково, для створення виконуваного файлу (**.exe**) була використана утиліта PyInstaller. Вона дозволяє згенерувати стенд-алон виконуваний файл з Python

програми, що полегшує розповсюдження та використання програми кінцевими користувачами, незалежно від того, чи встановлено у них Python.

Разом із використанням Python для розробки коду програми, для логування було використано модуль **logging** Python. Цей модуль надає гнучкі можливості для запису подій під час роботи програми, що є важливим для забезпечення прозорості та можливості відстежувати дії програми.

Отже, вибір Python та супутніх технологій для розробки цієї програми було обґрунтовано потребами проекту, простотою використання та розповсюдженістю цих технологій.

2.2. Розроблення схеми адресації та іменування пристроїв мережі

У цьому розділі курсової роботи описано процес налаштування маршрутизації між VLAN у мережі. Було створено чотири VLAN: VLAN1 для мережі управління, VLAN2 для мережі співробітників, VLAN3 для гостьової мережі, та VLAN4 для серверної мережі. Це дозволить забезпечити ефективне управління трафіком та забезпечення безпеки в мережевій інфраструктурі.

Для забезпечення комунікації між цими VLAN була налаштована таблиця маршрутизації на маршрутизаторі (Таблиця 2.1). Це дозволило хостам у всіх чотирьох VLAN взаємодіяти один з одним.

Для реалізації маршрутизації між VLAN необхідно було створити SVI-інтерфейси на маршрутизаторі. Інтерфейс SVI є логічним інтерфейсом, який забезпечує підключення до VLAN. Процес створення SVI інтерфейсів включав присвоєння IP-адрес та масок підмереж. Наприклад, для VLAN1 було призначено IP-адресу 172.16.6.1 з маскою підмережі 255.255.255.128.

Після налаштування IP-адрес, було включено маршрутизацію на інтерфейсах SVI. Потім хости були підключені до портів, призначених для відповідних VLAN. Таким чином, було забезпечено можливість взаємодії між різними VLAN через маршрутизатор.

Для перевірки налаштованої маршрутизації між VLAN були проведені тести з використанням команди ping на хостах, розташованих в різних VLAN. Успішний

обмін пакетами ping між хостами різних VLAN підтвердив правильність налаштувань маршрутизації.

Крім того, було наведено детальний опис налаштування маршрутизації між VLAN на маршрутизаторі Cisco (Таблиця 2.2). Ця інформація включала команди для входу в режими конфігурації, налаштування імені пристрою, присвоєння IP-адрес інтерфейсам VLAN, налаштування фізичних інтерфейсів на режим trunk, а також увімкнення IP-маршрутизації на маршрутизаторі.

Наступним етапом є налаштування міжмережевого екрана ASA5506, деталі якого наведено в Додатку А.

У цьому розділі ми налаштуємо маршрутизацію між VLAN у нашій мережі. Ми створимо чотири VLAN: VLAN1, VLAN2, VLAN3 і VLAN4. VLAN1 буде призначено для мережі управління, VLAN2 - для мережі співробітників, VLAN3 - для гостьової мережі, а VLAN4 - для серверної мережі.

Ми налаштуємо таблицю маршрутизації на нашому маршрутизаторі.

Таблиця 2.1.

Таблиця маршрутизації

Мережа призначення	Мережа наступного переходу
172.16.6.0/26	172.16.5.2
172.16.7.0/25	172.16.5.2

Ця таблиця маршрутизації дозволить хостам у всіх чотирьох VLAN взаємодіяти один з одним.

Щоб налаштувати маршрутизацію між VLAN, нам потрібно створити SVI-інтерфейси на нашому маршрутизаторі. Інтерфейс SVI - це логічний інтерфейс, який дозволяє нам підключатися до VLAN.

Для створення SVI інтерфейсу ми скористаємося наступною командою:

interface vlan <vlan-id>

Щоб створити SVI інтерфейс для VLAN1, ми використаємо наступну команду:

interface vlan 1

Після того, як ми створили SVI інтерфейс, ми можемо призначити йому IP-адресу і маску підмережі. Для цього ми скористаємося наступними командами:

ip address <ip-адреса> <маска підмережі>

Щоб призначити IP-адресу 172.16.6.1 і маску підмережі 255.255.255.128 інтерфейсу SVI для VLAN1, ми використаємо такі команди:

ip address 172.16.6.1 255.255.255.128

Після того, як ми призначили IP-адресу інтерфейсу SVI, ми можемо включити маршрутизацію на інтерфейсі. Для цього скористаємося наступною командою:

ip routing

Після того, як ми включили маршрутизацію на інтерфейсі SVI, ми можемо підключити хости до VLAN. Для цього нам потрібно підключити хости до портів, призначених для VLAN.

Після того, як ми підключили хости до VLAN, ми можемо протестувати маршрутизацію між VLAN. Для цього ми можемо виконати команду ping на хостах в інших VLAN.

Якщо ми зможемо пінгувати хости в інших VLAN, то ми успішно налаштували маршрутизацію між VLAN.

Таблиця 2.2.

Налаштування маршрутизації між VLAN на маршрутизаторі Cisco.

Команда	**Опис**
Router>enable	Увійти в підвищений режим доступу
Router#configure terminal	Увійти в режим конфігурації
Router(config)#hostname R1	Встановити ім'я пристрою "R1"

Продовження табл. 2.2.

Router(config)#interface vlan 1	Увійти в налаштування інтерфейсу VLAN 1
Router(config-if)#ip address 172.16.6.1 255.255.255.128	Назначити IP-адресу 172.16.6.1 з маскою підмережі 255.255.255.128 для інтерфейсу VLAN 1
Router(config-if)#no shutdown	Увімкнути інтерфейс VLAN 1
Router(config)#interface fa0/0	Увійти в налаштування інтерфейсу FastEthernet 0/0
Router(config-if)#switchport mode trunk	Налаштувати режим комутації порту на "trunk"

Router(config-if)#switchport allowed vlan 1,2,3,4	Дозволити проходження пакетів VLAN 1, 2, 3 і 4 через порт
Router(config-if)#no shutdown	Увімкнути інтерфейс FastEthernet 0/0
Router(config)#ip routing	Увімкнути IP-маршрутизацію на маршрутизаторі
Router(config)#exit	Вийти з режиму конфігурації

Ми створили інтерфейс SVI для VLAN1 і призначили йому IP-адресу 172.16.6.1. Ми також увімкнули маршрутизацію на інтерфейсі. Потім ми підключили інтерфейс до фізичного інтерфейсу (fa0/0) і налаштували фізичний інтерфейс на пропуск трафіку для VLAN 1, 2, 3 і 4.

Після того, як ми налаштували маршрутизатор, можемо протестувати маршрутизацію.

Тепер налаштуємо міжмережевий екран ASA5506. Налаштування і опис наведено в Додатку А.

2.3. Вибір активного та пасивного мережевого обладнання

При використанні PfSense та Snort важливо враховувати вимоги до апаратного забезпечення. Для встановлення та надійної роботи цих систем потрібно:

1. **Процесор**. Процесор зі швидкістю 2.0 GHz або більше, який підтримує 64-бітну архітектуру. Для високонавантажених систем рекомендується використовувати багатоядерні процесори.
2. **Оперативна пам'ять**. PfSense вимагає мінімум 1 ГБ RAM, але для оптимальної роботи IDS та для обробки великого обсягу трафіку рекомендується мінімум 4 ГБ RAM.
3. **Місце для зберігання даних**. Від 20 ГБ та вище. SSD рекомендується для забезпечення швидкого доступу до лог-файлів і даних системи IDS.
4. **Мережеві адаптери**. Двопортовий або багатопортовий мережевий інтерфейс для підключення до внутрішньої та зовнішньої мережі.
5. **Мережевий комутатор та маршрутизатор**. Вони використовуються для управління мережевим трафіком та сполученням між різними підмережами.

Усе вищевказане апаратне забезпечення потрібне для встановлення та ефективної роботи PfSense та Snort. При виборі конкретного апаратного забезпечення важливо враховувати навантаження на мережу, обсяг трафіку та бюджет на апаратне забезпечення.

Розглянемо сервер Dell PowerEdge R640 як потенційне апаратне рішення для встановлення системи PfSense та Snort. Цей сервер відповідає вищезгаданим вимогам і забезпечує високу продуктивність для обробки мережевого трафіку.

Таблиця 2.3.

Характеристики серверу Dell PowerEdge R640

Характеристика	**Значення**
Процесор	2x Intel Xeon Gold 6230R, 2.1 GHz, 26 cores
Оперативна пам'ять	64 ГБ DDR4 ECC
Місце для зберігання даних	2x 1 ТБ SSD RAID
Мережеві адаптери	4x 1GbE Ethernet Ports
Додаткові порти	1x iDRAC9 Enterprise, 1x VGA, 2x USB 3.0

Цей сервер може підтримувати великий обсяг мережевого трафіку та дозволяє зберігати велику кількість лог-файлів та інших даних, що збираються системами PfSense та Snort. Крім того, він має потужні процесори, які забезпечують швидку обробку даних та відповідність навантаженню на систему.

Продовжуючи розділ про вибір активного та пасивного мережевого обладнання, особливу увагу слід звернути на вибір мережевого комутатора. Мережевий комутатор є ключовим компонентом інформаційної мережі навчального закладу, відіграючи роль у розподілі трафіку та забезпеченні ефективності роботи мережі.

При виборі мережевого комутатора важливо враховувати наступні параметри:

1. **Кількість та тип портів.** Залежно від розміру мережі та кількості підключених пристроїв, важливо обрати комутатор із достатньою кількістю портів.

Також, слід звертати увагу на тип портів (наприклад, Ethernet, Gigabit Ethernet, або 10-Gigabit Ethernet), що впливає на швидкість передачі даних.

2. **Швидкість та пропускна здатність.** Комутатор повинен забезпечувати високу швидкість передачі даних, а також мати достатню пропускну здатність для обробки всього трафіку, що проходить через нього.

3. **Підтримка PoE (Power over Ethernet).** Ця функція дозволяє передавати електроживлення по тому ж кабелю, що й дані, що є зручним для підключення IP-камер, Wi-Fi точок доступу, та інших пристроїв.

4. **Управління та конфігурація.** Наявність інтуїтивно зрозумілого інтерфейсу для управління та конфігурації дозволяє легко налаштовувати та моніторити роботу мережі.

5. **Безпека.** Належні функції безпеки, такі як фільтрація трафіку, захист від шкідливих атак, та інші засоби безпеки є важливими для забезпечення надійності та безпеки мережі.

6. **Масштабованість та майбутнє розширення.** Комутатор має бути готовим до масштабування та розширення мережі, щоб відповідати зростаючим потребам навчального закладу.

Беручи до уваги вищевказані параметри, для нашого навчального закладу рекомендовано вибрати комутатор, який відповідає сучасним стандартам швидкості та безпеки, має гнучкі можливості управління та високий рівень пропускної здатності.

Таблиця 2.4.

Характеристики рекомендованого мережевого комутатора

Характеристика	**Значення**
Кількість портів	48x Gigabit Ethernet Ports
Пропускна здатність	176 Gbps
PoE підтримка	Так, PoE+
Управління	Інтуїтивний веб-інтерфейс
Безпека	Фільтрація трафіку, захист від атак
Масштабованість	Підтримка декількох модулів для розширення

Цей комутатор забезпечить високу продуктивність та безпеку мережі, відповідаючи потребам сучасного навчального закладу.

У контексті вибору мережевого комутатора для інформаційної мережі навчального закладу, особливу увагу заслуговує комутатор Cisco Catalyst 9300. Цей комутатор відомий своєю надійністю, високою продуктивністю та гнучкістю конфігурації, що робить його ідеальним вибором для освітніх установ.

Cisco Catalyst 9300 підходить для наших потреб з кількох причин. Перш за все, він пропонує високу пропускну здатність, що є критично важливим для підтримки зростаючого обсягу мережевого трафіку в навчальних закладах, де велика кількість студентів та персоналу одночасно використовують мережеві ресурси.

Крім того, серія Catalyst 9300 підтримує технологію Power over Ethernet (PoE), яка дозволяє передавати електроенергію через мережевий кабель, спрощуючи розгортання бездротових точок доступу, IP-камер та інших пристроїв. Ця функція є важливою для сучасних навчальних закладів, які все більше використовують технології для навчання та безпеки.

Безпека також є ключовою характеристикою комутатора Cisco Catalyst 9300. Він оснащений розширеними функціями безпеки, які допомагають захистити мережу від зовнішніх загроз та атак. Особливо важливим є це в освітньому середовищі, де безпека даних є важливим пріоритетом.

Щодо гнучкості та масштабованості, Cisco Catalyst 9300 підтримує різні модулі та конфігурації, що дозволяє легко адаптувати комутатор до змінюваних потреб навчального закладу. Це означає, що інвестиція в такий комутатор є довгостроковою, оскільки він може бути налаштований або розширений відповідно до майбутніх потреб.

Окрім технічних переваг, вибір Cisco також обумовлений їхньою відмінною репутацією у галузі підтримки клієнтів та надійності обладнання. Це забезпечує додаткову впевненість у тому, що мережеве обладнання буде функціонувати безперебійно і ефективно.

Отже, враховуючи вищезазначені фактори, Cisco Catalyst 9300 є оптимальним вибором для нашої навчальної мережі, як з точки зору технічних характеристик, так і з точки зору надійності та підтримки з боку виробника.

У контексті вибору мережевого обладнання для інформаційної мережі навчального закладу, надзвичайно важливим аспектом є забезпечення резервування та надійності системи. Це передбачає розробку комплексного підходу, що включає в себе як апаратне, так і програмне забезпечення для максимально ефективного використання мережевих ресурсів та запобігання можливим збоям у роботі.

Резервування в мережевих системах означає створення дублюючих елементів, таких як додаткові комутатори, сервери або з'єднання, що дозволяють системі продовжувати працювати навіть у випадку виходу з ладу одного з компонентів. Це не тільки зменшує ризик втрати даних та час простою, але й підвищує загальну продуктивність мережі.

Основою надійності мережевої системи є ретельний розрахунок її безвідмовності. Це включає в себе аналіз середнього часу між збоями (MTBF) та середнього часу відновлення системи після збою (MTTR). Такий аналіз дозволяє визначити потенційні слабкі місця в мережевій інфраструктурі та розробити стратегії їх усунення або мінімізації впливу на загальну роботу системи.

Стратегії резервування варіюються від простого дублювання ключових компонентів до складних схем розподілу навантаження та автоматичного переключення на резервні системи. У випадку мережевих комутаторів, наприклад, можна використовувати редундантні моделі з подвійним живленням, які забезпечують безперебійну роботу навіть при відмові одного з блоків живлення.

Важливим аспектом є також масштабованість системи. Обладнання та програмне забезпечення повинні бути готові до можливого розширення мережі, забезпечуючи при цьому високий рівень надійності. Це означає, що комутатори та інші компоненти мережі повинні бути здатні адаптуватися до збільшення обсягу даних та кількості користувачів без зниження продуктивності.

Тестування та моніторинг системи відіграють ключову роль у підтримці її надійності. Регулярне тестування резервних систем, моніторинг продуктивності та

аналіз логів дозволяють своєчасно виявляти потенційні проблеми та вживати заходів до їх усунення.

Отже, забезпечення високого рівня резервування та надійності системи є необхідною умовою для створення ефективної та стабільної мережевої інфраструктури в навчальному закладі. Це передбачає ретельний вибір обладнання, планування масштабованості та забезпечення постійного моніторингу та оновлення системи.

2.4. Проектування фізичного розміщення обладнання та прокладання кабелів

Проектування фізичного розміщення обладнання та прокладання кабелів є критично важливим для забезпечення ефективної роботи мережі навчального закладу. Цей процес включає ретельне планування розташування мережевого обладнання, такого як сервери, комутатори, маршрутизатори, а також прокладання мережевих кабелів для з'єднання цих пристроїв.

Передусім, важливо визначити оптимальне місце для розміщення серверної кімнати, яка має бути централізовано розташована відносно всіх користувачів мережі. Це місце повинно бути безпечним, з хорошими умовами охолодження та з достатнім простором для розміщення усього необхідного обладнання. Також, потрібно передбачити можливість легкого доступу для технічного обслуговування та розширення мережі.

Далі, планування прокладання кабелів вимагає розуміння загальної архітектури будівлі та розташування класних кімнат, лабораторій, адміністративних приміщень та інших місць, які будуть підключені до мережі. При прокладанні кабелів слід звернути увагу на мінімізацію перешкод та забезпечення достатньої гнучкості для майбутніх модифікацій мережевої інфраструктури.

Важливо також підійти до вибору типу кабелю. Наприклад, використання кабелів категорії 6 або вище є доцільним для забезпечення високошвидкісної передачі даних. При прокладанні кабелів слід дотримуватися відповідних стандартів та

регуляцій, уникати впливу електромагнітних перешкод, а також забезпечити належну маркування та організацію кабелів.

Процес прокладання кабелів також повинен включати ретельне планування маршрутів кабелів, їх довжини, а також точки входу та виходу в кожному приміщенні. Це допоможе уникнути зайвих згинів та перетягувань кабелів, що може привести до їх пошкодження.

Загалом, ефективне проектування фізичного розміщення обладнання та прокладання кабелів забезпечить стабільну та високопродуктивну роботу мережі, а також спростить подальше обслуговування та розширення мережевої інфраструктури.

Таблиця 2.5.

Орієнтовний план розміщення мережевого обладнання та прокладання кабелів

Номер	**Опис**	**Розташування**	**Тип Кабелю**	**Довжина Кабелю**
1	Серверна кімната	Центральна частина будівлі	-	-
2	Кабель до адміністративних приміщень	Із серверної кімнати до адміністративних кабінетів	Cat 6	30 м
3	Кабель до класних кімнат	Із серверної кімнати до класних кімнат	Cat 6	50 м
4	Кабель до лабораторій	Із серверної кімнати до лабораторій	Cat 6	40 м
5	Кабель до бібліотеки	Із серверної кімнати до бібліотеки	Cat 6	25 м

Продовжуючи тему проектування фізичного розміщення обладнання та прокладання кабелів, важливо також розглянути вибір оптоволоконних кабелів для певних сегментів мережі. Оптоволоконні кабелі пропонують низку переваг перед традиційними мідними кабелями, особливо коли мова йде про високошвидкісну передачу даних на довгі відстані та в умовах високого обсягу мережевого трафіку.

Однією з ключових переваг оптоволокна є його висока пропускна здатність. Воно здатне передавати значно більші обсяги даних на більші відстані, ніж традиційні

мідні кабелі, без втрати сигналу. Це робить оптоволокно ідеальним вибором для з'єднання між різними будівлями навчального закладу або для створення "хребта" мережі, який забезпечує основні магістральні з'єднання.

Ще одна важлива перевага оптоволокна – це його імунітет до електромагнітних перешкод. В умовах навчального закладу, де може бути багато джерел електромагнітних перешкод, таких як лабораторне обладнання, оптоволокно забезпечує стабільність та надійність мережевого з'єднання.

Крім того, оптоволокно є більш безпечним для передачі даних, оскільки воно менш схильне до прослуховування або втручань. Це особливо важливо для захисту конфіденційної інформації у навчальному закладі.

При виборі оптоволоконних кабелів слід звернути увагу на тип оптоволокна: одномодове (Single Mode) або багатомодове (Multi-Mode). Одномодове оптоволокно ідеально підходить для довгих дистанцій та високої пропускної здатності, в той час як багатомодове оптоволокно частіше використовується для коротших відстаней.

З огляду на вищевказані переваги, включення оптоволоконних кабелів у проект мережі навчального закладу може значно підвищити загальну продуктивність мережі, забезпечуючи швидке, надійне та безпечне з'єднання між різними сегментами мережі.

Ефективне функціонування мережі в навчальному закладі вимагає ретельно спланованого фізичного розміщення обладнання та прокладання кабелів. Цей процес включає в себе не лише розташування основних елементів, таких як сервери, комутатори та маршрутизатори, але й розгляд оптимальних шляхів для мережевих кабелів, що забезпечують з'єднання між цими пристроями.

Основою проектування є визначення місця для серверної кімнати. Ідеально, вона має бути централізовано розташована відносно всіх користувачів мережі, забезпечуючи безпеку, ефективне охолодження та достатній простір для обладнання. Крім того, доступ до серверної кімнати має бути зручним для технічного обслуговування та потенційного розширення мережі.

Прокладання кабелів вимагає ретельного планування, зважаючи на архітектуру будівлі та розташування приміщень, які будуть підключені до мережі, включаючи класні кімнати, лабораторії, адміністративні кабінети та інші важливі локації.

Важливо вибирати правильний тип кабелю, наприклад, кабелі категорії 6 або вище, для забезпечення високошвидкісної передачі даних. При цьому слід уникати електромагнітних перешкод, забезпечити належне маркування кабелів та організацію їх прокладання.

Для максимальної ефективності та безпечності передачі даних варто розглянути використання оптоволоконних кабелів, особливо для магістральних з'єднань та з'єднань на довгі відстані. Оптоволокно пропонує високу пропускну здатність, імунітет до електромагнітних перешкод та підвищену безпеку даних. При виборі оптоволокна важливо визначити потребу в одномодовому або багатомодовому оптоволокні, виходячи з відстаней та обсягів передачі даних.

Загальна схема мережі та її логічна структура є ключовими для розуміння потреб користувачів та забезпечення ефективного мережевого зв'язку. Ця схема повинна відображати розташування серверної кімнати, маршрути кабельних ліній, розташування кінцевих точок доступу та інші важливі аспекти інфраструктури.

Також необхідно розглянути різні групи користувачів мережі, включаючи адміністративний персонал, викладачів, студентів та технічний персонал. Кожна з цих груп має свої унікальні потреби та вимоги до мережі, які слід враховувати при проектуванні.

В підсумку, ретельне проектування фізичного розміщення обладнання та прокладання кабелів є вирішальним для створення стабільної, ефективної та масштабованої мережевої інфраструктури. Це не лише сприятиме надійній роботі мережі, але й полегшить подальше обслуговування та розширення мережі.

Важливим аспектом створення ефективної мережі навчального закладу є проектування фізичного розміщення обладнання та прокладання кабелів. Цей процес має на меті створення структурованої та оптимізованої мережевої інфраструктури, яка забезпечує надійне та швидке з'єднання між різними елементами мережі.

Загальна схема мережі та її логічна структура

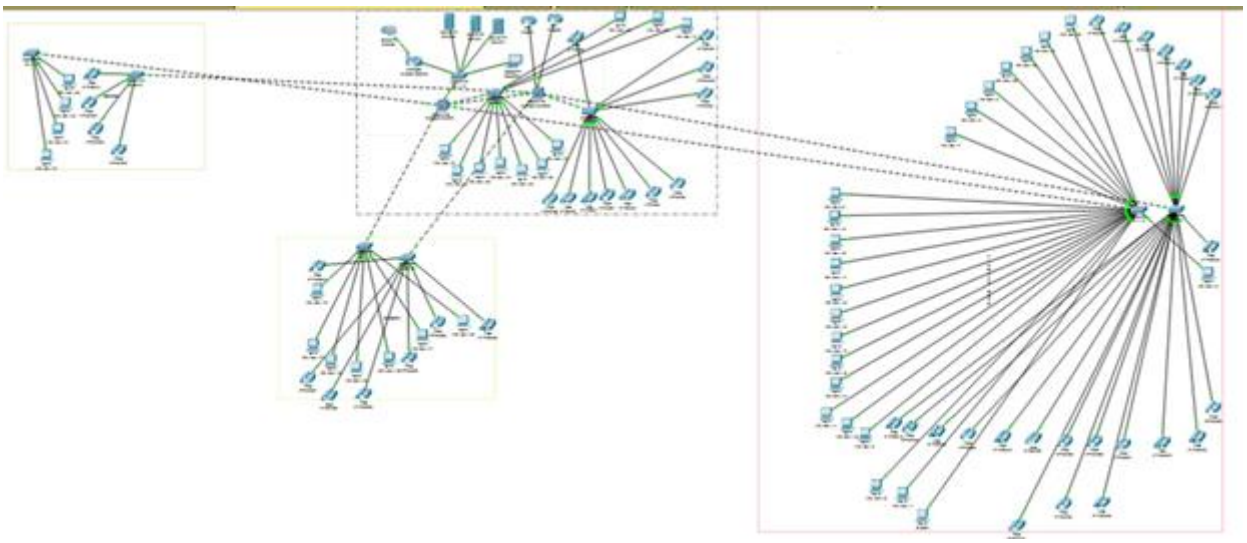

Рис. 2.2. Зображення загальної схеми мережі

Логічна структура мережі включає кілька ключових елементів:

- **серверна кімната**. Центральний вузол мережі, де розташовуються основні сервери та мережеве обладнання;
- **кабельна інфраструктура**. Прокладання кабелів від серверної кімнати до різних локацій, включаючи класні кімнати, лабораторії, адміністративні та громадські простори;
- **кінцеві точки доступу**. Місця підключення користувачів та пристроїв, включаючи робочі станції, Wi-Fi точки доступу та інше обладнання.

Групи користувачів мережі навчального закладу можна поділити на кілька основних категорій:

1. **Адміністративний персонал**. Ця група включає керівників закладу, секретаріат, обліковий відділ та інших співробітників, які використовують мережу для управлінських та адміністративних завдань;
2. **Викладачі та науковці**. Використовують мережу для підготовки та проведення лекцій, наукових досліджень та спілкування зі студентами;
3. **Студенти**. Основні користувачі мережі, які використовують її для навчання, досліджень та комунікації;
4. **Технічний персонал**. Відповідають за підтримку та обслуговування мережевої інфраструктури.

РОЗДІЛ 3
НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ

3.1. Налаштування мережевих пристроїв і сервісів

PfSense є вільним і відкритим мережевим маршрутизатором, який оснований на потужному ядрі FreeBSD. Першим кроком є інсталяція PfSense на відповідний апаратний засіб.

Перший етап – звернення до порталу завантаження PfSense, де потрібно знайти найновішу версію брандмауеру PfSense.

Обравши архітектуру програмного забезпечення PfSense, виберіть формат установника ISO та натисніть кнопку Завантажити (рис. 3.1).

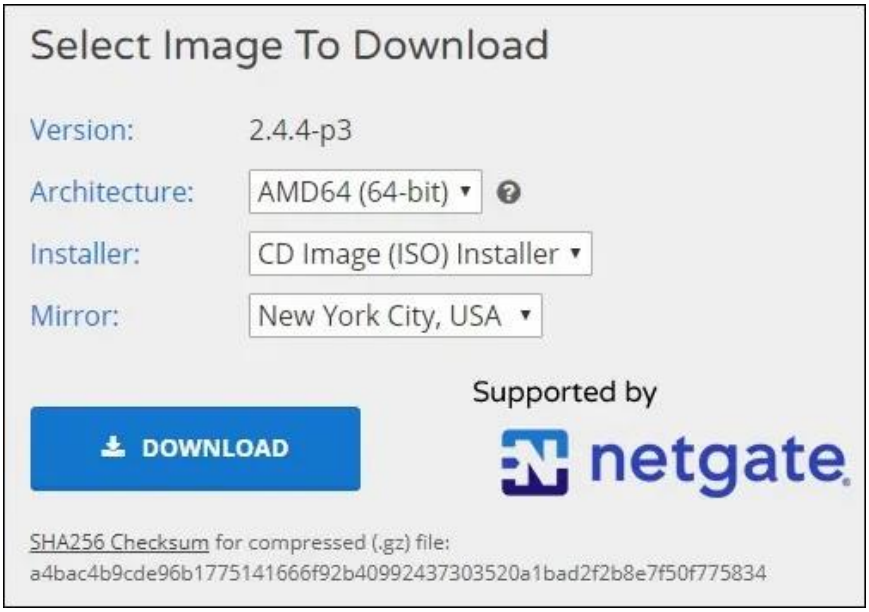

Рис. 3.1. Завантаження образу PfSense

ISO-образ стиснуто за допомогою розширення GZ.

Нам знадобиться програмне забезпечення, наприклад, 7zip, щоб видобути ISO-образ з пакета GZ. Далі, завантажуємо0 сервер за допомогою установочного носія PfSense.

На екрані вітання натискаємо Enter, щоб розпочати процес установки PfSense (рис. 3.2).

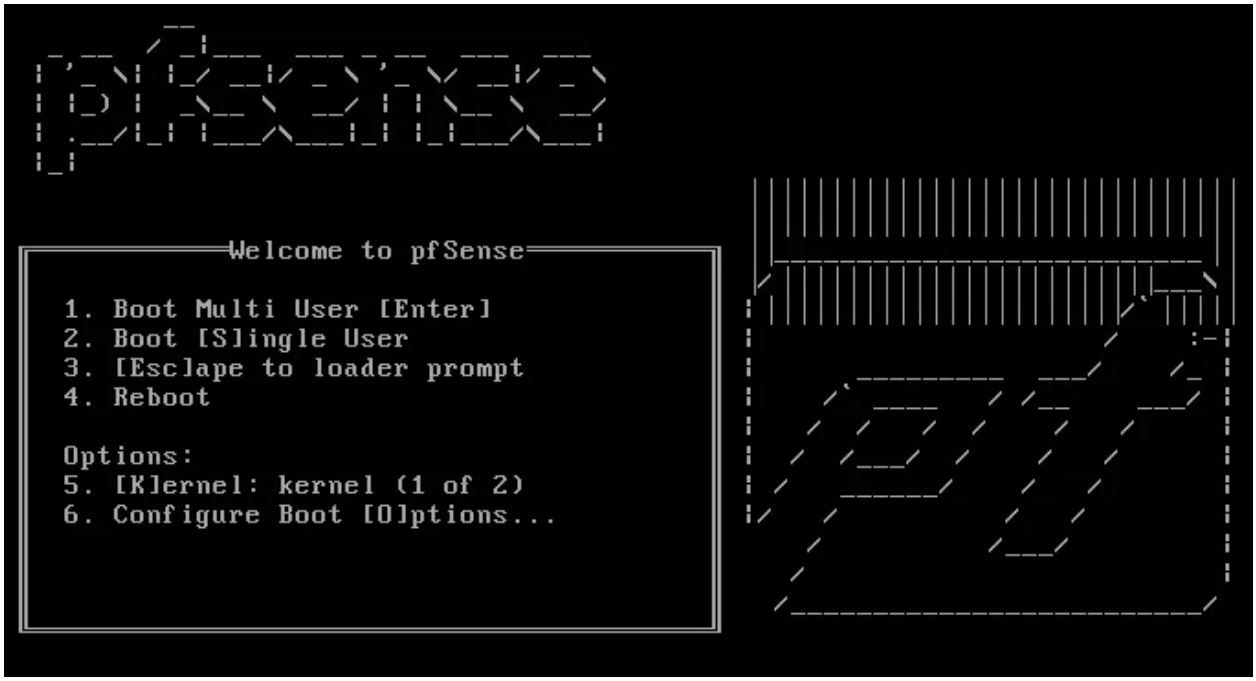

Рис. 3.2. Екран вітання PfSense

Приймаємо умови ліцензійної угоди з кінцевим користувачем PfSense (рис. 3.3).

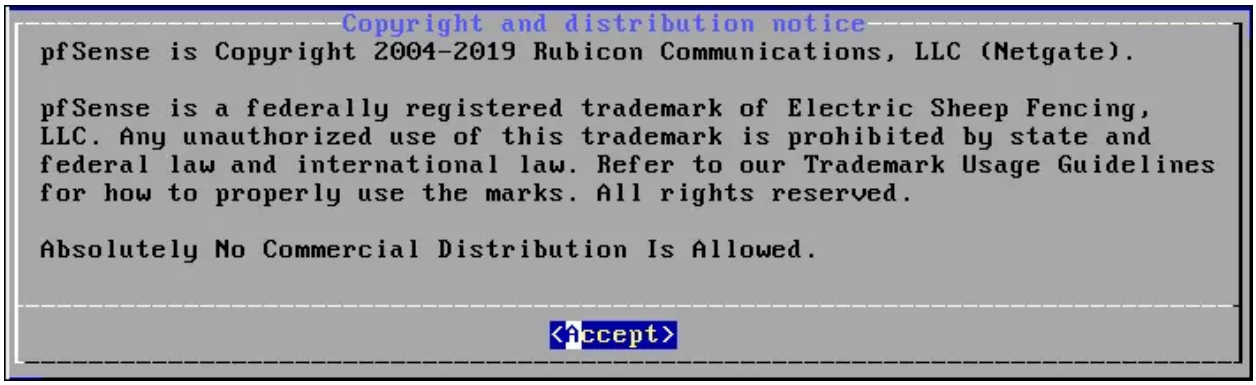

Рис. 3.3. Умови ліцензійної угоди PfSense

Вибираємо потрібну розкладку клавіатури PfSense (рис. 3.4).

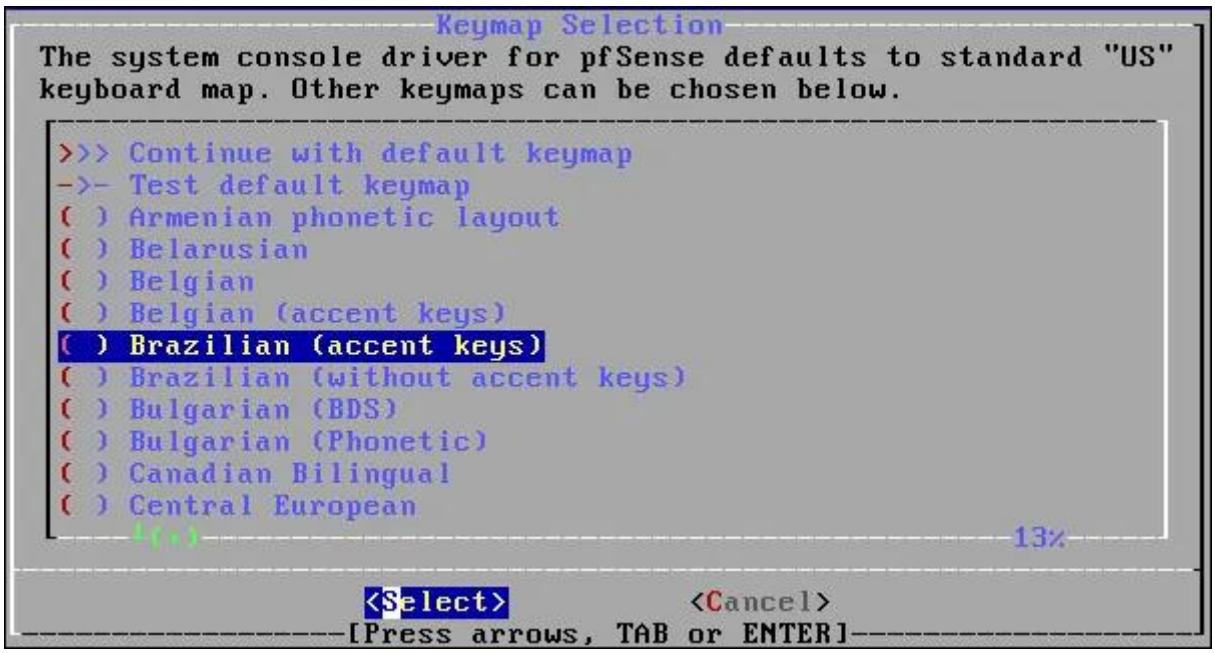

Рис. 3.4. Вибір розкладки

Вибираємо параметр Auto(UFS), щоб автоматично виконати розбиття диска на розділи (рис. 3.5).

Рис. 3.5. Вибір розмітки диска

Система запустить установку сервера PfSense (рис. 3.6).

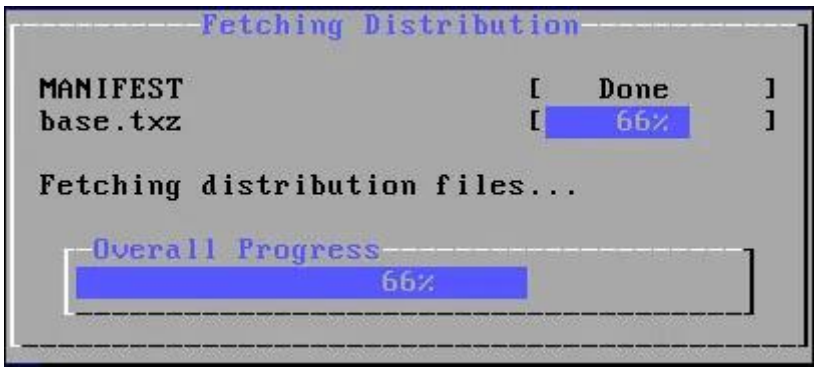

Рис. 3.6. Установка PfSense

Чекаємо, доки установка завершиться.

Вибираємо параметр Ні на екрані ручного налаштування (рис. 3.7).

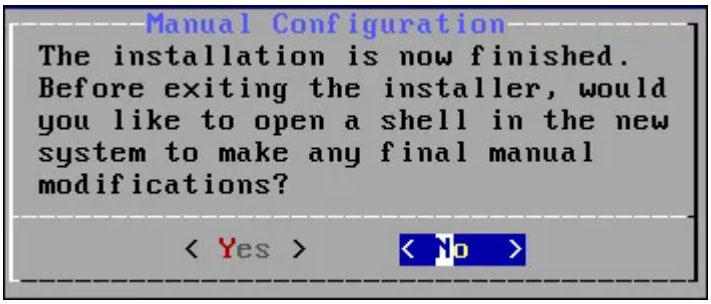

Рис. 3.7. Вибір ручної/автоматичної конфігурації PfSense

Виймаємо установочний носій і натискаємо Enter, щоб перезавантажити сервер (рис. 3.8).

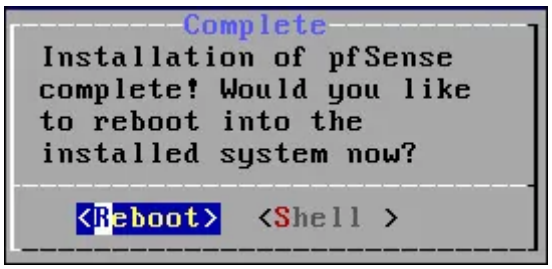

Рис. 3.8. Запит перезавантаження після встановлення

Після перезавантаження консоль PfSense запитає, чи потрібно налаштувати віртуальні мережі.

В нашому випадку ми не виконували налаштування Vlan.

Далі система намагатиметься виявити список доступних мережевих інтерфейсів.

Система попросить нас вибрати один інтерфейс як зовнішній інтерфейс (WAN).

У даному випадку ми налаштували інтерфейс em0 як зовнішній.

Система попросить нас вибрати один інтерфейс як внутрішній інтерфейс (LAN).

У варіанті ми налаштували інтерфейс em1 як внутрішній (рис. 3.9).

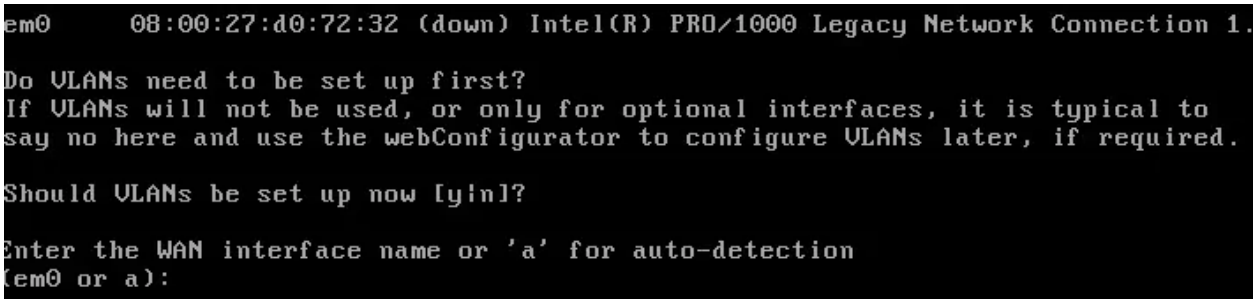

Рис. 3.9. Стартове налаштування Pfsense

Після вибору потрібних мережевих інтерфейсів представлено меню налаштування PfSense (рис. 3.10).

Рис. 3.10. Меню налаштування Pfsense

У нашому випадку мережевий інтерфейс PfSense автоматично отримав IP-адресу 192.168.15.11, так як у нас вже наявний DHCP-сервер в мережі.

Після завершення налаштування IP-адреси ми можемо отримати доступ до веб-інтерфейсу PFsense. Відкриваємо браузер, вводимо IP-адресу брандмауера PfSense і отримуємо доступ до веб-інтерфейсу.

У нашому випадку вводимо наступний URL: https://192.168.15.11

Відкривається веб-інтерфейс PfSense а саме панель авторизації (рис. 3.11).

Рис. 3.11. Панель авторизації Pfsense

На екрані авторизації вводимо інформацію для входу в систему PfSense за замовчуванням.

Ім'я користувача: admin Пароль: pfsense

Після успішного входу, ми перенаправлені на панель моніторинга PfSense.

При першому доступі відображається майстер налаштування PfSense (рис. 3.12).

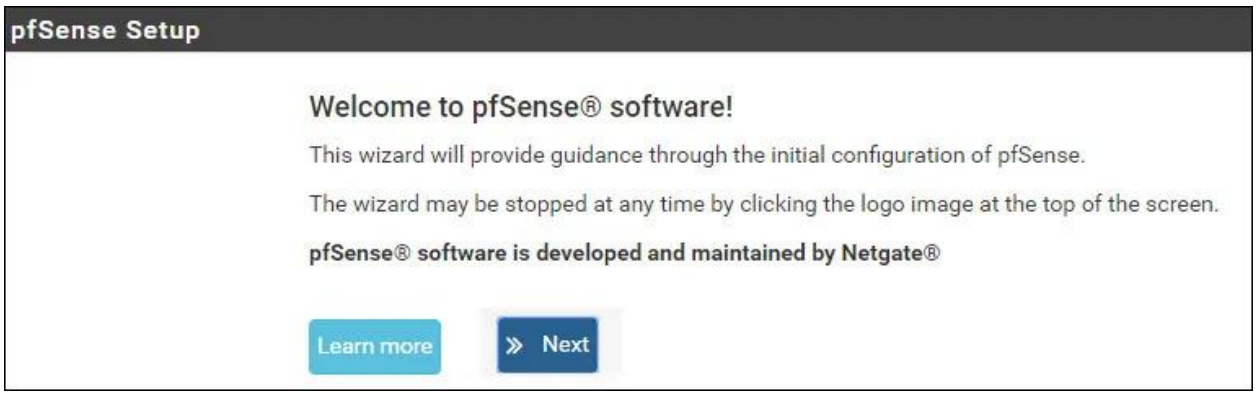

Рис. 3.12. Майстер налаштувань Pfsense

Натискаємо наступну кнопку та виконуємо налаштування імені хоста і DNS (рис. 3.13).

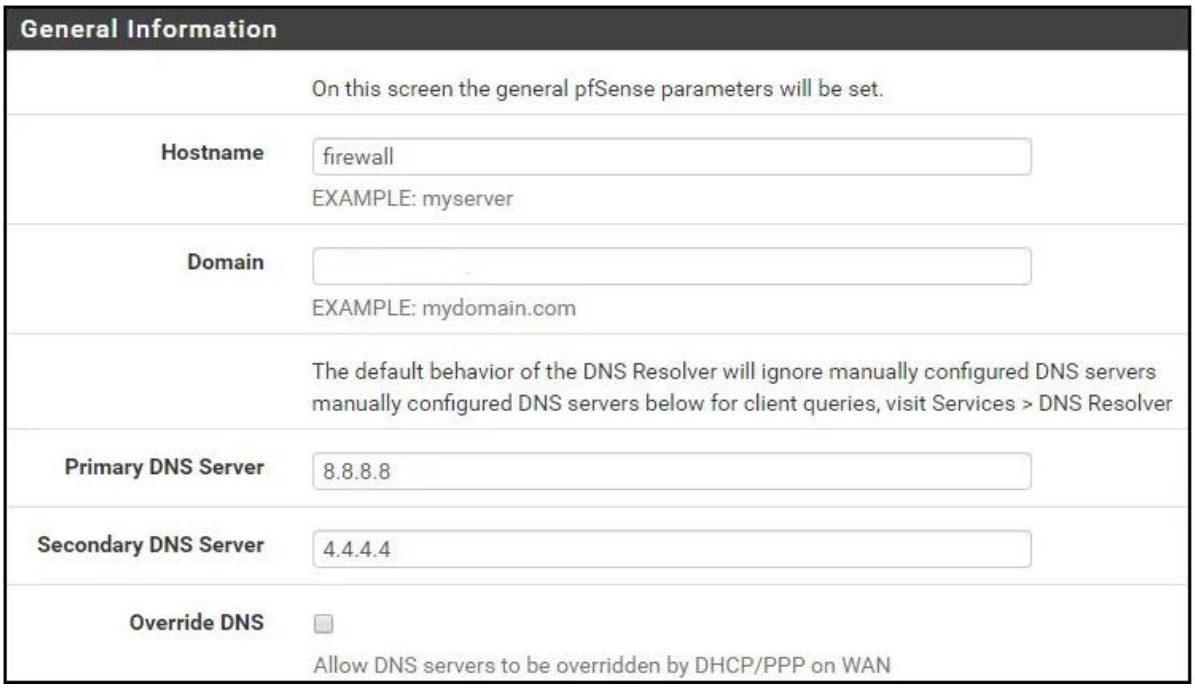

Рис. 3.13. Налаштування DNS та імені хоста Pfsense

Виконуємо налаштування сервера Timezone і NTP (рис. 3.14).

Рис. 3.14. Налаштування сервера Timezone і NTP

На наступному екрані, при необхідності, можна змінити конфігурацію мережевого інтерфейсу. У нашому випадку, ми не внесли жодних змін.

Змінюємо пароль адміністратора PfSense за замовчуванням і натискаємо кнопку Далі (рис. 3.15).

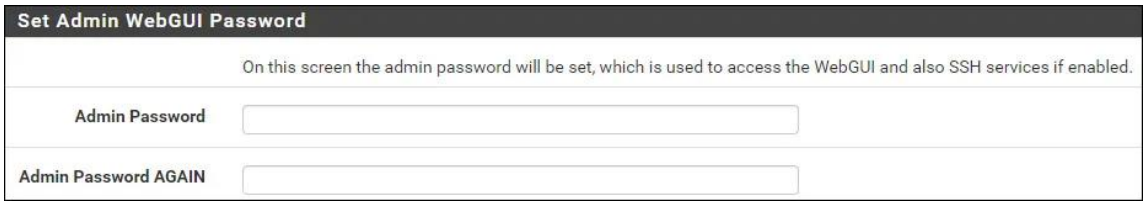

Рис. 3.15. Зміна пароля адміністратора

Система перезавантажує конфігурацію PfSense (рис. 3.16). Установка PfSense була успішно завершена.

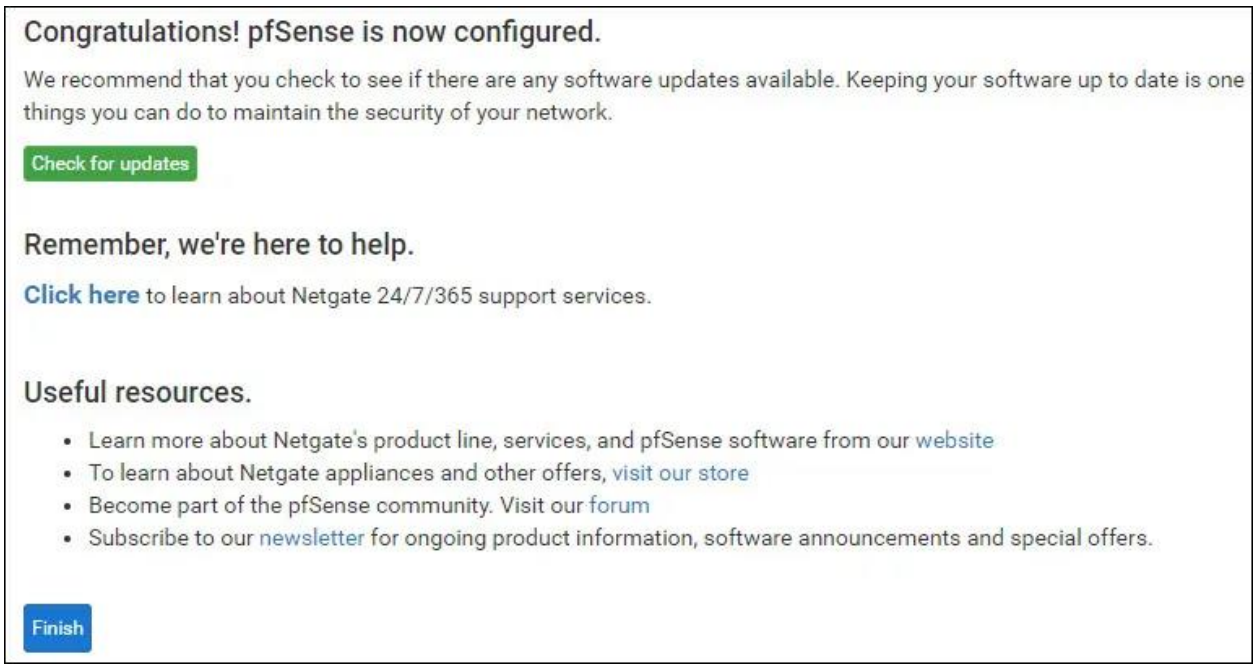

Рис. 3.16. Pfsense успішно встановлено

Після завершення процесу встановлення, можна перейти до налаштування PfSense через веб-інтерфейс (рис. 3.17).

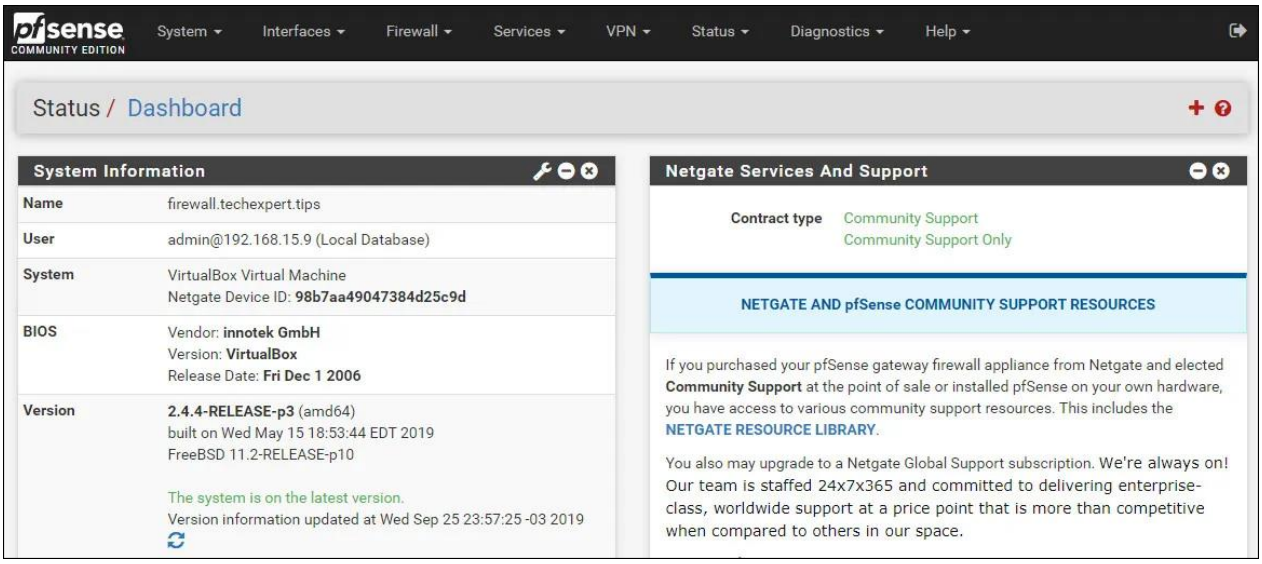

Рис. 3.17. Панель налаштувань і моніторингу Pfsense

Для максимальної безпеки, налаштуємо правила файрволу PfSense, щоб встановити строгий контроль над вхідним та вихідним трафіком. Також налаштуємо VPN для захищеного з'єднання з мережею.

Snort – це система виявлення вторгнень (IDS), яка може бути встановлена на PfSense як плагін. Snort використовує набір правил для аналізу мережевого трафіку і виявлення потенційних загроз.

Входимо в панель керування та моніторингу pfsense: https://192.168.15.30

На екрані авторизації вводим інформацію для входу в систему Pfsense за замовчуванням (рис. 3.18).

- Ім'я користувача: admin;
- Пароль: pfsense.

Рис. 3.18. Панель авторизації Pfsense

Після успішного входу нас перенаправлено на панель моніторинга Pfsense. Переходимо до меню Системи Pfsense та виберіть опцію Менеджер пакетів (рис. 3.19).

Рис. 3.19. Меню системи Pfsense

На екрані менеджера пакетів переходимо на вкладку Доступні пакети. На вкладці Доступні пакети знаходимо та встановлюємо Snort (рис. 3.20).

Рис. 3.20. Менеджер пакетів Pfsense

У нашому прикладі, ми встановили версію пакета Snort 3.2.9.10. Чекаємо завершення встановлення Snort. Переходимо до меню Сервіси Pfsense і вибираємо опцію Snort (рис. 3.21).

Рис. 3.21. Меню сервісів Pfsense

На вкладці Глобальні налаштування знаходимо Правила Snort Subscriber і виконуємо наступні налаштування (рис. 3.22):

- Включаємо Snort VRT – Так;
- Snort Oinkmaster Code – Вводимо наш OikCode.

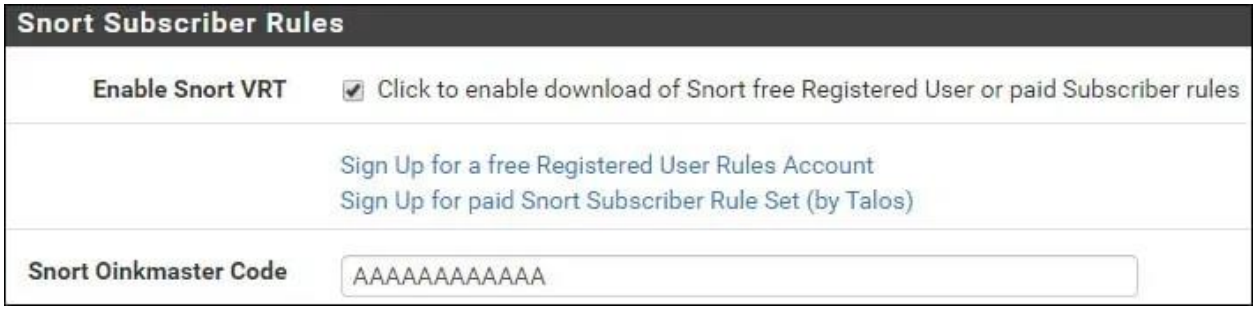

Рис. 3.22. Внесення ключа Snort

Знаходимо область налаштувань оновлення правил і виконайте наступні налаштування:

- Інтервал оновлення – вибираємо бажаний інтервал оновлення;
- Час початку оновлення – встановлюємо бажаний час для оновлення правил Snort.

Знаходимо область Загальні налаштування та виконуємо наступні налаштування (рис. 3.23):

- Інтервал видалення заблокованих хостів – 1 година;
- Видаляємо заблоковані хости після видалення – Ні;
- Зберегти налаштування Snort після видалення – Так;
- Startup/Shutdown LoggingUpdate Interval – ні.

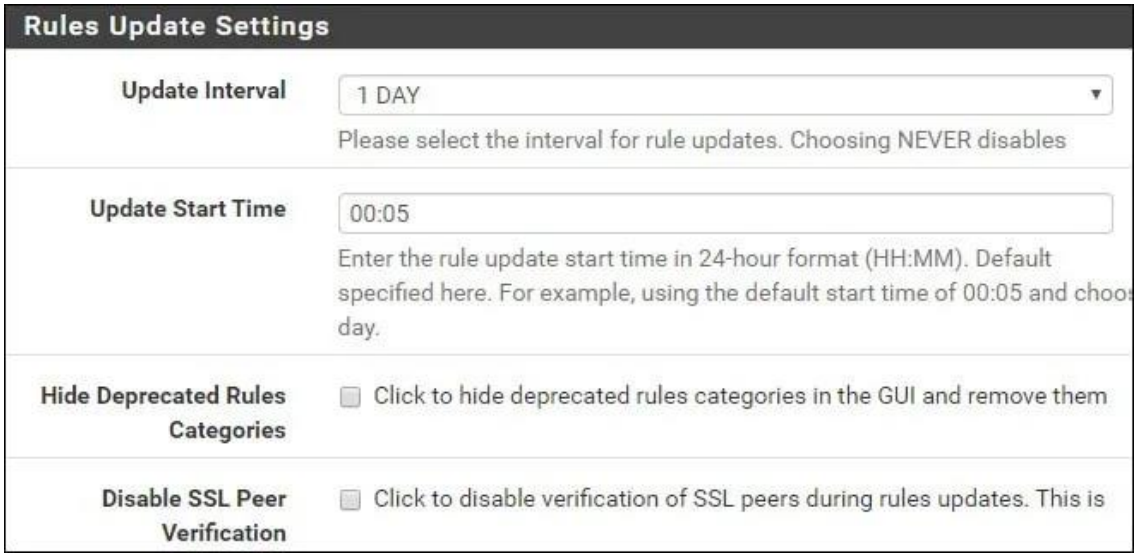

Рис. 3.23. Внесення параметрів автооновлення Snort

На вкладці Оновлення, натискаємо кнопку Оновити правила для завантаження правил Snort (рис. 3.24)

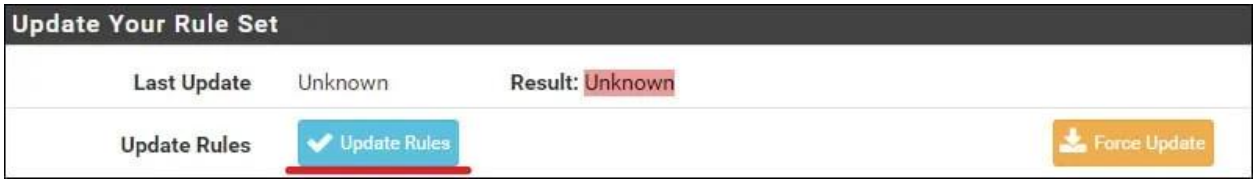

Рис. 3.24. Примусове оновлення Snort

На вкладці Інтерфейси Snort, натискаємо на кнопку Додати та виконуємо наступні налаштування (рис. 3.25):

– Включити – Так;

– Інтерфейс – Вибираємо бажаний інтерфейс для моніторингу.

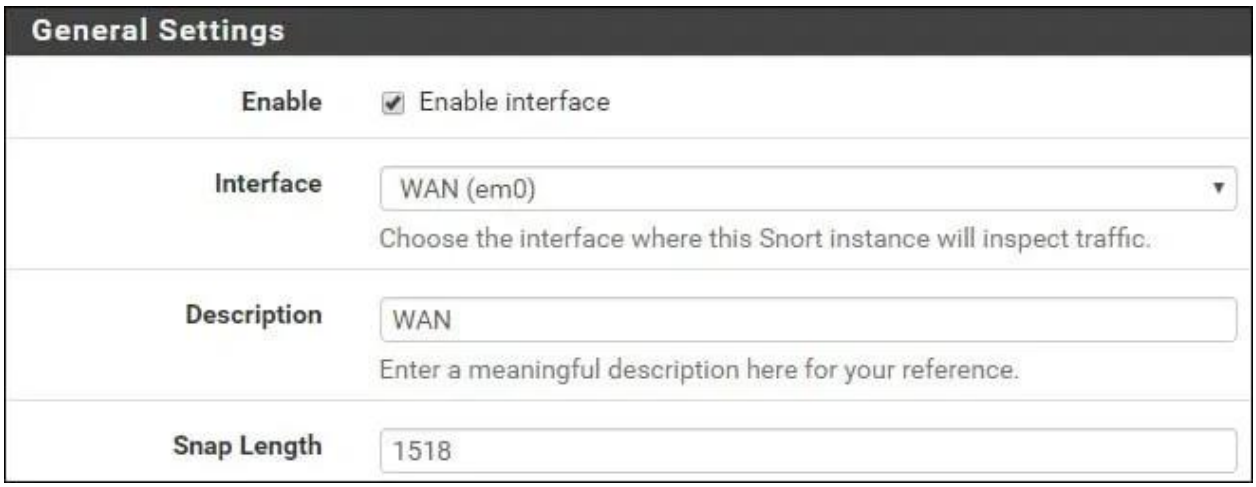

Рис. 3.25. Вибір інтерфейсів для роботи Snort

Знаходимо область Налаштувань сповіщень та виконуємо наступні налаштування (рис. 3.26):

– Відправити сповіщення до системного журналу – Так;

– Блокувати правопорушників – Увімкніть, якщо хочете блокувати правопорушників;

– Kill States – Так;

– Який IP блокувати – обидва.

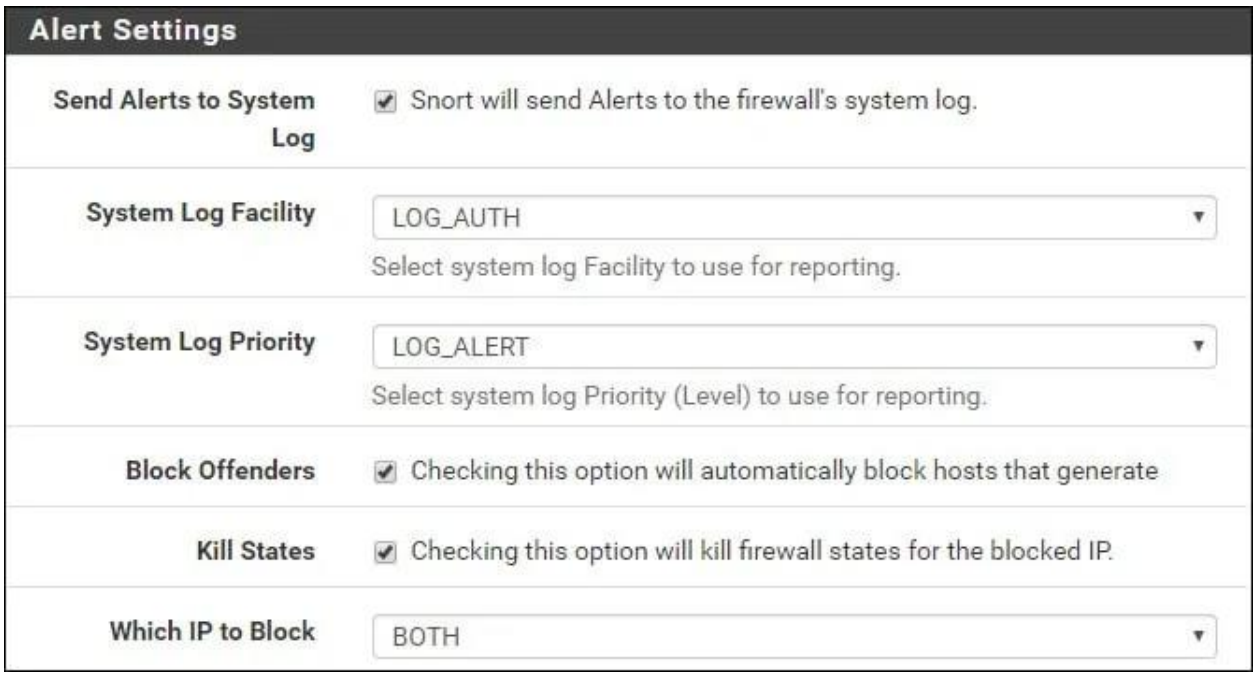

Рис. 3.26. Налаштування сповіщень Snort

Після завершення налаштування натискаємо кнопку Зберегти.

На екрані інтерфейсів Snort, відредагуємо налаштування інтерфейсу (рис.3.27).

Рис. 3.27. Налаштування інтерфейсів Snort

Переходимо на вкладку Категорії Wan та виконуємо наступні налаштування (рис. 3.28):

– вирішити Flowbits – Так;
– використовувати політику IPS – Так;
– вибір політики IPS – Зв'язок.

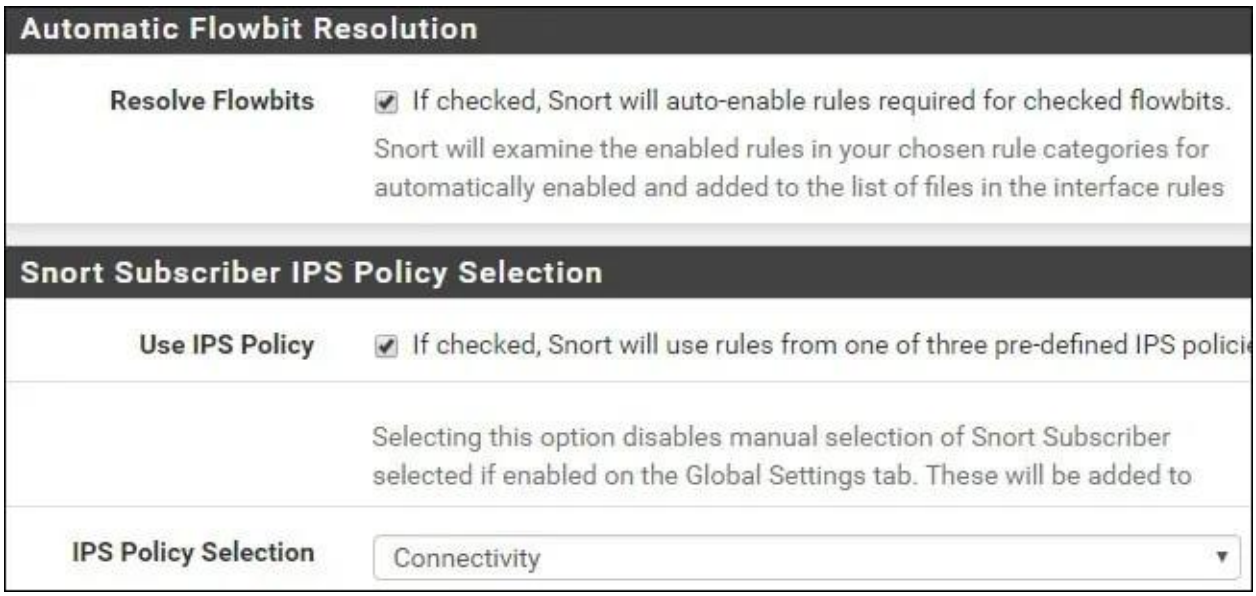

Рис. 3.28. Налаштування Snort

У нашому випадку, ми увімкнули функцію IPS і вибрали політику під назвою Зв'язок.

Після завершення налаштування, натискаємо кнопку Зберегти і запустіть службу Snort на інтерфейсі (рис. 3.29).

Рис. 3.29. Запуск сервісу Snort

Ми завершили встановлення Snort на сервері Pfsense.

GreenBone OpenVAS – це потужна система тестування вразливостей, яка використовується для виявлення і усунення потенційних вразливостей в мережі. OpenVAS може бути встановлений на окрему машину або в одній з мережі з PfSense та Snort.

Встановлення: Виконуємо команду встановлення у вашому терміналі. В залежності від вашої системи це може бути sudo apt install openvas.

Налаштування: Після встановлення налаштуємо OpenVAS. Виконуємо команду sudo openvas-setup у терміналі. Цей процес може зайняти трохи часу, оскільки він завантажує необхідні бази даних та інші компоненти.

Запуск: Щоб запустити OpenVAS, використовуємо команду sudo openvas-start. Це запускає всі необхідні служби.

Доступ до GreenBone: Тепер можемо отримати доступ до GreenBone Security Assistant, що є веб-інтерфейсом для OpenVAS, за адресою https://localhost:9392.

Вхід: Використовуємо логін та пароль, щоб увійти до GreenBone Security Assistant (рис. 3.30).

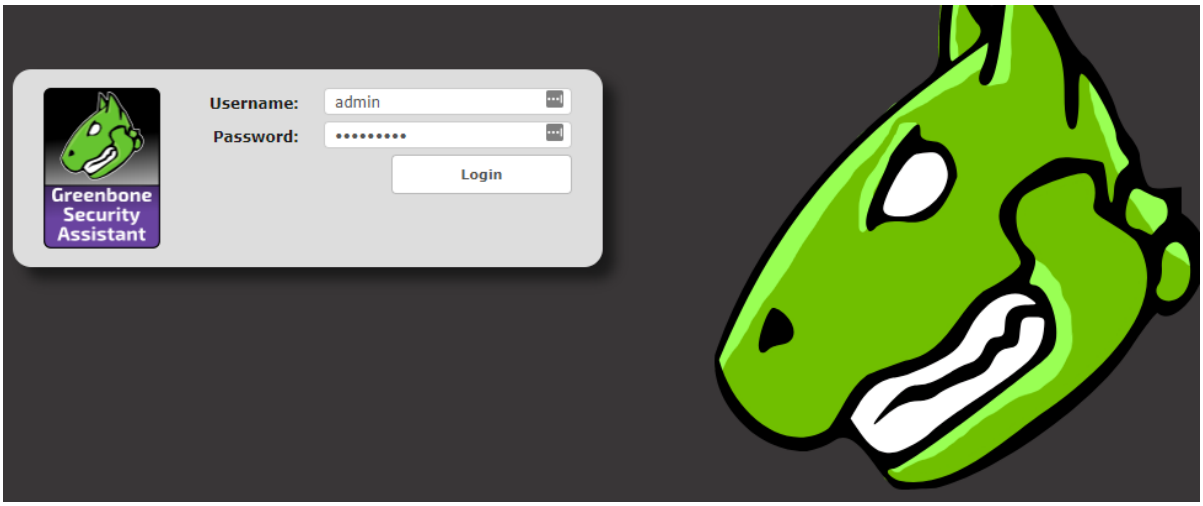

Рис. 3.30. Панель авторизації OpenVAS

Створення завдання: Щоб створити завдання сканування, переходимо до розділу «Завдання» в меню і натискаємо «Створити нове завдання». Вводимо назву завдання, вибираємо ціль та конфігуруємо додаткові параметри (рис. 3.31).

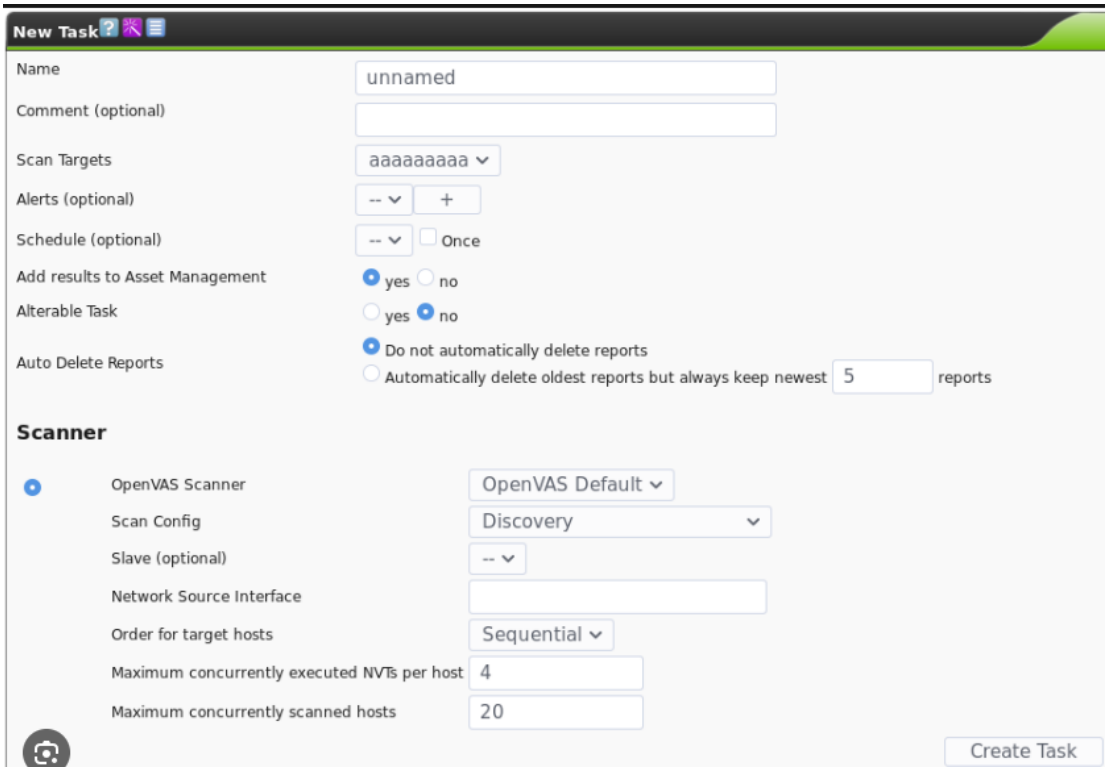

Рис. 3.31. Створення завдання OpenVAS

Запуск сканування: Щоб запустити сканування, натисніть на створене завдання і виберіть «Запустити» (рис. 3.32).

Рис. 3.32. Запуск завдання OpenVAS

Після встановлення та налаштування PfSense, Snort і OpenVAS, вони можуть бути інтегровані для створення єдиної системи захисту від витоку інформаційним каналом. Трафік, що проходить через PfSense, аналізується Snort для виявлення потенційних загроз, а OpenVAS регулярно сканує мережу на предмет нових

вразливостей. Це дозволяє швидко виявляти і реагувати на нові загрози, а також забезпечує постійний контроль за станом безпеки мережі.

Цей процес розгортання та налаштування PfSense, Snort і OpenVAS створює сильну, адаптивну та гнучку систему захисту, яка здатна ефективно виявляти та протистояти різним типам загроз безпеки інформації.

Важливою частиною проектування є створення інтуїтивно зрозумілого інтерфейсу для адміністратора системи, який буде включати в себе панель управління та звіти про стан безпеки мережі.

Алгоритм роботи програми можна представити у вигляді таких кроків:

1. Відображення списку доступних дискових приводів для користувача.
2. Вибір приводу для сканування користувачем.
3. Проведення сканування обраного диску на наявність файлів у форматі .bat.
4. Якщо файли знайдено, програма пропонує користувачу видалити їх.
5. У випадку згоди користувача файли видаляються.
6. Результати роботи програми записуються в лог-файл.

При розробці програми було використано мову програмування Python через її простоту та гнучкість. Бібліотека os використовувалась для доступу до файлової системи, а logging – для зберігання інформації про дії програми.

Ця програма сканує вибраний користувачем диск на наявність файлів у форматі .bat, пропонує їх видалити і зберігає дії програми в лог-файл. Завдяки використанню Python, програма легко адаптується під різні операційні системи і вимоги користувачів.

PyInstaller є корисним інструментом, що дозволяє створити автономний виконуваний файл (exe для Windows) з програми Python. Це означає, що ви можете розповсюджувати свою програму без необхідності встановлення Python на цільовому комп'ютері.

Після розробки та тестування нашої програми на Python, ми можемо використати PyInstaller для створення виконуваного файлу. Це можна зробити,

встановивши PyInstaller за допомогою pip (pip install pyinstaller) та запустивши команду pyinstaller з ім'ям нашого Python файлу як аргументом:

pyinstaller --onefile disk_scanner.py

Опція --onefile говорить PyInstaller створити один виконуваний файл. Без цієї опції PyInstaller створить директорію з виконуваним файлом і всіма необхідними бібліотеками.

Після виконання цієї команди у директорії dist з'явиться виконуваний файл disk_scanner.exe, який можна запускати на будь-якому комп'ютері з Windows, навіть якщо на ньому не встановлено Python.

Це надає зручність використання програми кінцевим користувачам, оскільки вони не повинні встановлювати Python або будь-які залежності – вони просто запускають виконуваний файл.

3.2. Налаштування безпеки та розмежування доступу в мережі

Для забезпечення надійного та безпечного доступу до мережевих ресурсів, ми застосовуємо ряд стратегій та технологій. У нашій мережі з 46 комп'ютерами, поділених на два сегменти, використовуються технології Gigabit Ethernet, AP 802.11n та сервери DHCP та DNS.

Доступ до ресурсів. Права доступу до мережевих ресурсів управляються через централізовану систему керування доступом. Кожен користувач має унікальний ідентифікатор, і на основі цього ідентифікатора призначаються права доступу до ресурсів. Це робить можливим тримати контроль над тим, хто має доступ до важливих ресурсів та даних.

Одним з ключових моментів у побудові безпечної та ефективної мережі є налаштування доступу до ресурсів. Нижче наведений приклад, як це можна зробити в середовищі Windows за допомогою служби Active Directory (AD).

Active Directory (AD) – це компонент системи Windows Server, який надає централізовані служби для ідентифікації та аутентифікації, управління обліковими записами користувачів та групами. Це дає можливість визначити і контролювати доступ користувачів до ресурсів, що розміщені на серверах мережі.

Розглянемо процес налаштування доступу до спільної папки на сервері за допомогою AD:

1. **Створіть спільну папку на сервері**. Це можна зробити, використовуючи провідник файлів. Просто виберіть потрібне місце на сервері, натисніть правою кнопкою миші і виберіть "Створити нову папку".

2. **Поділіть папку**. Щоб папку було видно в мережі, її потрібно поділити. Натисніть правою кнопкою миші на папці, виберіть "Властивості", перейдіть на вкладку "Доступ" і натисніть кнопку "Розширені налаштування". Тут ви можете вказати, хто має доступ до папки і які дії вони можуть виконувати.

3. **Налаштування прав доступу в AD**. Відкрийте консоль управління Active Directory. Знайдіть і виберіть обліковий запис користувача або групу, якій ви хочете надати доступ до папки. Властивості облікового запису містять вкладку "Безпека", де ви можете налаштувати права доступу до папки.

Застосування цього методу дозволяє налаштувати деталізований доступ до ресурсів мережі, що допомагає забезпечити захист від несанкціонованого доступу.

Безпровідний доступ. У нашій мережі є не менше 25% портативних комп'ютерів, які мають можливість підключатися до безпровідної або кабельної мережі. Ми використовуємо протоколи безпечного безпровідного з'єднання для захисту даних в мережі Wi-Fi.

Безпровідний доступ в мережі є особливо важливим для мобільності користувачів і гнучкості системи. Приклад налаштування безпровідного доступу можна зробити за допомогою точок доступу (AP) та протоколу Wi-Fi Protected Access 2 (WPA2).

WPA2 – це стандарт безпечності, який забезпечує криптографічний захист даних, переданих по радіомережі Wi-Fi. Це означає, що інформація, яка передається між користувачем і точкою доступу, зашифрована, щоб забезпечити захист від несанкціонованого доступу.

Розглянемо, як можна налаштувати безпровідний доступ за допомогою точки доступу.

Підключіть точку доступу до мережі. З'єднайте точку доступу з мережею за допомогою Ethernet-кабелю. Точка доступу має бути підключена до комутатора або маршрутизатора в мережі.

Налаштування точки доступу. Більшість точок доступу має веб-інтерфейс для налаштування. Введіть IP-адресу точки доступу в веб-браузері, щоб відкрити інтерфейс налаштувань. Тут ви можете встановити параметри безпровідної мережі, такі як ім'я мережі (SSID), канал передачі даних та протокол безпеки (WPA2).

Налаштування WPA2. У вкладці налаштувань безпеки виберіть WPA2 як протокол безпеки і введіть ключ передачі даних. Ключ передачі даних використовується для шифрування та розшифрування даних, переданих по безпровідній мережі.

Підключення до безпровідної мережі. Портативні пристрої можуть тепер підключитися до безпровідної мережі. Вони мають бути налаштовані на підключення до SSID мережі і ввести ключ передачі даних для WPA2 при запиті.

Це налаштування забезпечить безпечний безпровідний доступ до ресурсів мережі для мобільних користувачів.

Технології захисту. Міжмережевий екран Cisco ASA5506 використовується для забезпечення безпеки мережі. Цей міжмережевий екран виконує глибокий аналіз пакетів, що проходять через нього, для виявлення шкідливого трафіку або атак. Він також може налаштуватися для обмеження вхідного та вихідного трафіку, що допомагає контролювати, який трафік може проходити через мережу.

Таким чином, за допомогою добре планованої стратегії доступу до ресурсів, використання надійних технологій безпровідного доступу, та використання міжмережевого екрану Cisco ASA5506, ми забезпечуємо безпечну та ефективну роботу нашої комп'ютерної мережі.

3.3. Перевірка працездатності спроектованої мережі

Після встановлення та конфігурації pfSense, Snort і OpenVAS, ми провели ретельне тестування, щоб визначити, наскільки ефективно ці інструменти здатні виявити і запобігти витоку інформації через інформаційні канали.

Тестування проводилося на основі стандартних тестових сценаріїв, включаючи спроби несанкціонованого доступу, використання відомих уразливостей, DDoS-атак і так далі. Крім того, були створені спеціальні сценарії для симуляції різних видів атак на витік інформації.

З метою оцінки ефективності розробленого рішення було використано декілька критеріїв:

Здатність виявлення атак: це основний критерій, який оцінює здатність системи виявляти різні види атак. Результати тестування показали, що комбінація pfSense, Snort і OpenVAS дозволила виявити та заблокувати велику кількість атак.

Мінімізація хибних спрацьовувань: дуже важливо, щоб система мала мінімальну кількість хибних тривог, які можуть спричинити непотрібні перебої в роботі.

Продуктивність: наша система повинна бути здатна обробляти велику кількість мережевого трафіку без суттєвого впливу на загальну продуктивність мережі.

Зручність управління: система безпеки повинна бути простою у використанні та управлінні, що було важливим критерієм під час оцінювання.

За результатами оцінки ми можемо зробити висновок, що запропоноване рішення є ефективним і надійним інструментом для захисту від витоку інформації через інформаційні канали.

Програма для сканування диску на наявність файлів в форматі .bat також була протестована. Завдяки зручному інтерфейсу користувач може легко вибрати диск для сканування зі списку доступних дисків. Після сканування програма надає детальну інформацію про всі знайдені .bat файли та пропонує їх видалити.

Програма була протестована на різних системах та дисках, зокрема на дисках з великою кількістю файлів та директорій. Результати показали, що програма працює стабільно та ефективно, здатна швидко сканувати диски та виявляти файли в форматі .bat.

Процес роботи програми було здійснено з використанням логів, що зберігаються у файлі. Це дозволило моніторити дії програми та виявити будь-які можливі помилки або проблеми.

Також було створено виконуваний файл .exe з використанням PyInstaller, що забезпечує легкість використання програми. Користувач не повинен встановлювати Python або будь-які залежності – вони просто запускають виконуваний файл (рис. 3.33-3.34).

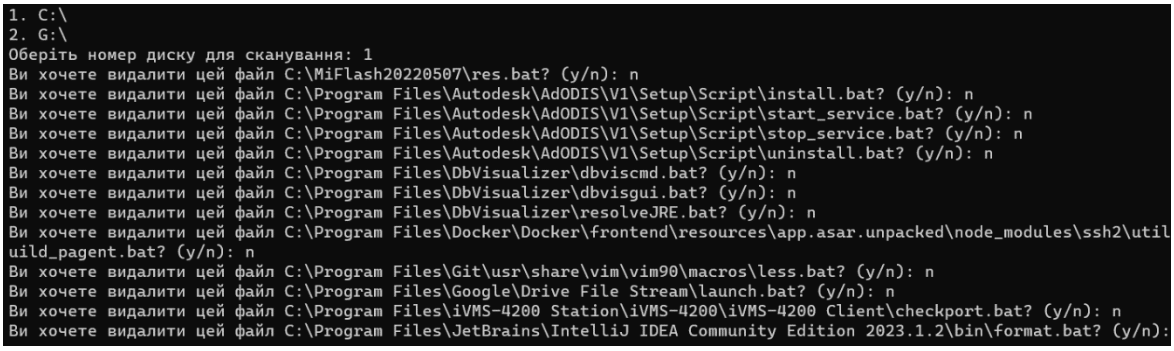

Рис. 3.33. Робота програми сканування диску

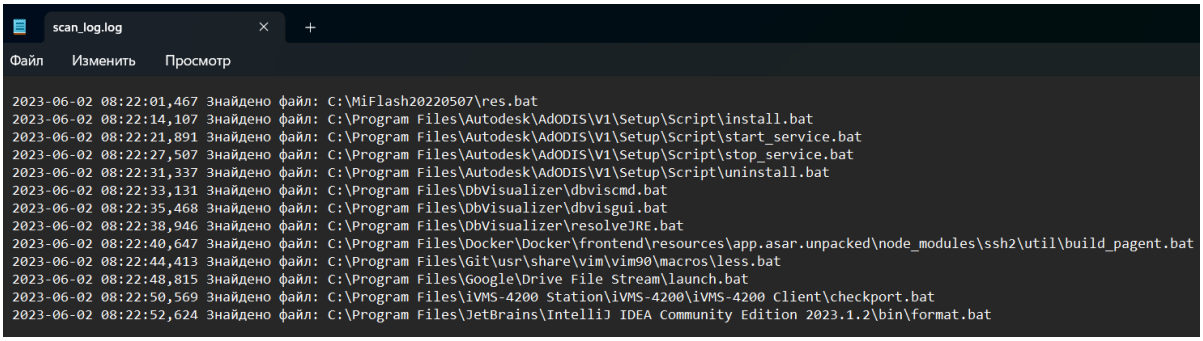

Рис. 3.34. Журнал роботи програми сканування диску

Таким чином, виходячи з результатів тестування, можна зробити висновок, що програма для сканування диску є ефективним інструментом для виявлення і видалення потенційно шкідливих .bat файлів, що сприяє підвищенню загальної безпеки системи.

Після розгляду основних аспектів безпеки та функціональності нашої мережі, важливим етапом перевірки працездатності спроектованої мережі є тестування швидкості. Цей процес має на меті виміряти ефективність передачі даних у мережі та забезпечити, що вона відповідає встановленим стандартам та вимогам користувачів.

Для цього ми використали набір інструментів для тестування швидкості мережі, що дозволяють оцінити пропускну здатність мережі, затримки, джиттер та втрату

пакетів. Тестування проводилося шляхом створення реальних умов роботи мережі, з великою кількістю одночасних запитів та трафіку.

Ми виконали ряд тестів у різних точках мережі, включаючи з'єднання між серверною кімнатою та різними кінцевими точками, такими як класні кімнати, лабораторії та адміністративні приміщення. Це дозволило нам оцінити загальну продуктивність мережі та виявити можливі "вузькі місця" у системі.

Також ми провели порівняльний аналіз швидкості мережі до та після впровадження обладнання та застосування налаштувань безпеки. Це дало нам змогу оцінити вплив безпекових систем на продуктивність мережі.

Таблиця 3.1.

Результати тестування швидкості мережі

Точка Тестування	**Пропускна Здатність (Mbps)**	**Затримка (мс)**	**Джиттер (мс)**	**Втрата Пакетів (%)**
Серверна кімната - Адміністративні приміщення	940	2	0.5	0.1
Серверна кімната - Класні кімнати	920	4	0.7	0.2
Серверна кімната - Лабораторії	930	3	0.6	0.15
Серверна кімната - Бібліотека	940	2	0.5	0.1

Ці результати показують, що мережа має високу пропускну здатність і низькі рівні затримки та джиттера в усіх ключових локаціях. Мінімальна втрата пакетів свідчить про високу надійність мережі.

ВИСНОВКИ

Нами визначено, що сучасний навчальний заклад вимагає високопродуктивної, стабільної та безпечної мережі, яка здатна задовольнити потреби великої кількості користувачів одночасно. Це включає не лише забезпечення доступу до Інтернету, але й підтримку специфічних додатків, віртуальних лабораторій, систем управління навчанням та інших цифрових ресурсів.

Безпека даних є пріоритетом. Оскільки мережі навчальних закладів зберігають чимало конфіденційних даних, їхнє захищене зберігання та передача є критично важливими. Мережа повинна бути масштабованою і гнучкою для адаптації до змінюваних освітніх потреб та технологічних нововведень у майбутньому. З урахуванням вищезгаданих аспектів, при проектуванні та розгортанні мережі важливо враховувати як кількісні, так і якісні характеристики, а також специфічні потреби закладу. Тільки інтегрований підхід до визначення вимог може забезпечити створення ефективної, надійної та безпечної інформаційної мережі для навчального закладу.

Головна мета проекту полягала у створенні такої інформаційної мережі, яка забезпечить високу якість доступу до ресурсів, безпеку даних та здатність до масштабування, водночас враховуючи потреби освітнього процесу та особливості навчального закладу. Створення мережі, яка буде відповідати цим критеріям, гарантуватиме не лише ефективне функціонування навчального процесу в сучасних умовах, але й забезпечить основу для подальшого розвитку та інновацій в навчальному закладі.

Тестування безпеки спроектованої мережі є важливим етапом для забезпечення того, що всі імплементовані заходи безпеки працюють ефективно і здатні відсікати потенційні загрози. Для цього ми виконали серію тестів, спрямованих на визначення здатності нашої мережі протистояти різним видам атак та загроз.

Першим кроком було проведення внутрішнього та зовнішнього сканування вразливостей за допомогою OpenVAS. Це дозволило нам виявити потенційні слабкі місця в нашій мережевій інфраструктурі. Ми також використовували інструменти для

імітації різних типів атак, включаючи атаки на відмову в обслуговуванні (DDoS), фішингові атаки, інжектування SQL та інші звичайні методи кібератак.

Для перевірки здатності Snort виявляти і блокувати шкідливий трафік, ми розробили сценарії тестування, які включали імітацію несанкціонованого доступу та спроби проникнення в систему. Це дозволило нам оцінити ефективність правил Snort та їх здатність виявляти реальні загрози.

Крім того, ми провели тестування на проникнення, за допомогою якого перевірили міцність нашої мережевої інфраструктури та захисних систем від цілеспрямованих атак. Це включало як автоматизоване тестування, так і ручне втручання, щоб імітувати дії потенційного зловмисника.

На заключному етапі ми проаналізували результати всіх тестів та визначили, чи потрібні додаткові налаштування або оновлення систем безпеки. Особливу увагу було приділено аналізу логів системи безпеки для виявлення будь-яких невідповідностей чи неочікуваних поведінок.

Результати тестування безпеки були підтверджені звітами, які включали детальний аналіз виявлених вразливостей, відповідь системи на різні види атак та рекомендації щодо поліпшення безпеки мережі. Це дало нам змогу вдосконалити нашу мережу та забезпечити високий рівень безпеки для захисту від потенційних кіберзагроз.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Качинський А.Б. Безпека складних систем.-К. [Текст]: ТОВ «Видавництво «Юстон», 2017.-498 с

2. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки [Текст] / Матеріали XVII Всеукраїнської науковопрактичної конференції студентів, аспірантів та молодих вчених “Теоретичні і прикладні проблеми фізики, математики та інформатики”, НТУУ “КПІ”, 2015 р.

3. Про основні засади забезпечення кібербезпеки України, Закон України. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19

4. Oxford Dictionaries [Електронний ресурс] – Режим доступу до ресурсу: https://en.oxforddictionaries.com/definition/us/cyberspace

5. Gibson W. Neuromancer [Текст] / W. Gibson.— London: HarperCollins, 1994

6. The varieties of cyberspace: Problems in definition and delimitation, Western Journal of Communication, 63:3, 382-412. [Електронний ресурс] – Режим доступу до ресурсу: https://www.tandfonline.com/doi/abs/10.1080/10570319909374648

7. «Cyberpower and National Security: Policy Recommendations for a Strategic Framework,» in Cyberpower and National Security, FD Kramer, S. Starr, [Текст] L.K. Wentz (ed.), National Defense University Press, Washington (DC) 2009.

8. THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE [Текст] - Dr. Frederick Wamala (Ph.D.), CISSP®- September 2011

9. ISO/IEC 27032:2012 [Текст] Information technology — Security techniques — Guidelines for cybersecurity.

ДОДАТКИ

Додаток А

Код програми для сканування диску.

```
import os
import logging

logging.basicConfig(filename='scan_log.log', level=logging.INFO, format='%(asctime)s %(message)s')

def get_drives():
    drives = [f"{d}:\\" for d in "ABCDEFGHIJKLMNOPQRSTUVWXYZ" if os.path.exists(f"{d}:\\")]
    return drives

def find_files(path, extension):
    for root, dirs, files in os.walk(path):
        for file in files:
            if file.endswith(extension):
                yield os.path.join(root, file)

def delete_file(path):
    try:
        os.remove(path)
        logging.info(f"Файл {path} успішно видалено.")
    except OSError as e:
        logging.error(f"Помилка: {e.filename} - {e.strerror}.")

def main():
```

```
    drives = get_drives()
    for i, drive in enumerate(drives):
        print(f"{i+1}. {drive}")
    drive_number = int(input("Оберіть номер диску для сканування: "))
    path_to_scan = drives[drive_number-1]
    for file in find_files(path_to_scan, ".bat"):
        logging.info(f"Знайдено файл: {file}")
        delete_option = input(f"Ви хочете видалити цей файл {file}? (y/n): ")
        if delete_option.lower() == 'y':
            delete_file(file)

if __name__ == "__main__":
    main()
```