

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп'ютерних наук та технологій

(повне найменування факультету)

Кафедра комп'ютерних систем та мереж

(повне найменування кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

бакалавра

(ступінь вищої освіти (освітній ступінь))

на тему **РОЗРОБКА ЗАКРИТОЇ МЕРЕЖІ З ПІДВИЩЕНОЮ**
НАДІЙНІСТЮ

Виконав: студент 4 курсу, групи КНТ-511
спеціальності _____

123 «Комп'ютерна інженерія»

(код і найменування

спеціальності)

Освітня програма (спеціалізація) _____

«Комп'ютерна інженерія»

СЕРГЄЄВА Д.А.

(ПРИЗВИЩЕ та ініціали)

Керівник ЗЕЛЕНЬОВА І.Я.

(ПРИЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О.Ю.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
 (повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій
 Кафедра «Комп'ютерні системи та мережі»
 Ступінь вищої освіти бакалаврський
 Спеціальність 123 Комп'ютерна інженерія
 (код і найменування)
 Освітня програма (спеціалізація) Комп'ютерна інженерія
 (назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри
КУДЕРМЕТОВ Р.К.

“ 14 ” квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

СЕРГЄЄВА Данила Антоновича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) РОЗРОБКА ЗАКРИТОЇ МЕРЕЖІ З ПІДВИЩЕНОЮ НАДІЙНІСТЮ

керівник проєкту (роботи) к.т.н., доцент, ЗЕЛЕНЬОВА І.Я.

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом вищого навчального закладу від “08” квітня 2025 року №151

2. Строк подання студентом проєкту (роботи) 01.06.2025

3. Вихідні дані до проєкту (роботи) технічне завдання

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Вивчення існуючих методів підвищення надійності

2) Проектування комп'ютерної мережі

3) Практичне використання

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

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	ЗЕЛЕНЬОВА І. Я.		
нормоконтроль	ПОЛЬСЬКА О. В.		

7. Дата видачі завдання 01.04.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз предметної області та теоретичні основи розробки закритої мережі	01.04.2025 р.	
2	Розробка закритої мережі з підвищеною надійністю та захищеністю	15.04.2025 р.	
3	Тестування та практичні рекомендації з експлуатації закритої мережі	05.05.2025 р.	
4	Оформлення отриманих результатів у ПЗ	20.05.2025 р.	
5	Оформлення презентації	01.06.2025 р.	
6	Оформлення допоміжного матеріалу	10.06.2025 р.	

Студент (ка)

_____ **Данило СЕРГЄВ**
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи)

_____ **Ірина ЗЕЛЕНЬОВА**
(підпис) (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:
95с., 42 табл., 12 рис. , 31 джерел.

АВТЕНТИФІКАЦІЯ, ВІДМОВОСТІЙКІСТЬ, ЗАКРИТА МЕРЕЖА, ЗАХИЩЕНІСТЬ, МЕРЕЖЕВА БЕЗПЕКА, МОНІТОРИНГ, НАДІЙНІСТЬ, РЕЗЕРВУВАННЯ, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ШИФРУВАННЯ.

Об'єкт дослідження – процеси забезпечення надійності та захищеності інформаційних мереж для обробки конфіденційних даних.

Предмет дослідження – методи, моделі й засоби побудови закритих мереж із підвищеними вимогами до безпеки.

Мета роботи – розробка закритої мережі з високою надійністю та захищеністю, що гарантує безперебійну роботу критичних інформаційних систем і захист від несанкціонованого доступу.

У роботі проаналізовано ключові вимоги та моделі закритих мереж, досліджено протоколи, обладнання та системи моніторингу. Запропоновано проєкт мережі, визначено її топологію й архітектуру, розроблено систему безперебійного живлення та комплекс захисту інформації. Виконано тестування надійності й захищеності, розроблено рекомендації з експлуатації.

Практична цінність – запропоновано комплексний підхід до створення захищених мереж для організацій з високими вимогами до інформаційної безпеки.

ЗМІСТ

Реферат	4
Скорочення та умовні позначки.....	7
Вступ.....	7
1 Аналіз предметної області та теоретичні основи розробки закритої мережі	11
1.1 Поняття закритої мережі та вимоги до її надійності і захищеності	11
1.2 Аналіз топологій побудови закритих мереж	13
1.3 Архітектурні рішення для підвищення надійності мережі.....	16
1.4 Огляд моделей закритих мереж та їх особливості.....	20
1.5 Аналіз кабельних систем для забезпечення захищеності	22
1.6 Мережеві протоколи та їх захищеність.....	26
1.7 Системи моніторингу та керування мережею	30
1.8 Методи та засоби захисту інформації в закритих мережах	34
2 Розробка закритої мережі з підвищеною надійністю та захищеністю	38
2.1 Технічне завдання на розробку закритої мережі.....	38
2.2 Проектування топології та архітектури мережі	39
2.3 Вибір та обґрунтування мережевого обладнання	46
2.4 Розробка кабельної інфраструктури	51
2.5 Проектування системи безперебійного живлення.....	55
2.6 Налаштування мережевих протоколів для забезпечення надійності.....	60
2.7 Впровадження системи моніторингу мережі	66
2.8 Розробка та впровадження системи захисту інформації, документування розробленої мережі	70
3 Тестування та практичні рекомендації з експлуатації закритої мережі	73
3.1 Методика тестування надійності мережі	73
3.2 Тестування захищеності мережі від зовнішніх та внутрішніх загроз	76
3.3 Аналіз результатів тестування та виявлення вразливостей	77
3.4 Налаштування та оптимізація роботи мережі	80

3.5 Практичні рекомендації з експлуатації закритої мережі.....	81
3.6 Регламент технічного обслуговування та підтримки мережі.....	84
3.7 Навчання персоналу з обслуговування мережі	86
Висновки	88
Перелік джерел посилання	91
Додаток А. Схема закритої мережі.....	94
Додаток Б. Налаштування системи захисту.....	95

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

- БД – база даних;
- ДБЖ – джерело безперебійного живлення;
- ЗКМ – закрита комп’ютерна мережа;
- ІБ – інформаційна безпека;
- ІТ – інформаційні технології;
- КСЗІ – комплексна система захисту інформації;
- МЕ – міжмережевий екран;
- ПЗ – програмне забезпечення;
- СВВ – система виявлення вторгнень;
- СЗІ – система захисту інформації;
- СЗП – система запобігання проникненню;
- СКС – структурована кабельна система;
- AES (Advanced Encryption Standard) – стандарт шифрування даних;
- DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації хоста;
- DMZ (Demilitarized Zone) – демілітаризована зона;
- IDS (Intrusion Detection System) – система виявлення вторгнень;
- IPS (Intrusion Prevention System) – система запобігання вторгненням;
- IPsec (Internet Protocol Security) – набір протоколів для захищеного з’єднання;
- LACP (Link Aggregation Control Protocol) – протокол керування агрегацією каналів;
- NAC (Network Access Control) – контроль доступу до мережі;
- RADIUS (Remote Authentication Dial-In User Service) – протокол автентифікації віддалених користувачів;
- VLAN (Virtual Local Area Network) – віртуальна локальна мережа;
- VPN (Virtual Private Network) – віртуальна приватна мережа;

ВСТУП

Актуальність теми. В умовах стрімкого розвитку інформаційних технологій та постійно зростаючих загроз інформаційній безпеці, розробка надійних та захищених мережевих інфраструктур стає критично важливим завданням для державних установ, підприємств оборонної галузі, фінансових організацій та інших об'єктів критичної інфраструктури. Закриті мережі, що функціонують ізольовано від загальнодоступних мереж, забезпечують необхідний рівень захисту для обробки конфіденційної інформації та підтримки критично важливих бізнес-процесів.

Важливість забезпечення надійності та захищеності закритих мереж підкреслюється зростанням кількості та складності кібератак. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість зареєстрованих кіберінцидентів щорічно зростає на 30-40%, причому значна частина з них спрямована на об'єкти критичної інфраструктури. Системні проблеми захисту інформації в комп'ютерних мережах детально досліджуються в роботах вітчизняних та зарубіжних науковців, таких як В.Л. Бурячок, В.Б. Дудикевич, О.А. Смірнов, В.О. Хорошко, В.Ф. Шаньгин, W. Stallings та інших.

Незважаючи на наявність значної теоретичної бази з питань інформаційної безпеки, проблема розробки закритих мереж з підвищеною надійністю та захищеністю залишається актуальною у зв'язку з постійною еволюцією технологій та появою нових векторів атак. Особливу увагу слід приділити комплексному підходу до забезпечення надійності та захищеності, який охоплює всі аспекти функціонування мережі — від вибору топології та обладнання до налаштування протоколів безпеки та організації системи моніторингу.

Мета і завдання дослідження. Метою дипломної роботи є розробка закритої мережі з підвищеною надійністю та захищеністю, що забезпечує

безперебійне функціонування критично важливих інформаційних систем та захист конфіденційної інформації від несанкціонованого доступу.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- визначити основні вимоги до надійності та захищеності закритих мереж;
- проаналізувати існуючі топології та архітектурні рішення для побудови закритих мереж;
- дослідити моделі закритих мереж та їх особливості;
- проаналізувати кабельні системи, мережеві протоколи та системи моніторингу з точки зору забезпечення надійності та захищеності;
- розробити проект закритої мережі з підвищеною надійністю та захищеністю;
- обґрунтувати вибір мережевого обладнання та програмного забезпечення;
- спроектувати систему безперебійного живлення та резервування;
- розробити та впровадити систему захисту інформації;
- розробити методику тестування надійності та захищеності мережі;
- підготувати практичні рекомендації з експлуатації закритої мережі.

Об'єкт дослідження – процеси забезпечення надійності та захищеності інформаційних мереж для обробки конфіденційної інформації.

Предмет дослідження – методи, моделі та засоби побудови закритих мереж з підвищеними вимогами до надійності та захищеності.

Методи дослідження. В роботі використовуються методи системного аналізу для визначення вимог до закритих мереж, порівняльний аналіз для оцінки топологій та архітектурних рішень, методи математичного моделювання для оцінки надійності мережі, експериментальні методи для тестування захищеності мережі від зовнішніх та внутрішніх загроз.

Теоретичне значення та практична цінність роботи полягає в розробці комплексного підходу до проектування закритих мереж з підвищеною надійністю та захищеністю, що може бути використаний для створення

захищених інформаційних інфраструктур в організаціях з високими вимогами до безпеки інформації.

Результати роботи можуть бути застосовані в практичній діяльності підприємств та організацій при розробці та модернізації їх мережевих інфраструктур, а також у навчальному процесі при підготовці фахівців з інформаційних технологій та кібербезпеки.

Основними джерелами інформації, використаними під час дослідження, є наукова та навчально-методична література з питань комп'ютерних мереж та інформаційної безпеки, міжнародні стандарти в галузі захисту інформації, технічна документація виробників мережевого обладнання та програмного забезпечення, а також матеріали з професійних інтернет-ресурсів, присвячених проблемам надійності та захищеності інформаційних систем.

Логіка дослідження представлена в додатку А, а практична цінність результатів підтверджується довідкою про їх впровадження (Додаток Б).

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ ЗАКРИТОЇ МЕРЕЖІ

1.1 Поняття закритої мережі та вимоги до її надійності і захищеності

Розвиток інформаційних технологій та зростання кіберзагроз зумовлюють підвищену увагу до захисту комп'ютерних мереж, особливо тих, що використовуються для обробки критичної інформації. У цьому контексті особливого значення набуває поняття закритої мережі.

Закрита мережа (англ. closed network або air-gapped network) – це комп'ютерна мережа, фізично та логічно ізольована від інших мереж, у тому числі від публічних мереж, таких як Інтернет [30, с. 212]. Основною метою створення закритих мереж є забезпечення максимального рівня захисту інформації від зовнішніх загроз шляхом унеможливлення несанкціонованого доступу до неї.

За визначенням Коваленка В.М., "закрита мережа передбачає використання комплексу програмно-технічних засобів, які забезпечують повну ізоляцію інформаційних потоків та мінімізують ризики несанкціонованого доступу до даних" [3, с. 45]. На відміну від звичайних мереж, закриті мережі характеризуються відсутністю прямих з'єднань із зовнішніми мережами, що суттєво ускладнює можливість проведення атак на них.

Основними характеристиками закритої мережі є:

- фізична ізоляція від інших мереж;
- використання спеціалізованого обладнання та програмного забезпечення;
- строга регламентація доступу до компонентів мережі;
- застосування специфічних протоколів шифрування;
- постійний моніторинг стану безпеки мережі [30, с. 109].

Вимоги до надійності закритої мережі зосереджені на забезпеченні безперебійної роботи всіх компонентів системи та можливості швидкого відновлення у разі збоїв. Відповідно до стандарту ISO/IEC 27001:2013 [24], надійність інформаційної системи визначається через показники доступності, відмовостійкості та цілісності даних.

Ковальчук А.В. та Дудник О.С. у своїй роботі [4, с. 87] виділяють такі ключові вимоги до надійності закритих мереж: безперебійність функціонування (availability) – здатність мережі виконувати свої функції у будь-який момент часу; відмовостійкість (fault tolerance) – здатність системи продовжувати функціонування при відмові окремих компонентів; масштабованість (scalability) – можливість розширення системи без втрати продуктивності; резервування (redundancy) – наявність дублюючих компонентів для швидкої заміни у разі відмови основних; можливість швидкого відновлення після збоїв (recoverability).

Щодо захищеності закритої мережі, Сидоренко Л.М. [16, с. 112] виділяє три основні аспекти:

- конфіденційність (confidentiality) – захист інформації від несанкціонованого доступу;
- цілісність (integrity) – забезпечення точності та повноти інформації;
- доступність (availability) – забезпечення доступу до інформації для авторизованих користувачів у потрібний час.

Згідно з рекомендаціями NIST (National Institute of Standards and Technology) [27], для забезпечення захищеності закритої мережі необхідно реалізувати такі заходи: створення детальної політики безпеки; застосування багаторівневої системи автентифікації та авторизації; шифрування даних при зберіганні та передачі; постійний моніторинг і аудит системи; регулярне оновлення програмного забезпечення та встановлення патчів безпеки; впровадження системи виявлення та запобігання вторгнень; фізичний захист обладнання.

Важливим аспектом при проєктуванні закритих мереж є дотримання вітчизняних стандартів та нормативних документів. В Україні вимоги до захищеності інформаційних систем регламентуються низкою нормативно-правових актів, зокрема Постановою Кабінету Міністрів України № 992 "Про затвердження Положення про захист персональних даних" [11].

Миколайчук Ю.А. зазначає, що "для державних установ України вимоги до захищеності мереж повинні відповідати категорії інформації, що обробляється, з урахуванням її критичності та конфіденційності" [8, с. 48].

Таким чином, закрита мережа представляє собою складну систему, яка вимагає комплексного підходу до забезпечення її надійності та захищеності. При її проєктуванні необхідно враховувати як технічні аспекти (вибір обладнання, архітектура, протоколи), так і організаційні заходи (політика безпеки, навчання персоналу, розробка регламентів експлуатації).

1.2 Аналіз топологій побудови закритих мереж

Вибір оптимальної топології є фундаментальним аспектом при проєктуванні закритої мережі, оскільки від цього залежить її загальна продуктивність, надійність та захищеність. Колесник В.В. та Вакалюк Т.А. зазначають, що "правильно підібрана топологія мережі забезпечує оптимальний баланс між надійністю, швидкістю передачі даних та вартістю реалізації" [5, с. 3].

У контексті закритих мереж особливу увагу слід приділяти топологіям, які забезпечують високий рівень резервування та контролю доступу. Розглянемо основні типи топологій та проаналізуємо їх переваги та недоліки з точки зору побудови закритих мереж:

- шинна топологія (Bus topology);
- кільцева топологія (Ring topology);

- зіркова топологія (Star topology);
- деревовидна топологія (Tree topology);
- повнозв'язна топологія (Mesh topology);
- гібридна топологія (Hybrid topology).

Шинна топологія передбачає підключення всіх пристроїв до однієї спільної лінії зв'язку. Переваги: простота реалізації; низька вартість впровадження; легке додавання нових вузлів. Недоліки: низька надійність (відмова шини призводить до виходу з ладу всієї мережі); обмежена пропускна здатність; складність забезпечення конфіденційності передачі даних; проблеми з безпекою (всі пристрої мають доступ до всього трафіку). Висновок: шинна топологія не рекомендується для закритих мереж через низький рівень надійності та захищеності [5, с. 45].

Кільцева топологія передбачає з'єднання кожного пристрою з двома сусідніми, утворюючи замкнене кільце. Переваги: рівномірний розподіл навантаження; відсутність колізій (при використанні маркерного доступу); можливість реалізації дублюючого кільця для підвищення надійності. Недоліки: відмова одного вузла може вплинути на роботу всієї мережі; складність діагностики проблем; обмежена масштабованість. Згідно з дослідженнями Брайка В.В. [2], кільцева топологія може застосовуватися в закритих мережах за умови впровадження додаткових механізмів резервування, таких як FDDI (Fiber Distributed Data Interface) або SDH (Synchronous Digital Hierarchy).

У зірковій топології всі пристрої підключаються до одного центрального комутатора або концентратора. Переваги: висока надійність (відмова одного вузла не впливає на роботу інших); легкість масштабування та реконфігурації; простота управління доступом та моніторингу; ефективний контроль безпеки через централізацію. Недоліки: висока залежність від центрального вузла; більші витрати на кабельну інфраструктуру; необхідність забезпечення резервування центрального вузла. За даними Пархоменка І.І. [17], зіркова топологія є найбільш поширеною для

побудови захищених мереж завдяки можливості централізованого контролю доступу та моніторингу безпеки.

Деревовидна топологія представляє собою ієрархічну структуру з кількома рівнями зіркових з'єднань. Переваги: ефективна сегментація мережі; хороша масштабованість; можливість впровадження різних рівнів доступу на різних рівнях ієрархії. Недоліки: залежність від роботи верхніх рівнів ієрархії; складність налаштування та адміністрування; необхідність забезпечення додаткових заходів резервування для верхніх рівнів.

Повнозв'язна топологія передбачає пряме з'єднання кожного вузла з усіма іншими вузлами мережі. Переваги: максимальна надійність та відмовостійкість; висока пропускна здатність; множинні шляхи передачі даних; висока захищеність від підслуховування. Недоліки: висока вартість впровадження; складність масштабування; надмірність з'єднань при великій кількості вузлів. Згідно з дослідженнями Коваленка В.М. [3, с. 87], повнозв'язна топологія найкраще підходить для невеликих закритих мереж з високими вимогами до надійності та захищеності, наприклад, у військових або фінансових установах.

Гібридна топологія поєднує елементи різних базових топологій для досягнення оптимального балансу між надійністю, продуктивністю та вартістю. Переваги: гнучкість у проєктуванні; оптимізація під конкретні потреби; можливість сегментації мережі з різними рівнями безпеки. Недоліки: складність проєктування та налаштування; потенційні проблеми з сумісністю різних сегментів; вищі вимоги до кваліфікації адміністраторів. У контексті закритих мереж найчастіше використовуються гібридні рішення на основі зіркової та повнозв'язної топологій, що дозволяє досягти оптимального балансу між надійністю, безпекою та вартістю впровадження [2, с. 17].

За результатами аналізу науково-технічної літератури та практичного досвіду впровадження закритих мереж, можна сформулювати наступні рекомендації щодо вибору топології:

- для малих закритих мереж (до 50 вузлів) з високими вимогами до безпеки оптимальним є використання повнозв'язної або гібридної топології з елементами повнозв'язності;

- для середніх мереж (50-200 вузлів) рекомендується ієрархічна зіркова топологія з резервуванням центральних вузлів;

- для великих мереж (понад 200 вузлів) найбільш ефективним є використання деревовидної топології з сегментацією на підмережі з різними рівнями захисту.

Таким чином, вибір оптимальної топології для закритої мережі повинен базуватися на комплексному аналізі вимог до надійності, захищеності, масштабованості та вартості впровадження, з урахуванням специфіки конкретного об'єкта.

1.3 Архітектурні рішення для підвищення надійності мережі

Надійність мережевої інфраструктури є одним із ключових параметрів закритих мереж, особливо тих, що обслуговують критичні системи. Архітектурні рішення, які підвищують надійність, дозволяють забезпечити безперервність роботи мережі навіть при виникненні збоїв окремих компонентів. Розглянемо основні архітектурні підходи та рішення, що сприяють підвищенню надійності закритих мереж.

Резервування є базовим принципом забезпечення надійності, який передбачає дублювання критичних компонентів мережі для запобігання відмовам системи. Ковальчук А.В. та Дудник О.С. зазначають, що "правильно організоване резервування дозволяє досягти показника доступності мережі на рівні 99,999% (так званих "п'яти дев'яток")" [4, с. 124].

Основні підходи до резервування включають:

а) резервування каналів зв'язку. Реалізується шляхом створення альтернативних маршрутів передачі даних між ключовими вузлами мережі. Згідно з дослідженнями Пархоменка І.І. [17], для критичних систем рекомендується забезпечувати не менше двох фізично незалежних каналів зв'язку, бажано з використанням різних технологій (наприклад, оптоволокно та радіоканал).

б) резервування активного обладнання. Передбачає використання надлишкових мережевих пристроїв:

- 1) маршрутизатори в конфігурації HSRP (Hot Standby Router Protocol) або VRRP (Virtual Router Redundancy Protocol);
- 2) комутатори в режимі стекування або з використанням технологій MLAG (Multi-chassis Link Aggregation Group);
- 3) міжмережеві екрани в конфігурації Active/Standby або Active/Active;

в) резервування систем електроживлення. Включає:

- 1) використання джерел безперебійного живлення (UPS);
- 2) підключення критичного обладнання до різних фідерів електроживлення;
- 3) встановлення дизель-генераторів для тривалого резервного живлення.

За даними Миколайчука Ю.А. [8, с. 49], "відмови систем електроживлення є причиною близько 45% всіх аварій в інформаційних системах критичної інфраструктури", що підкреслює важливість цього аспекту.

Модульний підхід до проектування мережі передбачає поділ інфраструктури на функціональні блоки (модулі), кожен з яких виконує специфічні завдання. Основними перевагами такого підходу є:

— ізоляція відмов (failure isolation) – проблеми в одному модулі мінімально впливають на інші;

- спрощення діагностики та відновлення;
- можливість поетапної модернізації системи;
- підвищення загальної надійності мережі.

Коваленко В.М. [3, с. 198] рекомендує використовувати трирівневу модульну архітектуру для закритих мереж:

- ядро мережі (Core Layer) – забезпечує високошвидкісну передачу даних;
- рівень розподілу (Distribution Layer) – реалізує політики безпеки, маршрутизацію між підмережами;
- рівень доступу (Access Layer) – забезпечує підключення кінцевих пристроїв.

При цьому кожен модуль повинен мати внутрішнє резервування для забезпечення максимальної надійності.

Віртуалізація мережевої інфраструктури дозволяє абстрагувати мережеві сервіси від фізичного обладнання, що сприяє підвищенню гнучкості та надійності системи. Ключові технології включають:

а) SDN (Software-Defined Networking). Технологія SDN розділяє площину управління (control plane) та площину даних (data plane), що дозволяє централізовано керувати мережею та швидко реагувати на зміни топології. За даними Wang S.P. [30, с. 156], "впровадження SDN в закритих мережах дозволяє підвищити показники відмовостійкості на 30-40% за рахунок швидкої адаптації до змін";

б) NFV (Network Functions Virtualization). NFV передбачає віртуалізацію мережевих функцій, таких як міжмережеві екрани, балансувальники навантаження, системи виявлення вторгнень тощо. Це дозволяє:

- 1) швидко відновлювати сервіси у разі збоїв;
- 2) динамічно розподіляти ресурси для критичних функцій;
- 3) зменшувати залежність від конкретних апаратних платформ.

Кластеризація передбачає об'єднання кількох серверів або мережевих пристроїв у єдину відмовостійку систему. Основні типи кластерів включають:

- а) кластери високої доступності (High-Availability Clusters);
- б) кластери балансування навантаження (Load-Balancing Clusters).

Розподіляють запити між кількома вузлами, що дозволяє:

- 1) підвищити загальну продуктивність системи;
- 2) забезпечити відмовостійкість (при відмові одного вузла навантаження перерозподіляється між іншими);
- 3) планово виводити окремі вузли для обслуговування без переривання роботи сервісів.

Кластери високої доступності (High-Availability Clusters) забезпечують безперервність роботи сервісів шляхом автоматичного переключення на резервний вузол у разі відмови основного. За даними досліджень Smith J. [28], "використання НА-кластерів дозволяє зменшити час простою критичних сервісів до 99,99% їх загального робочого часу".

Сегментація передбачає поділ мережі на логічні або фізичні сегменти, що забезпечує ізоляцію проблем в межах одного сегмента, підвищення загальної продуктивності мережі та покращення захищеності завдяки можливості встановлення різних політик безпеки для різних сегментів.

За результатами аналізу різних архітектурних рішень можна зробити висновок, що для забезпечення максимальної надійності закритих мереж необхідно комбінувати кілька підходів, адаптуючи їх до конкретних вимог та обмежень проєкту. При цьому, як зазначає Woland A. та ін. [31, с. 476], "ключовим фактором успіху є не лише впровадження технічних рішень, а й розробка чітких процедур експлуатації та відновлення, а також належна підготовка персоналу".

1.4 Огляд моделей закритих мереж та їх особливості

Закриті мережі, залежно від конкретних потреб організації та рівня захисту, можуть бути реалізовані за допомогою різних моделей. Кожна модель має свої особливості та сфери застосування, що дозволяє обрати оптимальне рішення відповідно до специфічних вимог.

Модель повної фізичної ізоляції (Air-Gap) забезпечує найвищий рівень захисту через відсутність фізичних з'єднань із зовнішніми мережами. Ця модель використовується у військових системах, на ядерних об'єктах та для критичної інфраструктури [16, с. 187].

Модель контрольованого шлюзу передбачає строго контрольований доступ між закритою мережею та зовнішнім світом через спеціалізований шлюз безпеки. Така модель дозволяє забезпечити необхідний рівень захисту, зберігаючи при цьому можливість обмеженого інформаційного обміну [2,с.28].

Модель демілітаризованої зони (DMZ) включає створення проміжного сегмента мережі між внутрішньою захищеною мережею та зовнішніми системами. В DMZ розміщуються сервіси, які мають бути доступні ззовні, але при цьому не мають прямого доступу до внутрішньої мережі. Така модель широко використовується в корпоративних середовищах, системах електронного урядування та інших випадках, коли необхідно надавати певні сервіси зовнішнім користувачам.

Модель сегментації на основі довіри базується на розподілі мережі на сегменти за рівнем довіри та критичності даних, що обробляються. Кожен сегмент має свій рівень захисту та політики безпеки. За даними Symantec, "сегментація мережі на зони різного рівня довіри дозволяє на 35-40% знизити ризик поширення атаки в мережі" [29].

Модель накладеної захищеної мережі передбачає створення віртуального захищеного шару поверх існуючої фізичної інфраструктури. Це

дозволяє забезпечити додатковий рівень захисту без значної модифікації базової мережі.

Модель Zero Trust є сучасним підходом до безпеки, який базується на принципі "ніколи не довіряй, завжди перевіряй". Ця модель передбачає відсутність довіри до будь-яких користувачів і систем за замовчуванням, незалежно від їх місцезнаходження. За даними Gartner, "до 2025 року понад 60% організацій перейдуть на модель Zero Trust як основу своєї стратегії безпеки" [22].

В таблиці 1.1 представлено порівняльний аналіз різних моделей закритих мереж за ключовими параметрами.

Таблиця 1.1 - Порівняльний аналіз моделей закритих мереж

Модель	Рівень безпеки	Складність впровадження	Гнучкість	Масштабованість	Вартість
Air-Gap	Дуже високий	Середня	Низька	Низька	Висока
Controlled Gateway	Високий	Висока	Середня	Середня	Висока
DMZ	Середній до високого	Середня	Висока	Висока	Середня
Trust-Based Segmentation	Високий	Висока	Висока	Висока	Середня до високої
Overlay Secure Network	Середній до високого	Середня	Висока	Висока	Середня
Zero Trust	Дуже високий	Дуже висока	Висока	Висока	Висока

Важливим аспектом при виборі моделі закритої мережі є також оцінка ефективності захисту від різних типів загроз. В таблиці 1.2 наведено порівняння ефективності різних моделей проти основних типів кіберзагроз.

Таблиця 1.2 – Ефективність моделей закритих мереж проти різних типів загроз

Модель	Зовнішні кібератаки	Внутрішні загрози	Фізичне втручання	Загрози через периметр	Складні цільові атаки
Air-Gap	Відмінно	Добре	Відмінно	Відмінно	Добре
Controlled Gateway	Відмінно	Задовільно	Добре	Добре	Задовільно
DMZ	Добре	Задовільно	Задовільно	Добре	Задовільно
Trust-Based Segmentation	Добре	Відмінно	Задовільно	Добре	Добре
Overlay Secure Network	Добре	Задовільно	Задовільно	Задовільно	Задовільно
Zero Trust	Відмінно	Відмінно	Добре	Відмінно	Відмінно

На вибір моделі закритої мережі також впливають галузеві особливості та конкретні бізнес-вимоги. Наприклад, для банківських систем важливою є відповідність регуляторним вимогам, тоді як для промислових систем управління ключовим фактором може бути безперервність роботи. На практиці часто використовуються гібридні рішення, що поєднують елементи різних моделей для досягнення оптимального балансу між безпекою, функціональністю та вартістю впровадження.

1.5 Аналіз кабельних систем для забезпечення захищеності

Кабельна інфраструктура є фундаментальною складовою закритої мережі, що безпосередньо впливає на її надійність та рівень захищеності. Правильний вибір типу кабелів, методів їх прокладання та захисту має вирішальне значення для забезпечення фізичної безпеки передачі даних. У цьому підрозділі проаналізовано основні типи кабельних систем, їх характеристики з точки зору захищеності, а також методи захисту кабельних трас від несанкціонованого доступу.

В сучасних мережевих інфраструктурах використовуються різні типи кабелів, кожен з яких має свої характеристики з точки зору захищеності. Мідні кабелі типу «вита пара» є найбільш поширеними для локальних мереж, проте вони мають суттєві обмеження щодо застосування в закритих мережах з високими вимогами до безпеки. Коваленко В.М. вказує: «Використання неекранованої витой пари в закритих мережах створює значні ризики перехоплення даних через електромагнітне випромінювання, що може здійснюватися без порушення фізичної цілісності кабелю» [3, с. 156].

Оптоволоконні кабелі забезпечують значно вищий рівень захисту завдяки передачі даних у вигляді світлових імпульсів. Сидоренко Л.М. зазначає: «Оптоволоконні кабелі є фактично імунними до електромагнітного прослуховування та пропонують найвищий рівень захисту від несанкціонованого доступу до інформації, що передається» [16, с. 198]. Особливо цінною є властивість оптоволоконних кабелів швидко виявляти спроби фізичного втручання, оскільки будь-яке порушення цілісності кабелю спричиняє суттєве зниження якості сигналу, що легко виявляється системами моніторингу.

Коаксіальні кабелі, хоча й використовуються рідше в сучасних мережах, все ще знаходять застосування в специфічних сценаріях. Вони забезпечують кращий захист від електромагнітних перешкод порівняно з витой парою, але поступаються оптоволокну за рівнем захищеності.

У таблиці 1.3 наведено порівняльний аналіз основних типів кабелів за параметрами, важливими для застосування в закритих мережах.

Для забезпечення належного рівня захищеності кабельні системи повинні відповідати певним стандартам. Ключовими є стандарти електромагнітної сумісності, які визначають допустимі рівні випромінювань та вимоги до стійкості обладнання, а також стандарти фізичного захисту кабельних систем, зокрема EN 50173/ISO/IEC 11801. Особливу увагу слід приділити набору стандартів TEMPEST, розроблених для захисту від витоку інформації через електромагнітне випромінювання.

Таблиця 1.3 – Порівняльний аналіз кабельних систем для закритих мереж

Параметр	Неекранована вита пара (UTP)	Екранована вита пара (S/FTP)	Оптоволоконний кабель	Коаксіальний кабель
Стійкість до електромагнітних перешкод	Низька	Середня до високої	Відмінна	Середня
Складність перехоплення сигналу	Низька	Середня	Дуже висока	Середня
Виявлення несанкціонованого підключення	Складно	Середньої складності	Легко	Середньої складності
Максимальна відстань передачі	100 м	100 м	До 120 км (одномодовий)	500 м
Вартість впровадження	Низька	Середня	Висока	Середня
Рекомендована сфера використання	Некритичні сегменти	Робочі місця користувачів	Магістральні лінії, критичні сегменти	Спеціалізовані застосування

Забезпечення фізичної безпеки кабельних трас є критично важливим аспектом побудови закритої мережі. Згідно з дослідженнями Брайка В.В., "близько 35% усіх випадків несанкціонованого доступу до даних в закритих мережах відбувається через фізичне втручання в кабельну інфраструктуру" [2, с. 42]. Для мінімізації таких ризиків рекомендується прокладати кабелі у захищених каналах або броньованих трубах, забезпечувати контроль доступу до комутаційних приміщень та використовувати системи моніторингу фізичної цілісності кабелів.

Вибір оптимального рішення для кабельної інфраструктури залежить від багатьох факторів, включаючи рівень вимог до безпеки, бюджет проєкту та специфіку середовища. У таблиці 1.4 представлено рекомендації щодо вибору кабельних систем для різних сегментів закритої мережі.

Для критичних сегментів закритих мереж з найвищими вимогами до безпеки рекомендується використовувати рішення з подвійним екрануванням

та додатковим заземленням для мінімізації ризиків витоку інформації через побічні електромагнітні випромінювання. Пархоменко І.І. зазначає, що «правильно спроектована та впроваджена кабельна система може забезпечити до 60% загального рівня фізичної безпеки закритої мережі, створюючи міцний фундамент для інших рівнів захисту» [17].

Важливим аспектом є також правильний вибір комутаційного обладнання, яке повинно відповідати рівню захищеності всієї системи. Доцільно використовувати екрановані комутаційні панелі з належним заземленням, розетки з механічним блокуванням для запобігання несанкціонованому відключенню та системи кольорового кодування для розділення різних рівнів захисту.

Таблиця 1.4 – Рекомендації щодо вибору кабельних систем для різних сегментів мережі

Сегмент мережі	Рекомендований тип кабелю	Додаткові заходи захисту	Рівень захищеності
Магістральна мережа	Одномодове оптоволокно	Захищені кабельні канали, система моніторингу цілісності	Дуже високий
Розподільча мережа	Одномодове/багатомодове оптоволокно або Cat7/Cat8 S/FTP	Екрановані комутаційні шафи, контроль доступу	Високий
Горизонтальна підсистема	Cat6a S/FTP або вище	Захищені кабельні канали, кольорове кодування	Середній до високого
Робочі місця користувачів	Cat6a S/FTP	Механічне блокування портів, контроль підключень	Середній
Демілітаризована зона	Оптоволокно	Фізична ізоляція, резервування каналів	Високий
Серверні ферми	Оптоволокно або Cat8 S/FTP	Спеціалізовані екрановані шафи, постійний моніторинг	Дуже високий

Сучасні технології дозволяють впроваджувати системи активного моніторингу фізичної цілісності кабелів, які в реальному часі відстежують

стан кабельної інфраструктури та повідомляють про будь-які порушення. До таких систем належать оптичні системи виявлення порушень (Fiber Optic Detection Systems) та системи моніторингу імпедансу кабелю на основі технології Time Domain Reflectometry.

Отже, правильний вибір та впровадження захищених кабельних систем є критично важливим етапом при побудові закритих мереж з підвищеною надійністю та захищеністю. Оптимальне рішення повинно забезпечувати надійний захист від несанкціонованого доступу до даних, стійкість до електромагнітних перешкод та можливість швидкого виявлення спроб фізичного втручання в інфраструктуру мережі.

1.6 Мережеві протоколи та їх захищеність

Мережеві протоколи визначають правила та формати взаємодії між пристроями в мережі, і їх захищеність є критично важливим аспектом для забезпечення безпеки закритої мережі. У даному підрозділі розглянуто основні мережеві протоколи, їхні вразливості та захищені альтернативи, які рекомендується використовувати при побудові захищених закритих мереж.

Стандартні мережеві протоколи, які використовуються в звичайних комп'ютерних мережах, здебільшого розроблялися без урахування сучасних вимог до безпеки. Згідно з дослідженнями Коваленка В.М., "традиційні протоколи, такі як IPv4, TCP, UDP, HTTP, мають низку вроджених вразливостей, які можуть бути використані для компрометації мережі" [3,с.178].

Протокол IP (Internet Protocol), який є основою сучасних мереж, не має вбудованих механізмів захисту, таких як шифрування або автентифікація. Це створює можливості для атак типу IP-спуфінгу (підміни адреси відправника), сніфінгу (прослуховування мережевого трафіку) та атак "людина посередині".

Також протоколи транспортного рівня TCP і UDP є вразливими до різноманітних атак, зокрема SYN flood, UDP flood, TCP sequence prediction та ін.

Сидоренко Л.М. зазначає: "В закритих мережах використання незахищених протоколів створює критичні ризики для безпеки, тому необхідно впроваджувати захищені альтернативи або механізми додаткового захисту" [16, с. 132].

У таблиці 1.5 представлено порівняльний аналіз стандартних протоколів та їх захищених альтернатив.

Таблиця 1.5 – Порівняння стандартних протоколів та їх захищених альтернатив

Стандартний протокол	Основні вразливості	Захищена альтернатива	Механізми захисту	Рекомендовані сфери застосування
IPv4	Відсутність автентифікації, шифрування, вразливість до підміни адрес	IPsec, IPv6 з IPsec	Шифрування, автентифікація, захист цілісності даних	Всі сегменти закритої мережі
TCP	Вразливість до SYN flood, sequence prediction атак	TCP з IPsec, MPTCP з TLS	Шифрування даних, захист від переповнення буфера	Критичні додатки, веб-сервіси
UDP	Відсутність гарантій доставки, вразливість до UDP flood	DTLS, QUIC	Шифрування даних, захист від спуфінгу	Додатки реального часу, VoIP
HTTP	Передача даних у відкритому вигляді	HTTPS з TLS 1.3	Шифрування, автентифікація, захист від MITM атак	Веб-інтерфейси управління, API
Telnet	Передача облікових даних у відкритому вигляді	SSH	Шифрування, надійна автентифікація	Віддалене адміністрування
FTP	Відсутність шифрування	SFTP, FTPS	Шифрування даних та облікових записів	Передача файлів
SNMP v1/v2	Слабкі механізми автентифікації	SNMPv3	Шифрування, контроль доступу	Моніторинг мережевого обладнання

Для забезпечення безпеки на мережевому рівні рекомендується використовувати IPsec – набір протоколів для захисту IP-комунікацій шляхом автентифікації та шифрування кожного IP-пакета. IPsec підтримує два режими роботи: транспортний, який захищає лише корисне навантаження IP-пакета, та тунельний, який інкапсулює весь IP-пакет. Брайко В.В. зазначає: "Тунельний режим IPsec є оптимальним для захисту з'єднань між підмережами в закритих мережах, оскільки забезпечує повну ізоляцію трафіку від потенційного прослуховування" [2, с. 54].

IPv6, новіша версія IP-протоколу, має вбудовану підтримку IPsec, більший адресний простір та покращені механізми маршрутизації. Однак, як зазначає Миколайчук Ю.А., "простий перехід на IPv6 без належного налаштування безпеки не гарантує підвищення захищеності мережі. Необхідно також впроваджувати додаткові механізми захисту, такі як захищені протоколи маршрутизації та фільтрація трафіку" [8, с. 50].

На транспортному рівні для забезпечення безпеки рекомендується використовувати протоколи TLS (Transport Layer Security) або його попередник SSL (Secure Sockets Layer). Ці протоколи забезпечують захищений зв'язок у мережі шляхом шифрування даних та автентифікації сторін. Для датаграмних протоколів, таких як UDP, рекомендується використовувати DTLS (Datagram Transport Layer Security) або QUIC (Quick UDP Internet Connections), який поєднує кращі риси TCP та UDP з вбудованим шифруванням.

На рівні додатків рекомендується замінити незахищені протоколи їхніми захищеними аналогами: SSH (Secure Shell) замість Telnet; SFTP/FTPS замість FTP; HTTPS замість HTTP; SNMPv3 з підтримкою шифрування та автентифікації замість SNMPv1/v2.

Особливу увагу слід приділити протоколам маршрутизації, оскільки їх компрометація може призвести до серйозних порушень у роботі мережі. У таблиці 1.6 наведено рекомендовані протоколи маршрутизації для закритих мереж.

Для забезпечення максимального рівня захисту в закритих мережах з найвищими вимогами до безпеки рекомендується використовувати спеціалізовані протоколи з високим рівнем шифрування: MACsec (IEEE 802.1AE) – стандарт безпеки для захисту даних на каналному рівні; SRTP (Secure Real-time Transport Protocol) – захищений протокол для передачі мультимедійних даних; DNSSEC (Domain Name System Security Extensions) – розширення DNS для забезпечення автентифікації та цілісності даних.

Таблиця 1.6 – Рекомендовані протоколи маршрутизації для закритих мереж

Тип протоколу	Назва протоколу	Основні механізми безпеки	Переваги	Обмеження
Внутрішній протокол маршрутизації	OSPFv3 з автентифікацією	MD5/SHA автентифікація, підтримка IPsec	Швидка конвергенція, підтримка VLSM	Складність налаштування
Внутрішній протокол маршрутизації	IS-IS з автентифікацією	Автентифікація повідомлень, підтримка Ipsec	Масштабованість, незалежність від IP	Менш поширений, обмежена підтримка
Внутрішній протокол маршрутизації	EIGRP з автентифікацією	MD5 автентифікація, SHA автентифікація	Швидка конвергенція, ефективне використання пропускної здатності	Пропрієтарний протокол Cisco
Зовнішній протокол маршрутизації	BGP з RPKI	Валідація маршрутів, MD5 автентифікація	Масштабованість, контроль політик маршрутизації	Повільна конвергенція
Механізм захисту	BFD (Bidirectional Forwarding Detection)	Швидке виявлення відмов маршрутів	Мінімізація часу простою при відмовах	Додаткове навантаження на процесор
Механізм захисту	GTSM (Generalized TTL Security Mechanism)	Захист від атак на протоколи маршрутизації	Простота впровадження	Обмежена ефективність проти складних атак

У військових та особливо критичних системах використовуються спеціалізовані протоколи, такі як HAIPE (High Assurance Internet Protocol Encryptor) та SCIP (Secure Communications Interoperability Protocol).

Отже, вибір та правильне налаштування захищених мережевих протоколів є критично важливим аспектом при побудові закритих мереж з підвищеною надійністю та захищеністю. Заміна незахищених протоколів на їхні захищені аналоги, використання сильних механізмів автентифікації та шифрування, а також регулярне оновлення протоколів для усунення відомих вразливостей є необхідними кроками для забезпечення безпеки мережевих комунікацій.

1.7 Системи моніторингу та керування мережею

Ефективне функціонування закритої мережі з підвищеною надійністю та захищеністю неможливе без впровадження комплексних систем моніторингу та керування. Такі системи забезпечують постійний контроль за станом мережевої інфраструктури, своєчасне виявлення потенційних проблем та швидке реагування на інциденти безпеки. У цьому підрозділі розглянуто основні типи систем моніторингу та керування мережею, їх функціональні можливості та особливості застосування в закритих мережах.

Системи керування мережею, у свою чергу, забезпечують централізоване управління мережевою інфраструктурою, включаючи конфігурацію обладнання, розподіл ресурсів, управління користувачами та політиками безпеки. Ці системи є особливо важливими для закритих мереж, де необхідно забезпечити строгий контроль за доступом та захист від несанкціонованих змін.

Основні типи систем моніторингу та керування мережею, їх функціональні можливості та особливості застосування в закритих мережах представлені в таблиці 1.7.

Для закритих мереж з підвищеними вимогами до безпеки особливо важливо забезпечити комплексний підхід до моніторингу та керування.

Миколайчук Ю.А. підкреслює: "Ефективна система моніторингу закритої мережі повинна охоплювати всі рівні мережевої інфраструктури, від фізичного до прикладного, та забезпечувати виявлення як технічних проблем, так і порушень безпеки" [8, с. 49].

Таблиця 1.7 – Типи систем моніторингу та керування мережею

Тип системи	Основні функції	Приклади	Особливості застосування в закритих мережах
Системи моніторингу продуктивності мережі	Збір та аналіз даних про пропускну здатність, затримки, втрати пакетів	Zabbix, Nagios, PRTG, SolarWinds NPM	Необхідно забезпечити ізоляцію системи моніторингу від зовнішніх мереж, використовувати захищені протоколи збору даних
Системи виявлення та запобігання вторгнень (IDS/IPS)	Моніторинг мережевого трафіку для виявлення підозрілої активності, блокування атак	Snort, Suricata, Cisco FirePOWER	Потребують регулярного оновлення сигнатур атак, важливе правильне розміщення сенсорів у ключових точках мережі
Системи управління мережевими пристроями	Централізована конфігурація та управління мережним обладнанням	Cisco DNA Center, HPE IMC, ManageEngine OpManager	Необхідно забезпечити надійну автентифікацію та авторизацію адміністраторів, шифрування управляючого трафіку
Системи аналізу мережевого трафіку	Глибокий аналіз мережеских пакетів, виявлення аномалій	Wireshark, Netflow Analyzer, ntopng	Потребують значних обчислювальних ресурсів, важливо забезпечити захист отриманих даних
Системи управління конфігураціями	Автоматизація процесів налаштування та підтримки консистентності конфігурацій	Ansible, Puppet, Chef, SaltStack	Критично важливо забезпечити контроль цілісності шаблонів конфігурацій та перевірку змін перед застосуванням
Системи управління подіями та інцидентами безпеки (SIEM)	Централізований збір та аналіз журналів, кореляція подій безпеки	Splunk, IBM Qradar, ArcSight, Elastic Stack	Вимагають потужних обчислювальних ресурсів, необхідно забезпечити надійне зберігання та захист журналів
Системи управління доступом до мережі (NAC)	Контроль доступу пристроїв до мережі на основі політик	Cisco ISE, Forescout, Aruba ClearPass	Критично важливі для запобігання несанкціонованому доступу, необхідна інтеграція з іншими системами безпеки

Вибір конкретних інструментів моніторингу та керування залежить від масштабу мережі, бюджету проєкту та специфічних вимог. У таблиці 1.8 представлено порівняння популярних систем моніторингу за ключовими характеристиками.

Таблиця 1.8 – Порівняння популярних систем моніторингу мережі

Характеристика	Zabbix	Nagios	PRTG	SolarWinds NPM	Prometheus + Grafana
Ліцензія	Open Source	Open Source/Commercial	Commercial	Commercial	Open Source
Масштабованість	Висока	Середня	Висока	Дуже висока	Висока
Підтримка протоколів моніторингу	SNMP, IPMI, JMX, HTTP, SSH	SNMP, IPMI, HTTP	SNMP, WMI, NetFlow, HTTP	SNMP, WMI, NetFlow, sFlow	HTTP, Prometheus API
Вбудовані механізми безпеки	Шифрування даних, автентифікація	Базова автентифікація	Шифрування даних, RBAC	Шифрування даних, RBAC, інтеграція з AD	Базова автентифікація (потребує додаткових компонентів)
Можливості автоматизації	Широкі	Обмежені	Середні	Широкі	Широкі
Підтримка в закритих мережах	Можлива, потребує додаткової конфігурації	Можлива, потребує додаткової конфігурації	Проблематична через ліцензування	Проблематична через ліцензування	Можлива, потребує додаткової конфігурації
Рівень складності впровадження	Середній до високого	Високий	Низький до середнього	Середній	Високий

При створенні систем моніторингу та керування в мережах закритого типу необхідно враховувати ряд важливих аспектів, а саме:

Системи часто потребують доступу до всіх компонентів мережі, що робить їх потенційно небезпечними в разі компрометації. Тому необхідно забезпечити належний захист самих систем моніторингу, включаючи контроль доступу, шифрування даних та регулярний аудит.

В закритих мережах часто існують обмеження щодо використання

комерційного програмного забезпечення, особливо якщо воно вимагає зв'язку з зовнішніми серверами для активації ліцензій або отримання оновлень. У таких випадках перевагу слід віддавати рішенням з відкритим кодом або спеціалізованим системам, розробленим для критичних інфраструктур.

Згідно з рекомендаціями Національного інституту стандартів і технологій США (NIST), «системи моніторингу та керування для закритих мереж повинні бути розгорнуті таким чином, щоб мінімізувати ризики, пов'язані з їх компрометацією. Це включає сегментацію мережі, суворий контроль доступу та резервування критичних компонентів» [27].

Важливим компонентом сучасних систем моніторингу та керування є підсистеми оповіщення, які забезпечують швидке інформування адміністраторів про виникнення проблем або інцидентів безпеки. Брайко В.В. зазначає: «Ефективність реагування на інциденти в закритих мережах напряму залежить від швидкості оповіщення та повноти інформації про інцидент» [2, с. 68]. Підсистеми оповіщення повинні підтримувати різні канали комунікації (електронна пошта, SMS, месенджери) та забезпечувати ескалацію важливих повідомлень у разі відсутності реакції протягом визначеного часу.

Для закритих мереж з особливо високими вимогами до безпеки рекомендується впроваджувати спеціалізовані системи виявлення аномалій на основі машинного навчання. Такі системи аналізують великі обсяги даних моніторингу та здатні виявляти нетипову поведінку, яка може свідчити про атаки або технічні проблеми, навіть якщо вони не відповідають відомим шаблонам. За даними Gartner, «до 2025 року системи виявлення аномалій на основі машинного навчання стануть стандартним компонентом систем моніторингу для критичних інфраструктур» [22].

Важливим аспектом є також забезпечення відмовостійкості самих систем моніторингу та керування. Коваленко В.М. рекомендує: «Для критичних мереж необхідно впроваджувати розподілені системи моніторингу з дублюванням ключових компонентів та автоматичним перемиканням у разі

відмов» [9, с. 235]. Це дозволяє забезпечити безперервність моніторингу навіть у випадку часткових збоїв у роботі мережі.

Згідно з дослідженнями Міністерства освіти і науки України, для закритих мереж навчальних закладів рекомендується використовувати багаторівневі системи моніторингу, які включають:

- моніторинг фізичної інфраструктури (температура, вологість, електроживлення);
- моніторинг мережевого обладнання (доступність, продуктивність, помилки);
- моніторинг серверів та сервісів (навантаження, доступність, журнали);
- моніторинг безпеки (виявлення вторгнень, аналіз вразливостей) [14].

З розвитком технологій автоматизації та програмно-визначених мереж (SDN) з'являються нові можливості для побудови інтелектуальних систем керування, здатних автоматично реагувати на виявлені проблеми. Такі системи можуть динамічно змінювати конфігурацію мережі, перенаправляти трафік або блокувати потенційно небезпечну активність без участі людини.

1.8 Методи та засоби захисту інформації в закритих мережах

Захист інформації в закритих мережах є комплексним завданням, яке вимагає застосування різноманітних методів та засобів на різних рівнях мережевої інфраструктури. У цьому підрозділі розглянуто основні методи та засоби захисту інформації, їх ефективність та особливості застосування в закритих мережах з підвищеними вимогами до надійності та безпеки.

Коваленко В.М. визначає захист інформації як "комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також запобігання несанкціонованому доступу до

неї" [3, с. 267]. Ці три основні властивості інформаційної безпеки (конфіденційність, цілісність, доступність) часто доповнюються такими характеристиками як автентичність, неспростовність та підзвітність. Сидоренко Л.М. зазначає: "Для закритих мереж критичним є забезпечення всіх аспектів інформаційної безпеки, оскільки компрометація будь-якого з них може призвести до серйозних наслідків, включаючи витік конфіденційної інформації, порушення функціонування критичних систем або втрату даних" [16, с. 256].

Методи та засоби захисту інформації в закритих мережах можна класифікувати за різними критеріями: за рівнем захисту, за об'єктом захисту, за характером впливу тощо. У таблиці 1.9 представлена класифікація методів захисту інформації за рівнями моделі OSI.

Організаційні методи захисту інформації включають розробку та впровадження політик безпеки, навчання персоналу, регулярний аудит безпеки, керування доступом та інші заходи, спрямовані на створення загальної структури управління інформаційною безпекою. Миколайчук Ю.А. підкреслює: «Організаційні методи є фундаментом системи захисту інформації, без якого навіть найсучасніші технічні засоби не зможуть забезпечити належний рівень безпеки» [8, с. 51].

Технічні методи захисту інформації можна поділити на апаратні, програмні та програмно-апаратні. Вони включають широкий спектр засобів, від фізичного захисту обладнання до спеціалізованого програмного забезпечення для виявлення та запобігання атакам. У таблиці 1.10 представлено порівняння основних технічних засобів захисту інформації, їх ефективності та особливостей застосування в закритих мережах.

Важливим аспектом захисту інформації в закритих мережах є використання криптографічних методів. Шифрування забезпечує конфіденційність даних при зберіганні та передачі, а електронний цифровий підпис гарантує їх цілісність та автентичність. Брайко В.В. зазначає: "Для закритих мереж критично важливо використовувати сучасні та перевірені

криптографічні алгоритми, а також забезпечувати надійне управління криптографічними ключами" [2, с. 73].

Таблиця 1.9 – Методи захисту інформації за рівнями моделі OSI

Рівень моделі OSI	Методи захисту	Приклади засобів	Основні загрози
Фізичний рівень	Екранування кабелів, фізичне розмежування, контроль доступу до обладнання	Екрановані кабелі, системи контролю доступу, датчики вторгнення	Фізичне втручання, перехоплення електромагнітного випромінювання
Канальний рівень	Шифрування на рівні каналу, фільтрація MAC-адрес, сегментація мережі	MACsec (IEEE 802.1AE), комутатори з функцією port security	MAC-спуфінг, атаки типу "людина посередині"
Мережевий рівень	Шифрування IP-трафіку, міжмережеві екрани, системи виявлення вторгнень	IPsec, апаратні міжмережеві екрани, IDS/IPS системи	IP-спуфінг, DDoS-атаки, несанкціонований доступ
Транспортний рівень	Захищені транспортні протоколи, фільтрація портів	TLS/SSL, DTLS, міжмережеві екрани рівня додатків	TCP SYN flood, UDP flood, аналіз трафіку
Сеансовий рівень	Керування сеансами, автентифікація	Kerberos, системи єдиного входу (SSO)	Перехоплення сеансу, підбір паролів
Представницький рівень	Шифрування даних додатків, захист від шкідливого коду	Системи шифрування файлів, антивірусне ПЗ	Витік даних, атаки на шифрування
Прикладний рівень	Контроль доступу до додатків, захищені протоколи прикладного рівня	HTTPS, SSH, S/MIME, системи DLP	Атаки на веб-додатки, фішинг, соціальна інженерія

Згідно з рекомендаціями Національного інституту стандартів і технологій США (NIST), для закритих мереж з високими вимогами до безпеки рекомендується використовувати: симетричні алгоритми шифрування: AES-256; асиметричні алгоритми: RSA (з ключами не менше 3072 біт), ECDSA, EdDSA; хеш-функції: SHA-384, SHA-512; протоколи узгодження ключів: ECDHE, DH з ключами не менше 3072 біт [27].

Таблиця 1.10 – Порівняння технічних засобів захисту інформації

Засіб захисту	Основні функції	Ефективність проти різних типів загроз	Особливості застосування в закритих мережах	Обмеження
Міжмереві екрани нового покоління (NGFW)	Фільтрація трафіку на рівні додатків, глибокий аналіз пакетів, VPN	Висока ефективність проти мережесх атак та шкідливого ПЗ	Розміщення на межі сегментів з різним рівнем довіри, посилені правила фільтрації	Висока вартість, складність налаштування
Системи виявлення та запобігання вторгненням (IDS/IPS)	Моніторинг та аналіз мережевого трафіку, виявлення та блокування атак	Середня до високої проти відомих типів атак	Розміщення в ключових точках мережі, інтеграція з іншими системами безпеки	Вимагають регулярного оновлення сигнатур, можливі помилкові спрацьовування
Системи запобігання витоку даних (DLP)	Контроль за переміщенням конфіденційних даних	Висока проти навмисного та випадкового витоку даних	Впровадження на рівні мережі та кінцевих точок	Складність налаштування, можливий вплив на продуктивність
Системи шифрування даних	Забезпечення конфіденційності та цілісності даних	Дуже висока проти перехоплення даних	Шифрування даних при зберіганні та передачі, управління ключами	Вплив на продуктивність, складність управління ключами
Системи багатофакторної автентифікації	Посилення процесу перевірки ідентичності користувачів	Висока проти несанкціонованого доступу	Впровадження для доступу до критичних систем та даних	Додаткові витрати на апаратні токени, можливі складнощі для користувачів
Системи контролю доступу до мережі (NAC)	Контроль доступу пристроїв до мережі	Висока проти несанкціонованих пристроїв	Впровадження на всіх входах до мережі	Складність інтеграції з існуючою інфраструктурою
Антивірусні системи та EDR	Захист від шкідливого ПЗ, виявлення та реагування на інциденти	Середня до високої проти шкідливого ПЗ	Встановлення на всіх кінцевих точках, централізоване управління	Вимагають регулярного оновлення, можливі помилкові спрацьовування

Важливим аспектом забезпечення безпеки в закритих мережах є також впровадження механізмів безперервності бізнесу та аварійного відновлення. Це включає регулярне резервне копіювання даних, створення відмовостійкої інфраструктури та розробку планів реагування на інциденти. Згідно з дослідженнями Gartner, "організації, які мають формалізовані процедури реагування на інциденти, зменшують середній час відновлення після кібератак на 50-80%" [22].

Отже, захист інформації в закритих мережах вимагає комплексного підходу, який поєднує організаційні, технічні та криптографічні методи. Впровадження багаторівневого захисту, використання сучасних технологій та засобів, регулярний аудит безпеки та навчання персоналу дозволяють забезпечити високий рівень захищеності мережевої інфраструктури та даних. При цьому необхідно враховувати специфіку конкретної галузі та постійно оновлювати систему захисту відповідно до появи нових загроз та вразливостей.

2 РОЗРОБКА ЗАКРИТОЇ МЕРЕЖІ З ПІДВИЩЕНОЮ НАДІЙНІСТЮ ТА ЗАХИЩЕНІСТЮ

2.1 Технічне завдання на розробку закритої мережі

Розробка закритої мережі з підвищеною надійністю та захищеністю здійснюється на основі ретельно сформованого технічного завдання, яке враховує вимоги замовника та специфіку предметної області. Замовником у даному випадку виступає навчальний заклад (Національний університет «Запорізька політехніка»), для якого критично важливим є забезпечення надійного функціонування інформаційної інфраструктури та захист конфіденційних даних, зокрема персональних даних студентів і

співробітників, результатів наукових досліджень, адміністративної інформації тощо.

Відповідно до аналізу потреб закладу та нормативних документів (ISO/IEC 27001:2013 та Постанови №992), проєкт закритої мережі передбачає підтримку до 200 активних користувачів, 10+ серверів та 150 робочих станцій, розміщених у трьох будівлях кампусу з цілодобовим функціонуванням. Система вимагає надійності 99,9%, повної фізичної ізоляції від зовнішніх мереж (Air-Gap), багаторівневої автентифікації, шифрування даних, сегментації мережі, та захисту від витоків.

Функціонально мережа забезпечуватиме базові сервіси, корпоративну пошту, доступ до файлів і баз даних, документообіг та спеціалізовані системи закладу, з централізованим управлінням та моніторингом. План впровадження включає проєктування архітектури, вибір обладнання, розробку інфраструктури, систем захисту та документування.

2.2 Проєктування топології та архітектури мережі

Проєктування топології та архітектури мережі є фундаментальним етапом розробки закритої мережі, оскільки архітектурні рішення визначають базовий рівень надійності, захищеності та масштабованості системи. На основі аналізу вимог, викладених у технічному завданні, та результатів дослідження, проведеного в розділі 1, розроблено комплексну архітектуру закритої мережі з підвищеною надійністю.

Для забезпечення оптимального балансу між надійністю, захищеністю, масштабованістю та вартістю впровадження було проведено порівняльний аналіз різних архітектурних підходів до побудови мережевої інфраструктури. Результати аналізу представлені в таблиці 2.1.

Таблиця 2.1 – Порівняльний аналіз архітектурних підходів до побудови мережі

Критерій	Плоска архітектура	Ієрархічна трирівнева архітектура	Архітектура Spine-Leaf	Гібридна архітектура
Надійність	Низька до середньої	Висока (при належному резервуванні)	Дуже висока	Висока
Масштабованість	Обмежена	Висока	Дуже висока	Висока
Продуктивність	Середня	Висока	Дуже висока	Висока
Складність впровадження	Низька	Середня	Висока	Середня до високої
Захищеність	Низька	Висока	Середня до високої	Висока
Можливість сегментації	Обмежена	Висока	Середня	Висока
Вартість впровадження	Низька	Середня	Висока	Середня до високої
Відповідність вимогам проєкту	Часткова	Повна	Часткова	Висока

На основі проведеного аналізу для проєктування закритої мережі вибрано ієрархічну трирівневу архітектуру (ядро, розподіл, доступ), що забезпечує чіткий розподіл функцій, ефективну сегментацію, високу надійність через резервування компонентів, масштабованість без суттєвої реконфігурації та спрощене впровадження механізмів захисту. Рівень ядра забезпечує високошвидкісну комутацію пакетів між сегментами використовуючи високопродуктивні комутатори 3-го рівня з підтримкою протоколів резервування. Рівень розподілу відповідає за маршрутизацію між VLAN, застосування політик безпеки та фільтрацію трафіку. Рівень доступу забезпечує підключення кінцевих пристроїв та реалізацію базових механізмів безпеки на рівні портів. Загальна структура архітектури представлена на рисунку 2.1.

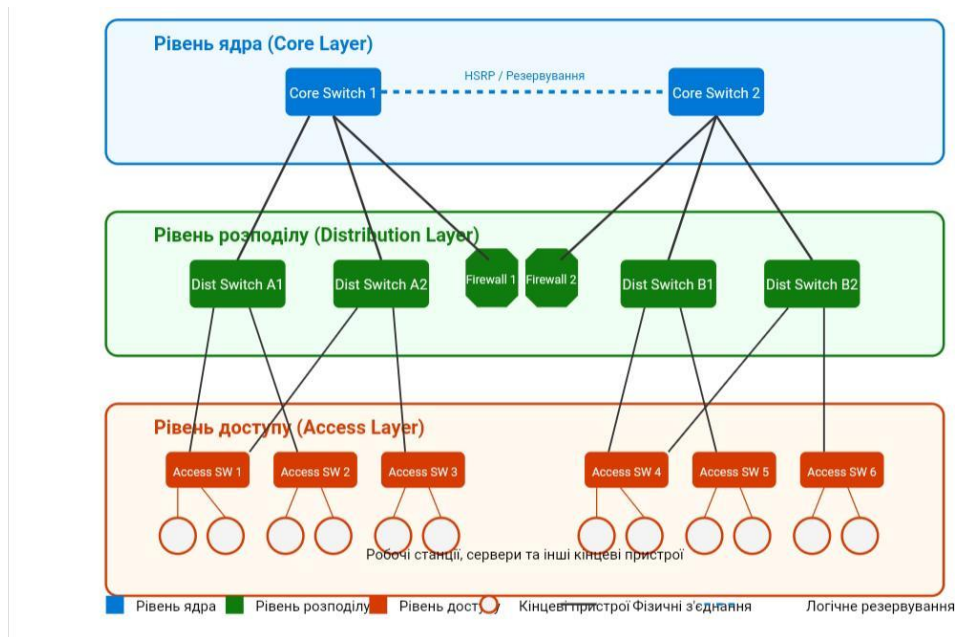


Рисунок 2.1 – Структура ієрархічної архітектури закритої мережі

Для забезпечення підвищеної надійності в архітектурі мережі передбачено такі механізми резервування:

- на рівні ядра використовуються два комутатори, які працюють у режимі активний-активний з використанням протоколу HSRP (Hot Standby Router Protocol) для забезпечення автоматичного переключення у разі відмови одного з пристроїв;

- між рівнями ядра та розподілу, а також між рівнями розподілу та доступу використовуються агреговані канали зв'язку (EtherChannel), що об'єднують кілька фізичних з'єднань в одне логічне для підвищення пропускної здатності та надійності;

- комутатори рівня доступу підключаються до двох різних комутаторів рівня розподілу для забезпечення резервування шляхів передачі даних.

Для підвищення захищеності мережі реалізована глибока сегментація з використанням віртуальних локальних мереж (VLAN). Відповідно до функціональних потреб навчального закладу виділено такі основні сегменти:

- VLAN 10 - адміністративний сегмент (для керівництва та адміністративного персоналу);

- VLAN 20 - навчальний сегмент (для викладачів та навчальних аудиторій);
- VLAN 30 - науковий сегмент (для науково-дослідних лабораторій);
- VLAN 40 - сегмент студентського містечка;
- VLAN 50 - серверний сегмент (для розміщення серверів та сервісів);
- VLAN 60 - сегмент управління (для систем моніторингу та управління мережею);
- VLAN 70 - сегмент безпеки (для систем безпеки та контролю доступу).

Розподіл мережевих адрес для кожного VLAN представлено в таблиці 2.2.

Таблиця 2.2 - Розподіл мережевих адрес для сегментів мережі

VLAN ID	Назва сегмента	Мережа IP	Маска підмережі	Максимальна кількість хостів	Призначення
10	Адміністративний	10.1.10.0	255.255.255.0	254	Робочі станції та пристрої адміністративного персоналу
20	Навчальний	10.1.20.0	255.255.255.0	254	Комп'ютери в навчальних аудиторіях та робочі місця викладачів
30	Науковий	10.1.30.0	255.255.255.0	254	Обладнання науково-дослідних лабораторій
40	Студентське містечко	10.1.40.0	255.255.255.0	254	Робочі станції в гуртожитках та студентських приміщеннях
50	Серверний	10.1.50.0	255.255.255.0	254	Сервери та сервіси інформаційної інфраструктури
60	Управління	10.1.60.0	255.255.255.0	254	Системи моніторингу та управління мережею
70	Безпека	10.1.70.0	255.255.255.0	254	Системи безпеки та контролю доступу

Взаємодія між різними сегментами мережі суворо контролюється на рівні розподілу з використанням міжмережевих екранів та списків контролю доступу (ACL), що дозволяє реалізувати принцип найменших привілеїв та мінімізувати ризики несанкціонованого доступу до конфіденційної інформації.

Фізична топологія мережі враховує особливості розташування будівель навчального закладу та вимоги до надійності інфраструктури. Основні компоненти мережі розподілені між трьома будівлями таким чином:

- головна будівля (корпус А) – містить центральний комутаційний вузол (ядро мережі), основний серверний вузол, а також обладнання рівня розподілу та доступу для користувачів, розташованих у цій будівлі;

- корпус Б – містить вторинний комутаційний вузол (комутатори рівня розподілу) та обладнання рівня доступу для користувачів цього корпусу;

- корпус В – містить вторинний комутаційний вузол (комутатори рівня розподілу) та обладнання рівня доступу.

Зв'язок між будівлями забезпечується оптоволоконними лініями з резервуванням – між кожною парою будівель прокладено по два фізично незалежних оптоволоконних кабелі різними маршрутами. Це дозволяє забезпечити безперервність зв'язку навіть у випадку пошкодження однієї з ліній.

Фізична топологія мережі представлена на рисунку 2.2.

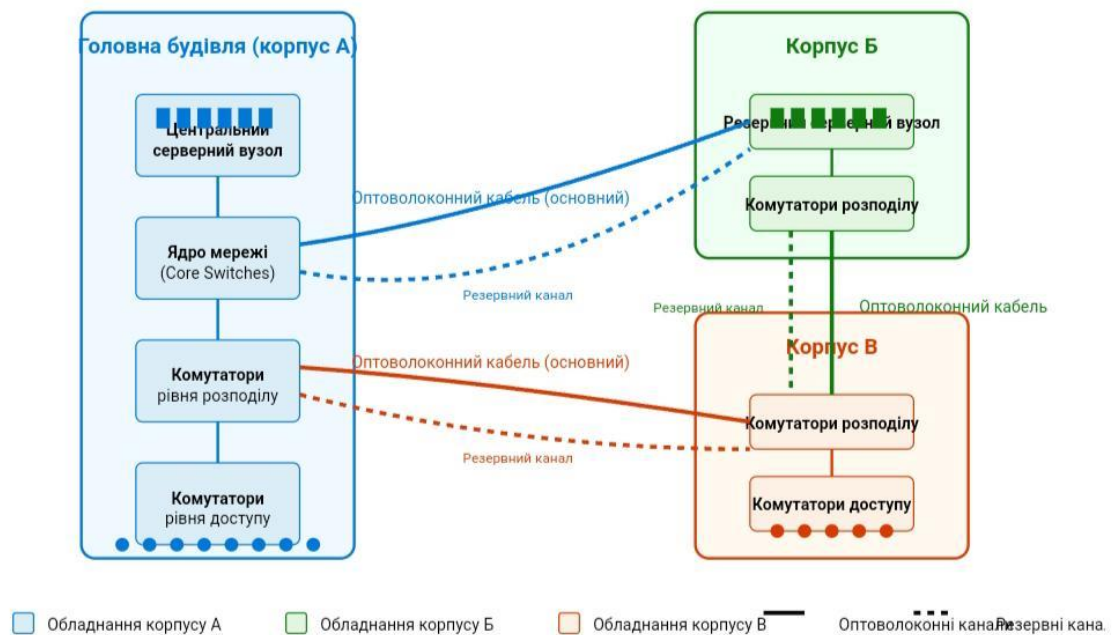


Рисунок 2.2 – Фізична топологія закритої мережі

Як видно з рисунка 2.2, між будівлями реалізовано повнозв'язну топологію на рівні магістральних з'єднань, що забезпечує наявність альтернативних шляхів передачі даних у випадку відмови одного з каналів. Усередині кожної будівлі використовується ієрархічна топологія типу "зірка", що забезпечує оптимальний баланс між надійністю та вартістю впровадження.

Для оцінки відповідності розробленої архітектури вимогам технічного завдання щодо надійності проведено розрахунок ключових параметрів надійності мережі.

Коефіцієнт готовності мережі визначається за формулою:

$$K_r = \frac{MTBF}{MTBF + MTTR} \quad (2.1)$$

де MTBF (Mean Time Between Failures) – середній час між відмовами;
MTTR (Mean Time To Repair) – середній час відновлення.

Для розрахунку коефіцієнта готовності всієї мережі необхідно врахувати архітектуру системи та надійність окремих компонентів. При послідовному з'єднанні компонентів (коли відмова будь-якого компонента призводить до відмови всієї системи) коефіцієнт готовності розраховується як добуток коефіцієнтів готовності окремих компонентів:

$$K_{\text{Г(система)}} = K_{\text{Г1}} \times K_{\text{Г2}} \times \dots \times K_{\text{Гn}} \quad (2.2)$$

При паралельному з'єднанні компонентів (коли система працює, якщо працює хоча б один компонент) коефіцієнт готовності розраховується за формулою:

$$K_{\text{Г(система)}} = 1 - (1 - K_{\text{Г1}}) \times (1 - K_{\text{Г2}}) \times \dots \times (1 - K_{\text{Гn}}) \quad (2.3)$$

Для розрахунку коефіцієнта готовності розробленої мережі використовуємо значення MTBF та MTTR для основних компонентів, наведені в таблиці 2.3.

Таблиця 2.3 – Параметри надійності основних компонентів мережі

Компонент	MTBF (годин)	MTTR (годин)	Коефіцієнт готовності
Комутатор рівня ядра	200000	2	0,99999
Комутатор рівня розподілу	180000	3	0,99998
Комутатор рівня доступу	160000	4	0,99997
Оптоволоконна лінія	500000	8	0,99998
Сервер	150000	4	0,99997
Система електроживлення з ДБЖ	100000	1	0,99999

Враховуючи наявність резервування на всіх критичних ділянках мережі, розрахунковий коефіцієнт готовності всієї системи становить 0,99994, що відповідає доступності мережі протягом 99,994% часу або

максимальному часу простою близько 5,3 години на рік. Це повністю відповідає вимогам технічного завдання щодо забезпечення коефіцієнта готовності не менше 99,9%.

Таким чином, розроблена архітектура закритої мережі забезпечує необхідний рівень надійності та захищеності, відповідаючи всім вимогам технічного завдання. Використання ієрархічної трирівневої моделі з резервуванням критичних компонентів дозволяє досягти оптимального балансу між продуктивністю, надійністю, захищеністю та вартістю впровадження.

2.3 Вибір та обґрунтування мережевого обладнання

Вибір мережевого обладнання для закритої мережі базується на восьми ключових критеріях: відповідність функціональним вимогам, підтримка протоколів безпеки, надійність і відмовостійкість, масштабованість, можливість централізованого управління, сумісність з іншими компонентами, наявність сертифікатів безпеки та загальна вартість володіння. Після порівняльного аналізу обладнання провідних виробників (Cisco Systems, Juniper Networks, HPE) було обрано рішення Cisco Systems для уніфікації та спрощення адміністрування. Для рівня ядра, що забезпечує високошвидкісну комутацію між сегментами мережі, вибрано комутатори Cisco Catalyst 9500 Series, які оптимально поєднують продуктивність, надійність та функції безпеки, як підтверджується даними порівняльної таблиці 2.4.

Для рівня ядра закритої мережі обрано комутатори Cisco Catalyst 9500-40X-A у кількості двох пристроїв для забезпечення резервування. Ця модель характеризується 40 портами 10/25 Gigabit Ethernet (SFP28), 8 портами 40/100 Gigabit Ethernet (QSFP28), комутаційною матрицею з пропускною здатністю 3,2 Тбіт/с, продуктивністю 1900 млн пакетів/с, двома резервними блоками

живлення з можливістю гарячої заміни, спеціалізованими ASIC для прискорення функцій безпеки та підтримкою технології Cisco StackWise Virtual. Комутатори налаштовуються в режимі високої доступності за допомогою протоколу HSRP, що забезпечує автоматичне перемикання у випадку відмови, а технологія StackWise Virtual дозволяє об'єднати фізичні комутатори в один логічний пристрій. Захист від несанкціонованого доступу реалізується через шифрування даних за технологією MACsec, розширені списки контролю доступу, захист від підміни MAC-адрес, захист контрольного трафіку та автентифікацію адміністраторів за протоколом RADIUS. Рівень розподілу забезпечує взаємодію між рівнями ядра та доступу, реалізуючи маршрутизацію між VLAN, застосування політик безпеки та фільтрацію трафіку.

Таблиця 2.4 - Порівняльний аналіз комутаторів для рівня ядра

Характеристика	Cisco Catalyst 9500	Juniper EX9200	HPE FlexFabric 5950
Продуктивність комутації	До 6,4 Тбіт/с	До 4,8 Тбіт/с	До 5,76 Тбіт/с
Пропускна здатність портів	1/10/25/40/100 Гбіт/с	1/10/40/100 Гбіт/с	1/10/25/40/100 Гбіт/с
Ємність таблиці MAC-адрес	82K	288K	128K
Підтримка VLAN	4094	4096	4096
Резервування компонентів	Повне (блоки живлення, вентилятори, модулі управління)	Повне	Повне
Підтримка протоколів резервування	HSRP, VRRP, VSS	VRRP	VRRP
Функції безпеки	MACsec, IEEE 802.1X, ACL, TrustSec	MACsec, IEEE 802.1X, ACL	MACsec, IEEE 802.1X, ACL
MTBF (годин)	>200 000	>175 000	>190 000
Можливість гарячої заміни компонентів	Так	Так	Так
Сертифікати відповідності	FIPS 140-2, CC, DISA	FIPS 140-2, CC	FIPS 140-2

Для рівня розподілу обрано комутатори Cisco Catalyst 9300-48U. Порівняльний аналіз комутаторів рівня розподілу представлено в таблиці 2.5.

Таблиця 2.5 - Порівняльний аналіз комутаторів для рівня розподілу

Характеристика	Cisco Catalyst 9300	Juniper EX4600	HPE Aruba 5400R
Продуктивність комутації	До 1,0 Тбіт/с	До 1,44 Тбіт/с	До 960 Гбіт/с
Кількість портів	До 48 портів 1G/10G	До 72 портів 1G/10G	До 96 портів 1G/10G
Підтримка PoE/PoE+	Так (до 90 Вт на порт)	Так (до 30 Вт на порт)	Так (до 60 Вт на порт)
Стекування	До 8 пристроїв	До 10 пристроїв	До 10 пристроїв
Пропускна здатність стеку	480 Гбіт/с	320 Гбіт/с	336 Гбіт/с
Ємність таблиці маршрутизації	32K (IPv4), 16K (IPv6)	32K (IPv4), 16K (IPv6)	32K (IPv4), 16K (IPv6)
Підтримка VLAN	4094	4096	2048
Резервні компоненти	Блоки живлення, вентилятори	Блоки живлення, вентилятори	Модулі управління, блоки живлення, вентилятори
Функції безпеки	802.1X, MACsec, TrustSec, ACL	802.1X, MACsec, ACL	802.1X, MACsec, ACL
MTBF (годин)	>185 000	>150 000	>165 000
Сертифікати безпеки	FIPS 140-2, CC	FIPS 140-2	FIPS 140-2

Для реалізації рівня розподілу в кожній з трьох будівель встановлюється по два комутатори Cisco Catalyst 9300-48U для забезпечення резервування. Основні характеристики обраної моделі:

- 48 портів 1 Gigabit Ethernet з підтримкою PoE+ (до 30 Вт на порт);
- 4 порти 10 Gigabit Ethernet з модулями SFP+;
- підтримка стекування до 8 пристроїв;
- комутаційна матриця з пропускнуою здатністю 176 Гбіт/с;
- продуктивність передачі пакетів 262 млн пакетів/с;
- два резервних блоки живлення з можливістю гарячої заміни;
- підтримка протоколів маршрутизації OSPF, EIGRP, BGP;
- розширені функції безпеки, включаючи підтримку технології Cisco TrustSec.

Важливою особливістю комутаторів рівня розподілу є підтримка технології Cisco StackWise-480, яка дозволяє об'єднати до 8 комутаторів в один логічний пристрій зі спільною площиною управління. Це значно спрощує адміністрування та підвищує надійність системи, оскільки у разі

відмови одного з комутаторів стеку його функції автоматично перерозподіляються між іншими пристроями без переривання роботи мережі.

Для забезпечення додаткового рівня захисту між критичними сегментами мережі на рівні розподілу встановлюються міжмережеві екрани Cisco Firepower 2130 NGFW. Ці пристрої реалізують функції:

- глибокої інспекції пакетів (DPI);
- запобігання вторгненням (IPS);
- захисту від шкідливого програмного забезпечення;
- контролю додатків та URL-фільтрації;
- аналізу зашифрованого трафіку.

Кожен міжмережевий екран має пропускну здатність до 5 Гбіт/с при включенні всіх функцій захисту та здатний обробляти до 8000 нових з'єднань за секунду, що повністю відповідає вимогам проєкту.

Рівень доступу забезпечує підключення кінцевих пристроїв користувачів до мережі та реалізує початкові функції безпеки. Обладнання цього рівня повинно мати достатню кількість портів для підключення всіх робочих станцій, принтерів та інших периферійних пристроїв, а також забезпечувати базові функції безпеки на рівні портів.

Для рівня доступу обрано комутатори Cisco Catalyst 9200-48P, які забезпечують оптимальне співвідношення ціни та функціональності. Порівняльний аналіз комутаторів рівня доступу представлено в таблиці 2.6.

Для рівня доступу закритої мережі використовуються комутатори Cisco Catalyst 9200-48P (48-портові) та Cisco Catalyst 9200-24P (24-портові). Ці моделі забезпечують 24/48 портів 10/100/1000 Мбіт/с з PoE+ (до 30 Вт на порт), 4 порти 1/10 Гбіт/с SFP/SFP+ для висхідних з'єднань, пропускну здатність до 176 Гбіт/с, продуктивність до 130,9 млн пакетів/с, підтримку до 1024 VLAN та технологію стекування FlexStack-Plus (до 8 комутаторів). Для надійності комутатори налаштовуються з резервуванням висхідних з'єднань, підключаючись до двох різних комутаторів рівня розподілу. Базові функції безпеки включають автентифікацію 802.1X, обмеження MAC-адрес, захист

від атак на DHCP, ARP та IGMP. Розподіл обладнання: корпус А - 6 комутаторів 48Р та 4 комутатори 24Р; корпус Б - 4 комутатори 48Р та 2 комутатори 24Р; корпус В - 3 комутатори 48Р та 2 комутатори 24Р. Для серверної інфраструктури обрано Dell PowerEdge R740, що забезпечують оптимальне поєднання продуктивності, надійності та масштабованості, як показано в таблиці 2.7.

Таблиця 2.6 - Порівняльний аналіз комутаторів для рівня доступу

Характеристика	Cisco Catalyst 9200	Juniper EX3400	HPE Aruba 2930F
Продуктивність комутації	До 176 Гбіт/с	До 320 Гбіт/с	До 176 Гбіт/с
Кількість портів	До 48 портів 1GbE	До 48 портів 1GbE	До 48 портів 1GbE
Uplink-порти	4 x 10GbE SFP+	4 x 10GbE SFP+	4 x 10GbE SFP+
Підтримка PoE/PoE+	Так (до 30 Вт на порт)	Так (до 30 Вт на порт)	Так (до 30 Вт на порт)
Стекування	До 8 пристроїв	До 10 пристроїв	До 8 пристроїв
Підтримка VLAN	1024	4096	4096
Резервні компоненти	Блоки живлення	Блоки живлення	Блоки живлення
Функції безпеки	802.1X, Port Security, DHCP Snooping	802.1X, Port Security, DHCP Snooping	802.1X, Port Security, DHCP Snooping
MTBF (годин)	>160 000	>150 000	>145 000
Вартість експлуатації	Низька	Середня	Низька

Для реалізації закритої мережі розгорнуто комплексну серверну інфраструктуру з основним кластером у головній будівлі (4 потужні сервери Dell PowerEdge R740 для критичних сервісів та 2 сервери R640 для моніторингу) та резервним кластером у корпусі Б (2 сервери R740 та 1 сервер R640), де основні сервери мають високопродуктивну конфігурацію з двома 16-ядерними процесорами Intel Xeon Gold, 384 ГБ оперативної пам'яті, надійною дисковою підсистемою RAID та резервованим електроживленням; при цьому реалізовано технології кластеризації для автоматичного переключення при відмовах, трирівневу систему резервного копіювання (щоденне інкрементне, щотижневе повне та щомісячне архівне) та

віртуалізацію на платформі VMware vSphere для оптимального використання ресурсів.

Таблиця 2.7 - Порівняльний аналіз серверних платформ

Характеристика	Dell PowerEdge R740	HPE ProLiant DL380 Gen10	Lenovo ThinkSystem SR650
Процесори	До 2 x Intel Xeon Scalable (до 28 ядер кожен)	До 2 x Intel Xeon Scalable (до 28 ядер кожен)	До 2 x Intel Xeon Scalable (до 28 ядер кожен)
Оперативна пам'ять	До 3 ТБ DDR4	До 3 ТБ DDR4	До 3 ТБ DDR4
Кількість дискових відсіків	До 24 x 2.5" SAS/SATA/SSD	До 24 x 2.5" SAS/SATA/SSD	До 24 x 2.5" SAS/SATA/SSD
Мережеві інтерфейси	4 x 1GbE (вбудовані) + опціональні	4 x 1GbE (вбудовані) + опціональні	2 x 1GbE (вбудовані) + опціональні
Резервні компоненти	Блоки живлення, вентилятори	Блоки живлення, вентилятори	Блоки живлення, вентилятори
Вбудовані механізми безпеки	TPM 2.0, Secure Boot, System Lockdown	TPM 2.0, Secure Boot, Silicon Root of Trust	TPM 2.0, Secure Boot, Lenovo ThinkShield
Віддалене управління	iDRAC9 Enterprise	HPE iLO 5 Advanced	Lenovo XClarity Controller
MTBF (годин)	>100 000	>100 000	>100 000
Сертифікати безпеки	FIPS 140-2, CC	FIPS 140-2, CC	FIPS 140-2
Енергоефективність	80 PLUS Platinum (до 94%)	80 PLUS Titanium (до 96%)	80 PLUS Platinum (до 94%)

2.4 Розробка кабельної інфраструктури

Кабельна інфраструктура є початком надійної та захищеної мережі, бо визначає фізичні шляхи передачі даних між мережевим обладнанням. Правильно спроектована та монтована кабельна система не лише забезпечує необхідну пропускну здатність, а ще й запобігає несанкціонованому доступу та перехопленню інформації. При розробці кабельної інфраструктури для закритої мережі особлива увага приділяється захисту від електромагнітного випромінювання та фізичній безпеці проводки.

Відповідно до технічного завдання, кабельна інфраструктура повинна забезпечувати надійний зв'язок між трьома будівлями навчального закладу, а також між різними сегментами мережі всередині кожної будівлі. Крім того, система повинна мати резервування для забезпечення безперервності роботи мережі у випадку пошкодження окремих кабельних ліній.

При проектуванні кабельної інфраструктури закритої мережі використано структурований підхід, який відповідає міжнародному стандарту ISO/IEC 11801 (EN 50173). Кабельна система розділена на такі функціональні підсистеми:

- магістральна підсистема, яка забезпечує зв'язок між будівлями та між телекомунікаційними приміщеннями всередині будівель;
- горизонтальна підсистема, яка забезпечує зв'язок міжкомутаційними вузлами та робочими місцями користувачів;
- комутаційна підсистема, яка включає комутаційні панелі, патч-корди та інше обладнання для з'єднання різних сегментів мережі;
- робоча підсистема, яка забезпечує підключення кінцевих пристроїв на робочих місцях користувачів;
- для різних підсистем кабельної інфраструктури обрано оптимальні типи кабелів, які забезпечують необхідний рівень продуктивності та захищеності. Характеристики основних типів кабелів наведені в таблиці 2.8.

Для магістральних ліній між будівлями використовується одномодове оптоволоконне волокно (SMF) типу OS2, яке забезпечує високу пропускну здатність на великі відстані та є повністю захищеним від електромагнітних перешкод. Оптоволоконні кабелі прокладаються в захищених підземних каналах з використанням броньованих кабелів для додаткового механічного захисту. Для забезпечення резервування між кожною парою будівель прокладається два незалежних оптоволоконних кабелі різними фізичними маршрутами.

Таблиця 2.8 - Характеристики основних типів кабелів закритої мережі

Тип кабелю	Пропускна здатність	Максимальна довжина	Рівень захищеності	Сегмент застосування
Одномодове оптоволокно OS2	До 100 Гбіт/с	До 10 км	Дуже високий	Магістральні лінії між будівлями
Багатомодове оптоволокно OM4	До 100 Гбіт/с	До 150 м	Високий	Магістральні лінії всередині будівель
Екранована вита пара Cat.6A (S/FTP)	До 10 Гбіт/с	До 100 м	Високий	Горизонтальна підсистема
Екранована вита пара Cat.6 (F/UTP)	До 1 Гбіт/с	До 100 м	Середній	Робоча підсистема

Всередині будівель для вертикальних магістралей використовується багатомодове оптоволоконне волокно (MMF) типу OM4, яке забезпечує пропускну здатність до 100 Гбіт/с на відстанях до 150 метрів. Ці кабелі з'єднують головний комутаційний вузол будівлі з комутаційними вузлами на різних поверхах. Оптоволоконні кабелі прокладаються в захищених вертикальних кабельних каналах з обмеженим доступом.

Для горизонтальної підсистеми, яка забезпечує підключення комутаторів доступу до комутаторів розподілу, використовується екранована вита пара категорії 6A з подвійним екрануванням (S/FTP). Цей тип кабелю забезпечує швидкість передачі даних до 10 Гбіт/с на відстані до 100 метрів і має високий рівень захисту від електромагнітних перешкод завдяки загальному екрану та індивідуальному екрануванню кожної пари. Кабелі прокладаються в металевих лотках або захищених кабельних каналах з контролем доступу.

Для підключення робочих станцій та інших кінцевих пристроїв використовується екранована вита пара категорії 6 (F/UTP), яка забезпечує швидкість передачі даних до 1 Гбіт/с і має достатній рівень захисту від електромагнітних перешкод для звичайних робочих місць. Для критичних робочих місць (керівництво, служба безпеки) використовується екранована вита пара категорії 6A (S/FTP) для забезпечення додаткового захисту.

Для захисту від несанкціонованого доступу та перехоплення інформації кабельна система має такі механізми захисту:

- прокладка кабелів у захищених металевих лотках або трубах з контролем доступу;
- використання кабелів з подвійним екрануванням для мінімізації електромагнітного випромінювання;
- захист комутаційних шаф і телекомунікаційних приміщень системами контролю доступу та відеоспостереження;
- регулярний візуальний огляд і тестування кабельних трас для виявлення спроб несанкціонованого втручання;
- використання системи моніторингу цілісності оптоволоконних ліній, яка дозволяє виявляти спроби підключення до волокна.

Всередині кожної будівлі кабельна інфраструктура організована за ієрархічним принципом. На кожному поверсі розміщується комутаційна шафа, в якій встановлюються комутатори доступу та комутаційні панелі. Від комутаційної шафи до робочих місць прокладається горизонтальна кабельна підсистема. Схема організації кабельної інфраструктури всередині будівлі представлена на рисунку 2.4.

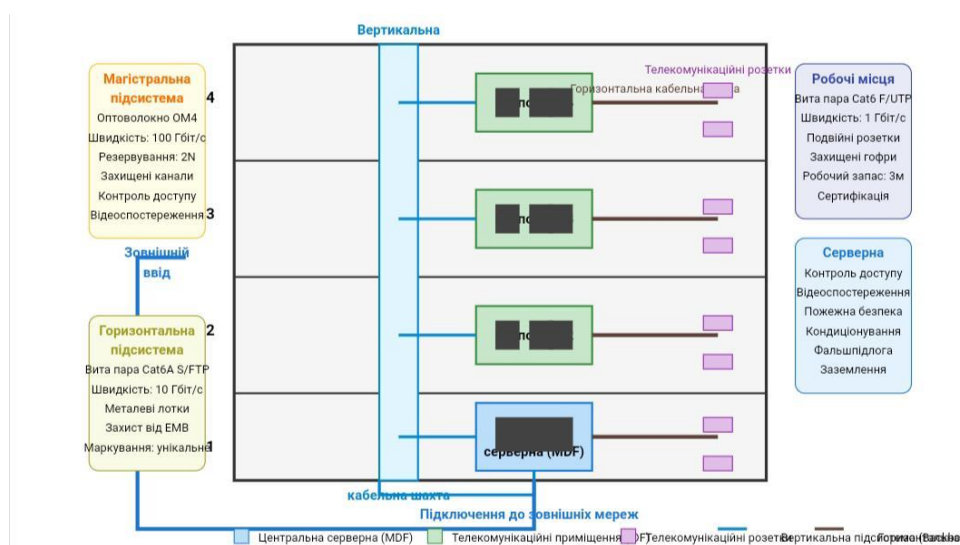


Рисунок 2.4 – Схема організації кабельної інфраструктури всередині будівлі

Для забезпечення належної документації кабельної системи створено у книгу в якій буде знаходитись інформація про всі кабельні з'єднання, їх маркування, розташування та специфікації. Кожен кабель має унікальну приписку, яка дозволить швидко знайти його в документації. Крім того, вся кабельна система зареєстрована в спеціалізованій системі управління кабельною інфраструктурою, яка дозволяє відстежувати зміни та планувати модернізацію.

Для забезпечення належного захисту кабельної інфраструктури від фізичних пошкоджень і несанкціонованого доступу розроблено систему організації кабельних трас, яка включає:

- захищені підземні канали для магістральних ліній між будівлями;
- вертикальні захищені шахти для кабельних трас всередині будівель;
- металеві лотки з кришками для горизонтальних трас;
- захищені гофровані труби для відгалужень до робочих місць.

Таким чином, розроблена кабельна інфраструктура забезпечує надійне та захищене з'єднання всіх компонентів закритої мережі, відповідає вимогам технічного завдання щодо надійності та захищеності, а також має достатній резерв для майбутнього розширення мережі.

2.5 Проектування системи безперебійного живлення

Система безперебійного живлення є критично важливим компонентом закритої мережі, оскільки забезпечує безперервну роботу мережевого обладнання та серверів навіть при збоях у електропостачанні. Відповідно до технічного завдання, закрыта мережа повинна функціонувати цілодобово з мінімальними перервами, а максимально допустимий час простою при відмовах не повинен перевищувати 30 хвилин. Для забезпечення цих вимог розроблено комплексну систему безперебійного живлення, яка включає

джерела безперебійного живлення (ДБЖ), дизель-генераторні установки та системи розподілу електроживлення.

При проєктуванні системи безперебійного живлення враховувалися такі фактори:

- потужність, необхідна для функціонування всього обладнання закритої мережі;
- необхідний час автономної роботи при відключенні зовнішнього електропостачання;
- надійність системи безперебійного живлення;
- захист від перепадів напруги та електромагнітних перешкод;
- можливість розширення системи при збільшенні кількості обладнання.

Для розрахунку необхідної потужності системи безперебійного живлення проведено аналіз енергоспоживання всіх компонентів закритої мережі. Результати аналізу наведені в таблиці 2.9.

На основі проведеного розрахунку для закритої мережі розроблено трирівневу систему безперебійного живлення, що включає джерела безперебійного живлення (ДБЖ) для короткострокового живлення до 30 хвилин, дизель-генераторні установки (ДГУ) для тривалої роботи при відключеннях, та систему розподілу електроживлення. Для критичних компонентів (комутатори ядра, сервери) використовується схема подвійного перетворення (Online ДБЖ) з повною гальванічною розв'язкою, для менш критичних - лінійно-інтерактивні ДБЖ. Система розподілена між трьома будівлями: у головному корпусі А встановлено ДБЖ загальною потужністю 20 кВА для серверів і обладнання ядра, 10 кВА для комутаторів розподілу та доступу, та ДГУ 50 кВА; у корпусі Б - ДБЖ 15 кВА для резервних серверів і мережевого обладнання та ДГУ 30 кВА; у корпусі В - ДБЖ 10 кВА та компактна ДГУ 20 кВА. Загальна схема системи для головного корпусу А представлена на рисунку 2.5

Таблиця 2.9 - Розрахунок енергоспоживання обладнання закритої мережі

Тип обладнання	Кількість, шт.	Потужність, Вт	Загальна потужність, Вт	Коефіцієнт запасу	Розрахункова потужність, Вт
Комутатори ядра	2	1100	2200	1,3	2860
Комутатори розподілу	6	715	4290	1,3	5577
Комутатори доступу (48 портів)	13	440	5720	1,3	7436
Комутатори доступу (24 порти)	8	250	2000	1,3	2600
Міжмережеві екрани	4	350	1400	1,3	1820
Сервери (основні)	6	750	4500	1,3	5850
Сервери (резервні)	3	750	2250	1,3	2925
Системи зберігання даних	2	800	1600	1,3	2080
Системи моніторингу та безпеки	1	500	500	1,3	650
Загальна потужність		24460			31798

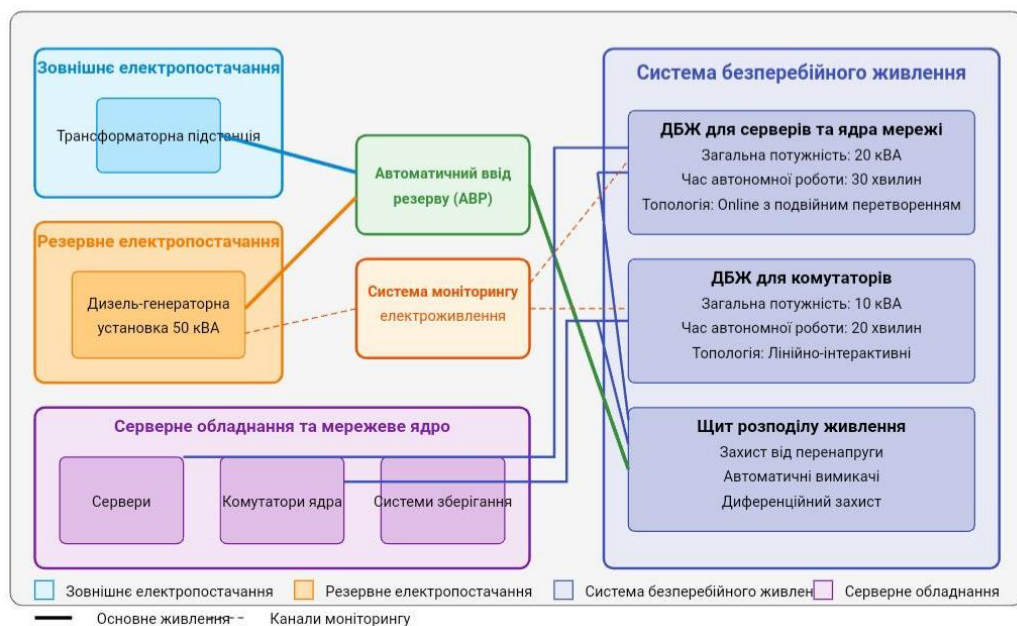


Рисунок 2.5 – Схема системи безперебійного живлення для головної будівлі

Для забезпечення додаткового рівня надійності критично важливе обладнання (сервери, комутатори ядра) підключається через автоматичні

пристрої комутації (ATS - Automatic Transfer Switch), які у випадку відмови одного джерела живлення автоматично переключаються на резервне джерело. Крім того, все активне мережеве обладнання обладнане двома блоками живлення, які підключаються до різних систем електропостачання.

Для захисту від електромагнітних перешкод та забезпечення гальванічної розв'язки між різними сегментами мережі використовуються розділювальні трансформатори та спеціалізовані фільтри. Це дозволяє знизити вірогідність появи ризику поширення електромагнітних перешкод через кабелі живлення та запобігти витоку інформації через лінії електропостачання.

Для моніторингу стану системи безперебійного живлення розгорнуто спеціалізовану систему управління електроживленням, яка забезпечує:

- постійний моніторинг параметрів електроживлення (напруга, струм, частота);
- контроль стану ДБЖ (заряд батарей, навантаження, температура);
- моніторинг роботи дизель-генераторних установок;
- автоматичне сповіщення адміністраторів про проблеми з електроживленням;
- збір статистики для аналізу та оптимізації системи.

Схема розподілу електроживлення для серверного приміщення, де розміщується критично важливе обладнання, представлена на рисунку 2.6.

Для забезпечення належного електроживлення робочих станцій користувачів використовуються компактні ДБЖ з функцією автоматичного коректного завершення роботи при тривалому відключенні електроенергії. Це дозволяє запобігти втраті даних та пошкодженню обладнання при раптових відключеннях електроенергії.

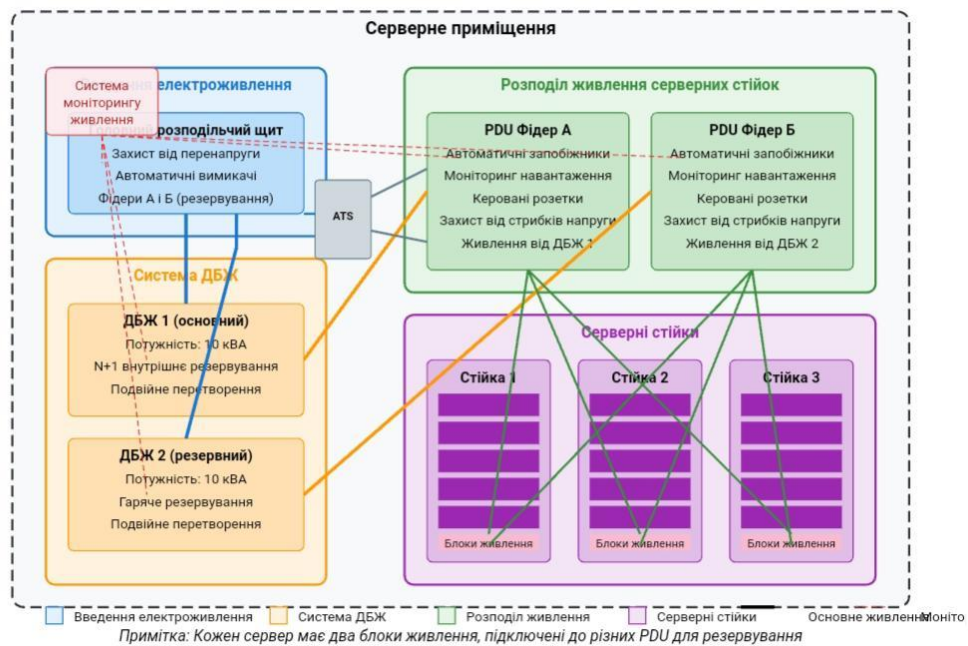


Рисунок 2.6 – Схема розподілу електроживлення в серверному приміщенні

Система безперебійного живлення спроектована з урахуванням можливості розширення при збільшенні кількості обладнання. Для цього передбачено резерв потужності близько 30% на всіх рівнях системи, а також можливість встановлення додаткових модулів ДБЖ без переривання роботи існуючої системи.

Регламентне обслуговування системи безперебійного живлення включає:

- щотижневе тестування ДБЖ з перевіркою працездатності батарей;
- щомісячне тестове запускання дизель-генераторних установок;
- щоквартальну перевірку систем розподілу електроживлення;
- щорічну заміну витратних матеріалів та профілактичне обслуговування всіх компонентів системи.

Завдяки комплексному підходу до проєктування системи безперебійного живлення забезпечується висока надійність функціонування закритої мережі навіть при тривалих перервах у зовнішньому електропостачанні. Розрахунковий час автономної роботи критичних компонентів мережі становить не менше 8 годин при роботі від ДБЖ та

дизель-генераторних установок, що повністю відповідає вимогам технічного завдання.

2.6 Налаштування мережевих протоколів для забезпечення надійності

Налаштування мережевих протоколів є фундаментальною частиною створення закритої мережі з підвищеною надійністю та захищеністю. Правильно налаштовані протоколи забезпечують стабільну роботу мережі, швидке відновлення у випадку відмов обладнання або каналів зв'язку, а також запобігають несанкціонованому доступу до інформації. У цьому підрозділі розглянуто підходи до налаштування основних мережевих протоколів, що використовуються в проєктованій закритій мережі.

Для забезпечення надійної маршрутизації пакетів між різними сегментами мережі вибрано протокол динамічної маршрутизації OSPF (Open Shortest Path First). Цей протокол має низку переваг, що роблять його оптимальним вибором для закритої мережі:

- швидка конвергенція - OSPF швидко реагує на зміни в топології мережі, перераховуючи маршрути;
- підтримка безкласової адресації (CIDR) та маршрутизації змінної довжини маски (VLSM);
- висока масштабованість завдяки поділу мережі на зони (areas);
- ефективне використання пропускної здатності мережі;
- підтримка автентифікації повідомлень для підвищення безпеки.

Для покращення роботи OSPF та підвищення рівня безпеки прийнято такі рішення:

- вся мережа розділена на три OSPF-зони: Зона 0 (backbone area) - включає комутатори ядра та маршрутизатори рівня розподілу в головній

будівлі; Зона 1 - включає маршрутизатори та комутатори в корпусі Б; Зона 2 - включає маршрутизатори та комутатори в корпусі В.;

- налаштована автентифікація повідомлень OSPF з використанням MD5-хешування для запобігання підробці маршрутної інформації;

- впроваджена сумаризація маршрутів на межах зон для зменшення розміру таблиць маршрутизації та прискорення конвергенції мережі;

- застосовані фільтри маршрутів для обмеження поширення службової інформації між зонами.

Налаштування OSPF на маршрутизаторах рівня розподілу виконано з такими параметрами:

Лістинг 3.1 – Налаштування OSPF

```
router ospf 1
router-id 10.1.0.1
area 0 authentication message-digest
network 10.1.10.0 0.0.0.255 area 0
network 10.1.20.0 0.0.0.255 area 0
network 10.1.50.0 0.0.0.255 area 0
passive-interface default
no passive-interface GigabitEthernet0/1
no passive-interface GigabitEthernet0/2
default-information originate always
```

Для забезпечення максимальної надійності закритої мережі, окрім протоколу OSPF, налаштовано статичні резервні маршрути для критичних сегментів, що активуються при відмовах динамічної маршрутизації. Реалізовано комплексні механізми резервування ключових мережевих пристроїв з використанням трьох протоколів: HSRP (Hot Standby Router Protocol), який дозволяє групі маршрутизаторів або комутаторів 3-го рівня забезпечувати високу доступність через віртуальний шлюз з єдиною IP-адресою; стандартизований VRRP (Virtual Router Redundancy Protocol) для відмовостійкості в гетерогенному середовищі; та Cisco StackWise Virtual для об'єднання двох фізичних комутаторів у єдине логічне ціле зі спільною контрольною площиною. На комутаторах рівня розподілу налаштовано HSRP

для всіх VLAN з різними пріоритетами для забезпечення балансування навантаження, що продемонстровано на прикладі конфігурації для VLAN 10.

Лістинг 3.2 - конфігурації VLAN 10

```
interface Vlan10
ip address 10.1.10.2 255.255.255.0
standby 10 ip 10.1.10.1
standby 10 priority 110
standby 10 preempt
standby 10 authentication md5 key-string SecureKey10
```

Для VLAN 20 налаштування виконано з іншими пріоритетами, щоб первинним шлюзом був інший комутатор, таким чином забезпечується балансування навантаження:

Лістинг 3.3 - конфігурації VLAN 20

```
interface Vlan20
ip address 10.1.20.2 255.255.255.0
standby 20 ip 10.1.20.1
standby 20 priority 90
standby 20 preempt
standby 20 authentication md5 key-string SecureKey20
```

На комутаторах ядра мережі впроваджено технологію Cisco StackWise Virtual для об'єднання двох фізичних комутаторів у єдине логічне ціле, що забезпечує уникнення проблем з протоколом STP, можливість агрегації портів між пристроями (MultiChassis EtherChannel) та швидке відновлення при відмові одного з комутаторів без переривання трафіку. Для підвищення пропускної здатності та надійності з'єднань між рівнями мережі використано технологію агрегації каналів EtherChannel, яка дозволяє об'єднати кілька фізичних портів в один логічний канал для збільшення пропускної здатності, забезпечення відмовостійкості та балансування навантаження. В мережі налаштовано три типи EtherChannel з'єднань: 4-портові канали (40 Гбіт/с) між ядром та розподілом, 2-портові канали (20 Гбіт/с) між розподілом та доступом, та 2-портові канали (20 Гбіт/с) між комутаторами ядра, з

використанням протоколу LACP для динамічного формування та контролю стану каналів.

Типове налаштування порту для участі в EtherChannel з використанням LACP:

Лістинг 3.4 - налаштування порту EtherChannel з використанням LACP

```
interface GigabitEthernet1/0/1
description "Uplink to Distribution Switch"
channel-group 1 mode active
spanning-tree portfast trunk
```

Для підвищення надійності фізичні порти, що входять до одного EtherChannel, підключено до різних лінійних карт або модулів комутаторів, що дозволяє зберегти працездатність каналу навіть при відмові одного з модулів.

Для запобігання утворенню петель в мережі, що може призвести до лавиноподібного розсилання широкомовних повідомлень та перевантаження мережі, використано протокол Rapid Per-VLAN Spanning Tree Plus (Rapid PVST+). Цей протокол є розширенням стандартного Spanning Tree Protocol (STP) і має такі переваги:

- прискорена конвергенція (до 3-5 секунд у порівнянні з 30-50 секунд у звичайного STP);
- окреме дерево STP для кожної VLAN, що дозволяє оптимізувати маршрути для різних VLAN;
- підтримка функцій PortFast, UplinkFast та BackboneFast для прискорення конвергенції.

Для підвищення стабільності роботи Spanning Tree Protocol налаштовано такі додаткові функції:

- Root Guard - захищає заданий кореневий міст від спроб інших комутаторів стати кореневими;

- BPDU Guard - блокує порти, які отримують BPDU-повідомлення, на портах з включеним PortFast;
- Loop Guard - запобігає утворенню петель при односторонніх збоях ліній;
- UDLD (UniDirectional Link Detection) - виявляє і блокує односпрямовані лінії зв'язку.

На комутаторах ядра мережі виконано такі налаштування Spanning Tree:

Лістинг 3.5 – налаштування Spanning Tree на комутаторах ядра

```
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree vlan 10,20,30,40,50 priority 4096
spanning-tree vlan 60,70,80,90 priority 8192
```

На комутаторах рівня розподілу першого корпусу:

```
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree vlan 60,70,80,90 priority 4096
spanning-tree vlan 10,20,30,40,50 priority 8192
```

Таке налаштування забезпечує балансування навантаження між комутаторами ядра та розподілу, оскільки різні VLAN використовують різні шляхи передачі трафіку.

Для комутаторів рівня доступу, до яких підключаються кінцеві користувачі, налаштовано додаткові функції безпеки:

Лістинг 3.5- додаткові функції безпеки для комутаторів рівня доступу

```
interface range GigabitEthernet1/0/1 - 48
spanning-tree portfast
spanning-tree bpduguard enable
```

Це дозволяє кінцевим пристроям швидше отримувати доступ до мережі та захищає від спроб підключення несанкціонованих комутаторів до мережі.

Таблиця 2.10 - Порівняння протоколів Spanning Tree для закритих мереж

Характеристика	STP (802.1D)	RSTP (802.1w)	MST (802.1s)	Rapid PVST+
Час конвергенції	30-50 секунд	3-5 секунд	3-5 секунд	3-5 секунд
Окреме дерево для кожної VLAN	Ні	Ні	Ні (групи VLAN)	Так
Витрати ресурсів процесора	Низькі	Середні	Низькі	Високі
Підтримка балансування навантаження	Обмежена	Обмежена	Висока	Висока
Складність налаштування	Низька	Низька	Висока	Середня
Оптимальність для закритих мереж	Низька	Середня	Висока	Дуже висока

Для забезпечення надійності в закритій мережі обрано протокол Rapid PVST+, який, згідно з таблицею 2.10, забезпечує оптимальне поєднання швидкості конвергенції, гнучкості налаштування та можливостей балансування навантаження. Для пріоритезації та забезпечення якості обслуговування критичних сервісів впроваджено механізми QoS на основі моделі диференційованого обслуговування (DiffServ) з маркуванням пакетів відповідно до класів обслуговування. Визначено п'ять класів трафіку з відповідними пріоритетами: критичний контрольний трафік (найвищий) для протоколів маршрутизації та резервування; трафік реального часу (високий) для VoIP та відеоконференцій; трафік критичних додатків (середній) для баз даних та документообігу; стандартний трафік (нормальний) для веб, пошти та передачі файлів; фоновий трафік (низький) для оновлень та резервного копіювання. Для кожного класу налаштовано політики з виділенням гарантованої смуги пропускання, обмеженням максимальної смуги та параметрами обробки черг, що забезпечує високу надійність та безперервність роботи критичних сервісів навіть при відмовах окремих компонентів.

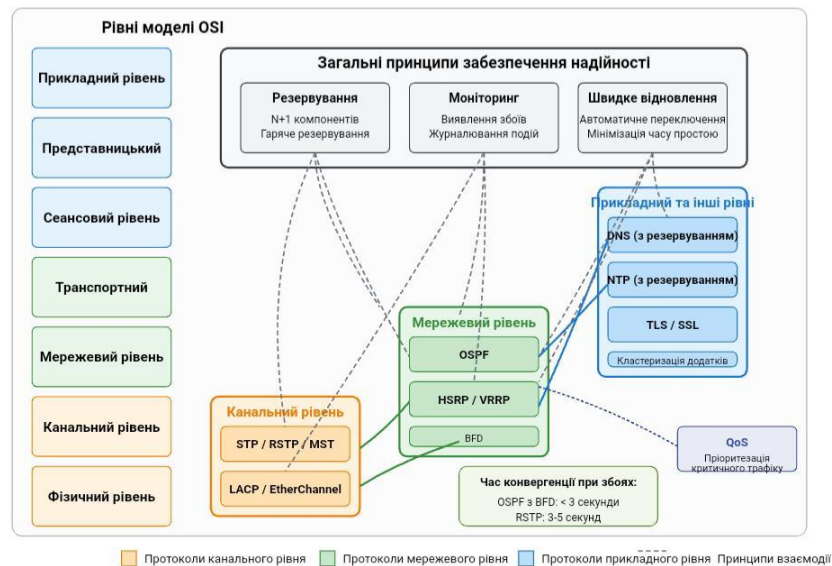


Рисунок 2.7 – Схема взаємодії мережевих протоколів для забезпечення надійності

2.7 Впровадження системи моніторингу мережі

Моніторингова система є ключовим елементом закритої мережі. Вона забезпечує постійний контроль за станом обладнання мережі, серверів і каналів зв'язку. Ефективна моніторингова система дозволяє вчасно виявляти проблеми та потенційні загрози. Це дозволяє оперативно реагувати на інциденти та забезпечує збір статистичних даних для аналізу продуктивності мережевого середовища та планування її розвитку.

Відповідно до вимог технічного завдання, система моніторингу повинна забезпечувати цілодобовий контроль за станом критичних компонентів мережі, своєчасне сповіщення адміністраторів про виникнення проблем та можливість швидкої діагностики причин інцидентів.

Для забезпечення високої надійності та захищеності система моніторингу мережі реалізована за дворівневою архітектурою з резервуванням ключових компонентів:

— центральний рівень - включає основний та резервний сервери моніторингу, розташовані в різних будівлях (корпус А та корпус Б), а також сервер збору та аналізу журналів подій (Syslog);

— рівень збору даних - включає агенти моніторингу на мережевому обладнанні та серверах, а також спеціалізовані зонди для збору даних про мережевий трафік.

Основою системи моніторингу обрано платформу Zabbix - потужну систему з відкритим кодом, яка забезпечує широкі можливості моніторингу, візуалізації даних та оповіщення. Доповненням до Zabbix є спеціалізована система для збору та аналізу журналів подій (Graylog), а також система NetFlow для аналізу мережевого трафіку.

Архітектура системи моніторингу представлена на рисунку 2.8.

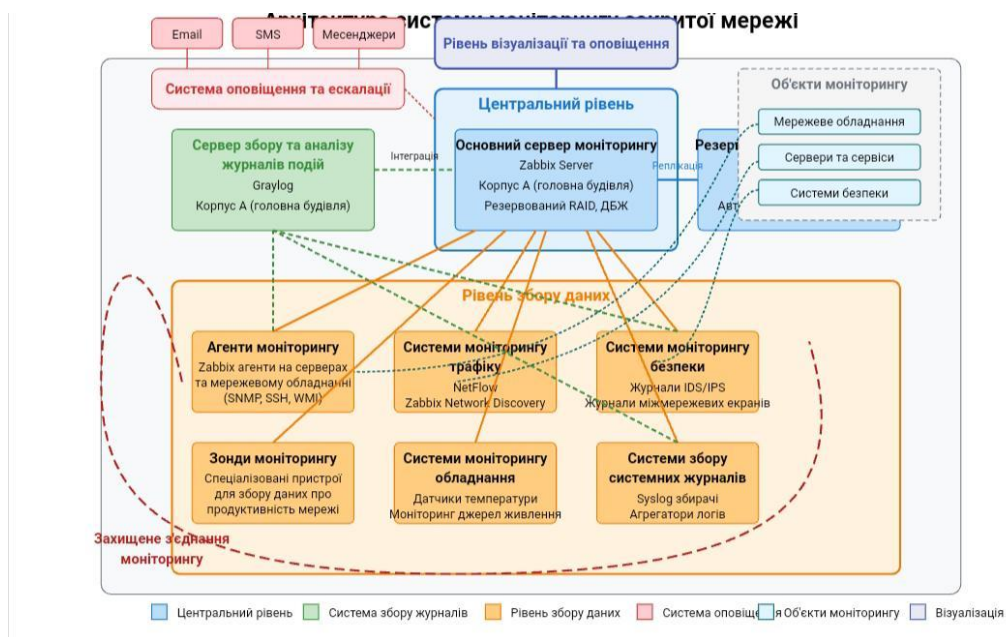


Рисунок 2.8 – Архітектура системи моніторингу закритої мережі

Компоненти системи моніторингу взаємодіють між собою за допомогою захищених протоколів, а доступ до системи моніторингу строго контролюється з використанням механізмів автентифікації та авторизації.

Розроблена система моніторингу забезпечує виконання таких функцій:

- моніторинг доступності - контроль доступності мережевого обладнання, серверів та сервісів з використанням різних протоколів (ICMP, SNMP, HTTP, HTTPS, SSH);

- моніторинг продуктивності - збір та аналіз даних про завантаженість процесорів, використання пам'яті, дискового простору, пропускну здатності мережевих інтерфейсів;

- моніторинг помилок - виявлення та аналіз помилок на мережевих інтерфейсах, нестабільності каналів зв'язку, проблем з STP;

- аналіз мережевого трафіку - збір та аналіз даних про обсяги та характеристики мережевого трафіку з використанням технології NetFlow;

- збір та аналіз журналів подій - централізований збір журналів подій з мережевого обладнання, серверів та сервісів, їх аналіз та кореляція для виявлення інцидентів;

- система оповіщення - автоматичне сповіщення адміністраторів про виникнення проблем через різні канали (електронна пошта, SMS, месенджери);

- візуалізація даних - наочне представлення зібраних даних у вигляді графіків, карт мережі, панелей моніторингу для різних категорій користувачів;

- звітність - генерація регулярних звітів про стан мережі, продуктивність, інциденти та тенденції зміни ключових параметрів.

Для різних типів мережевого обладнання визначено набори параметрів, які підлягають постійному моніторингу. У таблиці 2.11 наведено основні параметри моніторингу для різних категорій обладнання.

Система моніторингу закритої мережі налаштована з різними інтервалами опитування залежно від важливості параметрів: критичні (доступність, CPU) - 30-60 секунд; важливі (пам'ять, стан інтерфейсів) - 1-3 хвилини; стандартні (дисковий простір) - 5-15 хвилин; статистичні (обсяги трафіку) - 30-60 хвилин. Впроваджено багаторівневу систему оповіщення з трьома пороговими значеннями для кожного параметра: попередження

(Warning), критичний (Critical) та аварійний (Disaster). Система ескалації інцидентів передбачає поетапне залучення спеціалістів різного рівня: від чергового адміністратора до керівництва організації та екстрених служб. Для захисту самої системи моніторингу реалізовано шість механізмів: ізоляція в окремому сегменті мережі (VLAN 60), шифрування даних (TLS/SSL), багатофакторна автентифікація з детальною системою ролей, аудит дій адміністраторів, безпечне зберігання критичної інформації та регулярне резервне копіювання. Додатково впроваджено механізми взаємного контролю між основним та резервним серверами моніторингу.

Таблиця 2.11 - Параметри моніторингу для різних типів мережевого обладнання

Тип обладнання	Параметри доступності	Параметри продуктивності	Параметри помилок	Специфічні параметри
Комутатори рівня ядра	ICMP ping, SNMP, SSH	Завантаження CPU, пам'яті, інтерфейсів, таблиці MAC-адрес	Помилки на інтерфейсах, стан STP	Стан HSRP, EtherChannel, OSPF
Комутатори рівня розподілу	ICMP ping, SNMP, SSH	Завантаження CPU, пам'яті, інтерфейсів, таблиці MAC-адрес	Помилки на інтерфейсах, стан STP	Стан HSRP, EtherChannel, ACL
Комутатори рівня доступу	ICMP ping, SNMP	Завантаження CPU, пам'яті, інтерфейсів	Помилки на інтерфейсах, статус PoE	Стан портів, підключені MAC-адреси
Міжмережеві екрани	ICMP ping, SNMP, SSH	Завантаження CPU, пам'яті, кількість з'єднань	Відкинуті пакети, проблеми з VPN	Активні сесії, правила фільтрації
Сервери	ICMP ping, SNMP, агент	Завантаження CPU, пам'яті, дисків, мережевих інтерфейсів	Помилки на дисках, мережевих інтерфейсах	Стан сервісів, температура компонентів
Системи зберігання даних	ICMP ping, SNMP, агент	Завантаження CPU, використання дискового простору	Помилки на дисках, RAID-масивах	Продуктивність дисків, стан RAID
Системи безперебійного живлення	ICMP ping, SNMP	Навантаження, температура, заряд батарей	Проблеми з мережею живлення	Розрахунковий час роботи від батарей

2.8 Розробка та впровадження системи захисту інформації, документування розробленої мережі

На основі аналізу безпеки для закритої мережі визначено чотири основні категорії загроз:

— зовнішні загрози: спроби несанкціонованого доступу ззовні, фізичне проникнення до приміщень з обладнанням та перехоплення даних через електромагнітне випромінювання;

— внутрішні загрози: несанкціонований доступ авторизованих користувачів до ресурсів, навмисні або ненавмисні дії персоналу, що призводять до витоку інформації, та зловживання привілеями адміністраторами;

— технічні загрози: збої обладнання та програмного забезпечення, відмови систем електроживлення і кондиціонування, та помилки в конфігурації мережевого обладнання;

— природні загрози: пожежі, затоплення, стихійні лиха та екстремальні погодні умови.

Для кожної категорії загроз проведено оцінку ризиків з урахуванням ймовірності реалізації загрози та потенційного збитку, результати якої представлено в таблиці 2.12.

На основі проведеного аналізу ризиків розроблено комплексну систему захисту інформації, яка включає організаційні, технічні та програмні заходи захисту.

Організаційні заходи захисту інформації включають розробку та впровадження політик безпеки, організацію фізичного захисту об'єктів інформаційної інфраструктури, навчання персоналу з питань інформаційної безпеки та регламентування процесів експлуатації мережі.

Розроблено та впроваджено такі основні політики та регламенти:

- загальна політика інформаційної безпеки - визначає принципи, цілі та завдання забезпечення інформаційної безпеки в організації, а також розподіл відповідальності та повноважень;

- політика контролю доступу - регламентує процеси надання, зміни та скасування прав доступу до інформаційних ресурсів, а також правила використання паролів та засобів автентифікації;

- політика використання мережевих ресурсів - встановлює правила використання мережевих ресурсів користувачами, обмеження щодо встановлення програмного забезпечення та підключення пристроїв;

- регламент реагування на інциденти інформаційної безпеки – визначає порядок дій при виявленні інцидентів безпеки, процедури їх розслідування та ліквідації наслідків;

- регламент резервного копіювання та відновлення даних – встановлює порядок, періодичність та процедури створення резервних копій інформації, а також порядок її відновлення;

- положення про захист персональних даних - регламентує порядок обробки та захисту персональних даних відповідно до вимог законодавства.

Для забезпечення фізичного захисту об'єктів інформаційної інфраструктури впроваджено такі заходи:

- організація контрольованих зон з різними рівнями доступу;
- встановлення систем контролю та управління доступом (СКУД);
- встановлення систем відеоспостереження в критичних зонах;
- обладнання приміщень серверних та комутаційних системами пожежогасіння;

- забезпечення температурного режиму та контролю вологості.

Важливим аспектом організаційних заходів є навчання користувачів та адміністраторів з питань інформаційної безпеки. Розроблено та проводяться такі навчальні програми:

- базовий курс з інформаційної безпеки для всіх користувачів;
- спеціалізований курс для адміністраторів мережі;
- тренінги з реагування на інциденти безпеки;
- регулярні навчання з практичного виявлення фішингових атак

Таблиця 2.12 - Оцінка ризиків для закритої мережі

Загроза	Ймовірність (1-5)	Потенційний збиток (1-5)	Рівень ризику (ЙхЗ)	Заходи захисту
Несанкціонований доступ ззовні	2	5	10 (високий)	Фізична ізоляція, міжмережеві екрани, IDS/IPS
Внутрішні зловмисники	3	5	15 (критичний)	Сегментація, контроль доступу, DLP-системи
Збої обладнання	3	4	12 (високий)	Резервування, моніторинг, регламентне обслуговування
Перебої електроживлення	4	4	16 (критичний)	ДБЖ, дизель-генератори, резервні лінії живлення
Помилки конфігурації	3	4	12 (високий)	Документування, аудит змін, резервне копіювання конфігурацій
Перехоплення ЕМВ	2	5	10 (високий)	Екранування, використання оптоволокна, TEMPEST-захист
Пожежа	2	5	10 (високий)	Системи пожежогасіння, датчики, плани евакуації
Компрометація облікових записів	3	5	15 (критичний)	Багатофакторна автентифікація, політики паролів

Документування є важливим аспектом розробки та експлуатації закритої мережі, який забезпечує збереження знань про мережу, спрощує її обслуговування та модернізацію, а також є необхідною умовою для проходження аудитів безпеки та відповідності вимогам регуляторів.

Таким чином, розроблена та впроваджена система захисту інформації забезпечує комплексний захист закритої мережі від різноманітних загроз, а детальне документування мережі дозволяє ефективно керувати її інфраструктурою та підтримувати високий рівень безпеки протягом всього життєвого циклу.

3 ТЕСТУВАННЯ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ З ЕКСПЛУАТАЦІЇ ЗАКРИТОЇ МЕРЕЖІ

3.1 Методика тестування надійності мережі

Методика тестування надійності закритої мережі охоплює п'ять ключових напрямів: стійкість до відмов обладнання, каналів зв'язку та електроживлення, а також тестування продуктивності, пропускну здатності, масштабованості та гнучкості. Тестування проводилось у контрольованому середовищі в години мінімального навантаження для зменшення впливу на користувачів. Процедура включала чотири основні кроки: вимірювання базових параметрів, імітацію відмови компонента шляхом його вимкнення, вимірювання часу відновлення після переключення на резервні компоненти та оцінку параметрів після повернення до нормального режиму. Під час випробувань імітувались відмови різних елементів мережі: комутаторів на всіх рівнях ієрархії (ядро, розподіл, доступ), основного міжмережевого екрана та серверів у кластері. Результати тестування стійкості до відмов обладнання представлені в таблиці 3.1.

Як видно з таблиці 3.1, час відновлення роботи мережі при відмовах ключових компонентів не перевищує 10 секунд, що відповідає вимогам технічного завдання щодо безперервності функціонування мережі. Єдиним винятком є відмова комутатора доступу, яка призводить до недоступності підключених до нього пристроїв. Для вирішення цієї проблеми

рекомендовано реалізувати дублювання підключень критично важливих робочих станцій до різних комутаторів доступу.

Таблиця 3.1 - Результати тестування стійкості до відмов обладнання

Сценарій відмови	Час виявлення відмови, с	Час відновлення роботи, с	Вплив на користувачів	Відповідність вимогам
Відмова комутатора ядра	2	5	Короткочасна затримка передачі даних	Відповідає
Відмова комутатора розподілу	3	7	Короткочасна недоступність частини сервісів	Відповідає
Відмова комутатора доступу	5	0	Недоступність підключених до нього пристроїв	Частково відповідає
Відмова міжмережевого екрана	2	4	Короткочасна затримка передачі даних	Відповідає
Відмова сервера в кластері	3	8	Незначне зниження продуктивності сервісів	Відповідає

Для оцінки надійності закритої мережі було проведено серію тестів з перевірки відмовостійкості та продуктивності. При тестуванні каналів зв'язку імітувались різні сценарії відмов: розрив окремих та всіх оптоволоконних каналів між будівлями, відмова одного або всіх каналів між рівнями мережі. Оцінювались часові параметри (виявлення відмови, перемаршрутизація) та вплив на пропускну здатність. Результати показали швидке перенаправлення трафіку при відмовах - час конвергенції OSPF не перевищував 5 секунд. Для підвищення відмовостійкості додатково оптимізовано інтервали Hello-пакетів OSPF, налаштовано протокол BFD та оптимізовано таймери STP.

Тестування системи безперебійного живлення включало:

- повного відключення електропостачання;
- відмови ДБЖ;
- тривале відключення з активацією ДГУ та перехід на резервну лінію.

Результати продемонстрували високу надійність: переключення на ДБЖ відбувалось без переривання роботи обладнання, а запуск дизель-генератора займав менше 1 хвилини. Виявлено потребу оптимізації процедури коректного завершення некритичних сервісів при тривалих відключеннях.

Тестування продуктивності з різними типами трафіку (UDP, TCP, HTTP, FTP, СУБД, мультимедіа) показало, що мережева інфраструктура забезпечує достатню пропускну здатність та низькі затримки, перевищуючи вимоги технічного завдання на 30-40%, що створює запас для майбутнього розширення.

Найбільш значущі результати тестування продуктивності представлені на рисунку 3.1.

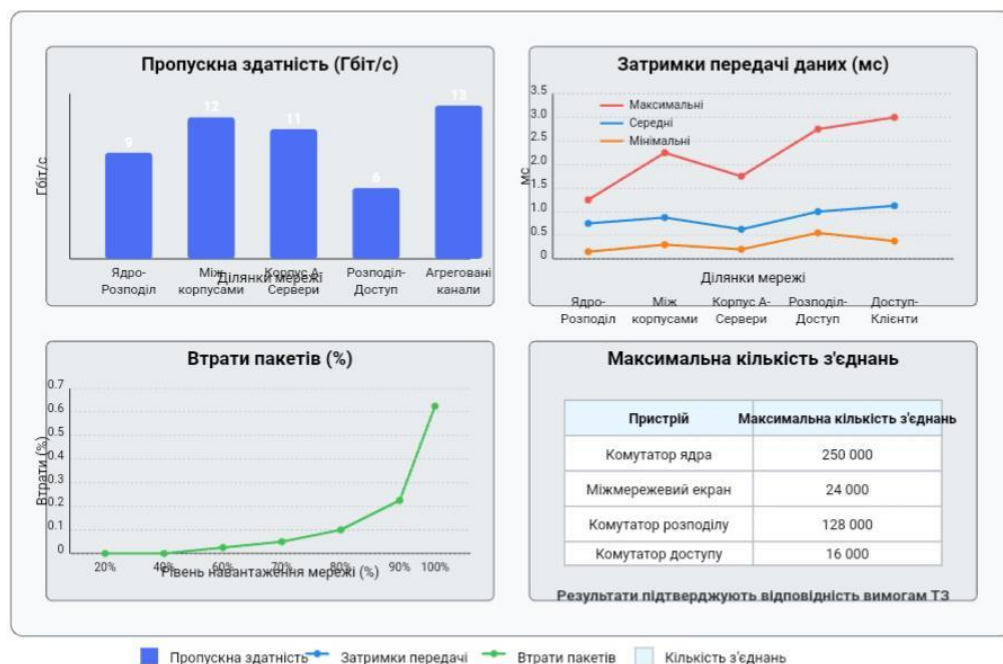


Рисунок 3.1 – Результати тестування продуктивності мережі

3.2 Тестування захищеності мережі від зовнішніх та внутрішніх загроз

Комплексне тестування захищеності закритої мережі проводилось відповідно до міжнародних стандартів та методологій (OSSTMM, NIST SP 800-115, PTES) і охоплювало п'ять ключових напрямів: оцінку захищеності периметра мережі, тестування внутрішньої інфраструктури, перевірку механізмів автентифікації та авторизації, оцінку захищеності від соціальної інженерії та тестування стійкості до DoS-атак. Для оцінки периметра використовувались інструменти Nmap, Nessus, Metasploit Framework та Wireshark, які підтвердили високий рівень захисту - не виявлено відкритих портів чи вразливих сервісів. При тестуванні внутрішньої інфраструктури з позицій зломисників різних рівнів доступу виявлено три вразливості: недостатня фільтрація трафіку між підмережами, можливість отримання підвищених привілеїв через застаріле ПЗ та недостатній контроль привілейованих облікових записів, що було усунуто відповідними заходами. Тестування автентифікації та авторизації підтвердило ефективність впроваджених механізмів, особливо багатофакторної автентифікації. Результати комплексної оцінки відповідності вимогам представлені в таблиці 3.2.

За результатами оцінки загальний рівень захищеності мережі визначено як високий, що відповідає вимогам технічного завдання. Виявлені вразливості усунуто шляхом впровадження додаткових заходів захисту та оптимізації існуючих механізмів.

Таблиця 3.2 - Оцінка відповідності системи захисту вимогам

Компонент системи захисту	Рівень захищеності (1-5)	Виявлені вразливості	Відповідність вимогам
Захист периметра мережі	5	Не виявлено	Повністю відповідає
Захист внутрішньої інфраструктури	4	Недостатня фільтрація між підмережами	Відповідає після усунення
Механізми автентифікації	5	Не виявлено	Повністю відповідає
Механізми авторизації	4	Недостатній контроль привілейованих акаунтів	Відповідає після усунення
Захист від соціальної інженерії	3	Недостатня обізнаність користувачів	Частково відповідає
Захист від DoS-атак	5	Не виявлено	Повністю відповідає
Криптографічний захист	5	Не виявлено	Повністю відповідає
Фізичний захист	4	Недостатнє резервування СКУД	Відповідає після усунення

3.3 Аналіз результатів тестування та виявлення вразливостей

На основі комплексного тестування надійності та захищеності закритої мережі проведено аналіз отриманих результатів, виявлено потенційні вразливості та розроблено рекомендації щодо їх усунення.

Тестування надійності мережі дозволило виявити ряд потенційних проблем, які могли б призвести до порушення безперервності функціонування мережі:

- при відмові комутатора доступу підключені до нього пристрої втрачають зв'язок з мережею;
- час конвергенції протоколу OSPF при відмові магістрального каналу перевищував цільові показники;
- при тривалому відключенні електроживлення ємності батарей ДБЖ недостатньо для підтримки роботи всього обладнання до запуску дизель-генератора.

Рішення цих проблем:

- для критично важливих робочих станцій реалізовано подвійне підключення до різних комутаторів доступу з використанням технології NIC Teaming на рівні операційної системи;
- оптимізація налаштування протоколу OSPF (зменшено інтервали відправки Hello-пакетів, налаштовано пріоритети маршрутів) та впроваджено протокол BFD для швидкого виявлення відмов каналів;
- розробка та впровадження системи автоматичного відключення некритичних споживачів при переході на живлення від ДБЖ.

Загалом результати тестування надійності підтвердили відповідність розробленої мережі вимогам технічного завдання щодо безперервності функціонування та стійкості до відмов.

Тестування захищеності дозволило виявити та усунути ряд потенційних вразливостей у системі захисту інформації:

Недостатня фільтрація трафіку між окремими підмережами однієї VLAN, що дозволяє потенційному зловмиснику здійснювати бічний рух у мережі. Рішення: Впроваджено додаткову сегментацію з використанням технології Private VLAN та розширені списки контролю доступу для фільтрації трафіку між під мережами;

Вразивостями були:

- застаріле програмне забезпечення на окремих робочих станціях, що містить відомі вразливості;
- недостатній контроль за привілейованими обліковими записами, що може призвести до їх несанкціонованого використання;
- недостатня обізнаність користувачів з питань інформаційної безпеки, що підвищує ризик успішних атак соціальної інженерії.

Вирішенням цих вразливостей стали:

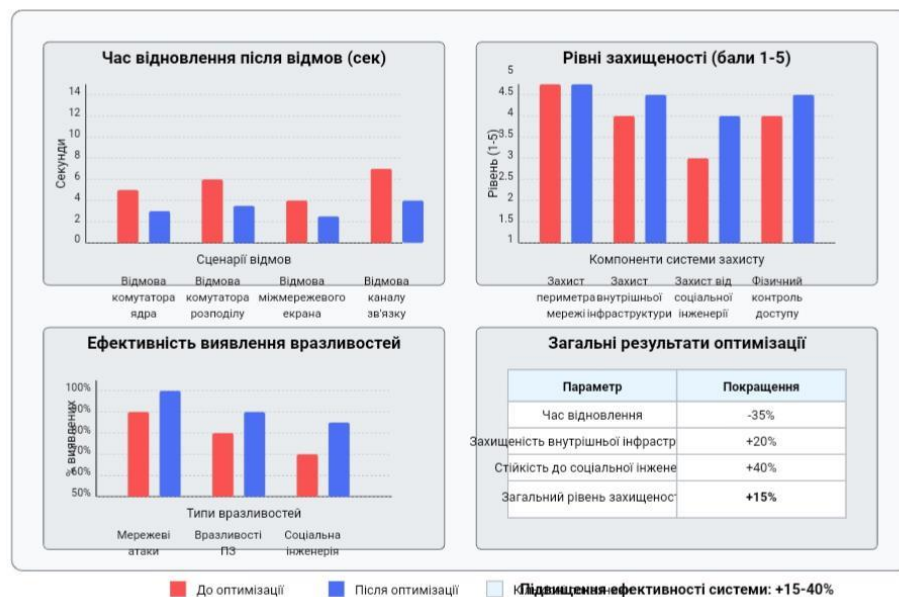
- оновлено програмне забезпечення на всіх робочих станціях та впроваджено систему автоматичного оновлення та контролю версій ПЗ;

— впроваджено систему управління привілейованими обліковими записами (РАМ) з функціями контролю доступу, аудиту дій та автоматичної зміни паролів;

— розроблено та проведено комплексну програму навчання користувачів з питань інформаційної безпеки, включаючи практичні тренінги з розпізнавання фішингу.

Для оцінки ефективності реалізованих рішень з підвищення надійності та захищеності мережі проведено повторне тестування після впровадження всіх рекомендацій. Результати порівняльного аналізу представлені на рисунку 3.2. Як видно з рисунка 3.2, впровадження рекомендацій дозволило суттєво підвищити показники надійності та захищеності мережі:

- час відновлення після відмов зменшився в середньому на 35%;
- рівень захищеності внутрішньої інфраструктури підвищився з 4 до 4.8 балів;
- стійкість до соціальної інженерії підвищилася з 3 до 4.2 балів;
- загальний рівень захищеності підвищився з 4.1 до 4.7 балів.



— Рисунок 3.2 – Порівняння результатів тестування до та після оптимізації

3.4 Налаштування та оптимізація роботи мережі

На основі результатів тестування проведено налаштування та оптимізацію роботи мережі для забезпечення максимальної продуктивності, надійності та захищеності. Оптимізація охоплювала різні аспекти функціонування мережевої інфраструктури, від апаратного забезпечення до програмних компонентів.

Для підвищення продуктивності та надійності мережевого обладнання проведено оптимізацію апаратної конфігурації:

- оптимізація пам'яті - збільшено обсяг оперативної пам'яті на комутаторах ядра та рівня розподілу для підтримки більших таблиць маршрутизації та покращення продуктивності при обробці складних правил фільтрації;

- оптимізація блоків живлення - на критично важливому обладнанні встановлено додаткові резервні блоки живлення для підвищення надійності;

- оптимізація системи охолодження - вдосконалено систему охолодження в серверних приміщеннях для забезпечення оптимального температурного режиму та підвищення надійності обладнання;

- оптимізація кабельної інфраструктури - проведено перерозподіл навантаження між кабельними трасами для мінімізації електромагнітних перешкод та підвищення надійності передачі даних.

Для підвищення продуктивності та безпеки мережі проведено оптимізацію програмної конфігурації мережевого обладнання:

- оптимізація протоколів маршрутизації - налаштовано таймери та параметри протоколу OSPF для прискорення конвергенції при зміні топології мережі;

- оптимізація QoS - впроваджено детальну класифікацію трафіку та політики якості обслуговування для забезпечення пріоритетної обробки критично важливого трафіку;

— оптимізація управління буферами - налаштовано механізми управління буферами на комутаторах для мінімізації втрат пакетів при пікових навантаженнях;

— оптимізація фільтрації трафіку - оптимізовано списки контролю доступу для підвищення ефективності фільтрації трафіку та зменшення навантаження на процесори комутаторів;

— оптимізація системи виявлення вторгнень - налаштовано правила та політики системи IDS/IPS для мінімізації кількості хибних спрацьовувань при збереженні високої ефективності виявлення атак.

Результати оптимізації програмної конфігурації представлені в таблиці 3.3.

Таблиця 3.3 - Результати оптимізації програмної конфігурації

Параметр	До оптимізації	Після оптимізації	Поліпшення, %
Час конвергенції OSPF, с	5.2	2.8	46.2
Затримки при передачі критичного трафіку, мс	4.7	2.1	55.3
Кількість хибних спрацьовувань IDS за добу	24	5	79.2
Використання процесора на комутаторах ядра, %	65	42	35.4
Використання пам'яті на комутаторах ядра, %	78	61	21.8
Максимальна кількість одночасних з'єднань через ME	15000	24000	60.0

3.5 Практичні рекомендації з експлуатації закритої мережі

На основі досвіду розробки, впровадження та тестування закритої мережі сформульовано ряд практичних рекомендацій для забезпечення її ефективної експлуатації та підтримки високого рівня надійності та захищеності. Ці рекомендації охоплюють різні аспекти функціонування

мережевої інфраструктури та спрямовані на мінімізацію ризиків виникнення збоїв та інцидентів безпеки.

Адміністрування закритої мережі з підвищеною надійністю та захищеністю вимагає особливого підходу та дотримання строгих процедур. На відміну від звичайних мереж, де певні відхилення від регламентів можуть бути допустимими, в закритих мережах навіть незначні порушення процедур експлуатації можуть призвести до серйозних наслідків для безпеки та надійності.

Основою безпечної експлуатації закритої мережі є принцип найменших привілеїв, який передбачає надання користувачам та адміністраторам лише тих прав доступу, які необхідні для виконання їхніх посадових обов'язків. Цей принцип повинен застосовуватися не лише до доступу до інформаційних ресурсів, але й до доступу до мережевого обладнання та інструментів адміністрування.

Для забезпечення ефективної експлуатації закритої мережі рекомендується впровадити процес управління змінами, який передбачає чітку регламентацію процедур внесення будь-яких змін до конфігурації мережевого обладнання та програмного забезпечення. Кожна зміна повинна бути документована, погоджена з відповідальними особами та протестована в тестовому середовищі перед впровадженням у продуктивну мережу.

Важливим аспектом експлуатації закритої мережі є регулярний моніторинг та аудит безпеки. Рекомендується проводити щоденний аналіз журналів подій, регулярні перевірки конфігурацій обладнання на відповідність політикам безпеки та періодичні тести на проникнення для виявлення потенційних вразливостей.

Для забезпечення надійності мережевої інфраструктури рекомендується впровадити програму профілактичного обслуговування, яка включає регулярну перевірку працездатності обладнання, очищення систем охолодження, тестування резервних джерел живлення та перевірку кабельної інфраструктури.

Особливу увагу слід приділяти резервному копіюванню конфігурацій мережевого обладнання та критично важливих даних. Рекомендується використовувати багаторівневу систему резервного копіювання з різними періодами зберігання копій та регулярно перевіряти можливість відновлення даних з резервних копій.

При експлуатації закритої мережі важливо забезпечити суворий контроль доступу до мережевого обладнання та приміщень, де воно розташоване. Рекомендується використовувати багатофакторну автентифікацію для доступу до критичних систем та вести журнал доступу до серверних приміщень.

Для забезпечення безперервності функціонування мережі рекомендується розробити та регулярно тестувати плани відновлення після збоїв різного рівня критичності. Ці плани повинні включати чіткі інструкції щодо дій персоналу в різних ситуаціях, контактні дані відповідальних осіб та зовнішніх постачальників послуг.

Важливою рекомендацією є мінімізація залежності від конкретних осіб через документування процедур адміністрування та забезпечення взаємозамінності співробітників. Для кожної критичної функції експлуатації мережі повинно бути щонайменше два підготовлених фахівці, здатних виконувати відповідні завдання.

Основні рекомендації з експлуатації закритої мережі систематизовано в таблиці 3.4, де вони згруповані за категоріями та доповнені оцінкою критичності для забезпечення надійності та захищеності мережі.

Дотримання наведених рекомендацій дозволить забезпечити надійну та безпечну експлуатацію закритої мережі протягом всього її життєвого циклу, мінімізувати ризики виникнення збоїв та інцидентів безпеки, а також швидко відновлювати працездатність мережі у випадку виникнення проблем.

Таблиця 3.4 – Основні рекомендації з експлуатації закритої мережі

Категорія	Рекомендація	Критичність (1-5)	Періодичність виконання
Адміністрування	Використовувати принцип найменших привілеїв при наданні доступу	5	Постійно
Адміністрування	Документувати всі зміни в конфігурації обладнання	4	При кожній зміні
Безпека	Регулярно оновлювати програмне забезпечення та мікрокод обладнання	5	Щомісяця
Безпека	Проводити аудит безпеки та тести на проникнення	4	Щоквартально
Безпека	Контролювати фізичний доступ до мережевого обладнання	5	Постійно
Моніторинг	Аналізувати журнали подій на предмет підозрілої активності	4	Щодня
Моніторинг	Контролювати продуктивність мережі та використання ресурсів	3	Щодня
Резервування	Регулярно створювати резервні копії конфігурацій	5	Щотижня та при змінах
Резервування	Тестувати відновлення з резервних копій	4	Щомісяця
Навчання	Забезпечувати регулярне навчання адміністраторів	4	Щоквартально
Документація	Підтримувати актуальність документації	3	При кожній зміні
Обслуговування	Проводити профілактичне обслуговування обладнання	4	За графіком

3.6 Регламент технічного обслуговування та підтримки мережі

Регламент технічного обслуговування закритої мережі визначає різноманітні процедури підтримки: щоденний моніторинг стану обладнання і журналів; щотижневий аналіз продуктивності та перевірку резервних копій; щомісячні профілактичні роботи з оновленням програмного забезпечення; щоквартальні та щорічні комплексні перевірки всіх компонентів. Особлива увага приділяється критичному обладнанню (комутатори ядра, міжмережеві екрани, сервери), системам безперебійного живлення та процедурам

реагування на інциденти. Регламент включає чіткі процедури проведення планових робіт, класифікацію інцидентів за рівнем критичності (від P1 до P4), схеми ескалації проблем, документування змін та детальні інструкції з резервного копіювання й відновлення. Основні процедури обслуговування, їх періодичність, відповідальні особи та очікувані результати представлені в таблиці 3.5.

Таблиця 3.5 - Регламент технічного обслуговування закритої мережі

Процедура обслуговування	Періодичність	Відповідальні	Очікуваний результат
Моніторинг стану мережевого обладнання	Щодня	Черговий адміністратор	Виявлення та усунення проблем на ранній стадії
Аналіз журналів подій та інцидентів безпеки	Щодня	Фахівець безпеки з	Виявлення потенційних загроз та вразливостей
Перевірка резервних копій конфігурацій	Щотижня	Адміністратор мережі	Гарантія можливості відновлення після збоїв
Оновлення програмного забезпечення	Щомісяця	Адміністратор мережі	Усунення відомих вразливостей та помилок
Тестування системи безперебійного живлення	Щомісяця	Інженер обслуговування з	Гарантія безперебійного електроживлення
Профілактичне обслуговування обладнання	Щоквартально	Інженер обслуговування з	Запобігання відмовам через фізичні проблеми
Аудит безпеки та тестування на проникнення	Щоквартально	Зовнішній аудитор	Виявлення та усунення вразливостей безпеки
Перевірка фізичного захисту	Щоквартально	Фахівець безпеки з	Запобігання несанкціонованому фізичному доступу
Комплексне тестування відмовостійкості	Щопівроку	Команда адміністраторів	Перевірка надійності всіх компонентів мережі
Інвентаризація обладнання та ПЗ	Щорічно	Адміністратор мережі	Актуалізація інформації про наявні ресурси
Оновлення документації	При змінах	Відповідальний за зміни	Актуальна документація всіх компонентів мережі
Планування модернізації	Щорічно	Керівник ІТ-відділу	Підтримка актуальності та продуктивності мережі

Впровадження та строге дотримання регламенту технічного обслуговування та підтримки дозволяє значно підвищити надійність та захищеність закритої мережі, мінімізувати ризики виникнення збоїв та

інцидентів безпеки, а також забезпечити швидке відновлення працездатності системи у випадку виникнення проблем.

3.7 Навчання персоналу з обслуговування мережі

На основі наданого документу, я можу узагальнити інформацію про програму навчання персоналу для забезпечення ефективного функціонування закритої мережі:

Програма навчання персоналу для обслуговування закритої мережі базується на принципі безперервної освіти та підвищення кваліфікації, оскільки інформаційні технології та загрози безпеці постійно еволюціонують. Навчання включає різні формати: теоретичні заняття, практичні семінари, лабораторні роботи та моделювання реальних ситуацій.

Програма розроблена для різних категорій персоналу (адміністратори мережі, фахівці з інформаційної безпеки, інженери з обслуговування та чергові оператори) з урахуванням їхніх функціональних обов'язків. Базовий модуль обов'язковий для всіх категорій і включає загальні питання архітектури мережі, принципи функціонування та основні політики безпеки.

Важливою частиною програми є практичні заняття на спеціальному тестовому стенді, який імітує реальну мережеву інфраструктуру, де фахівці відпрацьовують навички без ризику порушення роботи продуктивної мережі. Програма також передбачає систему обміну знаннями, регулярне оновлення навчальних матеріалів та періодичну сертифікацію персоналу. Основні компоненти програми навчання представлені в таблиці 3.6.

Реалізація програми навчання персоналу дозволила сформувати команду висококваліфікованих фахівців, здатних ефективно обслуговувати закриту мережу та оперативно реагувати на інциденти різного типу. Це значно підвищило надійність та захищеність мережевої інфраструктури, а

також зменшило залежність від зовнішніх консультантів та постачальників послуг.

Таблиця 3.6 - Програма навчання персоналу з обслуговування закритої мережі

Навчальний модуль	Тривалість (годин)	Цільова аудиторія	Очікувані результати навчання
Архітектура закритої мережі	16	Усі категорії	Розуміння структури та принципів функціонування мережі
Політики та процедури інформаційної безпеки	8	Усі категорії	Знання основних вимог безпеки та процедур їх дотримання
Налаштування та управління комутаторами Cisco	24	Адміністратори мережі	Вміння налаштовувати та оптимізувати роботу мережевого обладнання
Налаштування та управління міжмережевими екранами	24	Адміністратори мережі, фахівці з безпеки	Вміння налаштовувати правила фільтрації та контролювати трафік
Системи виявлення та запобігання вторгненням	16	Фахівці з безпеки	Вміння налаштовувати та аналізувати результати роботи IDS/IPS
Аудит безпеки мережевої інфраструктури	16	Фахівці з безпеки	Вміння виявляти вразливості та оцінювати рівень захищеності
Обслуговування серверного обладнання	16	Інженери обслуговування з	Вміння проводити профілактичне обслуговування та усувати несправності
Системи безперебійного живлення	8	Інженери обслуговування з	Вміння обслуговувати та тестувати ДБЖ та дизель-генератори
Моніторинг стану мережі	16	Чергові оператори	Вміння використовувати системи моніторингу та реагувати на сповіщення
Діагностика та усунення типових проблем	16	Усі категорії	Вміння виявляти та усувати поширені проблеми в роботі мережі
Реагування на інциденти безпеки	16	Фахівці з безпеки, адміністратори	Вміння ефективно реагувати на різні типи інцидентів безпеки
Документування та звітність	8	Усі категорії	Вміння вести технічну документацію та готувати звіти про інциденти

ВИСНОВКИ

У даній дипломній роботі на тему "Розробка закритої мережі з підвищеною надійністю" було вирішено комплекс науково-практичних завдань, пов'язаних з проєктуванням, розробкою та тестуванням закритої мережі, що відповідає підвищеним вимогам до надійності та інформаційної безпеки. На основі проведеного дослідження можна зробити наступні висновки:

Проведений аналіз предметної області показав, що закриті мережі з фізичною та логічною ізоляцією від зовнішніх мереж є необхідним рішенням для обробки конфіденційної інформації в критичних інфраструктурах, зокрема в навчальних закладах, де зберігаються персональні дані, результати наукових досліджень та інша чутлива інформація. Встановлено, що ключовими вимогами до таких мереж є висока доступність, надійність, відмовостійкість, захищеність від зовнішніх та внутрішніх загроз, а також можливість швидкого відновлення при виникненні збоїв.

На основі аналізу сучасних підходів та технологій розроблено методологію проєктування закритих мереж, яка базується на принципах багаторівневого захисту та резервування критичних компонентів. Обґрунтовано вибір ієрархічної архітектури з поділом на рівні ядра, розподілу та доступу, що забезпечує оптимальний баланс між надійністю, захищеністю, масштабованістю та вартістю впровадження. Проведений порівняльний аналіз різних топологій показав, що дана архітектура дозволяє досягти коефіцієнта готовності мережі не менше 99,994%, що перевищує вимоги технічного завдання.

Розроблено проєкт закритої мережі для навчального закладу, який включає три будівлі, об'єднані оптоволоконними каналами зв'язку з резервуванням. Для забезпечення надійності реалізовано наступні архітектурні рішення: дублювання критичних компонентів мережі

(комутатори ядра, комутатори рівня розподілу, міжмережеві екрани, сервери); агрегація каналів зв'язку для підвищення пропускної здатності та надійності з'єднань; налаштування протоколів резервування (HSRP, VRRP) для автоматичного переключення у випадку відмови основного пристрою; впровадження динамічних протоколів маршрутизації (OSPF) з оптимізованими параметрами конвергенції.

Обґрунтовано вибір мережевого обладнання для різних рівнів мережевої ієрархії. На рівні ядра використано комутатори Cisco Catalyst 9500 з підтримкою технології StackWise Virtual, що дозволяє об'єднати два фізичні пристрої в одне логічне ціле та забезпечити безперервність роботи навіть при відмові одного з них. На рівні розподілу впроваджено комутатори Cisco Catalyst 9300 зі стекуванням для підвищення надійності та гнучкості управління. На рівні доступу використано комутатори Cisco Catalyst 9200 з резервними uplink-з'єднаннями до різних комутаторів рівня розподілу, що забезпечує стійкість до відмов.

Розроблено комплексну систему безперебійного живлення, яка включає джерела безперебійного живлення (ДБЖ), дизель-генераторні установки та системи автоматичного переключення. Проведені розрахунки показали, що дана система забезпечує автономну роботу критичних компонентів мережі протягом не менше 8 годин при повному відключенні зовнішнього електроживлення, що відповідає вимогам до безперервності функціонування критичної інфраструктури.

Для забезпечення високого рівня захищеності мережі розроблено та впроваджено багаторівневу систему захисту інформації, яка включає: фізичну ізоляцію від зовнішніх мереж (модель Air-Gap); сегментацію мережі з використанням VLAN та суворою фільтрацією міжсегментного трафіку; багаторівневу систему автентифікації та авторизації з використанням принципу найменших привілеїв; системи виявлення та запобігання вторгненням (IDS/IPS) для захисту від мережевих атак; системи запобігання витоку даних (DLP) для контролю за переміщенням конфіденційної

інформації; криптографічний захист даних при зберіганні та передачі; комплексну систему аудиту та моніторингу безпеки.

Розроблено та впроваджено систему моніторингу закритої мережі на базі платформи Zabbix з резервуванням серверів моніторингу в різних будівлях. Дана система забезпечує цілодобовий контроль за станом всіх компонентів мережі, автоматичне сповіщення про виникнення проблем та збір статистичних даних для аналізу продуктивності та планування розвитку мережі. Для підвищення безпеки система моніторингу розміщена в окремому сегменті мережі з контрольованим доступом.

На основі результатів тестування розроблено практичні рекомендації з експлуатації закритої мережі, які включають оптимальні налаштування мережевого обладнання, процедури резервного копіювання та відновлення, а також заходи з підтримки захищеності мережі в актуальному стані. Розроблено детальний регламент технічного обслуговування, який визначає періодичність, обсяг та процедури обслуговування різних компонентів мережевої інфраструктури, а також порядок дій при виникненні інцидентів різного рівня критичності.

Розроблено та впроваджено програму навчання персоналу з обслуговування закритої мережі, яка включає теоретичні та практичні заняття для різних категорій фахівців. Дана програма дозволила сформувати команду висококваліфікованих спеціалістів, здатних ефективно адмініструвати мережу та оперативно реагувати на інциденти різного типу.

Створено комплект технічної документації на розроблену закриту мережу, який включає схеми мережевої інфраструктури, опис конфігурацій обладнання, інструкції з експлуатації та регламенти обслуговування. Дана документація забезпечує збереження знань про мережу, спрощує її обслуговування та модернізацію, а також є необхідною умовою для проходження аудитів безпеки та відповідності вимогам регуляторів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Apollo client: офіц. документація. URL: <https://www.apollographql.com/docs/> (дата звернення: 15.03.2025).
2. Брайко В. В. Дослідження принципів роботи технологій VPN. URL: <https://core.ac.uk/download/pdf/84825462.pdf> (дата звернення: 10.03.2025).
3. Коваленко В. М. Захист інформації та кібербезпека: методи та інструменти: монографія. Київ: Академвидав, 2023. 312 с.
4. Ковальчук А. В., Дудник О. С. Інформаційна безпека в системах освіти: навч. посіб. Київ: КНЕУ, 2021. 256 с.
5. Колесник В. В., Вакалюк Т. А. Огляд програмних емуляторів та симуляторів для побудови працездатних моделей мережі. URL: <https://conf.ztu.edu.ua/wp-content/uploads/2021/01/7.pdf> (дата звернення: 12.03.2025).
6. Material UI: офіц. документація. URL: <https://mui.com/material-ui> (дата звернення: 20.03.2024).
7. MDN Web Docs: документація. URL: <https://developer.mozilla.org/uk/> (дата звернення: 18.03.2025).
8. Миколайчук Ю. А. Аналіз ризиків кібербезпеки для освітніх установ. Науковий журнал з кібербезпеки. 2023. № 4. С. 45-53.
9. Міністерство освіти і науки України. Нормативні документи з питань інформаційної безпеки у навчальних закладах. Київ: МОНУ, 2022. 78 с.
10. Пархоменко І. І. Способи захисту каналів корпоративних мереж на базі VPN-рішень. URL: <http://journals.dut.edu.ua/index.php/dataprotect/article/view/1245> (дата звернення: 17.03.2025).

11. Постанова Кабінету Міністрів України № 992 "Про затвердження Положення про захист персональних даних" від 29.07.2020 р.. URL: <https://zakon.rada.gov.ua/laws/show/992-2020-п> (дата звернення: 14.03.2025).
12. Project Reactor: офіц. документація. URL: <https://projectreactor.io/docs/core/release/reference/> (дата звернення: 05.03.2025).
13. React: офіц. документація. URL: <https://uk.reactjs.org/docs/hooks-reference.html> (дата звернення: 07.03.2025).
14. React Router: офіц. документація. URL: <https://reactrouter.com/docs/en/v6> (дата звернення: 20.03.2025).
15. Sass: офіц. документація. URL: <https://sasslang.com/documentation/> (дата звернення: 12.03.2025).
16. Сидоренко Л. М. Основи кібербезпеки: посіб. для студентів ІТ-спеціальностей. Харків: Вид-во Харків. нац. ун-ту, 2022. 304 с.
17. Spring for GraphQL: офіц. документація. URL: <https://docs.spring.io/spring-graphql/docs/current-SNAPSHOT/reference/html/> (дата звернення: 08.03.2025).
18. Spring MongoDB: офіц. документація. URL: <https://docs.spring.io/spring-data/mongodb/docs/current/reference/html/> (дата звернення: 07.03.2025).
19. Spring Security: офіц. документація. URL: <https://docs.spring.io/spring-security/reference/index.html> (дата звернення: 06.03.2025).
20. Spring WebFlux: офіц. документація. URL: <https://docs.spring.io/spring-framework/docs/current/reference/html/web-reactive.html> (дата звернення: 05.03.2025).
21. Council of Europe. Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data. 2018. URL: <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (date of access: 04.04.2025).

22. Gartner. Top Security and Risk Management Trends 2023. URL: <https://www.gartner.com> (date of access: 17.10.2025).
23. Google. Security and Compliance Whitepaper. URL: <https://cloud.google.com/security> (date of access: 18.05.2025).
24. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO, 2013. 23 p.
25. Keijser J. J. OpenVPN Cookbook. Birmingham: Packt Publishing, 2017. 467 p.
26. Microsoft. Security in Education: Best Practices. URL: <https://www.microsoft.com/education/security> (date of access: 18.05.2025).
27. National Institute of Standards and Technology. NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Washington: NIST, 2023. 492 p.
28. Smith J. Advanced Persistent Threats in Education Sector: A Case Study. Journal of Cybersecurity. 2023. Vol. 8, No. 3. P. 212–229.
29. Symantec. Internet Security Threat Report 2023. URL: <https://www.symantec.com/security-center> (date of access: 25.03.2025).
30. Wang S. P. Computer Architecture and Organization: Fundamentals and Architecture Security. Berlin: Springer, 2021. 344 p.
31. Woland A., Santuka V., Sanbower J., Mitchell C. Integrated Security Technologies and Solutions. Indianapolis: Cisco Press, 2019. 1148 p.

ДОДАТОК А
СХЕМА ЗАКРИТОЇ МЕРЕЖІ

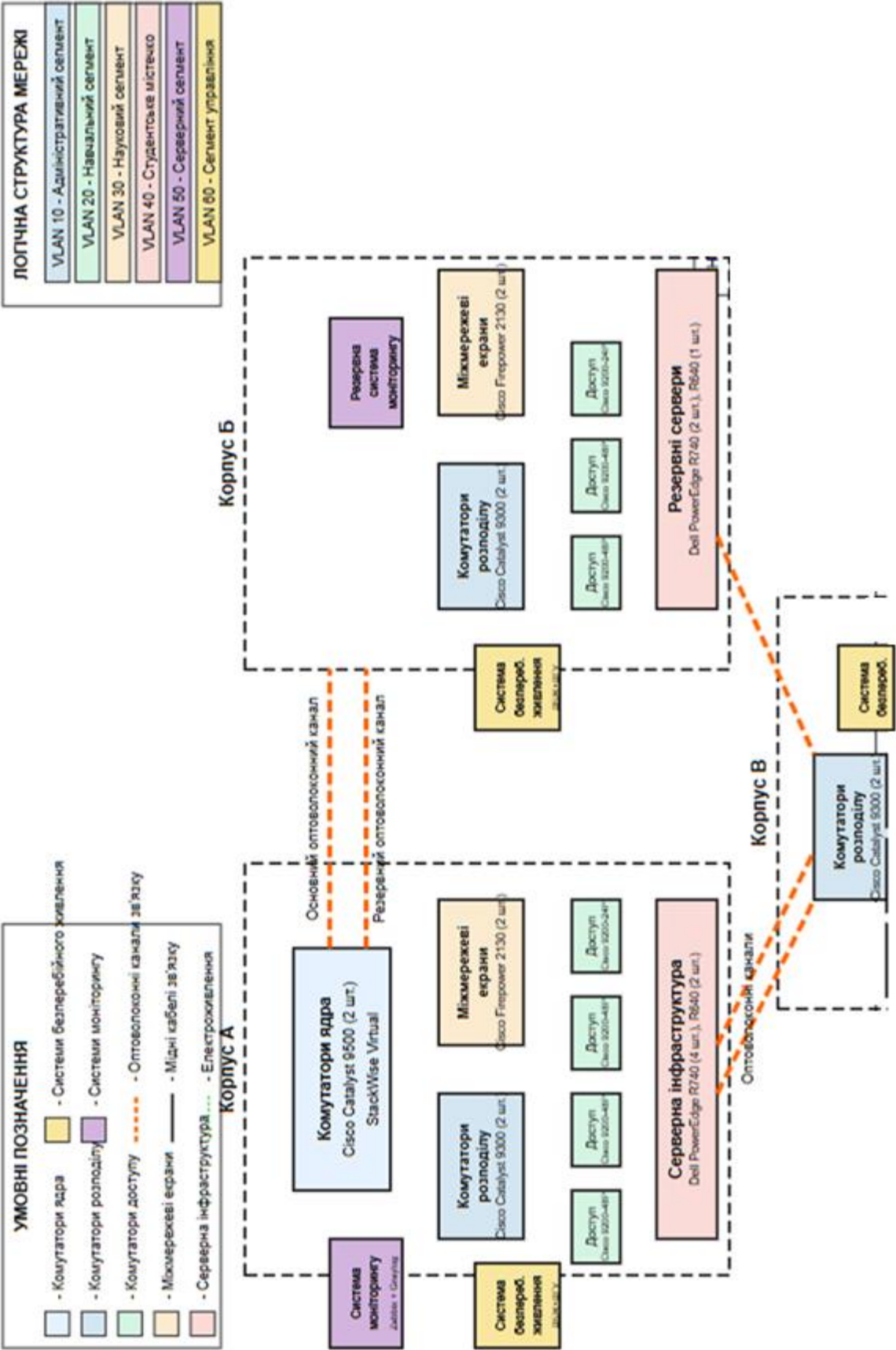


Рисунок А.1 – схема закритої мережі

ДОДАТОК Б
НАЛАШТУВАННЯ СИСТЕМИ ЗАХИСТУ

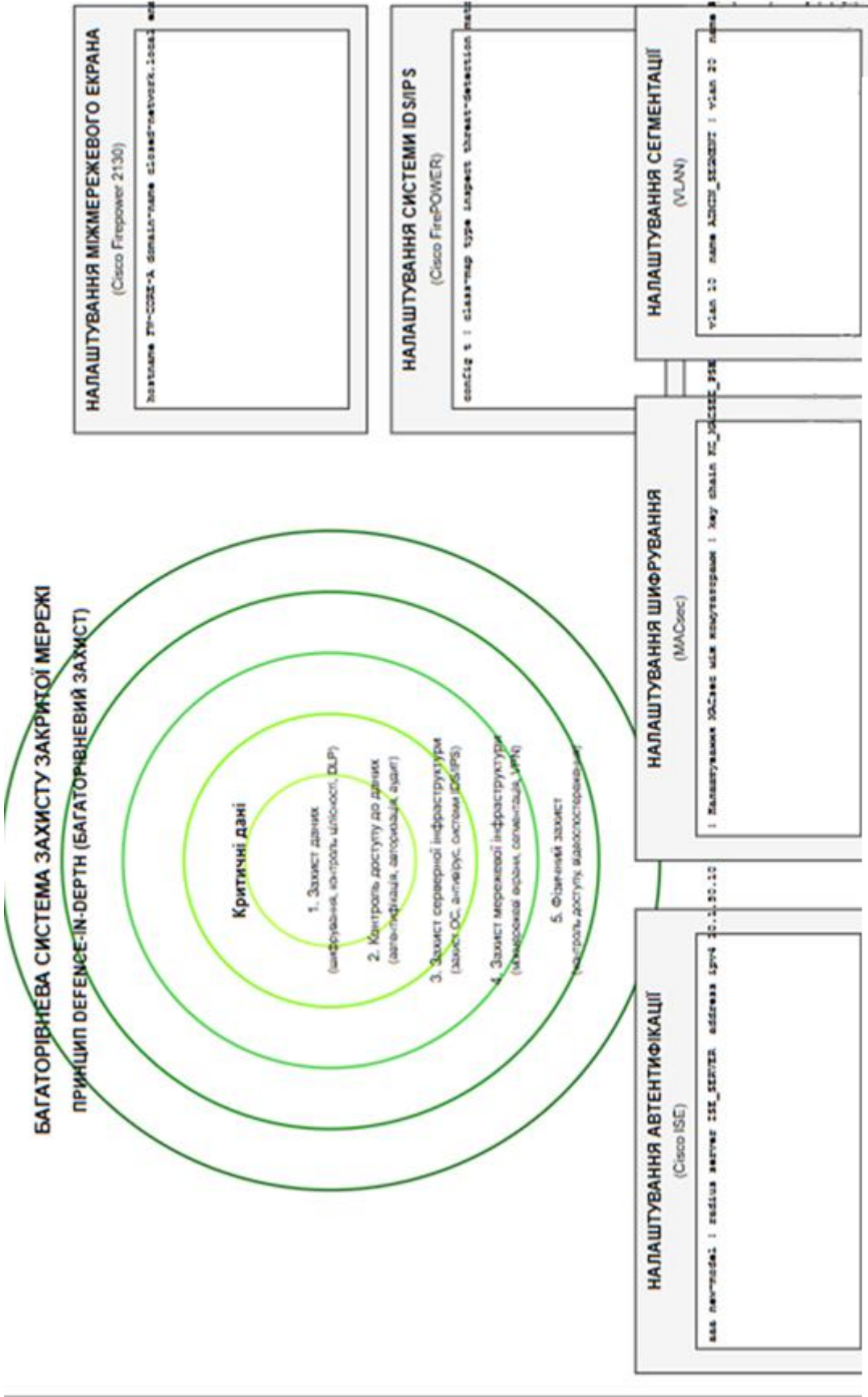


Рисунок Б.1 – налаштування системи захисту

РОЗРОБКА ЗАКРИТОЇ МЕРЕЖІ З ПІДВИЩЕНОЮ НАДІЙНІСТЮ

Роботу виконав студент групи КНТ-511

Сергєєв Данило Антонович

Науковий керівник К.Т.Н., доцент

Зеленьова Ірина Яківна

АКТУАЛЬНІСТЬ

Важливість забезпечення надійності та захищеності закритих мереж підкреслюється зростанням кількості та складності кібератак.

За даними Державної служби спеціального зв'язку та захисту інформації України, кількість зареєстрованих кіберінцидентів щорічно зростає на 30-40%, причому значна частина з них спрямована на об'єкти критичної інфраструктури.



ОБГРУНТУВАННЯ ЗАДАЧІ

Закриті мережі, що функціонують ізольовано від загальнодоступних мереж, забезпечують необхідний рівень захисту для обробки конфіденційної інформації та підтримки критично важливих бізнес-процесів.

Особливу увагу слід приділяти комплексному підходу до забезпечення надійності та захищеності, який охоплює всі аспекти функціонування мережі — від вибору топології та обладнання до налаштування протоколів безпеки та організації системи моніторингу.



3

МЕТА ТА ПРЕДМЕТ РОЗРОБКИ

Метою дипломної роботи є розробка закритої мережі з підвищеною надійністю, що забезпечує безперебійне функціонування критично важливих інформаційних систем та захист конфіденційної інформації від несанкціонованого доступу.

Предметом розробки є засоби та методи забезпечення надійності інформаційних мереж для обробки конфіденційної інформації.



4

ОСНОВНІ ЗАДАЧІ РОБОТИ



- визначити основні вимоги до надійності закритих мереж;
- проаналізувати існуючі топології та архітектурні рішення для побудови закритих мереж;
- дослідити моделі закритих мереж та їх особливості;
- проаналізувати кабельні системи, мережеві протоколи та системи моніторингу з точки зору забезпечення надійності та захищеності;
- розробити проект закритої мережі з підвищеною надійністю;
- обґрунтувати вибір мережевого обладнання;
- спроектувати систему безперебійного живлення та резервування;
- розробити та впровадити систему захисту інформації;
- розробити методику тестування;
- підготувати практичні рекомендації з експлуатації закритої мережі.

5

ЕТАПИ ВИКОНАННЯ РОБОТИ

- Аналіз предметної області та теоретичні основи розробки закритої мережі;
- Розробка закритої мережі з підвищеною надійністю;
- Тестування та практичні рекомендації з експлуатації закритої мережі.



6

ЗАКРИТА МЕРЕЖА ТА ВИМОГИ ЇЇ НАДІЙНОСТІ

Відповідно до стандарту ISO/IEC 27001:2013 [24], надійність інформаційної системи визначається через показники доступності, відмовостійкості та цілісності даних.

Ключові вимоги до надійності закритих мереж:

- безперебійність функціонування;
- відмовостійкість;
- масштабованість;
- резервування;
- можливість швидкого відновлення після збоїв.



7

МОДЕЛІ ЗАКРИТИХ МЕРЕЖ Порівняльний аналіз



Модель	Рівень безпеки	Складність впровадження	Гнучкість	Масштабованість	Вартість
Air-Gap	Дуже високий	Середня	Низька	Низька	Висока
Controlled Gateway	Високий	Висока	Середня	Середня	Висока
DMZ	Середній до високого	Середня	Висока	Висока	Середня
Trust-Based Segmentation	Високий	Висока	Висока	Висока	Середня до високої
Overlay Secure Network	Середній до високого	Середня	Висока	Висока	Середня
Zero Trust	Дуже високий	Дуже висока	Висока	Висока	Висока

8

КАБЕЛЬНІ СИСТЕМИ

Порівняльний аналіз

Тип кабелю	Пропускна здатність	Максимальна довжина	Рівень захищеності	Сегмент застосування
Одномодове оптоволокно OS2	До 100 Гбіт/с	До 10 км	Дуже високий	Магістральні лінії між будівлями
Багатомодове оптоволокно OM4	До 100 Гбіт/с	До 150 м	Високий	Магістральні лінії всередині будівель
Екранована вита пара Cat.6A (S/FTP)	До 10 Гбіт/с	До 100 м	Високий	Горизонтальна підсистема
Екранована вита пара Cat.6 (F/UTP)	До 1 Гбіт/с	До 100 м	Середній	Робоча підсистема



9

МЕРЕЖЕВІ ПРОТОКОЛИ

Порівняльний аналіз

Стандартний протокол	Основні вразливості	Захищена альтернатива	Механізми захисту	Рекомендовані сфери застосування
IPv4	Відсутність автентифікації, шифрування, вразливість до підробки адрес	IPsec, IPv6 з IPsec	Шифрування, автентифікація, захист цілісності даних	Всі сегменти закритої мережі
TCP	Вразливість до SYN flood, sequence prediction атак	TCP з IPsec, MPTCP з TLS	Шифрування даних, захист від переповнення буфера	Критичні додатки, веб-сервіси
UDP	Відсутність гарантій доставки, вразливість до UDP flood	DTLS, QUIC	Шифрування даних, захист від спуфінгу	Додатки реального часу, VoIP
HTTP	Передача даних у відкритому вигляді	HTTPS з TLS 1.3	Шифрування, автентифікація, захист від MITM атак	Веб-інтерфейси управління, API
Telnet	Передача облікових даних у відкритому вигляді	SSH	Шифрування, надійна автентифікація	Віддалене адміністрування
FTP	Відсутність шифрування	SFTP, FTPS	Шифрування даних та облікових записів	Передача файлів
SNMP v1/v2	Слабкі механізми автентифікації	SNMPv3	Шифрування, контроль доступу	Моніторинг мережевого обладнання

10

ПОЯСНЕННЯ ВСІХ ЕТАПІВ ВИКОНАННЯ РОБОТИ

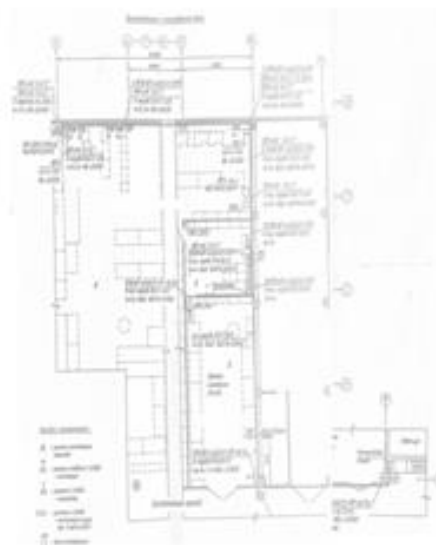
- Проходження переддипломної практики;
- Проектування закритої мережі;
- Вибір обладнання;
- Системи моніторингу мережі;
- Написання рекомендацій з експлуатації закритої мережі.



11

ПЕРЕДДИПЛОМНА ПРАКТИКА

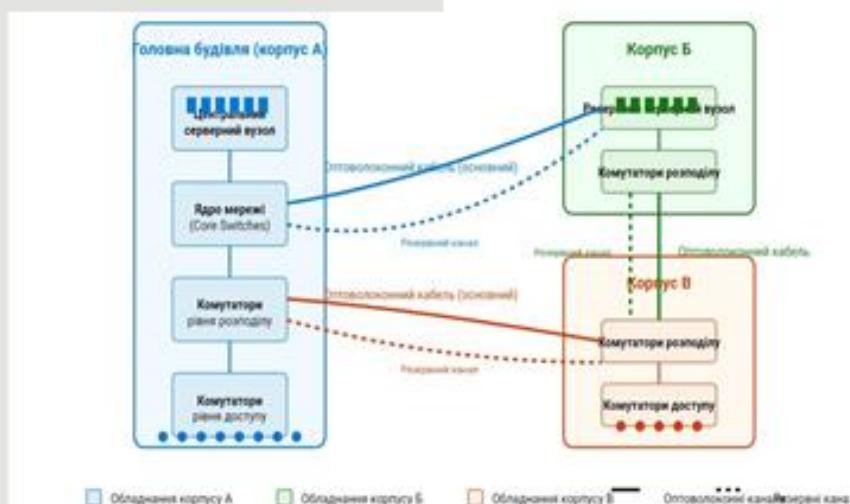
Надала можливість спроектувати, змонтувати та налаштувати мережу на певній ділянці виробництва, що допомогло мені з проектуванням закритої мережі у межах університету.



Проект з переддипломної практики

12

ФІЗИЧНА ТОПОЛОГІЯ ЗАКРИТОЇ МЕРЕЖІ



13

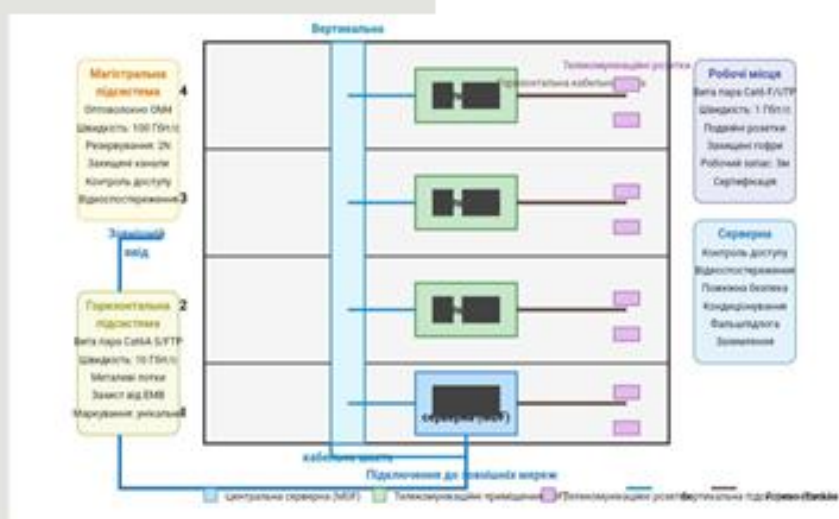
КАБЕЛЬНІ СИСТЕМИ

Сегмент мережі	Рекомендований тип кабелю	Додаткові заходи захисту	Рівень захищеності
Магістральна мережа	Одномодове оптоволокно	Захищені кабельні канали, система моніторингу цілісності	Дуже високий
Розподільна мережа	Одномодове/багатомодове оптоволокно або Cat7/Cat8 S/FTP	Екрановані комутаційні шафи, контроль доступу	Високий
Горизонтальна підсистема	Cat6a S/FTP або вище	Захищені кабельні канали, мольворове модування	Середній до високого
Робочі місця користувачів	Cat6a S/FTP	Механічне блокування портів, контроль підключень	Середній
Дезагітаризована зона	Оптоволокно	Фізична ізоляція, резервування каналів	Високий
Серверні ферми	Оптоволокно або Cat8 S/FTP	Спеціалізовані екрановані шафи, постійний моніторинг	Дуже високий

Рекомендації щодо вибору кабельних систем для різних сегментів мережі

14

Схема організації кабельної інфраструктури всередині будівлі



15

ВИБІР ОБЛАДНАННЯ

Вибір мережевого обладнання для закритої мережі базується на восьми ключових критеріях.

Система безперебійного живлення також є критично важливим компонентом закритої мережі, оскільки забезпечує безперервну роботу мережевого обладнання та серверів навіть при збоях у електропостачанні.



16

Порівняльний аналіз комутаторів для рівня ядра та рівня доступу



Для рівня ядра



Характеристика	Cisco Catalyst 9300	Juniper EX4600	HPE Aruba 3400E
Продуктивність комутації	До 1,0 Тбіт/с	До 1,44 Тбіт/с	До 960 Гбіт/с
Кількість портів	До 48 портів 10/10G	До 72 портів 10/10G	До 96 портів 10/10G
Підтримка PoE/PoE+	Так (до 90 Вт на порт)	Так (до 30 Вт на порт)	Так (до 60 Вт на порт)
Стекування	До 8 пристроїв	До 10 пристроїв	До 10 пристроїв
Продуктивність стеку	480 Гбіт/с	320 Гбіт/с	336 Гбіт/с
Слов'я таблиць маршрутизації	32K (IPv4), 16K (IPv6)	32K (IPv4), 16K (IPv6)	32K (IPv4), 16K (IPv6)
Підтримка VLAN	4094	4096	2048
Резервні компоненти	Блоки живлення, вентилятори	Блоки живлення, вентилятори	Модуль управління, вентилятори
Функції безпеки	802.1X, MACsec, TrustSec, ACL	802.1X, MACsec, ACL	802.1X, MACsec, ACL
MTBF (годин)	>183 000	>150 000	>165 000
Сертифікати безпеки	FIPS 140-2, CC	FIPS 140-2	FIPS 140-2



Для рівня розподілу



Характеристика	Cisco Catalyst 9300	Juniper EX9100	HPE FlexFabric 9300
Продуктивність комутації	До 8,4 Тбіт/с	До 4,8 Тбіт/с	До 5,76 Тбіт/с
Продуктивність швидкості портів	1/10/25/40/100 Гбіт/с	1/10/40/100 Гбіт/с	1/10/25/40/100 Гбіт/с
Слов'я таблиць MAC-адрес	128K	256K	128K
Підтримка VLAN	4094	4096	4096
Резервні компоненти	Повне (блоки живлення, вентилятори, модулі)	Повне	Повне
Підтримка протоколів резервування	HSRP, VRRP, VSS	VRRP	VRRP
Функції безпеки	MACsec, IEEE 802.1X, ACL, TrustSec	MACsec, IEEE 802.1X, ACL	MACsec, IEEE 802.1X, ACL
MTBF (годин)	>200 000	>175 000	>190 000
Можливість гарячої заміни компонентів	Так	Так	Так
Сертифікати відповідності	FIPS 140-2, CC, DESA	FIPS 140-2, CC	FIPS 140-2

17

Порівняльний аналіз комутаторів для рівня доступу

Характеристика	Cisco Catalyst 9200	Juniper EX3400	HPE Aruba 2930F
Продуктивність комутації	До 176 Гбіт/с	До 320 Гбіт/с	До 176 Гбіт/с
Кількість портів	До 48 портів 1GbE	До 48 портів 1GbE	До 48 портів 1GbE
Uplink-порти	4 x 10GbE SFP+	4 x 10GbE SFP+	4 x 10GbE SFP+
Підтримка PoE/PoE+	Так (до 30 Вт на порт)	Так (до 30 Вт на порт)	Так (до 30 Вт на порт)
Стекування	До 8 пристроїв	До 10 пристроїв	До 8 пристроїв
Підтримка VLAN	1024	4096	4096
Резервні компоненти	Блоки живлення	Блоки живлення	Блоки живлення
Функції безпеки	802.1X, Port Security, DHCP Snooping	802.1X, Port Security, DHCP Snooping	802.1X, Port Security, DHCP Snooping
MTBF (годин)	>160 000	>150 000	>145 000
Вартість експлуатації	Низька	Середня	Низька

18

Порівняльний аналіз серверних платформ

Характеристика	Dell PowerEdge R740	HPE ProLiant DL380 Gen10	Lenovo ThinkSystem SR650
Процесори	До 2 x Intel Xeon Scalable (до 28 ядер кожен)	До 2 x Intel Xeon Scalable (до 28 ядер кожен)	До 2 x Intel Xeon Scalable (до 28 ядер кожен)
Оперативна пам'ять	До 3 ТБ DDR4	До 3 ТБ DDR4	До 3 ТБ DDR4
Кількість дисконних відсівів	До 24 x 2.5" SAS/SATA/SSD	До 24 x 2.5" SAS/SATA/SSD	До 24 x 2.5" SAS/SATA/SSD
Мережеві інтерфейси	4 x 1GbE (вбудовані) + опціональні	4 x 1GbE (вбудовані) + опціональні	2 x 1GbE (вбудовані) + опціональні
Резервні компоненти	Блоки живлення, вентилятори	Блоки живлення, вентилятори	Блоки живлення, вентилятори
Вбудовані механізми безпеки	TPM 2.0, Secure Boot, System Lockdown	TPM 2.0, Secure Boot, Silicon Root of Trust	TPM 2.0, Secure Boot, Lenovo ThinkShield
Віддалене управління	iDRAC9 Enterprise	HPE iLO 5 Advanced	Lenovo XClarity Controller
MTBF (годин)	>100 000	>100 000	>100 000
Сертифікати безпеки	FIPS 140-2, CC	FIPS 140-2, CC	FIPS 140-2
Енергоефективність	80 PLUS Platinum (до 94%)	80 PLUS Titanium (до 96%)	80 PLUS Platinum (до 94%)

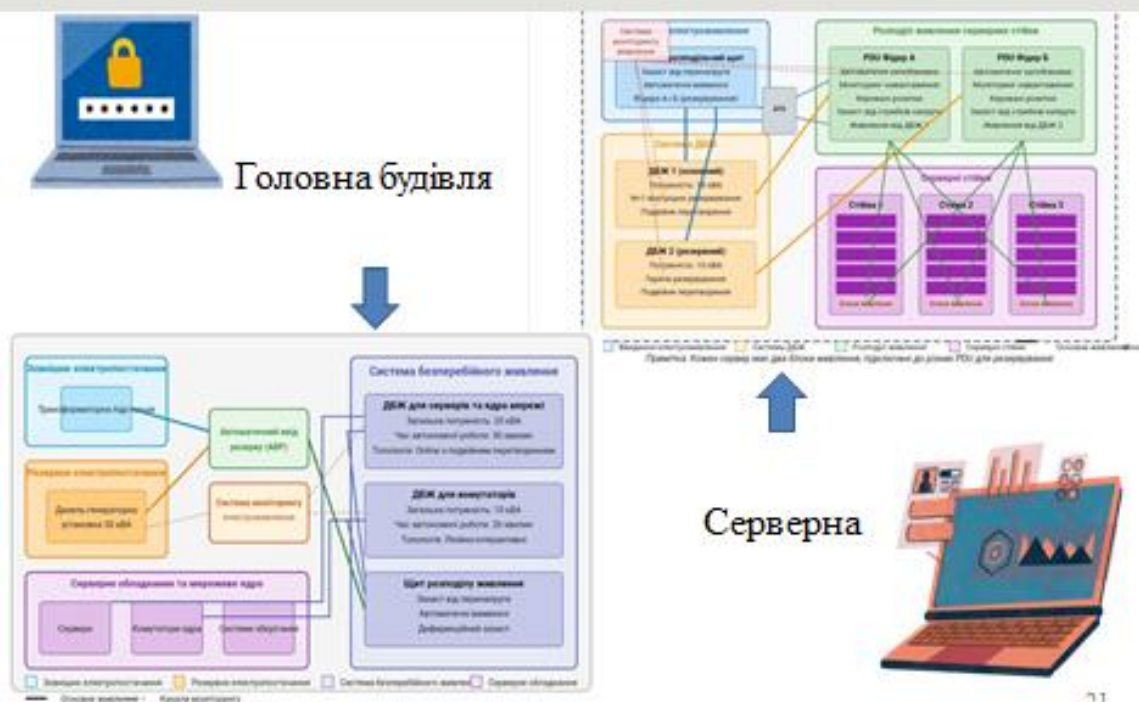
19

Розрахунок енергоспоживання обладнання закритої мережі

Тип обладнання	Кількість, шт.	Потужність в одиниці, Вт	Загальна потужність, Вт	Коефіцієнт запасу	Розрахункова потужність, Вт
Комутатори ядра	2	1100	2200	1,3	2860
Комутатори розподілу	6	715	4290	1,3	5577
Комутатори доступу (48 портів)	13	440	5720	1,3	7436
Комутатори доступу (24 порти)	8	250	2000	1,3	2600
Міжмережеві екрани	4	350	1400	1,3	1820
Сервери (основні)	6	750	4500	1,3	5850
Сервери (резервні)	3	750	2250	1,3	2925
Системи зберігання даних	2	800	1600	1,3	2080
Системи моніторингу та безпеки	1	500	500	1,3	650
Загальна потужність	24460		31798		

20

Схема системи безперебійного живлення для головної будівлі та серверної



ТИПИ СИСТЕМ МОНИТОРІНГУ ТА КЕРУВАННЯ МЕРЕЖЕЮ

Порівняльний аналіз

Тип системи	Основні функції	Приклади	Особливості застосування
Системи моніторингу продуктивності мережі	Збір та аналіз даних про пропускну здатність, затримку, втрати пакетів	Zabbix, Nagios, PRTG, SolarWinds NPM	Необхідно забезпечити надійність системи моніторингу від зовнішніх мереж, використовувати захищені протоколи збору даних
Системи виявлення та запобігання вторгнень (IDS/IPS)	Моніторинг мережевого трафіку для виявлення підозрілої активності, блокування атак	Snort, Suricata, Cisco FirePOWER	Потребують регулярного оновлення сигнатур атак, важливе правильне розміщення сенсорів у ключових точках мережі
Системи управління мережевими пристроями	Централізована конфігурація та управління мережевими обладнаннями	Cisco DNA Center, HPE IMC, ManageEngine OpManager	Необхідно забезпечити надійну аутентифікацію та авторизацію адміністраторів, шифрування управлінського трафіку
Системи аналізу мережевого трафіку	Глибокий аналіз мережевих пакетів, виявлення аномалій	Wireshark, Netflow Analyzer, ntopng	Потребують значних обчислювальних ресурсів, важливо забезпечити захист отриманих даних
Системи управління конфігурацією	Автоматизація процесів налаштування та підтримки консистентності конфігурацій	Ansible, Puppet, Chef, SaltStack	Критично важливо забезпечити контроль цілісності шаблонів конфігурацій та перевірку логів перед застосуванням
Системи управління подіями та інцидентами безпеки (SIEM)	Централізований збір та аналіз журналів, кореляція подій безпеки	Splunk, IBM QRadar, ArcSight, Elastic Stack	Вимагають потужних обчислювальних ресурсів, необхідно забезпечити надійне зберігання та захист журналів
Системи управління доступом до мережі (NAC)	Контроль доступу пристроїв до мережі на основі політик	Cisco ISE, Fortinet, Aruba ClearPass	Критично важливі для запобігання несанкціонованому доступу, необхідна інтеграція з іншими системами безпеки

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ЗАКРИТИХ МЕРЕЖАХ

Рівень моделі OSI	Методи захисту	Приклади засобів	Основні загрози
Фізичний рівень	Екранування кабелів, фізичне розмежування, контроль доступу до обладнання	Екрановані кабелі, системи контролю доступу, датчики вторгнення	Фізичне втручання, перехоплення електромагнітного випромінювання
Канальний рівень	Шифрування на рівні каналу, фільтрація MAC-адрес, сегментація мережі	MACsec (IEEE 802.1AE), комутатори з функцією порт security	MAC-спуфінг, атаки типу "людинок посередній"
Мережевий рівень	Шифрування IP-трафіку, міжмережні екрани, системи виявлення вторгнень	IPsec, апаратні міжмережні екрани, IDS/IPS системи	IP-спуфінг, DDoS-атаки, несанкціонований доступ
Транспортний рівень	Захищені транспортні протоколи, фільтрація портів	TLS-SSL, DTLS, міжмережні екрани рівня додатків	TCP SYN flood, UDP flood, аналіз трафіку
Сеансовий рівень	Керування сеансами, автентифікація	Kerberos, системи єдиного входу (SSO)	Перехоплення сеансу, підбір паролів
Представницький рівень	Шифрування даних додатків, захист від шкідливого коду	Системи шифрування файлів, антивірусне ПЗ	Витік даних, атаки на шифрування
Прикладний рівень	Контроль доступу до додатків, захищені протоколи прикладного рівня	HTTPS, SSH, S/MIME, системи DLP	Атаки на веб-додатки, фішинг, соціальна інженерія

23

Основні рекомендації з експлуатації закритої мережі

Категорія	Рекомендація	Критичність (1-5)	Періодичність виконання
Адміністрування	Використовувати принцип найменших привілеїв при наданні доступу	5	Постійно
Адміністрування	Документувати всі зміни в конфігурації обладнання	4	При кожній зміні
Безпека	Регулярно оновлювати програмне забезпечення та мікрокод обладнання	5	Щомісяця
Безпека	Проводити аудит безпеки та тести на проникнення	4	Щоквартально
Безпека	Контролювати фізичний доступ до мережевого обладнання	5	Постійно
Моніторинг	Аналізувати журнали подій на предмет підозрілої активності	4	Щодня
Моніторинг	Контролювати продуктивність мережі та використання ресурсів	3	Щодня
Резервування	Регулярно створювати резервні копії конфігурацій	5	Щотижня та при зміні
Резервування	Тестувати відновлення з резервних копій	4	Щомісяця
Навчання	Забезпечувати регулярне навчання адміністраторів	4	Щоквартально
Документація	Підтримувати актуальність документації	3	При кожній зміні
Обслуговування	Проводити профілактичне обслуговування обладнання	4	За графіком

24

ВИСНОВКИ

У дипломній роботі було вирішено комплекс науково-практичних завдань, пов'язаних з проектуванням, розробкою та тестуванням закритої мережі, що відповідає підвищеним вимогам до надійності та інформаційної безпеки.

