МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

кібербезпеки
(повна назва кафедри)

ДИПЛОМНА РОБОТА

РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Виконав: студент групи ПМК-41с
спеціальності
125 «Кібербезпеки»
(шифр і назва спеціальності)

(підпис) Стасюк О.В (прізвище та ініціали)

Керівник (підпис) Комар К.В (прізвище та ініціали)

Науковий консультант (підпис) Вайганг Г.О (прізвище та ініціали)

Рецензент (підпис) Гордєєв О.О. (прізвище та ініціали)

2023

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет Прикладної математики та інформатики
Кафедра Кібербезпеки
Спеціальність 125 «Кібербезпека»
(шифр і назва)

«ЗАТВЕРДЖУЮ»
Завідувач кафедри _____

"31 _ "серпня 2022 року

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

СТАСЮКА ОЛЕКСІЯ ВЯЧЕСЛАВОВИЧА

1 .Тема роботи. Розробка проекту захищеної корпоративної мережі підприємства.
Керівник роботи: Комар Катерина Вячеславівна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені Вченою радою факультету від **" 13" вересня 2022 року № 15**

2. Строк подання студентом роботи **13.06.2023р.**
3. Вихідні дані до роботи: аналіз вимог, проектування мережі, забезпечення безпеки, вибір обладнання та програмного забезпечення, впровадження та конфігурація, тестування та оптимізація, управління та підтримка.
4. Зміст дипломної роботи (перелік питань, які потрібно розробити)

1. Теоретичні основи
2. Аналіз потреб та ризиків підприємства
3. Проектування корпоративної мережі
4. Реалізація та налаштування корпоративної мережі
5. Тестування та оцінка ефективності корпоративної мережі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

1. Презентація доповіді, виконана в Microsoft PowerPoint.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Теоретичні основи	01.04.23	17.04.23
2	Аналіз потреб та ризиків підприємства	17.04.23	29.04.23
3	Проектування корпоративної мережі	29.04.23	13.05.23
4	Реалізація та налаштування корпоративної мережі	13.05.23	20.05.23
5	Тестування та оцінка ефективності корпоративної мережі	20.05.23	30.05.23

7. Дата видачі завдання **31 серпня 2022 р.**

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Уточнення постановки завдання	21.03. 2023 р.	
2	Аналіз літератури	28.03. 2023 р.	
3	Обґрунтування вибору рішення	31.03. 2023 р	
4	Збір даних	08.04. 2023 р.	
5	Теоретичні основи	17.04. 2023 р.	
6	Аналіз потреб та ризиків підприємства	29.04. 2023 р	
7	Проектування корпоративної мережі	13.05. 2023 р	
8	Реалізація та налаштування корпоративної мережі	20.05. 2023 р.	
9	Тестування та оцінка ефективності корпоративної мережі	30.05. 2023 р.	
10	Оформлення та друк пояснювальної записки	02.06. 2023 р	
11	Оформлення презентацій	06.06. 2023 р	
12	Отримання рецензій	10.06. 2022 р	
13	Захист в ЕК	15.06. 2023 р	

Студент _____ **Стасюк О.В**
(підпис) (прізвище та ініціали)

Керівник робот _____ **Комар К.В**
(підпис)(прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка дипломного проекту складається зі вступу, п’яти розділів, що містять 10 рисунків, висновків та списку використаних джерел з 11 найменувань. Загальний обсяг роботи становить 70 сторінок.

Об’єкт дослідження. Захищена корпоративна мережа підприємства. Це складна інформаційна система, яка забезпечує обробку, зберігання та передачу даних в межах підприємства. Робота включає аналіз потреб підприємства, розробку плану мережі, вибір обладнання, розробку програмного забезпечення, впровадження та налаштування, моніторинг та підтримку. Результат - забезпечення безпеки та ефективності мережі, зменшення ризиків втрати даних та стабільна робота підприємства.

Метою даної роботи. Створення надійної та безпечної корпоративної мережі. Аналіз потенційних загроз, розробка стратегії безпеки, плану відновлення після аварії, процедур моніторингу та аудиту безпеки, політик безпеки та навчання персоналу.

У першому розділі описуються основні характеристики, методи та підходи до безпеки в корпоративних мережах та стратегії захисту: цілісності, доступності і конфіденційності.

У другому розділі проводиться аналіз стану мережі підприємства, здійснюється оцінка вимог підприємства щодо мережевої інфраструктури та проводиться оцінка можливих загроз.

У третьому розділі виконується оцінка різних типів мережних архітектур, розробляється детальний план мережевої інфраструктури і проводиться вибір відповідних систем безпеки.

У четвертому розділі виконується фізична установка необхідного обладнання (маршрутизаторів, комутаторів, серверів) і налаштування мережевих параметрів також встановлення та налаштування систем безпеки.

У п’ятому розділі визначаються цілі тестування, розробляються тестові сценарії та план тестування, проводиться перевірка пропускної здатності

мережі, швидкості передачі даних та оцінка ефективності реалізованої системи безпеки.

Галузь застосування. Корпоративна мережа знаходить застосування у різних галузях, включаючи фінансовий сектор, медичну сферу, телекомунікації, виробництво, державні установи та інші. Вона допомагає забезпечити конфіденційність даних, захист від кібератак, забезпечення надійності та доступності мережевих ресурсів, а також дозволяє ефективно управляти та контролювати мережеві процеси в організації.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ, МЕРЕЖЕВИЙ МОНІТОРИНГ, БЕЗПЕЧНИЙ ДОСТУП ДО РЕСУРСІВ, РЕЗЕРВНЕ КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ.

ABSTRACT

The explanatory note of the diploma project consists of an introduction, five sections containing 10 figures, conclusions, and a list of 11 references used. The total volume of the work is 70 pages.

Research Object. Secured corporate network of the enterprise. It is a complex information system that ensures the processing, storage, and transmission of data within the enterprise. The work includes analyzing the enterprise's needs, developing a network plan, selecting equipment, developing software, implementation and configuration, monitoring, and support. The result is ensuring network security and efficiency, reducing the risks of data loss, and maintaining stable operation of the enterprise.

The purpose of this work is to create a reliable and secure corporate network. This includes analyzing potential threats, developing a security strategy, a disaster recovery plan, security monitoring and audit procedures, security policies, and personnel training.

The first chapter describes the main characteristics, methods, and approaches to security in corporate networks and protection strategies, focusing on integrity, availability, and confidentiality.

The second chapter conducts an analysis of the enterprise's network status, evaluates the requirements of the enterprise regarding the network infrastructure, and assesses potential threats.

The third chapter evaluates various types of network architectures, develops a detailed plan for the network infrastructure, and selects appropriate security systems.

The fourth chapter involves the physical installation of necessary equipment (routers, switches, servers) and configuration of network parameters, as well as the installation and configuration of security systems.

The fifth chapter establishes testing objectives, develops test scenarios and a testing plan, conducts network throughput verification, data transfer speed assessment, and evaluates the effectiveness of the implemented security system.

Field of application. Corporate networks are applied in various industries, including the financial sector, healthcare, telecommunications, manufacturing, government institutions, and others. They help ensure data confidentiality, protection against cyber attacks, reliability, and availability of network resources. Additionally, corporate networks enable efficient management and control of network processes within an organization.

Keywords: INFORMATION SECURITY, CYBERSECURITY, IDENTIFICATION, AUTHENTICATION, NETWORK MONITORING, SECURE ACCESS TO RESOURCES, BACKUP AND RECOVERY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP - internet protocol

DNS - domain name system

VLAN -virtual local area network

WLAN - wireless local area network

VPN - virtual private network

IDS - intrusion detection system

SIEM - Security information and event management

SSL - secure sockets layer

IPSec - internet protocol security

STP - spanning tree protocol

ВСТУП

Захищена корпоративна мережа є важливим елементом інформаційної інфраструктури будь-якого підприємства. Її розробка та впровадження дозволяють забезпечити безпеку і конфіденційність даних, що пересилаються та зберігаються в мережі. Крім того, корпоративна мережа дозволяє ефективно організувати роботу між співробітниками, незалежно від їх місця розташування, а також забезпечує доступ до важливих ресурсів підприємства.

Розробка проекту захищеної корпоративної мережі - це складний процес, який вимагає уважної підготовки та планування. У процесі розробки необхідно враховувати багато факторів, таких як обсяг трафіку, швидкість передачі даних, рівень захисту мережі від зовнішніх і внутрішніх загроз, інтеграцію з існуючими інформаційними системами підприємства та багато інших.

У цьому контексті розробка проекту захищеної корпоративної мережі є ключовим етапом створення інформаційної інфраструктури підприємства. Вона дозволяє не тільки забезпечити безпеку та захист інформації, а й підвищити ефективність роботи співробітників та знизити витрати на інформаційну інфраструктуру підприємства.

Актуальність теми

Захищена корпоративна мережа є надзвичайно важливою для будь-якого підприємства. Захист інформації є критично важливою задачею для забезпечення ділового успіху, оскільки компанії використовують значну кількість конфіденційної інформації, такої як важливі документи, персональні дані клієнтів, фінансові дані та інші. Несанкціонований доступ до такої інформації може призвести до серйозних наслідків, таких як виток конфіденційної інформації, порушення авторських прав, фінансові втрати та шкоди репутації.

У сучасному світі, коли все більше ділових операцій відбувається в онлайні, а хакерські атаки стають все більш хиткими і складними, забезпечення безпеки мережі є надзвичайно важливим завданням. Із

зростанням кількості кібератак, тривожних подій, таких як крадіжка даних та вимагання викупу, бізнеси повинні бути більш уважними та пильними у питаннях безпеки інформації.

Оскільки підприємства мають значні обсяги конфіденційної інформації, яка обробляється та передається по мережі, необхідно застосовувати заходи для забезпечення безпеки даних. Наразі, злочинні елементи все частіше використовують технології, щоб проводити кібератаки на підприємства, що може призвести до значних матеріальних та моральних збитків. Такі атаки можуть бути спрямовані на крадіжку конфіденційної інформації, розповсюдження вірусів Так кібератаки можуть бути спрямовані на розповсюдження вірусів, які можуть пошкодити комп'ютерні системи та викликати непередбачувані наслідки, такі як втрата даних або недоступність систем. Крім того, хакери можуть здійснювати фішингові атаки, які спрямовані на отримання конфіденційної інформації шляхом введення користувачів у оману.

Отже, розробка захищеної корпоративної мережі є необхідною для забезпечення безпеки інформації та захисту від кібератак. Для цього необхідно застосовувати сучасні технології та використовувати кваліфікованих фахівців, які зможуть розробити та налагодити систему захисту даних, а також регулярно проводити аудит безпеки та вдосконалювати систему з метою запобігання.

Мета дослідження розробки захищеної корпоративної мережі полягає в створенні надійної та безпечної інфраструктури, що забезпечує захист конфіденційної інформації та інших важливих ресурсів підприємства від зовнішніх та внутрішніх загроз.

Завдання дослідження включають:

Аналіз потенційних загроз передбачає вивчення можливих векторів атак, які можуть бути спрямовані на корпоративну мережу підприємства. Це можуть бути такі загрози, як віруси, черв'яки, троянські програми, шпигунський софт, фішингові атаки, DDoS-атаки, а також загрози з боку

зловмисних інсайдерів, тобто працівників компанії, які мають доступ до корпоративної мережі.

Розробка стратегії безпеки: на основі результатів аналізу потенційних загроз необхідно розробити стратегію безпеки, яка включає в себе забезпечення надійної ідентифікації та аутентифікації користувачів, застосування різноманітних механізмів шифрування, контроль доступу до ресурсів мережі, захист від вірусів та інших шкідливих програм.

Розробка плану відновлення після аварії: підприємство повинно мати план дій у разі виникнення аварійних ситуацій, таких як виход з ладу обладнання, кібератаки або інші непередбачувані ситуації. В плані відновлення мають бути чітко визначені кроки, які необхідно вжити для повного відновлення роботи мережі та систем підприємства.

Розробка процедур моніторингу та аудиту безпеки: необхідно розробити процедури моніторингу та аудиту безпеки, щоб вчасно виявляти можливі загрози та уразливості і забезпечувати постійний контроль за станом безпеки мережі підприємства.

Розробка політик безпеки та навчання персоналу: має бути розроблена політика безпеки, яка визначає правила та процедури щодо захисту інформації та інших ресурсів підприємства. До складу політики безпеки можуть входити вимоги до паролів, правил використання програмного забезпечення, процедури резервного копіювання даних та інші важливі вимоги. Крім того, навчання персоналу щодо правильної поведінки в мережі підприємства, включаючи процедури безпеки та виявлення можливих загроз. Навчання повинно бути регулярним та охоплювати всіх працівників, які мають доступ до корпоративної мережі.

Крім того, до завдань дослідження можуть входити розробка політик щодо зберігання та обробки конфіденційної інформації, захисту від соціального інженерінгу та інших видів атак, а також забезпечення безпечного використання мобільних пристроїв та інших засобів роботи з даними поза межами корпоративної мережі.

Об'єкт дослідження - захищена корпоративна мережа підприємства. Ця мережа є складною інформаційною системою, яка об'єднує різні пристрої та сервери підприємства для забезпечення ефективної обробки, зберігання та передачі даних в межах підприємства.

Це означає проектування та впровадження комплексу заходів забезпечення безпеки мережі для захисту від несанкціонованого доступу, злому та інших кібератак. Основні етапи роботи включають:

– Аналіз потреб підприємства. Необхідно визначити потреби в корпоративній мережі та визначити, які вимоги до безпеки мережі повинні бути задоволені.

– Розробка плану мережі. На основі аналізу потреб підприємства, необхідно розробити план мережі, включаючи топологію мережі, розташування серверів та пристроїв, а також інфраструктуру безпеки.

– Вибір обладнання. Необхідно вибрати необхідне обладнання для розміщення серверів та пристроїв, а також забезпечення безпеки мережі, таке як firewalls, системи виявлення вторгнень та інші.

– Розробка програмного забезпечення. Для забезпечення безпеки мережі необхідно розробити відповідне програмне забезпечення, таке як системи ідентифікації користувачів, системи шифрування даних та інші.

– Впровадження та налаштування. Після розробки плану мережі та вибору обладнання необхідно впровадити встановлення та налаштування всіх компонентів мережі. Це включає установку серверів, налаштування пристроїв мережі, настройку програмного забезпечення безпеки та проведення тестів на проникнення.

– Моніторинг та підтримка. Після встановлення та налаштування мережі необхідно проводити моніторинг та підтримку мережі, щоб забезпечити її безпеку та ефективність роботи. Це включає контроль доступу, виявлення та відновлення випадків порушення безпеки мережі, резервне копіювання даних та оновлення програмного забезпечення.

Загальні завдання проекту включають розробку та впровадження комплексу заходів забезпечення безпеки мережі, забезпечення захисту від кібератак, встановлення та настройку пристроїв та програмного забезпечення, а також проведення тестів та моніторингу мережі.

Під час розробки проекту необхідно враховувати специфіку підприємства, його розмір, склад та обсяг інформації, яку необхідно передавати в мережі. Також необхідно враховувати вимоги до безпеки даних та стандарти безпеки, які необхідно дотримуватись.

Результатом успішної розробки та впровадження захищеної корпоративної мережі підприємства є забезпечення безпеки та ефективності роботи інформаційної системи, що зменшує ризики втрати даних та забезпечує стабільну роботу всіх підрозділів підприємства.

Методи дослідження

Один з можливих методів дослідження, що може бути застосований для забезпечення безпеки інформації в корпоративній мережі підприємства, полягає у вивченні вимог до безпеки інформації та розробці архітектури мережі.

Цей метод дослідження можна розбити на наступні етапи:

1. Вивчення вимог до безпеки інформації. На цьому етапі необхідно визначити, які вимоги до безпеки інформації повинні бути враховані під час розробки захищеної корпоративної мережі. Наприклад, це можуть бути вимоги до захисту від зовнішніх і внутрішніх загроз, вимоги до захисту від несанкціонованого доступу до даних, вимоги до резервного копіювання даних тощо.

2. Розробка архітектури мережі. На цьому етапі необхідно розробити архітектуру захищеної корпоративної мережі, враховуючи вимоги до безпеки інформації, а також специфічні потреби та особливості підприємства. Розробка архітектури може включати в себе визначення топології мережі, вибір обладнання та програмного забезпечення, розробку

політик безпеки мережі, а також встановлення правил і процедур щодо управління мережею.

3. Тестування та аудит захищеної корпоративної мережі. На цьому етапі необхідно провести тестування та аудит захищеної корпоративної мережі з метою перевірки її ефективності та відповідності вимогам до безпеки інформації. Тестування може включати в себе проведення пенетраційного тестування, визначення рівня захисту мережі в залежності від типу загроз, проведення тестування на проникнення з метою виявлення потенційних уразливостей мережі та їх подальшого усунення. Аудит може включати в себе перевірку дотримання політик безпеки, перевірку доступу до ресурсів мережі, перевірку резервного копіювання даних та інших параметрів безпеки мережі.

4. Вдосконалення та підтримка захищеної корпоративної мережі. Після тестування та аудиту необхідно внести вдосконалення до захищеної корпоративної мережі з метою забезпечення її стійкості до нових загроз, які можуть виникнути з часом. Також необхідно забезпечити підтримку мережі та вчасно відповідати на потенційні проблеми та уразливості.

Отже, для забезпечення безпеки інформації в корпоративній мережі підприємства можуть бути використані різні методи дослідження, включаючи вивчення вимог до безпеки інформації, розробку архітектури мережі, тестування та аудит мережі, а також вдосконалення та підтримку мережі.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ

1.1 Поняття корпоративної мережі та її складових

У складі інформаційної системи можна виділити дві відносно самостійні складові. Перша — це фактична комп’ютерна інфраструктура організації в широкому сенсі (мережа, телекомунікації, програмне забезпечення, інформація, організаційна інфраструктура — тобто корпоративна мережа). Друга складова — це взаємопов’язані функціональні підсистеми, що забезпечують вирішення організаційних завдань і досягнення цілей [1].

Перший компонент – базис, який є основою для інтеграції функціональних підсистем і повністю визначає атрибути інформаційної системи, що є вирішальним для успішного функціонування інформаційної системи. Його вимоги уніфіковані та стандартизовані, а методи його побудови добре відомі та неодноразово перевірені на практиці.

Другий компонент повністю побудований на першому компоненті та передає функціональні можливості програми в інформаційну систему. Вимоги до нього складні і часто суперечливі, оскільки висуваються фахівцями з різних галузей застосування.

Розробка захищеної мережі ґрунтується на кількох теоретичних основах, включаючи технології мережі, інформаційну безпеку та управління мережею.

1. Технології мережі [2].

Захищена корпоративна мережа підприємства складається з комп'ютерів, серверів, маршрутизаторів та інших мережевих пристроїв, які взаємодіють між собою.

Для забезпечення безпеки цієї мережі використовуються такі технології мережі, як VLAN, VPN та Firewall. VLAN дозволяє розділити мережу на окремі логічні сегменти, що забезпечує безпеку та контроль доступу до різних даних в мережі. VPN використовується для створення безпечного

тунелю між різними вузлами мережі, що забезпечує безпечну передачу даних. Firewall контролює рух даних в мережі та забезпечує захист від несанкціонованого доступу до мережі [3].

2. Інформаційна безпека.

Інформаційна безпека включає в себе захист інформації від несанкціонованого доступу, використання, зміни або знищення. Для забезпечення інформаційної безпеки в корпоративній мережі підприємства використовуються різні технології, такі як шифрування даних, контроль доступу, аутентифікація користувачів та моніторинг дій користувачів [4].

Шифрування даних дозволяє захистити дані від несанкціонованого доступу під час переглядом відкритого тексту. Контроль доступу відбувається за допомогою встановлення прав доступу до різних ресурсів мережі для різних користувачів. Аутентифікація користувачів дозволяє перевірити ідентифікацію користувачів та забезпечити захист від несанкціонованого доступу до мережі. Моніторинг дій користувачів дозволяє виявити та запобігти несанкціонованим діям в мережі [5].

3. Управління мережею.

Управління мережею включає в себе планування, налаштування та моніторинг мережі для забезпечення безпеки та ефективності роботи. Для забезпечення ефективності роботи мережі необхідно забезпечити належну її налаштування, моніторинг та управління її ресурсами [6].

Для забезпечення безпеки мережі необхідно регулярно проводити аудит безпеки та виявляти та усувати потенційні загрози.

4. Захист від зовнішніх загроз.

Для забезпечення безпеки мережі необхідно вживати заходів для захисту від зовнішніх загроз, таких як віруси, шкідливі програми та хакерські атаки [7].

Це може включати в себе встановлення програмного забезпечення антивірусного захисту, мережевих брандмауерів, IDS, SIEM.

5. Захист від внутрішніх загроз.

Забезпечення захисту від внутрішніх загроз також є важливим аспектом розробки захищеної корпоративної мережі підприємства.

Це може включати в себе встановлення систем контролю доступу, які дозволяють обмежити права доступу до конфіденційної інформації тільки до необхідних працівників, а також використання технологій шифрування для захисту від незаконного доступу до конфіденційної інформації.

6. Резервне копіювання та відновлення даних.

Резервне копіювання та відновлення даних є необхідною частиною розробки захищеної корпоративної мережі підприємства. Резервні копії даних дозволяють відновлювати важливу інформацію в разі її втрати, пошкодження або викрадення.

Необхідно регулярно проводити резервне копіювання даних та перевіряти їх наявність та функціональність.

7. Аудит та моніторинг мережі.

Аудит та моніторинг мережі дозволяють виявляти потенційні загрози та вразливості системи та своєчасно вживати заходів для їх запобігання. Для цього можна використовувати системи журналювання подій, що дозволяють відслідковувати дії користувачів та системи, а також використовувати системи моніторингу мережі, які дозволяють виявляти загрози та вразливості в реальному часі [8].

8. Захист від соціального інжинірингу.

Соціальний інжиніринг є одним з найбільш поширених методів атак на корпоративні мережі. Це може бути спроба отримати доступ до конфіденційної інформації шляхом зламу паролів або переконання працівників надати доступ до системи [9].

Для запобігання соціального інжинірингу необхідно проводити навчання та підвищення свідомості працівників щодо безпеки інформації та вживати заходів для захисту паролів та ідентифікаційних даних.

9. Створення плану реагування на інциденти безпеки.

Створення плану реагування на інциденти безпеки є важливим аспектом розробки захищеної корпоративної мережі підприємства.

План повинен включати в себе процедури щодо виявлення та реагування на інциденти безпеки, включаючи процедури повідомлення випадків порушення безпеки, встановлення причин та заходи для запобігання подібним інцидентам у майбутньому.

Комплексний захист мережі та інформації в ній є результатом врахування раніше згаданих основ розробки захищеної корпоративної мережі підприємства. Реалізація цих аспектів відповідальна за зменшення ризиків виникнення інцидентів безпеки та збереження важливої інформації компанії в безпеці [10].

Крім того, розробка захищеної мережі включає в себе відповідну організацію робочих місць та комп'ютерних систем, захист електронної пошти та інших форм комунікації, забезпечення безпеки даних в хмарних сервісах та на мобільних пристроях, а також захист від зовнішніх загроз, таких як кібератаки, шпигунство та крадіжки даних.

Розробка захищеної мережі є складним та багатогранним процесом, який потребує відповідної експертизи та досвіду в області кібербезпеки. Однак, з урахуванням зростаючої кількості кібератак та збільшення кількості крадіжок та витоків даних, розробка захищеної мережі стає надзвичайно важливою для забезпечення безпеки бізнесу та захисту важливої інформації.

Корпоративна мережа - це комп’ютерна мережа, що забезпечує обмін даними між комп’ютерами та іншими пристроями на підприємстві. Основною метою корпоративної мережі є підвищення ефективності та продуктивності бізнесу шляхом спільної роботи та обміну інформацією між різними підрозділами та співробітниками [11].

Складові корпоративної мережі можна розділити на три основні категорії (рис 1.1).

Рисунок 1.1 – Основні складові елементи корпоративної мережі

Для успішної розробки захищеної корпоративної мережі підприємства необхідно детально вивчити всі складові мережі, а також зрозуміти взаємозв'язки між ними. При проектуванні мережі необхідно враховувати потреби підприємства, зокрема його розмір, обсяг даних, тип діяльності та особливості роботи з даними, а також потреби в мережевих засобах та програмному забезпеченні. Необхідно також враховувати вимоги до безпеки мережі та захисту інформації.

Основні етапи розробки проекту захищеної корпоративної мережі підприємства наведені на рис. 1.2 [12].

У проекті розробки захищеної корпоративної мережі підприємства можна розглянути основні технології мережі, такі як протоколи маршрутизації, протоколи безпеки, VPN-технології та інші. Це допоможе краще зрозуміти, як вони працюють та як їх можна використовувати для захисту мережі та інформації.

Рисунок 1.2 – Етапи розробки проекту захищеної корпоративної мережі

У розділі дипломної роботи представлені основні поняття корпоративної мережі та її складові, для розуміння потреб побудови захищеної мережі підприємства. Складові компоненти корпоративної мережі представлені у табл.1.1 [13].

Таблиця 1.1 – Основні елементи побудови корпоративної мережі

Елемент	**Основна функція**
Сервери	це центральні комп'ютери, які забезпечують обробку та зберігання інформації та надання доступу до неї користувачам. Для захисту мережі важливо мати захищені сервери з встановленими захисними програмами.
Робочі станції	це комп'ютери, які використовуються працівниками підприємства для роботи з даними та програмним забезпеченням. Важливо захищати робочі станції від вірусів та інших загроз.
Мережеві комутатори	це пристрої, які забезпечують з'єднання різних комп'ютерів та

Елемент	Основна функція
	інших пристроїв в мережі. Для захисту мережі важливо використовувати комутатори з підтримкою безпеки.
Мережеві маршрутизатори	це пристрої, які забезпечують маршрутизацію даних в мережі. Для захисту мережі важливо використовувати маршрутизатори з підтримкою безпеки та захисту мережі від зовнішніх атак.
Firewall	це пристрій або програмне забезпечення, яке захищає мережу від зовнішніх загроз, фільтруючи вхідні та вихідні пакети даних.
VPN	це технологія, яка дозволяє створювати безпечне з'єднання між двома точками в мережі Інтернет. Використання VPN дозволяє забезпечити безпеку передачі даних між різними підрозділами підприємства та зовнішніми користувачами.
Антивірусне програмне забезпечення	це програмне забезпечення, яке захищає комп'ютери від вірусів, шпигунських програм та інших загроз.
Системи контролю доступу	це технології, які дозволяють обмежувати доступ користувачів до різних ресурсів в мережі. Для захисту мережі важливо використовувати системи контролю доступу з підтримкою різних рівнів доступу та аутентифікації користувачів.
Системи моніторингу та логування	це технології, які дозволяють відстежувати дії користувачів та виявляти відхилення в роботі мережі. Для захисту мережі важливо мати системи моніторингу та логування з підтримкою виявлення загроз та аналізу поведінки користувачів.
Фізичні засоби захисту	це засоби, які використовуються для захисту компонентів мережі від фізичних атак, таких як крадіжка або пошкодження обладнання. Для захисту мережі важливо використовувати фізичні засоби захисту, такі як камери спостереження, контроль доступу до приміщень та інші.

При проектуванні захищеної корпоративної мережі підприємства, необхідно враховувати всі складові мережі та забезпечити їх відповідними захисними заходами. Забезпечення безпеки мережі є важливим елементом у забезпеченні успішної діяльності підприємства.

Для досягнення цієї мети можна використовувати різні методи та технології, такі як встановлення захисту від вірусів та шкідливих програм, шифрування даних, контроль доступу та інші. Також враховувати потреби та вимоги користувачів мережі.

Наприклад, якщо підприємство має велику кількість віддалених користувачів, то може бути необхідно використовувати VPN-з'єднання для забезпечення безпеки передачі даних.

Для розробки захищеної корпоративної мережі підприємства необхідно спроектувати та реалізувати етапи (рис 1.3).

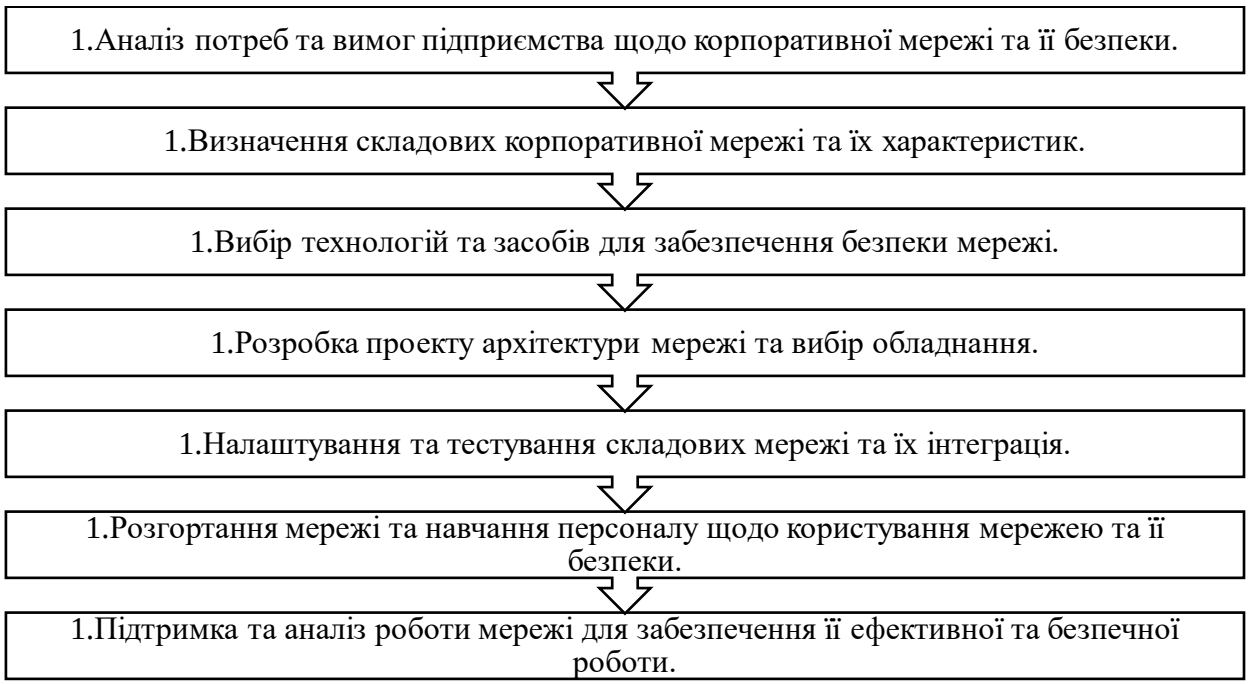


Рисунок 1.3 – Етапи проекту захищеної корпоративної мережі

Розробка захищеної корпоративної мережі підприємства є складним та відповідальним процесом, що вимагає детального вивчення технологій та методів захисту мережі. Головною метою проекту є створення безпечної та надійної мережі, яка забезпечує ефективну роботу підприємства та захист від можливих загроз.

Крім того, у проекті використовують визначені компоненти комунікативної підсистеми корпоративної мережі (рис.1.4).

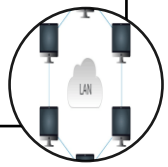
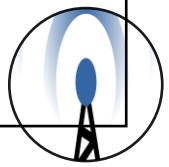
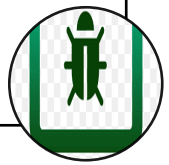
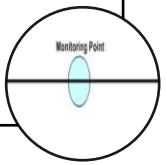
це мережа, яка об'єднує комп'ютери та інші пристрої в рамках одного приміщення або декількох близько розташованих будівель. Локальна мережа дозволяє обмінюватися даними між користувачами мережі та ділитися ресурсами, такими як принтери, файлові сервери тощо.	це мережа, яка об'єднує комп'ютери та інші пристрої на великій відстані, наприклад, між різними офісами підприємства в різних містах. Розширена мережа дозволяє обмінюватися даними та ділитися ресурсами між різними офісами підприємства.	це мережа, яка дозволяє підключатися до мережі без застосування дротів, за допомогою радіохвиль. Бездротова мережа дозволяє підключатися до мережі з різних місць та забезпечує більшу мобільність користувачів мережі.	це мережа, яка дозволяє підключатися до мережі з віддаленого місця через Інтернет. VPN-з'єднання забезпечує захист даних під час їх передачі через Інтернет та дозволяє з'єднувати віддалені користувачі до корпоративної мережі підприємства.
–Локальна мережа (LAN) 	–Розширена мережа (WAN) 	–Бездротова мережа (Wi-Fi) 	–Віртуальна приватна мережа (VPN) 
це програмне та/або апаратне забезпечення, яке призначене для захисту мережі від зовнішніх атак. Брандмауер контролює доступ до мережі та фільтрує вхідні та вихідні дані з метою запобігання несанкціонованого доступу до мережі.	це система, яка дозволяє управляти доступом користувачів до різних ресурсів мережі підприємства. Система ідентифікації та автентифікації користувачів забезпечує безпеку мережі та дозволяє контролювати доступ до різних ресурсів мережі.	це програмне забезпечення, яке призначене для захисту комп'ютерів та інших пристроїв в мережі від вірусів та інших шкідливих програм.	це система, яка дозволяє контролювати стан мережі та виявляти можливі проблеми в роботі мережі. Система моніторингу мережі дозволяє швидко виявляти та вирішувати проблеми, що виникають в мережі.
–Брандмауер (firewall) 	–Система ідентифікації та автентифікації користувачів (Identity and Access Management System) 	–Антивірусне програмне забезпечення 	–Система моніторингу мережі (Network Monitoring System) 

Рисунок 1.4 – Компоненти корпоративної мережі [14]

Під час розробки корпоративної мережі для підприємства можуть визначатися різноманітні складові мережі, що відповідають вимогам та потребам конкретного підприємства. Однак, важливо пам'ятати про забезпечення безпеки та захисту мережі від різних загроз.

1.2 Системи безпеки в мережах

У сучасному світі комп'ютерні мережі стали необхідною складовою частиною функціонування більшості підприємств. Зростання кількості інформації, яка обробляється в мережах, а також поява нових загроз з боку зловмисників змушують компанії активно застосовувати системи безпеки в комп'ютерних мережах. У цьому розділі розглянемо основні аспекти безпеки в комп'ютерних мережах та методи захисту від різних загроз.

Однією з найбільш серйозних загроз для комп'ютерних мереж є хакерські атаки. Хакерські атаки можуть мати різні цілі: викрадення конфіденційної інформації, завдання шкоди роботі системи, встановлення шпигунського програмного забезпечення, використання мережі для злочинних цілей та інше. Крім того, комп'ютерні мережі можуть бути підвернуті атакам з боку вірусів, черв'яків, троянських програм та інших шкідливих програм [15].

Основними складовими систем безпеки в комп'ютерних мережах є: аутентифікація та авторизація користувачів, шифрування даних, firewalls та інші системи перевірки на проникнення, антивірусне програмне забезпечення та системи виявлення вторгнень.

Планування та впровадження систем безпеки в комп'ютерні мережі є критично важливим для забезпечення безпеки та захисту від потенційних загроз. Підприємства повинні ретельно аналізувати свої потреби у безпеці та забезпечити відповідну систему захисту від потенційних загроз.

Загрози для комп'ютерних мереж стають все більш серйозними, і тому системи безпеки в комп'ютерних мережах стають необхідністю. Для

забезпечення найвищого рівня безпеки комп'ютерної мережі не обхідно ретельно аналізувати потенційні загрози та використовувати найефективніші методи захисту, такі як аутентифікація, авторизація, шифрування даних та системи виявлення вторгнень [16]. Планування та впровадження систем безпеки повинні бути проведені з урахуванням специфіки конкретного підприємства та його потреб у безпеці.

Захист від потенційних загроз комп'ютерної мережі є необхідним для забезпечення продуктивності та ефективності роботи підприємства. Системи безпеки в комп'ютерних мережах є ключовим фактором у забезпеченні безпеки та захисту від можливих загроз, тому необхідно вкладати зусилля у їх розробку та впровадження [17].

У цьому розділі ми розглянули основні загрози, які становлять потенційну небезпеку для комп'ютерних мереж, а також методи та системи, що використовуються для забезпечення безпеки в комп'ютерних мережах. Важливість планування та впровадження систем безпеки в комп'ютерні мережі була підкреслена, щоб наголосити на необхідності ретельно аналізувати потенційні загрози та використовувати ефективні методи захисту для забезпечення безпеки в комп'ютерних мережах.

1.3 Методи захисту даних у корпоративних мережах

Однією з основних функцій корпоративних мереж є забезпечення безпеки та захисту конфіденційної інформації, що обмінюється між пристроями та користувачами в мережі. У зв'язку з цим, у мережах зазвичай використовуються різні методи захисту даних, що дозволяють забезпечити конфіденційність, цілісність та доступність даних [18].

Актуальні проблема захисту інформації від загроз різного типу, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем/мереж відбувається з таких причин (рис. 1.5) [19].

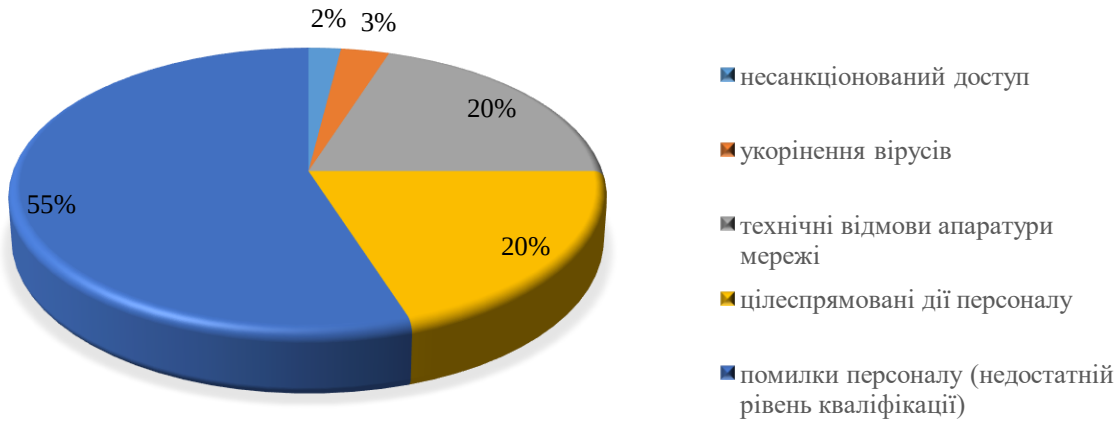


Рисунок 1.5 – Причини порушення захисту мереж

Шифрування даних є одним з найбільш ефективних методів захисту даних в корпоративних мережах (табл. 1.2) [20]. Шифрування може бути застосоване для захисту даних від несанкціонованого доступу під час їх передачі через мережу, а також для захисту даних, що зберігаються на комп'ютерах та серверах. Використання шифрування також може допомогти запобігти злому мережі через використання безпечного каналу зв'язку між комп'ютерами та серверами.

Таблиця 1.2 – Переваги та недоліки методів шифрування

Методи шифрування	**Переваги**	**Недоліки**
Симетричне шифрування	– Висока швидкість шифрування. – Менша довжина ключа, ніж в асиметричному шифруванні. – Проста реалізація.	– Публічна передача ключів, враховуючи велику ймовірність порушення секретності ключа. – Квадратична залежність числа ключів при великій кількості користувачів.
Асиметричне шифрування, або шифрування з відкритим ключем	– Вирішена проблема розподілу ключів між користувачами, так як кожен користувач може згенерувати	– Повільніше ніж симетричне шифрування, оскільки при шифруванні і розшифрування

Методи шифрування	Переваги	Недоліки
	свою пару ключів сам, а відкриті ключі користувачів можуть вільно публікуватися. – Зникає квадратична залежність числа ключів від числа користувачів (2N та N(N-1)/2).	використовуються досить ресурсомісткі операції. – Необхідність захисту відкритих ключів від підміни. – Немає математичних доказів незворотності використовуваних функцій.

Метод захисту даних - це використання систем авторизації та аутентифікації користувачів в мережі. Системи авторизації та аутентифікації дозволяють обмежувати доступ до конфіденційних даних лише користувачам з необхідними правами доступу. Це може бути досягнуто через використання паролів, біометричних методів аутентифікації та інших методів ідентифікації користувачів [21].

Системи контролю доступу до даних є ще одним методом захисту даних в корпоративних мережах. Ці системи дозволяють обмежувати доступ до даних лише користувачам з необхідними правами доступу. Такі системи можуть бути встановлені на різних рівнях мережі, включаючи рівень комп'ютерів та серверів, рівень мережевого обладнання та рівень фізичного доступу до приміщень з комп'ютерами та серверами.

Ще одним із методів захисту даних є використання систем моніторингу та виявлення загроз. Такі системи дозволяють відстежувати та аналізувати активність користувачів у мережі, виявляти загрози та зловмисну діяльність та приймати заходи для їх усунення. Системи моніторингу та виявлення загроз можуть бути використані як для захисту мережі в режимі реального часу, так і для аналізу подій, які вже сталися [22].

Додатковим методом захисту даних в корпоративних мережах є використання систем резервного копіювання даних. Системи резервного копіювання дозволяють зберігати копії даних на інших серверах або зовнішніх пристроях з метою забезпечення доступності даних у разі втрати основних копій [23]. Регулярне створення резервних копій даних є важливим

елементом стратегії захисту даних та може допомогти зменшити наслідки випадків втрати або пошкодження даних.

Важливим аспектом методів захисту даних в корпоративних мережах є також їх інтеграція з політикою безпеки підприємства. Ефективна політика безпеки повинна визначати не лише технічні методи захисту даних, а й принципи та процедури використання цих методів, а також відповідальність за їх виконання. Крім того, ефективна політика безпеки повинна забезпечувати навчання та тренінги користувачів мережі з питань безпекної поведінки та забезпечувати проактивний підхід до захисту даних [24].

Одним з ефективних методів інтеграції методів захисту даних в політику безпеки підприємства є використання стандартів та нормативних документів. Такі документи можуть містити рекомендації та вимоги щодо захисту даних, які можуть бути використані як основа для розробки політики безпеки та вибору методів захисту даних.

Окрім технічних методів захисту даних, важливим елементом захисту даних в корпоративних мережах є забезпечення фізичної безпеки. Це означає захист приміщень з комп'ютерами та серверами від несанкціонованого доступу та забезпечення контролю за фізичним доступом до обладнання. Для забезпечення фізичної безпеки можуть використовуватися різноманітні засоби, включаючи системи контролю доступу, відеоспостереження та засоби ідентифікації користувачів.

Узагальнюючи, методи захисту даних в корпоративних мережах можуть включати різноманітні технічні та організаційні заходи. Ефективний захист даних вимагає інтеграції різних методів та підходів, включаючи технічні засоби захисту даних, політику безпеки підприємства, навчання та тренінги користувачів та забезпечення фізичної безпеки. Використання стандартів та нормативних документів може допомогти вибрати та інтегрувати ефективні методи захисту даних.

РОЗДІЛ 2. АНАЛІЗ ПОТРЕБ ТА РИЗИКІВ ПІДПРИЄМСТВА

2.1 Оцінка поточного стану мережі підприємства

Вибір концепції побудови конкретної корпоративної мережі визначається цілою низкою чинників: затребувані інформаційні послуги, обсяги переданого трафіку, існуюча інфраструктура і т. д. Але існують і загальні вимоги до корпоративних мереж. Мережі підприємств повинні бути побудовані на основі перевірених технологій, що володіють такими якостями, як масштабованість, гнучкість, мультисервісність, і найголовніше – надійність [25].

Першим кроком в аналізі потреб є вивчення поточного стану мережі та її вимог щодо безпеки. Це включає огляд існуючих систем безпеки, ідентифікацію поточних проблем безпеки та визначення обсягу даних, що потребують захисту. Для цього можуть використовуватися методи опитування користувачів та технічних спеціалістів, аудит мережі та її складових, а також вивчення правових вимог щодо захисту даних.

Другим кроком є визначення потенційних ризиків для мережі та її даних. Це може включати аналіз історії інцидентів безпеки, ідентифікацію можливих загроз, оцінку рівня вразливості мережі та її компонентів, а також вивчення загроз від зовнішніх атак.

Після вивчення потреб та ризиків підприємства, можна розробити план заходів щодо забезпечення безпеки мережі. Цей план має включати рекомендації щодо вдосконалення існуючих систем безпеки, використання нових систем та технологій, встановлення політик безпеки та процедур, навчання користувачів та персоналу, а також розробку плану відновлення після інцидентів безпеки.

Підсумовуючи, аналіз потреб та ризиків є важливою складовою ефективної розробки захищеної корпоративної мережі. Цей аналіз допомагає підприємству зрозуміти свої потреби щодо безпеки мережі та виявити потенційні ризики для неї. Результатом аналізу є план заходів щодо

забезпечення безпеки мережі, який має включати рекомендації щодо вдосконалення існуючих систем безпеки, встановлення політик безпеки та процедур, використання нових технологій та розробку плану відновлення після інцидентів безпеки. Ці заходи допоможуть забезпечити надійний та ефективний захист мережі та її даних від потенційних загроз [26].

Цей аналіз дозволяє отримати повну картину поточного стану мережі, що може бути використана для планування майбутнього розвитку мережі та покращення її ефективності.

Один з перших кроків в аналізі поточного стану мережі полягає в огляді існуючої інфраструктури мережі. Це включає огляд апаратного та програмного забезпечення, топології мережі, розташування мережевих пристроїв та їх конфігурацію, наявність резервних копій даних та процедури відновлення після непередбачуваних ситуацій.

Далі слід провести аудит мережі, що дозволить виявити можливі проблеми та вразливості, а також з'ясувати, чи відповідає мережа поточним вимогам підприємства. Для цього можна використовувати різні інструменти та методики, наприклад, пакетний аналізатор мережі, сканер вразливостей, перевірку на дотримання стандартів безпеки мережі [27].

Для забезпечення високої продуктивності мережі необхідно провести аналіз трафіку, що протікає через мережу. Це дозволить виявити надмірну витрату ресурсів мережі та знайти шляхи їх оптимізації. Для аналізу трафіку можуть використовуватися спеціальні інструменти моніторингу трафіку.

Наступним кроком в аналізі поточного стану мережі є вивчення поточних проблем з безпекою мережі та її компонентів. Це включає огляд стандартів безпеки, які використовуються в мережі, аналіз потенційних загроз та вразливостей мережі та оцінку ризику безпеки. Для цього можуть використовуватися спеціалізовані інструменти, такі як сканер вразливостей та програмне забезпечення для аналізу безпеки мережі.

Після проведення всіх необхідних аналізів поточного стану мережі слід зібрати отримані дані та підготувати звіт про результати аналізу. Цей звіт має

містити опис існуючої мережевої інфраструктури, виявлені проблеми та вразливості, а також рекомендації щодо покращення безпеки та ефективності мережі.

Отримані результати аналізу поточного стану мережі можуть бути використані для планування майбутнього розвитку мережі та покращення її ефективності. На основі зібраних даних можуть бути запропоновані різні рішення, такі як модернізація апаратного та програмного забезпечення, оптимізація трафіку мережі, впровадження нових технологій та забезпечення високої безпеки мережі.

2.2 Визначення потреб у новій корпоративній мережі

Цей етап передбачає аналіз бізнес-потреб та вимог користувачів до мережі, що дозволяє визначити функціональні вимоги та характеристики, які має мати нова мережа (рис. 2.1) [28].

Рисунок 2.1 – Схема корпоративної мережі

Для визначення потреб у новій корпоративній мережі необхідно спілкуватися з різними групами користувачів, включаючи керівництво підприємства, менеджерів з інформаційних технологій, адміністраторів

мережі та звичайних користувачів. Важливо з'ясувати їх поточні проблеми з мережею, що вони хотіли б покращити, а також очікування від нової мережі.

Далі необхідно провести аналіз поточних бізнес-процесів та їх взаємодії з мережею. Це дозволить визначити, які функції та можливості повинна мати нова мережа для забезпечення ефективної роботи бізнес-процесів підприємства.

Під час визначення потреб у новій корпоративній мережі слід також звернути увагу на майбутні потреби підприємства. Наприклад, якщо підприємство планує збільшення кількості працівників, то мережа повинна бути масштабованою та готовою до збільшення навантаження [29].

Визначення потреб у новій корпоративній мережі є важливим етапом, який дозволяє зрозуміти, які характеристики мережі потрібні для задоволення бізнес-потреб та вимог користувачів. Це в свою чергу допускає процес проектування та розробки мережі, що відповідає потребам підприємства та сприяє його успішному функціонуванню.

Після визначення потреб у новій корпоративній мережі можна скласти технічне завдання на проектування та розробку мережі, яке повинно включати в себе всі вимоги та характеристики, що були виявлені на етапі визначення потреб. Крім того, на основі визначених потреб можна вибрати оптимальні рішення щодо технологій та обладнання, що будуть використовуватися в мережі.

У процесі визначення потреб у новій корпоративній мережі слід також звернути увагу на безпеку даних та мережі загалом. Важливо враховувати потенційні загрози та ризики, що можуть виникнути в процесі використання мережі, та визначити необхідні заходи для їх запобігання.

Визначення потреб у новій корпоративній мережі є ключовим етапом в проектуванні мережі для підприємства. Цей етап дозволяє визначити функціональні вимоги та характеристики мережі, що необхідні для забезпечення ефективної роботи бізнес-процесів підприємства та задоволення вимог користувачів.

2.3 Визначення ризиків безпеки в мережі підприємства

Ризики безпеки пов'язані з можливими загрозами, які можуть призвести до порушення конфіденційності, цілісності та доступності даних підприємства, а також до підключення мережі [30].

Виходячи з проведеного аналізу, всі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи (рис. 2.2) [31].

Рисунок 2.2 – Джерела загроз

Для визначення ризиків безпеки необхідно провести аналіз потенційних загроз та вразливостей мережі, які можуть бути використані для злому та несанкціонованого доступу до даних. Серед можливих загроз можуть бути віруси, троянські програми, хакерські атаки, фішинг, витоки інформації та інші.

Також необхідно проаналізувати заходи безпеки, які вже існують в мережі, та визначити їх ефективність. Якщо поточні заходи безпеки не задовольняють потреб підприємства, то необхідно розробити нові стратегії безпеки та внести необхідні зміни до проекту корпоративної мережі.

Для запобігання можливим ризикам безпеки необхідно встановити процедури і правила, які регулюватимуть доступ до мережі, забезпечать захист від зломів та забезпечать резервне копіювання даних. Також необхідно встановити систему моніторингу мережі, яка дозволить вчасно виявляти загрози та проводити аналіз їхнього впливу на мережу.

Визначення ризиків безпеки в мережі підприємства є важливим етапом проектування корпоративної мережі, оскільки це дозволяє запобігти можливим загрозам та забезпечити захист від несанкціонованого доступу до даних підприємства [32].

РОЗДІЛ 3. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Вибір архітектури мережі

Проектування корпоративної мережі - це процес розробки детального плану нової мережі для підприємства, який включає в себе визначення технічних вимог, вибір обладнання та програмного забезпечення, налаштування мережі та її тестування [33].

Першим кроком у проектуванні корпоративної мережі є визначення архітектури мережі. Це включає визначення типу мережі (локальна, міська, глобальна) та топології мережі (зірка, дерево, лінія). Також потрібно визначити типи з'єднань між мережевими пристроями, наприклад, бездротові або дротові з'єднання.

Другим кроком є вибір обладнання та програмного забезпечення для нової мережі. Необхідно вибрати мережеві пристрої (маршрутизатори, комутатори, firewalls) та серверне обладнання, що відповідає вимогам підприємства. Також необхідно вибрати програмне забезпечення для керування мережею та забезпечення безпеки даних.

Третім кроком є налаштування мережі та її тестування. Це включає встановлення налаштувань на мережевих пристроях, налаштування безпеки мережі та перевірку правильності функціонування мережі. Тестування мережі важливо для виявлення можливих проблем та їх виправлення до використання мережі в бізнес-процесах.

Проектування корпоративної мережі - це важливий етап у створенні ефективної та безпечної мережі для підприємства. Цей процес дозволяє визначити потреби підприємства у новій мережі та підібрати найкраще обладнання та програмне забезпечення для задоволення цих потреб. Добре спроектована мережа допоможе підприємству забезпечити ефективну роботу співробітників, зберігання та обмін даними, а також зменшити ризики виникнення проблем з безпекою. Крім того, корпоративна мережа може бути

скаладною та масштабованою, що дозволить легко додавати нові компоненти та розширювати мережу у майбутньому [34].

Вибір архітектури мережі - це важливий етап проектування корпоративної мережі, який передбачає вибір типу мережі та її топології. Від правильного вибору архітектури мережі залежить ефективність та безпека її функціонування [35].

Першим кроком у виборі архітектури мережі є визначення типу мережі. Це може бути локальна мережа (LAN), міська мережа (MAN) або глобальна мережа (WAN). Локальна мережа призначена для зв'язку комп'ютерів та інших мережевих пристроїв у межах одного приміщення або будівлі. Міська мережа забезпечує зв'язок між комп'ютерами та іншими пристроями у межах міста або регіону. Глобальна мережа, така як Інтернет, забезпечує зв'язок між комп'ютерами та іншими пристроями по всьому світу [36].

Другим кроком є вибір топології мережі. Топологія мережі визначає, як пристрої підключені до мережі та як вони комунікують між собою.

Найпоширеніші топології мережі - це зірка, дерево, кільце та лінія (рис. 3.1) [37].

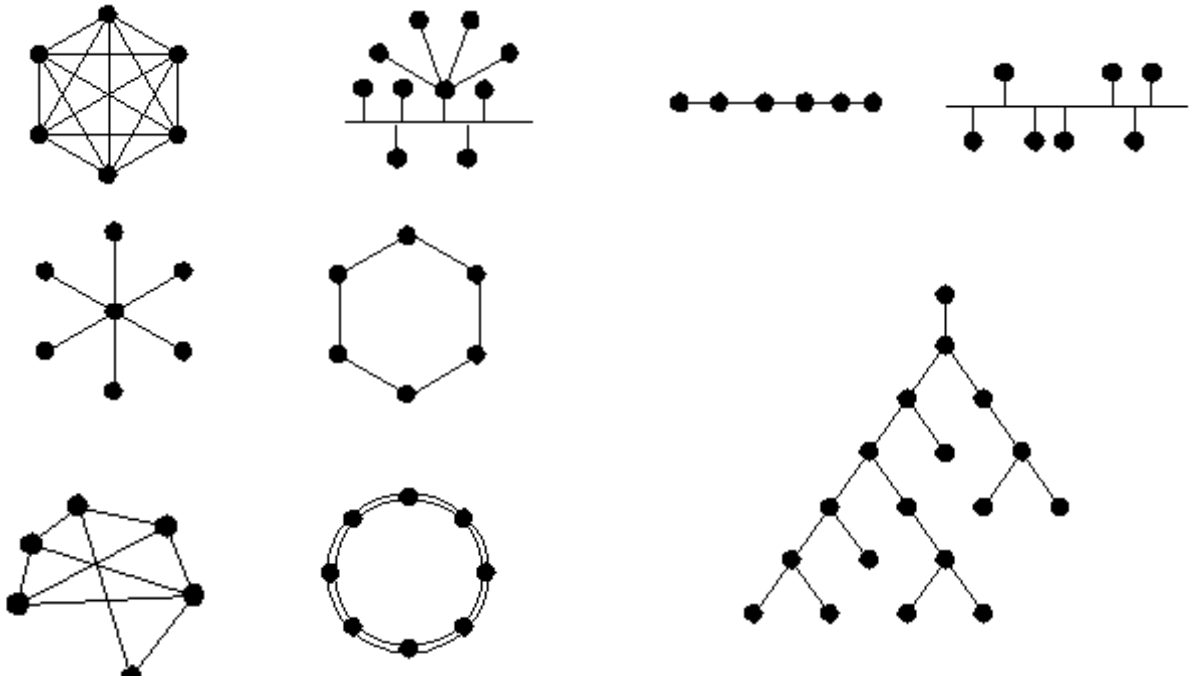


Рисунок 3.1 – Види топології мереж

У топології зірки, всі пристрої підключені до центрального пристрою (зазвичай це комутатор або концентратор). Кожен пристрій може спілкуватись з центральним пристроєм, але не може безпосередньо спілкуватись з іншими пристроями, не використовуючи центральний пристрій.

У топології дерева, пристрої підключені до інших пристроїв в ієрархічній структурі, утворюючи деревоподібну топологію. Кожен рівень мережі може мати свій центральний пристрій, до якого підключені інші пристрої, і так далі.

У топології лінії, пристрої підключені один до одного у лінію. Кожен пристрій може спілкуватись тільки з пристроями, які безпосередньо підключені до нього.

У топології кільця, пристрої підключені один до одного у кільце. Кожен пристрій може спілкуватись тільки з пристроями, які знаходяться поруч з ним, але дана топологія дозволяє створити дві зв'язані шляхи між будь-якими двома пристроями, що забезпечує зменшення впливу випадкових відмов. Переваги та недоліки представлені у табл. 3.1.

Таблиця 3.1 – Переваги та недоліки основних видів топології мережі

Топологія	Переваги	Недоліки
Зірка	Простота керування, надійність, простота розширення	Один вузол може спричинити відмову всієї мережі
Коло	Дуже надійна, простота розширення	Відмова одного вузла може призвести до відмови всієї мережі
Лінія	Простота реалізації, дешевизна	Низька надійність, відмова одного вузла перериває всю мережу, обмежена пропускна спроможність
Дерево	Надійність, простота керування, підтримка великої кількості вузлів	Залежність від кореневого вузла, відмова кореневого вузла може викликати відмову дерева

При виборі архітектури мережі важливо враховувати потреби та мету мережі. Наприклад, якщо мережа призначена для невеликої компанії з обмеженим бюджетом, то вибір локальної мережі з топологією зірки може бути оптимальним рішенням. Якщо мережа повинна забезпечити зв'язок між віддаленими офісами компанії, то глобальна мережа з топологією VPN може бути кращим варіантом.

Також важливо враховувати рівень безпеки та стійкості мережі. Наприклад, топологія зірки забезпечує високий рівень доступності та легкість управління, але може бути менш стійкою до відмов пристроїв. Топологія дерева забезпечує більшу стійкість до відмов, але може бути складнішою управляти. Вибір архітектури мережі повинен бути зроблений з урахуванням компромісів між різними факторами, такими як ефективність, безпека та стійкість.

Нарешті, важливо вибрати правильні пристрої для мережі, такі як комутатори, маршрутизатори та firewalls, які відповідають вибраній архітектурі мережі. Наприклад, для мережі з топологією зірки необхідні комутатори з достатньою кількістю портів, а для мережі з топологією VPN необхідні маршрутизатори з підтримкою протоколів маршрутизації та безпеки.

Узагальнюючи, вибір архітектури мережі - це важливий етап проектування корпоративної мережі, який вимагає уважного аналізу потреб та мети мережі, а також урахування рівня безпеки та стійкості.

3.2 Проектування мережевої інфраструктури

Проектування мережевої інфраструктури - це процес створення детального плану мережі, включаючи її архітектуру, топологію, обладнання, програмне забезпечення, комунікаційні протоколи та інші складові. Цей процес вимагає ретельного аналізу потреб користувачів та бізнес-вимог до мережі, щоб забезпечити надійність, ефективність та безпеку мережі.

Один з перших кроків у проектуванні мережевої інфраструктури - це визначення географічного розташування мережі та її розмірів. Це дозволить визначити необхідність обладнання, кількість вузлів та вузлів мережі, а також пропускну здатність мережі [38].

Наступним кроком є вибір архітектури мережі та її топології, які повинні відповідати потребам бізнесу та користувачів. Наприклад, велика корпорація, що має кілька офісів у різних містах, може використовувати WAN для забезпечення зв'язку між офісами, а також LAN для зв'язку в межах окремих офісів.

Після вибору архітектури мережі та її топології необхідно вибрати обладнання, таке як маршрутизатори, комутатори, сервери та інші мережеві пристрої, які будуть використовуватися у мережі. При виборі обладнання необхідно враховувати його характеристики, такі як швидкість передачі даних, об'єм пам'яті, кількість портів та інші.

Далі необхідно вибрати програмне забезпечення, яке буде використовуватися для управління та роботи мережі. Програмне забезпечення може включати в себе операційну систему для мережевих пристроїв, системи безпеки, програмне забезпечення для моніторингу мережі та інші.

Після вибору обладнання та програмного забезпечення необхідно розробити план встановлення та налаштування мережевої інфраструктури. Цей план повинен включати процес встановлення та налаштування обладнання, встановлення програмного забезпечення, налаштування параметрів мережі та інші кроки.

Також важливим аспектом проектування мережевої інфраструктури є забезпечення безпеки мережі. Для цього можуть бути використані різні методи, такі як налаштування прав доступу до мережі, використання систем автентифікації та авторизації, налаштування firewalls та інші заходи безпеки.

Останнім етапом проектування мережевої інфраструктури є тестування та налагодження мережі. Під час тестування необхідно перевірити роботу

мережі та її складових, визначити можливі проблеми та вирішити їх. Налагодження мережі повинно включати налаштування параметрів мережі та її складових для забезпечення максимальної продуктивності та ефективності роботи.

Узагальнюючи, проектування мережевої інфраструктури - це складний процес, який вимагає детального аналізу потреб користувачів та бізнес-вимог до мережі, вибору оптимальної архітектури та топології мережі, вибору обладнання та програмного забезпечення, розробки плану встановлення та налаштування мережі, забезпечення безпеки мережі та тестування та налагодження мережі. Цей процес важливий для будь-якої компанії або організації, яка має потребу в мережевій інфраструктурі. Правильно спроектована мережева інфраструктура допоможе забезпечити надійну та ефективну роботу мережі, що, у свою чергу, сприятиме ефективному функціонування бізнесу або організації. Тому, проектування мережевої інфраструктури є важливим етапом у будь-якому IT проекті та потребує професійного підходу та досвіду в цій сфері.

3.3 Вибір системи безпеки та методів захисту даних

Мета системи безпеки полягає в тому, щоб забезпечити захист мережі від несанкціонованого доступу, зберігати цілісність та конфіденційність даних, а також забезпечувати належну продуктивність мережі [39].

Під час вибору системи безпеки потрібно враховувати бізнес-вимоги до захисту даних та відповідність законодавчим вимогам щодо захисту персональних даних. Необхідно також звернути увагу на обсяг та тип даних, які будуть передаватись та зберігатись у вашій корпоративній мережі.

Основні методи захисту даних, включають (рис. 3.2.) [40]:

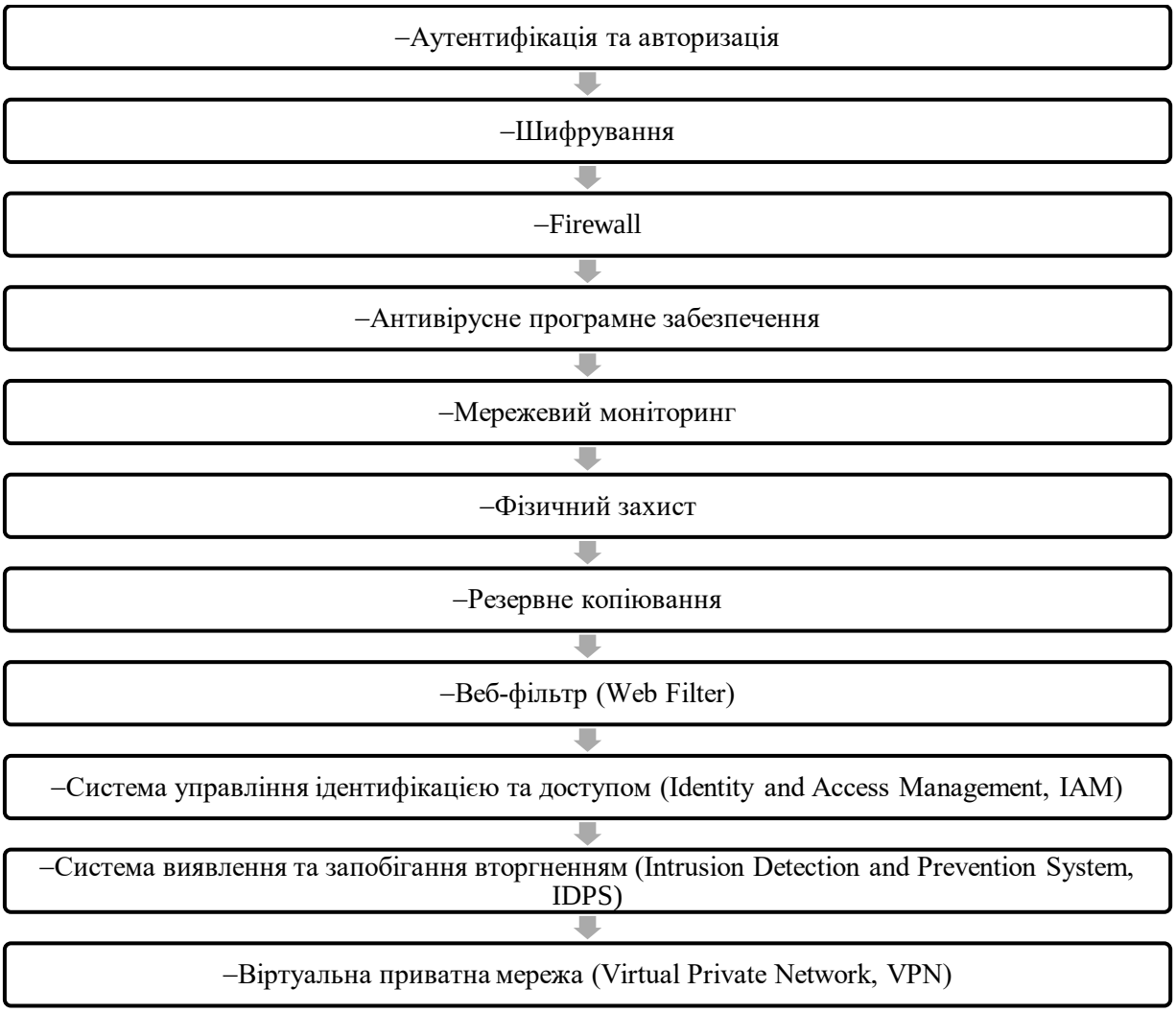


Рисунок 3.2 – Методи захисту даних

– Аутентифікацію та авторизацію: ці методи дозволяють забезпечити доступ до мережі лише для авторизованих користувачів. Для цього використовуються різні методи аутентифікації, такі як логіни та паролі, біометричні дані, токени або смарт-карти [41].

– Шифрування: цей метод захисту даних дозволяє забезпечити конфіденційність даних, переданих по мережі, шляхом перетворення зрозумілого тексту на зашифрований, незрозумілий для сторонніх осіб, які не мають прав доступу до даних. Для шифрування можна використовувати різні методи, такі як SSL, VPN або IPSec. SSL дозволяє зашифрувати трафік між веб-сайтом та користувачем, VPN створює захищену тунельну зону між двома точками, щоб захистити дані, які передаються по мережі, а IPSec

забезпечує конфіденційність та цілісність даних, що передаються по Інтернету. Вибір методу шифрування залежить від потреб конкретного підприємства, його розміру та інфраструктури мережі.

– Firewall: цей метод захисту даних дозволяє забезпечити захист мережі від несанкціонованого доступу та зберегти цілісність даних. firewall дозволяє контролювати доступ до мережі, блокувати небезпечний трафік та запобігати злому мережі. Є два типи firewalls: мережевий та програмний. Мережевий firewall встановлюється на роутер або комутатор та контролює трафік, що проходить через нього. Програмний firewall встановлюється на окремий комп'ютер та контролює трафік, що приходить на цей комп'ютер. Вибір firewall залежить від розміру та типу мережі, потреб користувачів та бізнес-вимог щодо захисту даних [41].

– Антивірусне програмне забезпечення: цей метод захисту даних дозволяє забезпечити захист мережі від вірусів та шкідливого програмного забезпечення. Антивірусне програмне забезпечення здатне виявляти та блокувати віруси та інші.

– Мережевий моніторинг - цей метод дозволяє відстежувати активність мережі та виявляти потенційні загрози. Використовуються різні інструменти моніторингу, такі як системи моніторингу подій, системи виявлення вторгнень та інші.

– Фізичний захист - цей метод включає фізичний доступ до серверних кімнат та інших приміщень, в яких знаходиться мережне обладнання. Це може включати використання систем контролю доступу, відеоспостереження та інші методи.

– Резервне копіювання - цей метод дозволяє зберегти копію важливих даних та інформації в разі їх втрати або пошкодження. Використовуються різні методи резервного копіювання, такі як регулярне копіювання на зовнішні пристрої або використання хмарних сервісів.

– Веб-фільтр (Web Filter) - це програмне або апаратне забезпечення, що використовується для контролю та фільтрації доступу до веб-сайтів на основі заздалегідь визначених правил і політик. Його головна мета полягає в блокуванні доступу до шкідливих, небажаних або нецензурних веб-сторінок або категорій контенту. Веб-фільтри можуть використовуватися в різних середовищах, включаючи домашні мережі, школи, підприємства та інші організації. Вони можуть реалізовувати різні методи фільтрації, такі як ключові слова, URL-адреси, категорії контенту, списки блокування та інші параметри, щоб визначити, які веб-сайти чи типи контенту можуть бути доступні або блоковані для користувачів мережі.

– Система управління ідентифікацією та доступом (Identity and Access Management, IAM) - це набір процесів, політик, технологій та інструментів, які дозволяють організаціям керувати правами доступу користувачів до різних ресурсів їхньої мережі та систем. IAM забезпечує контроль над ідентифікацією користувачів, їхніми аутентифікаційними даними і авторизацією, що дозволяє визначити, які користувачі мають доступ до яких ресурсів та які дії вони можуть виконувати в цьому контексті

– Система виявлення та запобігання вторгненням (Intrusion Detection and Prevention System, IDPS) - це комплексний набір технологій та процесів, які призначені для виявлення, моніторингу та запобігання спробам несанкціонованого доступу до мережі або комп'ютерних систем. IDPS використовується для виявлення різних видів загроз, таких як злам, вторгнення, шкідливе програмне забезпечення, атаки на мережеві протоколи та інші аномальні активності. Він працює на основі аналізу мережевого трафіку, системних журналів, подій і спеціальних сигнатур атак, щоб виявити потенційно шкідливі або небезпечні дії.

– Віртуальна приватна мережа (Virtual Private Network, VPN) - це технологія, яка створює безпечне з'єднання та шифрує передачу даних між віддаленими користувачами та корпоративною мережею через незахищену публічну мережу, таку як Інтернет. VPN дозволяє створити віртуальний

тунель між користувачем та мережею, який забезпечує конфіденційність, цілісність та захист передачі даних. Всі дані, які передаються через VPN, шифруються, що ускладнює можливість перехоплення або читання інформації третіми особами.

Під час вибору системи безпеки та методів захисту даних, слід враховувати бізнес-вимоги підприємства, характеристики мережевої інфраструктури, бюджет підприємства та законодавчі вимоги щодо захисту даних. Для досягнення максимальної ефективності, можна розглянути використання комплексної системи захисту, що включає різноманітні методи та технології.

РОЗДІЛ 4. РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Встановлення та налаштування мережевого обладнання

Цей етап передбачає фізичне встановлення необхідного обладнання, налаштування мережевих пристроїв та програмного забезпечення.Першим кроком в реалізації корпоративної мережі є встановлення мережевого обладнання, такого як комутатори, маршрутизатори та firewalls. Після встановлення обладнання необхідно налаштувати мережеві пристрої та програмне забезпечення для забезпечення оптимальної продуктивності мережі.

Один з ключових елементів налаштування корпоративної мережі - це встановлення IP-адрес та мережевих параметрів для кожного мережевого пристрою. Це дозволяє забезпечити належну роботу пристроїв та оптимальну передачу даних по мережі.

Для забезпечення безпеки мережі необхідно правильно налаштувати firewall та інші засоби захисту даних, такі як VPN та антивірусне програмне забезпечення [42]. Налаштування firewall дозволяє контролювати доступ до мережі та блокувати небезпечний трафік, а VPN забезпечує захист даних, переданих по мережі.

Для забезпечення належної продуктивності мережі необхідно налаштувати роутери та комутатори таким чином, щоб забезпечити оптимальний розподіл трафіку та уникнути перевантаження мережі. Для цього використовуються різні методи, такі як VLAN, QoS та інші.

Окрім налаштування мережевих пристроїв, важливим етапом реалізації корпоративної мережі є налаштування серверів та програмного забезпечення, необхідного для роботи мережі [43].

Налаштування серверів передбачає встановлення необхідного програмного забезпечення, налаштування операційної системи, створення

користувачів та груп, налаштування доступу до ресурсів мережі, налаштування безпеки та інших параметрів.

Для належної роботи мережі також необхідно налаштувати різноманітне програмне забезпечення, таке як системи керування базами даних, електронної пошти, веб-сервери, firewalls та інші. Налаштування цього програмного забезпечення має бути виконане з урахуванням бізнес-вимог та вимог до безпеки даних.

Після налаштування мережевих пристроїв, серверів та програмного забезпечення, необхідно забезпечити тестування та відлагодження мережі. Тестування мережі має на меті перевірити налаштування мережевих пристроїв, серверів та програмного забезпечення, а також перевірити пропускну здатність та навантаження мережі. Тестування також допомагає виявити можливі проблеми та забезпечити належний рівень функціональності та безпеки мережі.

Після успішного тестування мережі, необхідно провести навчання персоналу, який буде використовувати мережу. Це має на меті забезпечити належне розуміння користувачами принципів роботи мережі, її можливостей та обмежень, а також вимог до безпеки даних та захисту мережі від несанкціонованого доступу.

Встановлення та налаштування мережевого обладнання є ключовим етапом при розробці захищеної корпоративної мережі. Цей процес включає в себе встановлення та налаштування різноманітного обладнання, такого як комутатори, маршрутизатори та firewall.

Першим етапом є вибір необхідного мережевого обладнання з урахуванням потреб підприємства. Для забезпечення високої доступності та масштабованості мережі, можна використовувати комутатори з підтримкою технологій STP та Virtual LANs (VLANs), а також маршрутизатори з підтримкою динамічного маршрутизування [44].

Після вибору необхідного обладнання, наступним етапом є його встановлення та фізичне підключення до мережі. При цьому слід

дотримуватись рекомендацій виробників та стандартів, щоб забезпечити надійну та безпечну роботу мережевого обладнання.

Далі необхідно налаштувати параметри мережевого обладнання, такі як IP-адреси, підмережі, шлюзи, DNS-сервери та інші параметри. Важливо дотримуватись загальних принципів налаштування мережі, таких як використання маршрутизації, сегментації мережі та використання VPN для забезпечення безпеки мережі.

Наступним етапом є налаштування мережевої безпеки, включаючи налаштування firewalls, системи ідентифікації та аутентифікації користувачів, інспекції пакетів та інших заходів безпеки. Ці заходи забезпечують надійний захист мережі від зловмисних атак та несанкціонованого доступу до даних.

Також важливим етапом встановлення та налаштування мережевого обладнання є моніторинг та діагностика мережі. Для цього можна використовувати спеціальне програмне забезпечення, яке дозволяє відстежувати стан мережі, виявляти проблеми та швидко їх вирішувати.

При розгортанні корпоративної мережі необхідно також дотримуватись правил безпеки, таких як використання складних паролів, захист від несанкціонованого доступу, резервне копіювання даних та інші заходи безпеки.

Усі етапи встановлення та налаштування мережевого обладнання мають бути проведені професійними фахівцями, які мають достатній рівень знань та досвіду у цій галузі. Також слід звернути увагу на регулярне оновлення програмного забезпечення та апаратного забезпечення мережі для забезпечення її безпеки та надійності.

Отже, встановлення та налаштування мережевого обладнання є важливим етапом при розробці корпоративної мережі, який вимагає пильної уваги та професійного підходу для забезпечення безпеки та надійності мережі.

4.2 Встановлення та налаштування системи безпеки

Встановлення та налаштування системи безпеки є важливим етапом при розробці захищеної корпоративної мережі. Цей процес включає в себе налаштування антивірусного програмного забезпечення, системи виявлення та запобігання вторгнень, системи моніторингу та аудиту мережі, а також резервного копіювання даних.

Першим етапом встановлення системи безпеки є вибір необхідного програмного забезпечення. Найбільш поширеними рішеннями є комерційні продукти, такі як McAfee, Symantec та Kaspersky, але також існує безліч безкоштовних антивірусних програм, таких як Avast та AVG. Для системи виявлення та запобігання вторгнень можна використовувати різноманітне програмне забезпечення, таке як Snort, Suricata та OSSEC.

Другим етапом є встановлення та налаштування програмного забезпечення системи безпеки. Для цього слід встановити програмне забезпечення на всі комп'ютери та сервери в мережі та налаштувати його відповідно до потреб організації. Налаштування включає в себе встановлення правил фільтрації, налаштування сканування систем та розкладу оновлень.

Третім етапом є створення правил безпеки, які визначають, які користувачі мають доступ до певних ресурсів та які дії вони можуть виконувати. Правила безпеки повинні бути створені з урахуванням потреб організації та повинні бути належним чином налаштовані та оновлюватись відповідно до змін у мережі.

Четвертим етапом є моніторинг та аудит мережі, щоб виявляти можливі загрози безпеці. Для цього можна використовувати системи моніторингу та аудиту мережі можна використовувати різноманітні системи моніторингу, такі як Nagios, Zabbix, або PRTG. Ці системи дозволяють відстежувати стан мережевих пристроїв, серверів та додатків, а також надсилати повідомлення про можливі проблеми або несправності. Аудит

мережі дозволяє відслідковувати дії користувачів у мережі та виявляти можливі загрози безпеці.

Останнім етапом є створення резервних копій даних. Резервне копіювання даних є важливим елементом системи безпеки, оскільки дозволяє відновити дані у випадку їх втрати або пошкодження. Для забезпечення ефективного резервного копіювання необхідно розробити стратегію зберігання даних та визначити, які дані слід регулярно копіювати.

Усі ці етапи встановлення та налаштування системи безпеки повинні бути виконані з урахуванням потреб організації та її інфраструктури. Крім того, важливо регулярно оновлювати програмне забезпечення та перевіряти наявність оновлень для забезпечення безпеки мережі.

РОЗДІЛ 5. ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ

5.1 Етапи підготовки до процесу тестування

Тестування це тип тестування безпеки, який використовується для перевірки рівня безпеки. Він проводиться з метою виявлення ризиків чи загроз безпеки, які можуть бути наявні у мережі [45].

Якщо мережа не захищена, то будь-який зловмисник може порушити її або отримати авторизований доступ до цієї системи. Ризик безпеки, як правило, є випадковою помилкою, що виникає під час розробки та впровадження програмного забезпечення. Наприклад, помилки конфігурації, помилки оформлення, помилки програмного забезпечення тощо.

Існує алгоритм для проведення тестування та оцінки ефективності захисту мережі, що часто називають каскадом. Загальний вигляд процесу підготовки та планування до процесу тестування наведено на рис.5.1.

Рисунок 5.1 – Етапи тестування

Першим етапом тестування мережі є виконання сканування портів та вразливостей мережі. Цей процес допоможе виявити можливі вразливі місця в мережі та забезпечити вчасне виправлення проблем. Можна використовувати спеціальні програми, такі як Nmap, Nessus, OpenVAS та інші для виконання цих завдань.

Другим етапом є проведення тестування з підробкою атак на мережу. Це може включати в себе тестування на проникнення, фішингові атаки, DOS-атаки та інші. Це допоможе виявити, наскільки ефективна система безпеки та чи можуть зловмисники зламати захист мережі.

Третім етапом є визначення рівня безпеки мережі. Це можна зробити, використовуючи різні метрики безпеки, такі як індекс CWE/SANS TOP 25, CVSS, OWASP Top 10 та інші [46]. Визначення рівня безпеки допоможе побачити, наскільки добре захищена мережа та в яких місцях можна покращити захист.

Четвертим етапом є виконання аудиту мережі. Це допоможе переконатися, що системи безпеки налаштовані належним чином та працюють ефективно. Аудит може включати в себе перевірку наявності оновлень, перевірку налаштувань, перевірку доступу користувачів та інше.

На основі результатів тестування та аудиту, можна зробити висновки про ефективність та безпеку мережі та розробити план заходів для покращення її безпеки та ефективності. Цей план може включати в себе рекомендації щодо оновлення програмного забезпечення, змін налаштувань мережі, змін політик безпеки та інші заходи.

Для оцінки ефективності мережі можна використовувати різні метрики, такі як доступність, швидкість передачі даних, пропускна здатність та інші. Важливо визначити, які метрики є найбільш важливими для підприємства та забезпечити їх відповідний рівень.

Також можна використовувати моніторинг мережі для відстеження роботи мережі та виявлення проблем в реальному часі. Це допоможе забезпечити вчасне виявлення та вирішення проблем.

Узагальнюючи, тестування та оцінка ефективності корпоративної мережі є важливим етапом в розробці мережі підприємства. Виконання сканування портів та вразливостей, тестування з підробкою атак, визначення рівня безпеки мережі та аудит мережі допоможуть виявити можливі проблеми та зробити висновки про ефективність та безпеку мережі. На основі цих висновків можна розробити план заходів для покращення безпеки та ефективності мережі, а також використовувати відповідні метрики для оцінки її роботи.

5.2 Тестування мережі на пропускну здатність та стабільність

Щоб впевнитися, що мережа працює та забезпечує необхідну швидкість передачі даних і стабільність під час роботи, потрібно проводити методи тестування мережі на пропускну здатність та стабільність мережі [46].

Першим етапом тестування мережі на пропускну здатність є визначення максимальної швидкості передачі даних між пристроями в мережі. Це можна зробити, використовуючи програми для вимірювання пропускної здатності, такі як iPerf, LAN Speed Test, NetStress та інші. Ці програми дозволяють вимірювати швидкість передачі даних між двома пристроями в мережі та забезпечують інформацію про швидкість передачі даних у різних умовах мережі.

Другим етапом є визначення пропускної здатності мережі. Це можна зробити, використовуючи спеціальні програми, такі як Jperf, NetStress, LAN Speed Test та інші. Ці програми дозволяють вимірювати пропускну здатність мережі за допомогою передачі тестових пакетів між пристроями в мережі.

Третім етапом є визначення стабільності мережі. Це можна зробити, використовуючи програми для тестування стабільності мережі, такі як PingPlotter, WinMTR та інші. Ці програми дозволяють визначити наявність проблем зі стабільністю мережі, таких як втрати пакетів, підвищення часу відповіді та інші.

На основі результатів тестування мережі на пропускну здатність та стабільність можна зробити висновки про ефективність роботи мережі та знайти причини проблем, які можуть виникати. Якщо результати тестування показують, що мережа працює належним чином, то можна переходити до наступного етапу розробки проекту. Якщо ж результати тестування показують проблеми, то необхідно вжити заходів для їх вирішення та повторно протестувати мережу.

Крім тестування мережі на пропускну здатність та стабільність, необхідно також врахувати різні сценарії використання мережі [47]. Наприклад, можна провести тестування на здатність мережі працювати з великою кількістю пристроїв, одночасно використовуючи різні послуги та програми. Також можна провести тестування на стійкість мережі до відмови пристроїв або відключення ділянок мережі.

У разі виявлення проблем під час тестування, можна вжити різних заходів для вирішення цих проблем. Наприклад, можна перевірити налаштування пристроїв мережі та змінити їх налаштування для поліпшення пропускної здатності та стабільності мережі. Також можна додатково встановити обладнання для розширення мережі та поліпшення її роботи [48].

Це дозволяє виявити проблеми з роботою мережі та прийняти заходи для їх вирішення.

5.3 Оцінка ефективності системи безпеки

Першим етапом оцінки ефективності системи безпеки є визначення потенційних загроз мережі. Це можна зробити, проведучи аналіз можливих векторів атак на мережу та визначивши, які заходи безпеки вже встановлені, а які потребують додаткової роботи. Аналіз можливих загроз мережі може включати перевірку наявності вразливостей в системах та програмному забезпеченні, перевірку дотримання правил безпеки, оцінку ризиків в результаті можливих атак, та інші дії.

Другим етапом є оцінка наявних заходів безпеки та їх ефективності. Для цього можна використовувати спеціальні програми для виявлення вразливостей та оцінки заходів безпеки, такі як Nessus, OpenVAS, Metasploit та інші. Ці програми дозволяють виявляти можливі вразливості в системах та програмному забезпеченні, тестувати заходи безпеки та допомагати забезпечити належний рівень захисту мережі.

Третім етапом є тестування системи безпеки на рівень захисту від реальних атак. Це може включати проведення вимушених атак на мережу, щоб визначити її реакцію та ефективність заходів безпеки. Тестування може проводитися з використанням підрядних організацій, які спеціалізуються на тестуванні систем безпеки. Такі організації можуть провести широкий спектр тестів на проникнення, включаючи фішингові атаки, атаки з використанням вразливостей програмного забезпечення, атаки з використанням соціальної інженерії та інші.

Четвертим етапом є аналіз результатів тестування та визначення слабких місць системи безпеки. Це може включати аналіз звітів від тестуючих організацій та визначення заходів, які потребують покращення або додаткової роботи. Також можуть бути запроваджені нові заходи безпеки для забезпечення належного рівня захисту.

П'ятим етапом є розробка та впровадження плану покращення системи безпеки. На основі результатів аналізу слабких місць системи безпеки розробляється план дій для поліпшення безпеки мережі. Це може включати встановлення нових заходів безпеки, оновлення програмного забезпечення, зміну правил безпеки та інші дії. План повинен бути реалістичним та враховувати можливості підприємства з точки зору фінансових ресурсів та ресурсів часу та працівників.

Цей процес допомагає виявити потенційні загрози мережі, оцінити наявні заходи безпеки та їх ефективність, тестувати систему безпеки на рівень захисту від реальних атак, визначити слабкі місця системи безпеки та розробити план дій для покращення безпеки мережі. Цей процес може

зайняти деякий час та вимагати значних фінансових та людських ресурсів, проте він є надзвичайно важливим для забезпечення безпеки мережі та захисту від потенційних кібератак.

Підприємства повинні розуміти, що безпека мережі є постійним процесом, який потребує постійного оновлення та покращення. Нові загрози та вразливості постійно з'являються, тому системи безпеки повинні постійно оновлюватись та адаптуватись до нових викликів.

Цей процес включає проведення аудиту безпеки мережі, тестування на проникнення, аналіз результатів тестування, розробку та впровадження плану покращення системи безпеки. Підприємства повинні розуміти, що безпека мережі є постійним процесом та потребує постійного оновлення та покращення.

ВИСНОВКИ

Основним завданням дослідження було розроблення захищеної корпоративної мережі підприємства з використанням сучасних технологій та заходів безпеки. Для досягнення цього були розглянуті та проаналізовані різні методи та засоби захисту мережі.

Результати дослідження показали, що підприємство має деякі слабкі місця у своїй системі безпеки, що можуть призвести до потенційних загроз. Основні проблеми були пов'язані з неактуальним програмним забезпеченням, слабкими паролями та відсутністю контролю за доступом до мережі.

Для поліпшення захисту мережі було запропоновано кілька рекомендацій. Перш за все, потрібно провести аудит системи безпеки та оновити всі програмні засоби до останньої версії. Також потрібно встановити сильні паролі та забезпечити контроль за доступом до мережі.

Для підвищення ефективності заходів безпеки, рекомендується залучити кваліфікованих спеціалістів, які спеціалізуються на тестуванні систем безпеки. Такі спеціалісти можуть провести широкий спектр тестів на проникнення та допомогти виявити потенційні загрози мережі.

Крім того, для забезпечення максимального рівня захисту мережі, рекомендується встановити додаткові заходи безпеки, так як двофакторну аутентифікацію та шифрування даних, які можуть запобігти несанкціонованому доступу до мережі та збереженню конфіденційної інформації.

Також було запропоновано забезпечити регулярне навчання та інструктування співробітників щодо безпеки мережі та використання захисних засобів. Це допоможе збільшити рівень свідомості та відповідальності працівників у виконанні правил безпеки та підвищити загальний рівень безпеки мережі підприємства.

Крім того, для забезпечення максимальної ефективності системи безпеки, рекомендується проводити регулярні перевірки та оновлення системи безпеки, а також встановлювати спеціальні програмні засоби для

виявлення потенційних загроз та захисту мережі від шкідливих програм та вірусів.

У підсумку, розробка захищеної корпоративної мережі підприємства є важливою складовою успішної діяльності підприємства в умовах зростаючої кількості кібератак та загроз безпеці мережі. Рекомендації, запропоновані у даному дослідженні, можуть допомогти підприємству забезпечити максимальний рівень захисту мережі та зберегти конфіденційність інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М. Технології забезпечення безпеки мережевої інфраструктури. Київ : КУБГ, 2019. С. 131-174.
2. Скопень, М. М.; Будя, О.П. Особливості моделювання та конфігурування віртуальних мереж з доступом до Інтернет засобами системи Cisco Packet Tracer/Механізми державного регулювання конкурентоспроможності національної економіки та міграційних процесів: матеріали Всеукраїнської науково-практичної конференції (13 березня 2021 року). Одеса: ОНУ імені І.І Мечникова, 2021, 89-93.
3. XIA, Wenfeng, et al. A survey on software-defined networking. IEEE Communications Surveys & Tutorials, 2014, 17.1 p. 27-51.
4. Северина С.В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету. Економічні науки, 2016, №1,С. 155-161.
5. Морозюк А.А., Ніколюк П.К. Шифрування даних. Комп’ютерні технології обробки даних, 2022, С. 80-82.
6. Варфоломеєва О.Г., Бондарчук А.П., Лавренюк Ю.Л. Розробка функціональної моделі системи управління мережею наступного покоління на рівні доступу. Зв'язок, 2015, № 4:49.
7. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Mechanism of Economic Regulation, 2014, № 1 С. 68-75.
8. Чунарьова А.В. Сучасні методи аудиту та моніторингу в задачах захисту інформації. Проблеми інформатизації та управління, 3(43). С. 87-91.
9. Тушук І. Тестування корпоративної мережі організації на несанкціонований доступ, Кібербезпека: освіта, наука, техніка. 2(18) С. 39–48, 2022.
10. Коробейнікова Т. Методи та засоби комплексного захисту корпоративної мережі. Матеріали конференцій МЦНД, 2023, Рівне, Україна. С. 97-102.

11. Корнієнко Б.Я., Галата Л.П. Оптимізація системи захисту інформації корпоративної мережі. Математичне та комп'ютерне моделювання. Серія: Технічні науки, 2019, С. 56-62.
12. Тюх О.В. Комп’ютерна система підприємства з детальним опрацюванням побудови та налаштування захищеної корпоративної мережі на основі технології VPN. 2020.
13. Бахтіяров Д.І.; Козлюк І.О. Методика модернізації моделі розповсюдження радіохвиль в середині приміщення для побудови контрольованої зони корпоративної мережі. Science-based technologies, 2019, 43(3). С. 349-356.
14. Yuskov I.O., Stroganova E.P. Analysis of neural network model design for telecommunication corporate network monitoring. In: 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). IEEE, 2019. p. 1-4.
15. Казмірчук С.В., Корченко, А.О., Паращук Т.І. Аналіз систем виявлення вторгнень. Захист інформації, 2018, 20 (4). С. 259-276.
16. Novokhrestov A., Konev A., Shelupanov A. Model of threats to computer network software. Symmetry, 2019, 11(12). p. 1506.
17. Tasril V. et al. Threats of computer system and its prevention. International Journal of Scientific Research in Science and Technology, 2017, 3(6). p. 448-451.
18. Захарченко С.М., Войцеховська О.В., Куцак Ю.В. Метод багаторівневого захисту даних в корпоративних мережах. 2020. PhD Thesis. ВНТУ.
19. Mallaboyev, N. M., et al. Information security issues. In: Conference Zone. 2022. p. 241-245.
20. Морозюк А.А., Ніколюк П.К. Шифрування даних. Комп’ютерні технології обробки даних, 2022. С. 80-82.
21. Тарнавський Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп’ютерні науки»; КПІ ім.

Ігоря Сікорського. Електронні текстові дані (1 файл: 2,04 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.

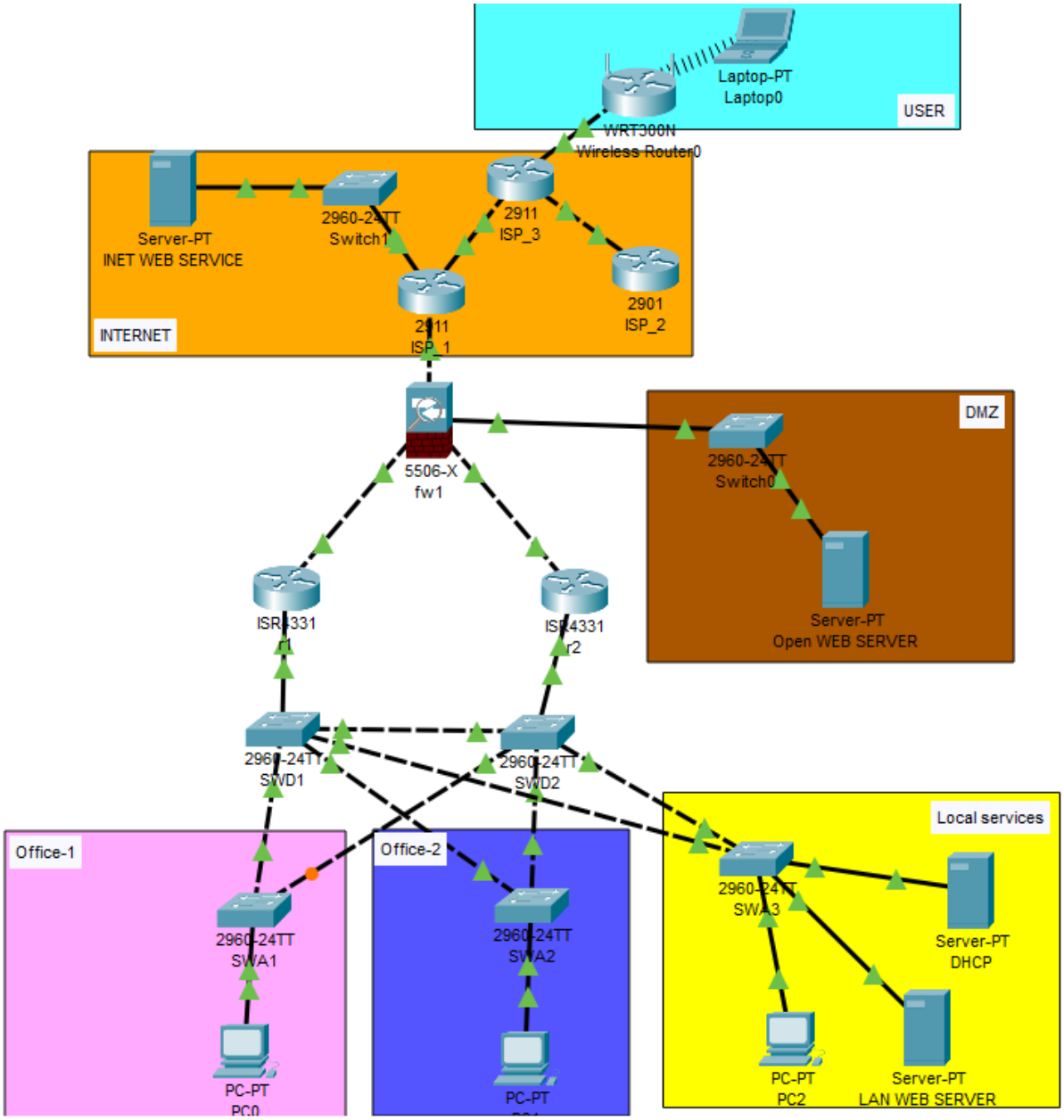
22. Коробейнікова Т., Федорченко В. Системний моніторинг мережевої безпеки в ТРІАДІ SIEM-EDR-NDR. Grail of Science, 2023. 27 р. 354-360.
23. Буров Є. Комп`ютерні мережі. Львів : 1999. 447 с.
24. Мельник М.О., Нікітин Г.Д, Мезенцева К.О. Аналіз побудови моделі політики інформаційної безпеки підприємства. Системи обробки інформації. 2(148). С. 126-128.
25. Азаров О. Д., Захарченко С. М., Кадук О. В. Комп’ютерні мережі : навчальний посібник. Вінниця : ВНТУ, 2013. 371с.
26. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціальний аспект. Київ : ДУТ 2015. С. 112-148.
27. Матюха М. М. Комп’ютерний аудит: опор. Курс лекцій для студ. екон. спец. дистанційної форми навчання. Київ : ДП «Вид. дім «Персонал», 2018. 228 с.
28. Лінгур Л. Роль корпоративної соціальної відповідальності у формуванні стратегії розвитку підприємства: сучасний підхід. Економіка та суспільство, 2023, С. 49.
29. Горбась І., Синюк С.. Сучасні напрямки розвитку структурування організацій. Молодий вчений, 2023, 1 (113). С. 151-157.
30. Мосіна М.О., Фрунза С.А. Методика подолання ризиків на підприємстві. Рекомендовано до друку та поширення через мережу Інтернет Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 10 від «24» листопада 2022 р.), 187 с.
31. Лобода О.М., Фесенець В.С. Застосування системи захисту інформаційних ресурсів підприємства. «Сучасна молодь в світі інформаційних технологій»: матеріали, 2023. С. 17.
32. Тупкало В.М. Комплексна модель інжинірингу системи інформаційної безпеки підприємства. Бізнес, інновації, менеджмент: проблеми та перспективи, 2023. С. 70-71.

33. Коробейнікова Т.І., Шостак С.В. Методи та засоби створення захищеної корпоративної мережі на базі обладнання компанії CISCO. URL: https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/15838
34. Кулаков Ю.О. Комп'ютерні мережі : підручник. Київ : Юніор, 2003. 400с.
35. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп'ютерні мережі [навчальний посібник] Київ : Компрінт, 2017. 821с.
36. Микитишин А.Г. et al. Комп'ютерні мережі. Книга 1. 2013.
37. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки, 151 – Автоматизація та комп'ютерно-інтегровані технології, 126 – Інформаційні системи та технології) Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 99 с.
38. Norige Eric, Liu Alex X., Torng Eric. A ternary unification framework for optimizing TCAM-based packet classification systems. IEEE/ACM Transactions on Networking, 2018, 26.2. p. 657-670.
39. Балацька В.С., Шабатура М.М. дослідження комп'ютерної мережі сканером вразливості NESSUS. Вісник ЛДУБЖД. 2019 №20 С. 6-9.
40. Коробейнікова Т.І. Куцак Ю.В. методи та засоби безпечної передачі даних в корпоративних мережах.URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/%206606/5491
41. Тарнавський Ю.А., Кузьменко І.М. Організація комп'ютерних мереж. Київ : КПІ ім. Ігоря Сікорського 2018. С. 109-116.
42. Liang Junyan, Kim Yoohwan. Evolution of firewalls: Toward securer network using next generation firewall. In: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022. p. 0752-0759.
43. Каланча А.А., Клімушин П.С. Аналіз мережевого трафіку як спосіб протидії кіберзлочинності. Протидія кіберзлочинності та торгівлі людьми: зб. матеріалів Міжнар. наук.-практ. конф. Харків: ХНУВС, 2022. С. 42-43.

44. Кулеша К.В. Впровадження інноваційних методів та технологій продажів у діяльність підприємства. Вісник Хмельницького національного університету. Економічні науки. 2019. №5. С. 157-161.
45. Бобрікова І.С., Барабаш Т.Н. Особливості функціонування і налаштувань маршрутизаторів в різних областях дії протоколу динамічної маршрутизації OSPF. Refrigeration Engineering and Technology, 54(1). https://doi.org/10.15673/ret.v54i1.990
46. Офіційний сайт компанії CISCO. URL: https://www.netacad.com/
47. Документація з настройки обладнання фірми Cisco. URL: http://www.cisco.com
48. Тертичний В.О. Мережна безпека, системи виявлення та протидії атакам, відмовостійкість мереж. С. 100-101. URL: https://openarchive.nure.ua/server/api/core/bitstreams/7234e22b-f216-42d3-ade4-f665f2f0cb80/content

ДОДАТКИ

Топологія корпоративної мережі в cisco packet tracer.



ДОДАТКИ 2

Конфігурація Firewall.

```
interface GigabitEthernet1/5
nameif ISP
security-level 0
ip address 1.1.1.2 255.255.255.0
interface GigabitEthernet1/6
nameif DMZ
security-level 50
ip address 192.168.20.1 255.255.255.0
interface GigabitEthernet1/7
nameif TO_R2
security-level 100
ip address 192.168.30.1 255.255.255.0
interface GigabitEthernet1/8
nameif TO_R1
security-level 100
ip address 192.168.10.1 255.255.255.0
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
object network DMZ_WEB_SERVER
host 192.168.20.100
nat (DMZ,ISP) static 1.1.1.2
object network LAN1
subnet 192.168.0.0 255.255.0.0
nat (TO_R1,ISP) dynamic interface
```

```
object network LAN2
subnet 10.10.0.0 255.255.0.0
nat (TO_R2,ISP) dynamic interface
route TO_R1 10.10.0.0 255.255.0.0 192.168.10.2 1
route TO_R2 10.10.0.0 255.255.0.0 192.168.30.2 100
route ISP 0.0.0.0 0.0.0.0 1.1.1.1 1
access-list LAN_TO_DMZ extended permit tcp any any eq www
access-list LAN_TO_DMZ extended permit icmp any any
access-list DMZ_LAN_ACL extended deny ip any 10.10.0.0 255.255.0.0
access-list ISP_DMZ extended permit icmp any host 192.168.20.100
access-list ISP_DMZ extended permit tcp any host 192.168.20.100 eq www
access-list LAN_nat0 extended permit ip 10.10.0.0 255.255.0.0 any
access-group LAN_TO_DMZ in interface TO_R1
access-group LAN_TO_DMZ in interface TO_R2
access-group ISP_DMZ in interface ISP
class-map inspection_default
match default-inspection-traffic
class-map INS_DEF
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect tftp
policy-map GLOBAL_POLICY
class INS_DEF
inspect http
```

inspect icmp

Конфігурація першого маршрутизатора

interface GigabitEthernet0/0/0

description TO_FW

ip address 192.168.10.2 255.255.255.0

duplex auto

speed auto

interface GigabitEthernet0/0/1.10

encapsulation dot1Q 10

ip address 10.10.10.2 255.255.255.0

ip helper-address 10.10.30.10

standby version 2

standby 10 ip 10.10.10.1

standby 10 priority 110

standby 10 preempt

interface GigabitEthernet0/0/1.20

encapsulation dot1Q 20

ip address 10.10.20.2 255.255.255.0

ip helper-address 10.10.30.10

standby version 2

standby 20 ip 10.10.20.1

standby 20 priority 110

standby 20 preempt

interface GigabitEthernet0/0/1.30

encapsulation dot1Q 30

ip address 10.10.30.2 255.255.255.0

ip helper-address 10.10.30.10

standby version 2

standby 30 ip 10.10.30.1

standby 30 priority 110

standby 30 preempt

interface GigabitEthernet0/0/1.86

encapsulation dot1Q 86

ip address 10.10.86.2 255.255.255.0

standby version 2

standby 86 ip 10.10.86.1

standby 86 priority 110

standby 86 preempt

interface GigabitEthernet0/0/2

no ip address

duplex auto

speed auto

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip route 0.0.0.0 0.0.0.0 192.168.10.1

ip flow-export version 9

line con 0

login local

line aux 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

Конфігурація другого маршрутизатора

interface GigabitEthernet0/0/0

```
description TO_FW
ip address 192.168.30.2 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet0/0/1.10
encapsulation dot1Q 10
ip address 10.10.10.3 255.255.255.0
ip helper-address 10.10.30.10
standby version 2
standby 10 ip 10.10.10.1
standby 10 preempt
interface GigabitEthernet0/0/1.20
encapsulation dot1Q 20
ip address 10.10.20.3 255.255.255.0
ip helper-address 10.10.30.10
standby version 2
standby 20 ip 10.10.20.1
standby 20 preempt
interface GigabitEthernet0/0/1.30
encapsulation dot1Q 30
ip address 10.10.30.3 255.255.255.0
ip helper-address 10.10.30.10
standby version 2
standby 30 ip 10.10.30.1
standby 30 preempt
interface GigabitEthernet0/0/1.86
encapsulation dot1Q 86
ip address 10.10.86.3 255.255.255.0
standby version 2
standby 86 ip 10.10.86.1
```

standby 86 preempt

interface GigabitEthernet0/0/2

no ip address

duplex auto

speed auto

shutdown

interface Vlan1

no ip address

shutdown

ip classless

ip route 0.0.0.0 0.0.0.0 192.168.30.1

ip flow-export version 9

line con 0

login local

line aux 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

Конфігурація switch (SWD1)

nterface FastEthernet0/1

description TO_SWA1

switchport trunk allowed vlan 10,86

switchport mode trunk

interface FastEthernet0/2

description TO_SWA2

switchport trunk allowed vlan 20,86

switchport mode trunk

interface FastEthernet0/3
description TO_SWA3
switchport trunk allowed vlan 30,86
switchport mode trunk
interface GigabitEthernet0/1
description TO_R1
switchport trunk allowed vlan 10,20,30,86
switchport mode trunk
interface GigabitEthernet0/2
description TO_SWD2
switchport trunk allowed vlan 10,20,30,86
switchport mode trunk
interface Vlan86
ip address 10.10.86.4 255.255.255.0
ip default-gateway 10.10.86.1
line con 0
login local
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh

Конфігурація switch (SWD2)

interface FastEthernet0/1
description TO_SWA1
switchport trunk allowed vlan 10,86
switchport mode trunk
interface FastEthernet0/2
description TO_SWA2

switchport trunk allowed vlan 20,86

switchport mode trunk

interface FastEthernet0/3

description TO_SWA3

switchport trunk allowed vlan 30,86

switchport mode trunk

description TO_R2

switchport trunk allowed vlan 10,20,30,86

switchport mode trunk

interface GigabitEthernet0/2

description TO_SWD1

switchport trunk allowed vlan 10,20,30,86

switchport mode trunk

interface Vlan86

ip address 10.10.86.5 255.255.255.0

ip default-gateway 10.10.86.1

line con 0

login local

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

Конфігурація switch (SWA1)

interface FastEthernet0/1

description TO_SWD1

switchport trunk allowed vlan 10,86

switchport mode trunk

interface FastEthernet0/2

description TO_SWD2

switchport trunk allowed vlan 10,86

switchport mode trunk

interface Vlan86

ip address 10.10.86.10 255.255.255.0

ip default-gateway 10.10.86.1

line con 0

login local

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

Конфігурація switch (SWA2)

interface FastEthernet0/1

description TO_SWD1

switchport trunk allowed vlan 20,86

switchport mode trunk

interface FastEthernet0/2

description TO_SWD2

switchport trunk allowed vlan 20,86

switchport mode trunk

interface GigabitEthernet0/2

interface Vlan86

ip address 10.10.86.20 255.255.255.0

ip default-gateway 10.10.86.1

line con 0

login local

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

Конфігурація switch (SWA3)

interface FastEthernet0/1

description TO_SWD2

switchport trunk allowed vlan 30,86

switchport mode trunk

interface Vlan86

ip address 10.10.86.30 255.255.255.0

ip default-gateway 10.10.86.1

line con 0

login local

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh