

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПISKA

до випускної кваліфікаційної роботи бакалавра

на тему: «**Проект захищеної PON-мережі
підприємства критичної інфраструктури**»

Виконав: студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»



Роман КОПЕНСОВ

Керівник: завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент



Андрій ЄФІМЕНКО

Рецензент: старший викладач кафедри комп'ютерної
інженерії та кібербезпеки



Ігор ФАЛЬКОВСЬКИЙ

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Коренєв Роман Петрович

Тема роботи: **«Проект захищеної PON-мережі підприємства критичної інфраструктури»**

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 9 червня 2024 р.

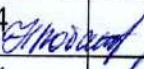
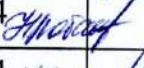
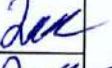
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Топологія мережі
2. Постачальники мережевого обладнання

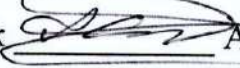
Обладнання та програмне забезпечення:

1. Cisco Packet Tracer
2. Juniper SRX 100

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Надія Лобанчикова	06.03.2024 	06.03.2024 
2	Надія Лобанчикова	10.04.2024 	10.04.2024 
3	Надія Лобанчикова	07.05.2024 	07.05.2024 

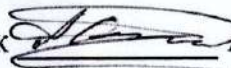
Студент  Роман КОРЕНЄВ

Керівник  Андрій ЄФІМЕНКО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 березня 2024	Виконано
2	Розробка плану проєкту	7- 15 березня 2024	Виконано
3	Вибір програмного забезпечення	15-22 березня 2024	Виконано
4	Пошук теоретичної інформації	22-29 березня 2024	Виконано
5	Розробка проєкту	29 березня - 8 квітня 2024	Виконано
6	Вибір обладнання	8 – 22 квітня 2024	Виконано
7	Створення в програмному додатку проєкту	22-30 квітня 2024	Виконано
8	Створення в програмному додатку схеми для тестування захисту	30 квітня - 10 травня 2024	Виконано
9	Тестування проєкту	10- 17 травня 2024	Виконано
10	Оформлення пояснювальної записки та презентації	17 травня-31 травня 2024	Виконано
11	Отримання відгуку та рецензії	3-7 червня 2024	Виконано
12	Захист кваліфікаційної роботи	Відповідно до графіку	Виконано

Студент  Роман КОРЕНЧ

Керівник  Андрій ЄФІМЕНКО

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра на тему «Проект захищеної PON-мережі підприємства критичної інфраструктури» складається з вступу, трьох розділів, висновків, списку використаної літератури та додатку.

Основна текстова частина викладена на 54 сторінках друкованого тексту.

Пояснювальна записка має 16 сторінок додатків. Список використаних джерел містить 28 найменування і займає 3 сторінки. В роботі наведено 17 рисунків. Загальний обсяг роботи – 80 сторінок.

У першому розділі було розглянуто основи мережної архітектури, теоретичну інформацію про протоколи та технології.

У другому розділі розглянуто основні етапи та особливості проекту. Розроблено фізичну та логічну топологію, систему адресації, допоміжну інфраструктуру, підсистеми захисту.

У третьому розділі вибрано обладнання. Проведено налагодження обладнання. Проведено тестування складових елементів.

Висновок містить в собі результати виконаної роботи проектування мережі (захищеної PON-мережі) підприємства критичної інфраструктури.

У додатках представлено схему мережі, конфігураційні файли обладнання.

Ключові слова: PON-МЕРЕЖА, КРИТИЧНА ІНФРАСТРУКТУРА, БЕЗПЕКА.

					КІК.КР.Б - 125 - 11 - КБ			
Зм.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Коренев Р.П.	<i>[підпис]</i>	16.06.	Проект захищеної PON-мережі підприємства критичної інфраструктури Пояснювальна записка	Літ.	Арк.	Аркушів
Керівник		Єфіменко А.А.	<i>[підпис]</i>	16.06.			4	80
Реценз.		Фальковський І.	<i>[підпис]</i>			ФІКТ, Гр. КБ-20-2		
Н. контр.		Єфіменко А.А.	<i>[підпис]</i>	15.06.				
Затверд.		Єфіменко А.А.	<i>[підпис]</i>	15.06.				

ANNOTATION

The explanatory note for the bachelor's qualification work on the topic "Project of a secured PON network for a critical infrastructure enterprise" consists of an introduction, three chapters, conclusions, a list of references, and an appendix.

The text part is presented on 54 pages of printed text.

The explanatory note has 16 pages of appendices. The list of references contains 28 items and takes up 3 pages. The work includes 17 figures. The total volume of the work is 81 pages.

The first chapter examines the basics of network architecture, theoretical information about protocols and technologies.

The second chapter covers the main stages and features. Physical and logical topology, addressing system, auxiliary infrastructure, and protection subsystems have been developed.

The third chapter focuses on equipment selection. Equipment setup has been carried out. Testing of the constituent elements has been conducted.

The conclusion contains the results of the completed work on designing a network (secured PON network) for a critical infrastructure enterprise.

The appendices present the network diagram and equipment configuration files.

Keywords: PON NETWORK, CRITICAL INFRASTRUCTURE, SECURITY.

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ ЗАХИЩЕНОЇ PON-МЕРЕЖІ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ	10
1.1 Огляд технології пасивної оптичної мережі (PON)	10
1.2 Основні принципи побудови мереж для критичної інфраструктури	15
1.3 Вимоги до серверних кімнат, серверних стійок та оптичної інфраструктури для PON-мереж	20
1.4 Види кібератак, що становлять загрозу для мережі	24
1.5 Види кіберінцидентів природнього та техногенного характеру, що становлять небезпеку для мережі та засоби профілактики	32
Висновки до першого розділу	33
РОЗДІЛ 2 РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОЇ PON-МЕРЕЖІ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ	34
2.1 Особливості та етапи створення проєкту захищеної PON-мережі підприємства критичної інфраструктури	34
2.2 Розробка схеми адресації	36
2.3 Розробка допоміжної сервісної інфраструктури та підсистем захисту	38
Висновки до другого розділу	39
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ	40
3.1 Вибір обладнання та програмного забезпечення для розробки проєкту	40
3.2 Базове налагодження мережних пристроїв	45
3.3 Налagodження засобів підсистем захисту	50
3.4 Тестування складових елементів захищеної мережі	55
Висновки до третього розділу	59
ВИСНОВКИ	60
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	61
ДОДАТКИ	64

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA – authentication, authorization, accounting

DHCP – Dynamic Host Configuration Protocol

OLT - Оптичний лінійний термінал

ONT - Оптичні мережеві термінали

PON – PassiveOpticalNetwork

SSH – Secure SHell

VLAN – Virtual Local Area Network

ЦОД - центр обробки даних

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми зумовлена критичною важливістю забезпечення надійної та захищеної передачі даних для підприємств критичної інфраструктури, таких як енергетичні компанії, транспортні системи, телекомунікаційні оператори та інших. Ці організації відіграють життєво важливу роль у функціонуванні суспільства та економіки, тому їх мережева інфраструктура повинна бути стійкою до різних загроз та кібератак.

Технологія пасивної оптичної мережі (PON) дозволяє передавати дані на великі відстані з високою швидкістю та надійністю, використовуючи оптоволоконні кабелі. Проте, для підприємств критичної інфраструктури важливо забезпечити не лише швидкість та ефективність, а й належний рівень безпеки. Саме тому проєкт захищеної PON-мережі є актуальним та необхідним для забезпечення безперебійної роботи підприємств критичної інфраструктури.

Метою кваліфікаційної роботи є проєктування захищеної PON-мережі для підприємства критичної інфраструктури.

Визначена мета обумовлює наступні завдання:

- аналіз необхідних технологій, протоколів та методів, що використовуються для побудови захищених PON-мереж;
- розгляд існуючих рішень та обладнання для створення захищених PON-мереж;
- проєктування захищеної PON-мережі з урахуванням вимог безпеки та надійності;
- моделювання та тестування спроєктованої мережі.

Об'єктом дослідження є процес проєктування захищеної PON-мережі для підприємства критичної інфраструктури, технології та методи забезпечення безпеки.

Предметом дослідження є архітектура захищеної PON-мережі, протоколи та механізми захисту, а також обладнання та рішення провідних виробників, таких як Cisco, Juniper, BDCOM та інші.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

У процесі виконання кваліфікаційної роботи розроблено проєкт захищеної PON-мережі для підприємства критичної інфраструктури з використанням емуляторів та симуляторів, таких як Cisco Packet Tracer та GNS3. Реалізовано підсистеми захисту, протестовано їх роботу та проаналізовано ефективність запропонованих рішень.

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ ЗАХИЩЕНОЇ PON-МЕРЕЖІ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Огляд технології пасивної оптичної мережі (PON)

Пасивна оптична мережа (PON) – це телекомунікаційна технологія, яка використовує оптичне волокно для передачі даних між оптичним лінійним терміналом (OLT) та декількома оптичними мережевими терміналами (ONT). PON працює за принципом точка-багатоточка, де один OLT з'єднується з багатьма ONT за допомогою оптичного розгалужувача [1-28].

1. Основні переваги PON [24,25]:

- висока швидкість передачі даних;
- економічна ефективність;
- велика відстань передачі (до 20 км без регенерації сигналу);
- масштабованість.

2. Вимоги до безпеки PON-мереж для підприємств критичної інфраструктури. Підприємства критичної інфраструктури мають підвищені вимоги до безпеки своїх мереж, зокрема вони включають:

- конфіденційність даних;
- цілісність даних;
- доступність;
- автентифікація та контроль доступу;
- моніторинг та аудит;
- фізична безпека.

3. Архітектура захищеної PON-мережі. Типова архітектура захищеної PON-мережі для підприємства критичної інфраструктури включає:

- захищений центр обробки даних (ЦОД);
- оптичний лінійний термінал (OLT);
- оптичні мережеві термінали (ONT);
- систему управління безпекою;
- резервні канали зв'язку;

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

- систему резервного копіювання та відновлення даних.

4. Технології та протоколи для побудови PON мережі критичної інфраструктури. Для забезпечення високого рівня надійності, безпеки та стійкості до збоїв можна використовувати наступні технології та протоколи [23-25]:

- Технологія хвильового мультиплексування WDM.
- Резервування оптичних ліній.
- Стекування комутаторів OLT.
- Протокол VLAN.
- Протоколи QoS.
- Шифрування даних.
- Системи моніторингу і управління.

5. Топології PON-мереж. Вибір оптимальної топології залежить від конкретних умов проєктування. Можливі топології включають, рис.1.1 [1]:

- дерево;
- зірка;
- кільце;
- кожен з кожним;
- шина;
- осередки;
- лінійка;
- точка-точка.

6. Архітектурні рішення для різних сценаріїв. Вибір архітектури залежить від щільності розміщення абонентів:

- FTTB (Fiber to the Building) - для багатоповерхових житлових будинків.
- FTTC (Fiber to the Curb) або FTTH (Fiber to the Home) - для приватної забудови або офісів, залежно від потреб замовника.

7. Забезпечення безперервності роботи. Для забезпечення безперервної роботи критичної інфраструктури важливо реалізувати:

- Автоматичне перемикання на резервні канали.

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

- Швидке відновлення зв'язку у разі збоїв.
- Балансування навантаження між обладнанням.
- Пріоритезацію критичного трафіку.

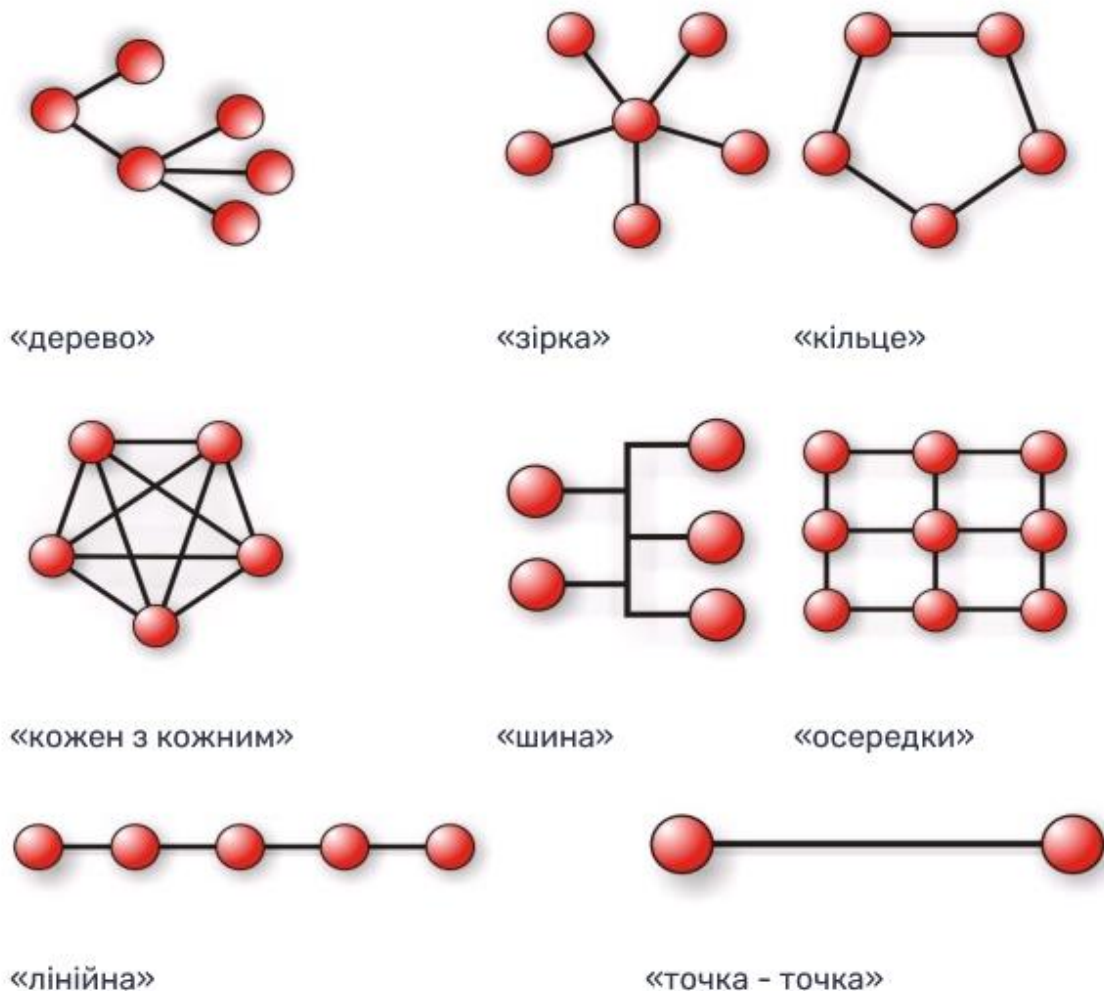


Рисунок 1.1 – Схематичне зображення топології PON-мереж

8. Захист від кібератак [2-6, 14-16]. Для захисту від кібератак необхідно:
- Впровадити систему виявлення та запобігання вторгнень (IDS/IPS).
 - Проводити регулярне оновлення програмного забезпечення.
 - Проводити періодичне навчання персоналу з питань кібербезпеки.
 - Проводити регулярні аудити безпеки.

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Управління доступом та ідентифікацією. Для забезпечення належного рівня безпеки важливо впровадити ефективну систему управління доступом та ідентифікацією, зокрема:

- Використовувати багатофакторну автентифікацію.
- Впровадити систему управління привілеями користувачів.
- Проводити регулярний аудит та перегляд прав доступу.
- Застосовувати принцип найменших привілеїв.

10. Шифрування даних в PON-мережах. Для захисту конфіденційності інформації, що передається через PON-мережу необхідним є:

- Використання сучасних алгоритмів шифрування (наприклад, AES-256).
- Впровадження захищених протоколів передачі даних (SSL/TLS).
- Забезпечення безпечного управління ключами шифрування.
- Регулярна зміна ключів шифрування.

11. Моніторинг та аналіз безпеки. Для своєчасного виявлення та реагування на загрози безпеці необхідним є:

- Впровадження системи збору та аналізу логів (SIEM).
- Використання засобів поведінкового аналізу мережі.
- Створення центру оперативного реагування на інциденти (SOC).
- Проведення регулярних тестів на проникнення.

12. Фізична безпека PON-інфраструктури [23-25]. Захист фізичних компонентів мережі є критично важливим, тому необхідним є:

- Забезпечення контролю доступу до приміщень з обладнанням.
- Встановлення систем відеоспостереження.
- Використання датчиків несанкціонованого доступу до обладнання.
- Захист оптичних ліній від фізичного пошкодження.

13. Резервування та відмовостійкість. Для забезпечення безперервності роботи критичної інфраструктури необхідним є:

- Впровадження географічно розподілених резервних центрів обробки даних.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Використання технологій автоматичного перемикавання на резервні канали.

- Забезпечення резервного живлення для критичного обладнання.

- Регулярне тестування процедур відновлення після збоїв.

14. Управління змінами та оновленнями. Для мінімізації ризиків, пов'язаних зі змінами в мережевій інфраструктурі рекомендоване:

- Впровадження формалізованого процесу управління змінами.

- Тестування оновлень перед впровадженням у виробниче середовище.

- Створення процедур швидкого відкату змін у разі виникнення проблем.

- Регулярне оновлення програмного забезпечення та прошивок обладнання.

- Навчання та підвищення кваліфікації персоналу. Людський фактор відіграє ключову роль у забезпеченні безпеки, тому необхідним є проведення регулярних тренінгів з кібербезпеки для співробітників; навчання персоналу щодо виявлення та реагування на інциденти безпеки; створення культури безпеки в організації; регулярне оновлення знань технічного персоналу щодо нових загроз та методів захисту

15. Відповідність нормативним вимогам. Для забезпечення відповідності законодавчим та галузевим стандартам необхідним є:

- Регулярний аудит на відповідність вимогам (наприклад, ISO 27001, GDPR).

- Впровадження процесів для забезпечення постійної відповідності.

- Документування всіх процедур та політик безпеки.

- Регулярне оновлення політик безпеки відповідно до змін у законодавстві.

16. Планування безперервності бізнесу. Для забезпечення швидкого відновлення роботи у разі серйозних інцидентів необхідним є:

- Розробка та регулярне оновлення плану безперервності бізнесу.

- Проведення регулярних тестувань плану відновлення після аварій.

- Визначення критичних бізнес-процесів та їх пріоритезація.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

- Створення процедур кризового управління.

Провівши огляд технології пасивної оптичної мережі, розглянемо основні принципи побудови мереж для критичної інфраструктури[1].

1.2 Основні принципи побудови мереж для критичної інфраструктури

Під критичною інфраструктурою зазвичай розуміють системи та ресурси, життєво важливі для підтримки основних функцій суспільства, економіки та безпеки держави. До критичної інфраструктури можна віднести енергетичні системи, транспортні мережі, системи зв'язку, банківський сектор, системи водопостачання та очищення стічних вод, системи охорони здоров'я та багато іншого. Порухення функціонування цих систем може мати катастрофічні наслідки для населення та економіки [1, 17,23-25, 28].

Тому при побудові мереж для критичної інфраструктури необхідно дотримуватися низки принципів, які забезпечать надійність, безпеку та стійкість цих мереж до різноманітних загроз та збоїв [1-6]. Ці принципи включають:

1. Надійність (Reliability).
2. Резервування (Redundancy).
3. Безпека (Security).
4. Стійкість (Resilience).
5. Масштабованість (Scalability).
6. Керованість (Manageability).

Надійність є одним з найважливіших принципів при побудові мереж для критичної інфраструктури. Це означає, що мережа повинна забезпечувати безперервну та стабільну роботу, мінімізуючи ризик збоїв та відмов. Для досягнення високої надійності необхідно використовувати високоякісне обладнання та компоненти від перевірених виробників, а також ретельно планувати та реалізовувати мережеву архітектуру.

1. Надійність (Reliability):

- Використання надлишкових компонентів (резервних джерел живлення, модулів, кабелів тощо).

		Корень Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

- Застосування стійких до збоїв топологій мережі (наприклад, кільце або сітка).
- Впровадження систем моніторингу та оповіщення про несправності.
- Регулярне технічне обслуговування та оновлення обладнання та програмного забезпечення.
- Використання систем безперебійного живлення (UPS) для захисту від відключень електроенергії.
- Забезпечення належного охолодження та захисту від зовнішніх факторів (вологість, пил, температура тощо).

2. Резервування (Redundancy). Резервування є ключовим принципом при побудові мереж для критичної інфраструктури, адже воно забезпечує можливість безперервної роботи системи у випадку відмови одного або декількох її компонентів. Резервування може бути реалізоване на різних рівнях, включаючи:

- Резервування каналів зв'язку (наприклад, використання декількох різних маршрутів або носіїв для передачі даних).
- Резервування мережевого обладнання (наприклад, використання резервних маршрутизаторів, комутаторів або серверів).
- Резервування центрів обробки даних (наприклад, створення резервного ЦОД на відстані від основного).

Для забезпечення ефективного резервування необхідно передбачити механізми автоматичного перемикавання на резервні компоненти у разі виникнення збоїв. Ці механізми можуть включати:

- Протоколи маршрутизації з підтримкою резервування (наприклад, VRRP, HSRP).
- Технології резервування каналів зв'язку (наприклад, MPLS, DWDM).
- Кластеризацію та реплікацію серверів та баз даних.

3. Безпека (Security) [2-6, 13, 16, 17]. Забезпечення безпеки є критично важливим для мереж критичної інфраструктури, оскільки вони є потенційними цілями для кібератак, шпигунства та саботажу. Порушення безпеки таких мереж може мати катастрофічні наслідки для функціонування систем життєзабезпечення,

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

економіки та національної безпеки. Для забезпечення безпеки необхідно впровадити комплексний підхід, який включає:

- Фізичну безпеку (контроль доступу, відеоспостереження, охорона об'єктів).
- Мережеву безпеку (брандмауери, системи виявлення та запобігання вторгнень, шифрування даних).
- Безпеку додатків та систем (оновлення програмного забезпечення, контроль привілеїв користувачів, аудит дій).
- Безпеку персоналу (перевірка співробітників, навчання з питань безпеки, політики безпеки).
- Планування на випадок інцидентів (плани реагування, відновлення після інцидентів).

Важливо також регулярно проводити аудити безпеки, тестування на проникнення та оцінку ризиків для своєчасного виявлення та усунення вразливостей.

4. Стійкість (Resilience). Стійкість є здатністю мережі продовжувати функціонувати та відновлюватися після збоїв, аварій або навмисних атак. Для забезпечення стійкості необхідно передбачити механізми, які дозволять мережі адаптуватися до змін та швидко відновлюватися після інцидентів. Деякі ключові аспекти забезпечення стійкості:

- Використання розподілених та децентралізованих архітектур, які не мають єдиної точки відмови.
- Впровадження механізмів автоматичного відновлення та перемаршрутизації трафіку.
- Створення резервних копій критичних даних та систем в географічно віддалених локаціях.
- Забезпечення можливості швидкого розгортання тимчасових рішень (наприклад, мобільних базових станцій або резервних каналів зв'язку).
- Використання модульних та масштабованих рішень, які можна легко змінювати або розширювати.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Стійкість також тісно пов'язана з принципами надійності та резервування, адже саме ці фактори дозволяють мережі продовжувати функціонувати та відновлюватися після збоїв.

5. Масштабованість (Scalability). Принцип масштабованості передбачає, що мережа повинна мати можливість легко розширюватися та адаптуватися до зростаючих вимог та навантажень. Це особливо важливо для мереж критичної інфраструктури, оскільки з часом збільшуються вимоги до пропускної здатності, кількості підключених пристроїв та нових додатків. Деякі ключові аспекти забезпечення масштабованості:

- Використання модульних та розширюваних архітектур мереж та систем.
- Застосування технологій віртуалізації для ефективного використання обчислювальних ресурсів.
- Впровадження хмарних рішень для забезпечення гнучкого масштабування ресурсів.
- Використання протоколів та технологій, які підтримують масштабування (наприклад, MPLS, IPv6).
- Забезпечення можливості легкого додавання нових вузлів, сегментів або розширення існуючих компонентів.
- Планування майбутніх потреб та вимог на етапі проєктування мережі.

Масштабованість також тісно пов'язана з принципом керованості, оскільки ефективне управління та моніторинг є критично важливими для забезпечення належного функціонування масштабованих мереж.

6. Керованість (Manageability). Керованість є важливим принципом для забезпечення ефективної роботи та підтримки мереж критичної інфраструктури. Це включає в себе можливість централізовано контролювати, конфігурувати та моніторити всі компоненти мережі. Деякі ключові аспекти забезпечення керованості:

- Використання систем централізованого управління та моніторингу мережею (Network Management Systems, NMS).

		Корень Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

- Впровадження стандартизованих протоколів управління (SNMP, NETCONF, RESTCONF).
- Забезпечення уніфікованого інтерфейсу управління для різноманітного обладнання та систем.
- Автоматизація процесів розгортання, конфігурування та оновлення мережевих компонентів.
- Збір та аналіз статистичних даних про роботу мережі для виявлення проблем та оптимізації.
- Інтеграція систем управління з системами моніторингу безпеки та інцидентами.

Належна керованість дозволяє оперативно реагувати на інциденти, проводити профілактичне обслуговування та вносити необхідні зміни в конфігурацію мережі для забезпечення її безперебійної роботи.

Стандарти та рекомендації [13-20]. При побудові мереж для критичної інфраструктури також важливо дотримуватися відповідних стандартів та рекомендацій. Ось деякі ключові з них:

1. ISO/IEC 27001 "Information technology - Security techniques - Information security management systems - Requirements" - стандарт, що визначає вимоги до системи управління інформаційною безпекою.

2. ISO/IEC 27002 "Information technology - Security techniques - Code of practice for information security controls" - стандарт, що містить рекомендації щодо практичного впровадження заходів безпеки.

3. NIST SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" - набір вказівок та рекомендацій від Національного інституту стандартів та технологій США (NIST) щодо безпеки інформаційних систем.

4. IEC 62443 "Industrial communication networks - Network and system security" - серія стандартів безпеки для промислових мереж та систем автоматизації.

5. ITU-T X.805 "Security architecture for systems providing end-to-end communications" - рекомендації Міжнародного союзу електрозв'язку (ITU) щодо архітектури безпеки для кінцевих комунікаційних систем.

		Корень Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

6. CPNI (Centre for the Protection of National Infrastructure) - набір рекомендацій та кращих практик з питань безпеки національної критичної інфраструктури від Великобританії.

На наступному етапі розглянемо вимоги до серверних кімнат, серверних стійок та оптичної інфраструктури для роn-мереж [18].

1.3 Вимоги до серверних кімнат, серверних стійок та оптичної інфраструктури для роn-мереж

1. Вимоги до серверних кімнат та серверних стійок. Серверні кімнати та стійки відіграють ключову роль у забезпеченні належного функціонування центрів обробки даних (ЦОД) та ІТ-інфраструктури організацій. Вони повинні відповідати суворим вимогам для захисту критично важливого обладнання та забезпечення безперебійної роботи систем. Ось основні вимоги, які необхідно враховувати при проектуванні та експлуатації серверних кімнат та стійок [2-6]:

1. Фізична безпека:

- Контрольовані та обмежені зони доступу з використанням систем контролю доступу (СКУД), як-от карткових замків, біометричних систем тощо.
- Система відеоспостереження для моніторингу та запису всіх дій у серверній кімнаті.
- Надійні замки, металеві двері та стіни, що захищають від несанкціонованого проникнення.
- Наявність сигналізації та системи виявлення вторгнень.

2. Захист від природних та техногенних загроз:

- Розташування в безпечній зоні, що не підпадає під ризики повеней, землетрусів або інших стихійних лих.
- Захист від пожеж, включаючи системи виявлення та гасіння пожеж (газові, водяні або інші), протипожежні стіни та двері.
- Захист від електромагнітних завад та блискавок.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

- Надійна система вентиляції та кондиціонування для підтримки оптимальної температури та вологості.

3. Енергопостачання та резервне живлення:

- Надійне та стабільне енергопостачання з декількома незалежними лініями живлення.
- Система безперебійного живлення (ДБЖ) для забезпечення безперервної роботи обладнання у випадку збоїв електропостачання.
- Резервні генератори для забезпечення тривалого автономного живлення в разі тривалих відключень електроенергії.
- Моніторинг та управління системами електроживлення для своєчасного виявлення та усунення проблем.

4. Охолодження та кондиціонування:

- Потужна система кондиціонування повітря для підтримання оптимальної температури та вологості в серверній кімнаті.
- Резервні системи охолодження для забезпечення безперебійної роботи у випадку відмови основної системи.
- Моніторинг температури та вологості для своєчасного виявлення проблем та регулювання систем охолодження.
- Належна вентиляція та розподіл потоків повітря для ефективного охолодження обладнання.

5. Структуровані кабельні системи:

- Використання стандартизованих кабельних систем для передачі даних, живлення та інших сигналів.
- Належне маркування та організація кабелів для полегшення обслуговування та пошуку несправностей.
- Достатня місткість кабельних трас та коробів для розміщення майбутніх кабелів та додаткового обладнання.
- Використання кабельних лотків, коробів або підлог для організації та захисту кабелів.

6. Серверні стійки та шафи:

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- Стандартизовані серверні стійки та шафи для розміщення серверів, мережевого обладнання та систем зберігання даних.
- Достатня місткість для розміщення необхідного обладнання з урахуванням майбутнього розширення.
- Належна вентиляція та охолодження стійок для відведення тепла від обладнання.
- Організована прокладка кабелів усередині стійок для забезпечення належного охолодження та полегшення обслуговування.
- Стійки повинні бути надійно закріплені до підлоги або стіни для запобігання перекиданню.

7. Моніторинг та управління інфраструктурою:

- Централізована система моніторингу та управління всіма компонентами інфраструктури серверної кімнати, включаючи системи електроживлення, охолодження, безпеки тощо.
- Збір та аналіз даних про стан обладнання, температуру, вологість, споживання енергії тощо.
- Система оповіщень про критичні події та несправності для своєчасного реагування.
- Можливість віддаленого моніторингу та управління для полегшення обслуговування.

8. Резервування та відмовостійкість:

- Резервування критичних компонентів інфраструктури, таких як системи електроживлення, охолодження, зв'язку тощо.
- Використання відмовостійких конфігурацій обладнання та систем для забезпечення безперебійної роботи у випадку відмови окремих компонентів.
- Наявність резервних ЦОД або серверних кімнат на віддалених майданчиках для забезпечення безперервності бізнес-процесів.

9. Дотримання стандартів та нормативів:

- Дотримання відповідних стандартів та нормативних вимог, таких як TIA-942, BICSI, NFPA та інших.

		Корень Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

- Впровадження кращих практик та рекомендацій галузевих організацій, таких як Uptime Institute, ANSI/TIA тощо.
- Регулярні аудити та сертифікація відповідності вимогам безпеки, надійності та ефективності.

2. Вимоги до інфраструктури для pon-мереж:

1. Оптичне волокно:

- Використання одномодового оптичного волокна (SMF) для PON-мереж.
- Дотримання стандартів ITU-T G.652 або G.657 для волокна.
- Забезпечення захисту волокна від механічних пошкоджень та впливу навколишнього середовища.
- Регулярна перевірка цілісності та якості оптичних ліній.

2. Оптичні сплітери (розгалужувачі):

- Вибір сплітерів з відповідним коефіцієнтом розгалуження (1:32, 1:64 тощо).
- Забезпечення низьких втрат сигналу на сплітерах (типово <3.7 дБ для 1:32).
- Використання каскадного з'єднання сплітерів для оптимізації мережевої архітектури.
- Розміщення сплітерів у захищених боксах або шафах для захисту від зовнішніх впливів.

3. Процес зварювання оптики:

- Використання спеціалізованого обладнання для зварювання оптичних волокон.
- Забезпечення чистоти та правильної підготовки волокон перед зварюванням.
- Дотримання технології зварювання для мінімізації втрат на зварних з'єднаннях (типово <0.1 дБ).
- Захист зварних з'єднань за допомогою термоусадкових гільз або касет.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

- Проведення тестування якості зварних з'єднань за допомогою рефлектометра (OTDR).

4. Оптичні роз'єми та патч-корди:

- Використання стандартизованих оптичних роз'ємів (SC, LC тощо) відповідно до вимог обладнання.
- Забезпечення чистоти оптичних роз'ємів для мінімізації втрат та відбиття сигналу.
- Використання якісних патч-кордів з низькими втратами для з'єднання обладнання.

5. Тестування та діагностика оптичної мережі:

- Проведення вимірювань оптичної потужності на різних ділянках мережі.
- Використання оптичного рефлектометра (OTDR) для визначення характеристик лінії та локалізації пошкоджень.
- Регулярна перевірка бюджету втрат оптичної лінії для забезпечення надійної роботи PON-мережі.

6. Документація оптичної інфраструктури:

- Створення та підтримка актуальної схеми оптичної мережі.
- Маркування всіх оптичних компонентів для полегшення обслуговування.
- Ведення журналу змін та обслуговування оптичної інфраструктури.

Проведемо аналіз кібератак, що становитимуть загрози для мережі об'єктів критичної інфраструктури[19][20].

1.4 Види кібератак, що становлять загрозу для мережі

У сучасному світі, де більшість процесів та систем залежать від інформаційних технологій та мереж, забезпечення кібербезпеки стає критично важливим завданням. Зловмисники постійно вдосконалюють свої методи атак, намагаючись отримати несанкціонований доступ до конфіденційних даних, порушити роботу систем чи навіть захопити повний контроль над мережами та

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

пристроями [2-6]. Розуміння різних видів кіберінцидентів та кібератак є ключовим для розробки ефективних стратегій захисту та мінімізації ризиків. У цьому розділі ми розглянемо основні види загроз, з якими можуть зіткнутися мережі організацій.

1. Зловмисне програмне забезпечення (Malware). Зловмисне програмне забезпечення, або малвар (malware), є одним із найпоширеніших видів кібератак. Воно включає різноманітні шкідливі програми, такі як віруси, черв'яки, троянські коні, шпигунське програмне забезпечення (spyware), програми для крадіжки даних (keyloggers) та багато інших. Метою малвару може бути крадіжка конфіденційних даних, шпигунство, порушення роботи систем або отримання неправомірного доступу до мережі та ресурсів. Види малвару:

- Віруси: Це шкідливі програми, які самореплікуються та поширюються, інфікуючи інші файли чи системи.
- Черв'яки: Автономні програми, які здатні самостійно поширюватися через мережі та інтернет, використовуючи вразливості в програмному забезпеченні.
- Троянські коні: Зловмисні програми, які маскуються під легітимні додатки, але насправді виконують шкідливі дії, такі як надання зловмиснику віддаленого доступу до системи.
- Ransomware: Шкідливе програмне забезпечення, яке шифрує дані на пристрої або мережі та вимагає викуп за їх розшифрування.
- Роткіти: Програми, які дозволяють зловмисникам отримати повний контроль над системою, обходячи механізми безпеки.
- Бекдори: Таємні "лазівки" в програмному забезпеченні, які дозволяють обійти стандартні механізми автентифікації та отримати несанкціонований доступ.

2. Фішинг та соціальна інженерія. Фішинг та соціальна інженерія є методами, які використовують психологічні прийоми для обману користувачів і змушення їх розкрити конфіденційну інформацію або вчинити певні дії, які можуть скомпрометувати безпеку мережі. Види фішингових атак:

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

- Електронний фішинг: Розсилка підроблених електронних листів, які імітують легітимні джерела (наприклад, банки чи соціальні мережі), з метою викрасти облікові дані користувачів.
- Веб-фішинг: Створення підроблених веб-сайтів, які імітують справжні сайти, для крадіжки даних, що вводяться користувачами.
- Фішинг через SMS: Розсилка шахрайських SMS-повідомлень із зловмисними посиланнями або інструкціями.
- Фішинг через голосові дзвінки: Зловмисники телефонують жертві, видаючи себе за представників легітимних організацій, і намагаються отримати конфіденційні дані.

Соціальна інженерія може включати різноманітні методи психологічного впливу, такі як імітація авторитетних джерел, створення відчуття терміновості, використання соціальних зв'язків або апелювання до почуття допомоги.

3. Атаки відмови в обслуговуванні (DDoS). Атаки відмови в обслуговуванні (Distributed Denial of Service, DDoS) спрямовані на перевантаження мережевих ресурсів або систем шляхом генерації величезної кількості трафіку або неправомірних запитів. Це може призвести до переривання роботи сервісів, веб-сайтів або навіть повного виведення з ладу мережевої інфраструктури. Види DDoS-атак:

- Об'ємні атаки: Генерація величезної кількості мережевого трафіку, яка перевищує пропускну здатність каналів зв'язку або можливості обробки трафіку мережевими пристроями.
- Атаки на протоколи: Експлуатація вразливостей у мережевих протоколах для генерації великої кількості підроблених запитів, які важко відфільтрувати.
- Атаки на рівень додатків: Генерація величезної кількості запитів до веб-додатків або інших сервісів, що призводить до вичерпання ресурсів серверів.

4. Атаки на програми та веб-додатки. Веб-додатки та інші програмні рішення часто стають вразливими точками для зловмисників через наявність

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

вразливостей у кодi. Атаки на додатки можуть призвести до витоку даних, несанкціонованого доступу до систем або навіть повного компрометування мережі.

Види атак на програми та веб-додатки:

- Ін'єкції: Введення шкідливого коду в додатки через невалідовані вхідні дані, що може призвести до витоку даних або отримання контролю над системою.
- Міжсайтовий скриптинг (XSS): Вставка зловмисного коду у веб-сайти через вразливості, що дозволяє викрадення облікових даних, сеансів користувачів або виконання шкідливих дій в браузері.
- Несанкціоноване тестування на проникнення: Зловмисники використовують різноманітні інструменти та методи для виявлення вразливостей у додатках та систем захисту.
- Підбір облікових даних: Автоматизовані атаки з метою підбору паролів або обхід механізмів автентифікації в додатках.

5. Атаки на бездротові мережі. Бездротові мережі можуть бути особливо вразливими до певних видів атак через їх відкритий характер та broadcast-природу передачі даних. Ось деякі поширені типи атак на бездротові мережі:

- Перехоплення трафіку (Sniffing): Зловмисники використовують інструменти для перехоплення та аналізу бездротового трафіку, що може призвести до крадіжки конфіденційних даних, таких як паролі, номери кредитних карток тощо.
- Злам паролів (Cracking): Використання спеціалізованих програм та методів для підбору паролів і отримання несанкціонованого доступу до бездротових мереж, обладнання та ресурсів.
- Спуфінг (Spoofing): Підміна MAC-адрес або IP-адрес для маскування під легітимні пристрої або створення підробленої точки доступу для перехоплення трафіку.
- Атаки відмови в обслуговуванні (DoS): Генерація великої кількості бездротового трафіку або зловмисних запитів для перевантаження точок доступу або блокування доступу легітимним користувачам.

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

- Злам WEP/WPA ключів: Атаки на протоколи шифрування бездротових мереж, такі як WEP або WPA, з метою отримання ключів шифрування та доступу до мережі.
- Атаки з бічним каналом: Використання фізичних характеристик бездротового сигналу, таких як час прибуття пакетів або відбитки потужності сигналу, для визначення місця розташування пристроїв або отримання інформації про трафік.
- Підслуховування (Eavesdropping): Пасивне перехоплення бездротового трафіку в зоні покриття точки доступу для збору конфіденційної інформації.

6. Атаки на мережеве обладнання. Мережеве обладнання, таке як маршрутизатори, комутатори та брандмауери, є критичними компонентами будь-якої мережі. Зловмисники можуть намагатися експлуатувати вразливості в цьому обладнанні для отримання несанкціонованого доступу, перехоплення трафіку або навіть повного компрометування мережі. Види атак на мережеве обладнання:

- Експлуатація вразливостей: Використання відомих вразливостей у програмному забезпеченні мережевих пристроїв для отримання доступу або виконання шкідливого коду.
- Злам паролів адміністратора: Підбір або крадіжка паролів адміністраторів для отримання повного контролю над мережевим обладнанням.
- Відмова в обслуговуванні (DoS): Генерація великої кількості запитів або некоректних пакетів, що призводить до перевантаження або відмови роботи мережевих пристроїв.
- Маршрутний перехват (Route Hijacking): Маніпуляція таблицями маршрутизації для перенаправлення мережевого трафіку через підконтрольні зловмисникам системи.
- MITM-атаки (Man-in-the-Middle): Перехоплення та модифікація мережевого трафіку між двома сторонами для крадіжки даних або вставки шкідливого вмісту.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

- Злам протоколів управління: Експлуатація вразливостей у протоколах управління мережевим обладнанням, таких як SNMP, для несанкціонованого доступу або зміни конфігурацій.

7. Внутрішні загрози. Не всі загрози для мережі походять ззовні – деякі можуть виникати і від співробітників або колишніх працівників організації. Ці внутрішні загрози можуть бути навмисними або ненавмисними, але їх наслідки часто є серйозними. Види внутрішніх загроз:

- Зловмисні інсайдери: Співробітники, які навмисно зловживають своїми привілеями для крадіжки даних, саботажу систем або отримання несанкціонованого доступу з корисливих мотивів чи помсти.
- Неуважні користувачі: Співробітники, які через неуважність або недостатню обізнаність про безпеку порушують політики та процедури, що може призвести до витоку даних або компрометації систем.
- Фішингові атаки на співробітників: Зловмисники можуть використовувати соціальну інженерію для обману співробітників і змушення їх розкрити конфіденційну інформацію або надати доступ до систем.
- Втрата або крадіжка пристроїв: Втрата або крадіжка мобільних пристроїв, ноутбуків або носіїв даних співробітниками може призвести до витоку або несанкціонованого доступу до конфіденційної інформації.
- Неавторизований доступ до ресурсів: Співробітники можуть намагатися обійти існуючі механізми контролю доступу для отримання несанкціонованого доступу до систем або даних, до яких вони не мають дозволу.

8. Загрози для критичної інфраструктури. Критична інфраструктура, така як системи енергопостачання, транспортні мережі, системи зв'язку та комунальні служби, є особливо вразливою до кібератак. Порушення їх роботи може мати катастрофічні наслідки для суспільства та економіки. Види загроз для критичної інфраструктури:

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

- Кібершпигунство та кібершахрайство: Зловмисники можуть намагатися викрасти конфіденційні дані або інтелектуальну власність, пов'язану з критичною інфраструктурою.
- Кібератаки з метою саботажу: Навмисні атаки на системи управління та контролю критичної інфраструктури з метою порушення їх роботи або нанесення фізичної шкоди.
- Кібертероризм: Використання кібератак для залякування або нанесення шкоди критичній інфраструктурі з політичних, ідеологічних або екстремістських мотивів.
- Апаратні вразливості: Експлуатація вразливостей у апаратному забезпеченні обладнання, вбудованих систем або мікросхем, що використовуються в інфраструктурі.

Атаки на системи управління промисловими процесами (ICS/SCADA): Зловмисники можуть намагатися отримати несанкціонований доступ або втрутитися в роботу систем управління промисловими процесами (ICS/SCADA), які контролюють критично важливу інфраструктуру.

- Компрометація ланцюжків постачання: Зловмисники можуть впроваджувати шкідливий код або апаратні "вістря" на ранніх етапах виробництва обладнання, щоб згодом використати їх для атак на критичну інфраструктуру.

Захист критичної інфраструктури є пріоритетним завданням для урядів та організацій через потенційно катастрофічні наслідки кібератак у цій сфері. Необхідно вживати жорсткі заходи безпеки, проводити регулярні аудити та впроваджувати передові технології захисту.

9. Атаки на Інтернет речей (IoT) [3,5]. Із зростанням кількості підключених пристроїв, таких як розумні будинки, гаджети та промислові датчики, Інтернет речей (IoT) стає новою сферою для кіберзагроз. Ці пристрої часто мають обмежені можливості безпеки та можуть бути вразливими до різних видів атак. Види атак на Інтернет речей (IoT):

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

- Ботнети IoT: Зловмисники можуть заражати та контролювати великі мережі вразливих IoT-пристроїв для здійснення атак відмови в обслуговуванні або інших кібератак.
- Атаки за допомогою підробленого трафіку: Генерація підробленого трафіку для обману або перевантаження IoT-пристроїв та систем.
- Експлуатація вразливостей: Використання відомих вразливостей у прошивці, програмному забезпеченні або протоколах зв'язку IoT-пристроїв для отримання несанкціонованого доступу або виконання шкідливого коду.
- Крадіжка даних: Перехоплення та крадіжка конфіденційних даних, що передаються між IoT-пристроями та хмарними сервісами.
- Злам системи управління пристроями: Отримання контролю над системами управління та моніторингу великих мереж IoT-пристроїв для несанкціонованих дій.
- Атаки на фізичну безпеку: Зловмисники можуть намагатися отримати фізичний доступ до IoT-пристроїв для підключення шкідливого обладнання або внесення змін у конфігурацію.

Захист екосистеми Інтернету речей вимагає комплексного підходу з урахуванням особливостей та обмежень цих пристроїв, а також впровадження відповідних механізмів автентифікації, шифрування та оновлення безпеки.

Цей список не є вичерпним, оскільки злочинці постійно розробляють нові методи атак та експлуатації вразливостей. Важливо регулярно оновлювати знання про актуальні кіберзагрози, впроваджувати передові засоби захисту та приділяти належну увагу питанням кібербезпеки для захисту критичних мереж та систем від потенційних інцидентів [8, 11, 12].

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

1.5 Види кіберінцидентів природного та техногенного характеру, що становлять небезпеку для мережі та засоби профілактики

Існує кілька видів кіберінцидентів природного та техногенного характеру, які можуть становити загрозу для мережі:

1. Природні катастрофи (повені, урагани, землетруси тощо):

- Можуть призвести до фізичного пошкодження обладнання та мережевої інфраструктури.
- Спричинити відключення електроенергії та порушення зв'язку.

2. Техногенні аварії (пожежі, вибухи, витоки шкідливих речовин):

- Здатні пошкодити або знищити обладнання центрів обробки даних та мережеві компоненти.
- Створити небезпечні умови, що унеможливлюють доступ персоналу для обслуговування.

3. Відмови обладнання та програмного забезпечення:

- Збої в роботі серверів, маршрутизаторів, комутаторів можуть порушити мережевий зв'язок.
- Помилки в програмному забезпеченні можуть призвести до відмови або некоректної роботи систем.

Засоби профілактики та захисту:

1. Резервне копіювання даних та обладнання, планування відновлення після аварій.
2. Використання надійних та резервних джерел живлення (генератори, акумулятори).
3. Розміщення критичної інфраструктури в безпечних приміщеннях зі стійкими конструкціями.
4. Регулярне оновлення програмного забезпечення та обладнання.
5. Моніторинг стану мережі та своєчасне виявлення проблем.
6. Навчання персоналу діям в надзвичайних ситуаціях.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

7. Укладання угод про надання послуг з альтернативними провайдерами.

8. Впровадження відмовостійких топологій мережі та резервування каналів зв'язку.

Дотримання цих заходів допоможе зменшити ризики та наслідки кіберінцидентів природного та техногенного характеру для мережі.

Висновки до першого розділу

Проведено огляд технології пасивної оптичної мережі в результаті якого виявлено переваги та недоліки, а також особливості побудови. Розглянуто теоретичні засади, проблем та нюанси які можуть виникнути під час проектування PON-мережі.

Розглянуто особливості побудови комп'ютерних мереж для об'єктів критичної інфраструктури в результаті якого визначено основні принципи побудови таких мереж.

Проведено аналіз найімовірніших загроз для мережі об'єкту критичної інфраструктури, що дозволило виділити основні напрямки захисту при подальшому проєктуванні.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 2 РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОЇ PON-МЕРЕЖІ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Особливості та етапи створення проєкту захищеної PON-мережі підприємства критичної інфраструктури.

Для створення проєкту захищеної PON-мережі підприємства критичної інфраструктури, що виробляє ключові вузли для промисловості, доцільно розглянути такі зони та структуру, рис.2.1:

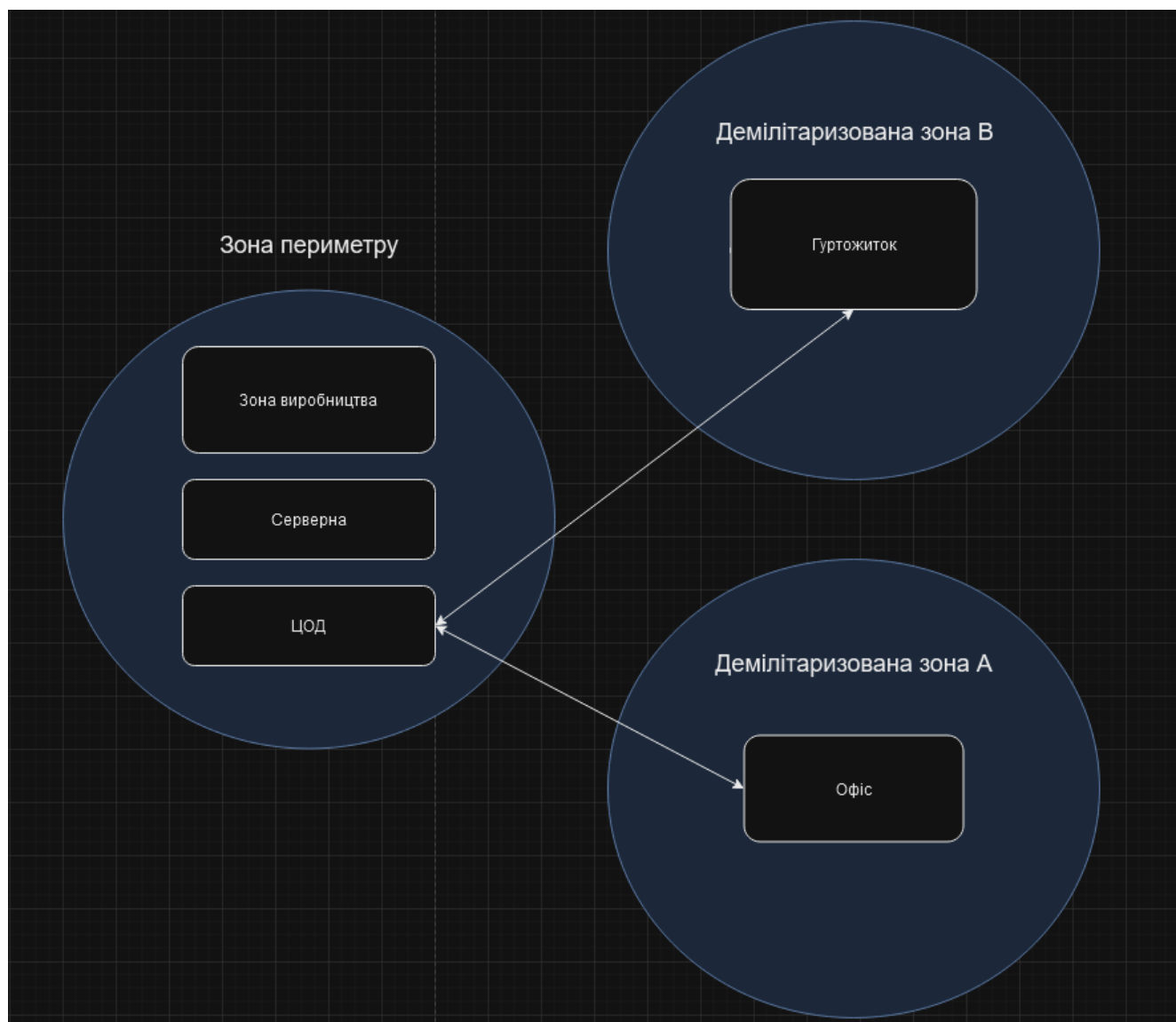


Рисунок 2.1 – Підприємство критичної інфраструктури зображене у вигляді зон

1. Зона виробництва. Ця зона має включати мережеві підключення для виробничих ліній, промислових контролерів, систем управління виробництвом

		Коренев Р.П.			<i>КІК.КР.Б – 125 – 11 – КБ</i>	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

(SCADA) та інших критичних систем, задіяних у виробничому процесі. Слід забезпечити високий рівень захисту та ізоляцію цієї зони від інших мереж для запобігання втручанню та порушенню виробничого процесу.

2. Зона офісних приміщень. Ця зона має охоплювати мережеві підключення для офісних комп'ютерів, серверів, принтерів та іншого офісного обладнання. Рівень безпеки в цій зоні може бути дещо нижчим, ніж у виробничій зоні, але все одно потрібно забезпечити належний захист від зовнішніх загроз.

3. Зона периметру. Ця зона повинна включати мережеві підключення для систем контролю доступу, відеоспостереження, охоронної сигналізації та інших систем безпеки об'єкта. Необхідно забезпечити високий рівень захисту та ізоляції цієї зони для недопущення несанкціонованого доступу та маніпуляцій.

4. Демілітаризована зона. Ця зона призначена для розміщення публічно доступних ресурсів, таких як веб-сервери, сервери електронної пошти тощо. Також має бути ізольована як від внутрішніх мереж підприємства, так і від зовнішніх мереж для забезпечення додаткового рівня безпеки.

5. Центр обробки даних. Ця зона повинна включати мережеві підключення для серверів, систем зберігання даних, резервного копіювання та відновлення. Центр обробки даних потребує високого рівня фізичного та логічного захисту для збереження цілісності та конфіденційності критичних даних.

6. Зона управління мережею. Ця зона призначена для розміщення обладнання управління мережею, таких як маршрутизатори, комутатори, системи моніторингу та управління. Необхідно забезпечити надійний захист цієї зони, оскільки вона є центральною точкою управління всією мережевою інфраструктурою.

Топологія мережі представлена на рис.2.2. Кожна зона повинна бути ізольована та мати свій рівень безпеки відповідно до чутливості даних та критичності операцій, що в ній виконуються. Крім того, потрібно врахувати канали зв'язку між зонами та застосувати відповідні заходи безпеки, такі як міжмережеві екрани, системи виявлення вторгнень, шифрування трафіку тощо.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

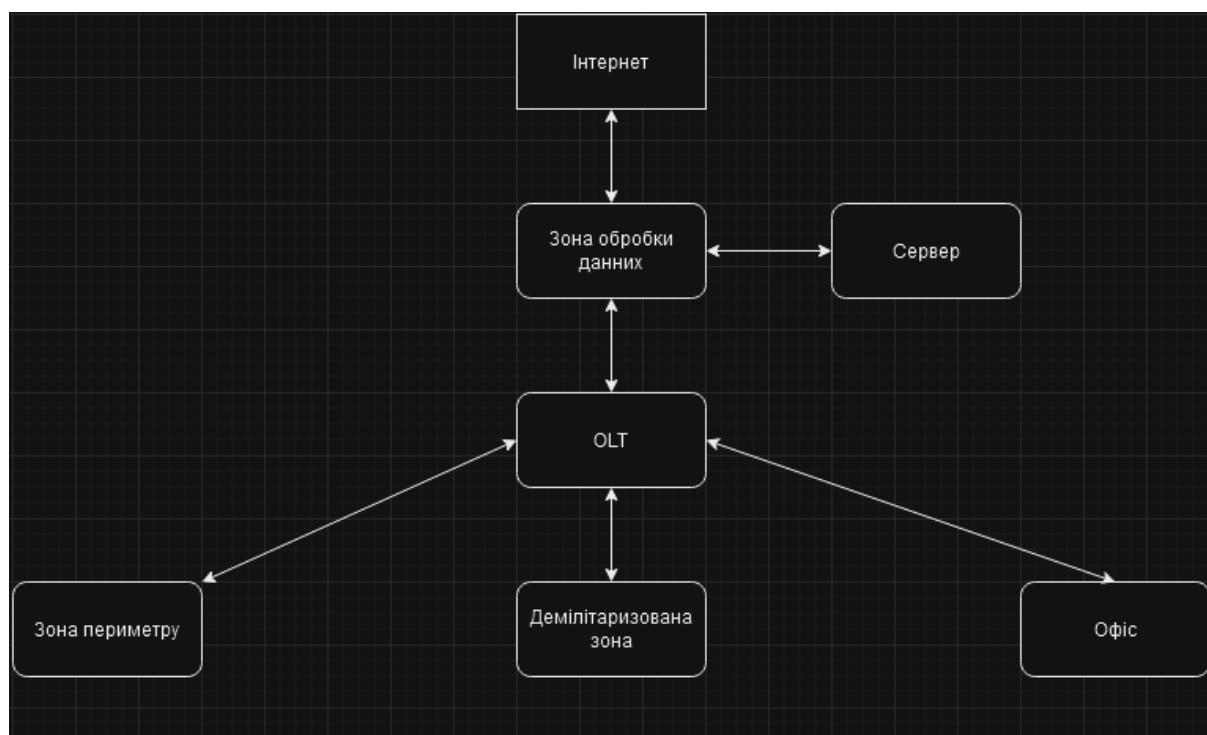


Рисунок 2.2 – Топологія мережі

Загалом, структура захищеної PON-мережі має бути спроектована з урахуванням принципів сегментації, захисту периметру, багаторівневої безпеки та відповідності нормативним вимогам для забезпечення належного рівня захисту критичної інфраструктури підприємства.

2.2 Розробка схеми адресації

Спочатку назначимо IP адреси для серверу, Juniper, та OLT. При розробці мережі для обладнання бажано використовувати адреси з одного діапазону.

Таблиця 2.1

Назва мережі	Призначення	Адреса мережі	Маска	Префікс
A	ЦЗД – SR-1	192.168.20.2	255.255.255.0	/24
B	ЦОД – R-1	192.168.20.8	255.255.255.0	/24
C	OLT – R-2	192.168.20.10	255.255.255.0	/24

Далі назначимо діапазон адрес для кожної зони підприємства критичної інфраструктури.

Таблиця 2.2

Назва мережі	Адреса мережі	Маска	Префікс
DZ-A	192.168.101.0	255.255.255.0	/24
DZ-B	192.168.102.0	255.255.255.0	/24
Office	192.168.103.0	255.255.255.0	/24
Production zone	192.168.111.0	255.255.255.0	/24
Perimeter zone	192.168.100.0	255.255.255.0	/24
Management	192.168.11.0	255.255.255.0	/24

Комутаційне обладнання буде налаштоване на отримання статичної IP-адреси в межах VLAN, призначеного для управління мережевими пристроями. Це забезпечить стабільний та передбачуваний доступ до обладнання для цілей віддаленого адміністрування та моніторингу.

Натомість, кінцеві користувачі отримуватимуть IP-адреси динамічно за допомогою протоколу DHCP (Dynamic Host Configuration Protocol). DHCP-сервер буде автоматично призначати доступні адреси з визначеного пулу, а також надавати додаткову мережеву інформацію, таку як адреси DNS-серверів та шлюз за замовчуванням.

Така конфігурація дозволить:

1. Забезпечити надійний доступ до мережевого обладнання для адміністраторів.
2. Спростити управління адресами для великої кількості користувацьких пристроїв.
3. Зменшити ймовірність конфліктів IP-адрес.
4. Полегшити масштабування мережі при додаванні нових пристроїв.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Додатково можна налаштувати резервування адрес на DHCP-сервері для певних пристроїв, які потребують стабільної адреси, але не є частиною комутаційного обладнання.

2.3 Розробка допоміжної сервісної інфраструктури та підсистем захисту

Для забезпечення надійного та безпечного функціонування PON-мережі підприємства критичної інфраструктури необхідно розробити допоміжну сервісну інфраструктуру та впровадити ефективні підсистеми захисту. У рамках проєкту допоміжна інфраструктура включатиме систему аутентифікації AAA (Authentication, Authorization, Accounting) з використанням RADIUS-сервера. Це забезпечить централізоване управління доступом до мережевих ресурсів, підтримку багатофакторної аутентифікації для підвищення безпеки та ведення журналів доступу та аудиту для моніторингу активності користувачів. Крім того, буде реалізовано пряме підключення до ядра мережі для надання доступу до інтернету пристроям в офісі, що забезпечить високошвидкісне та надійне з'єднання з впровадженням механізмів фільтрації та моніторингу трафіку.

Щодо підсистем захисту, проєкт передбачає налаштування інтерфейсів рівня доступу на маршрутизаторах для розділення користувачів від адресного простору комутаторів та впровадження механізмів ізоляції та сегментації мережі. Буде налаштовано віддалений доступ до пристроїв з використанням RADIUS-сервера для аутентифікації та авторизації, обмеження доступу до пристроїв мережею офісу та впровадження шифрованих протоколів для віддаленого управління.

Особлива увага приділяється захисту комутаторів від поширених атак. Це включає захист від MAC-Flooding через впровадження Port Security та обмеження кількості MAC-адрес на порт, захист від MAC-Spoofing з використанням Dynamic ARP Inspection та IP Source Guard, захист від атак на протоколи STP/PVST+ шляхом налаштування BPDU Guard та Root Guard, а також захист від ARP-атак та атак на DHCP.

Специфічні заходи захисту для PON-мережі включають шифрування даних на рівні PON з використанням AES, впровадження механізмів автентифікації

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

ONT/ONU, моніторинг оптичної потужності для виявлення несанкціонованих підключень та використання ізольованих VLAN для різних груп користувачів або служб.

Проект також передбачає впровадження систем моніторингу та виявлення вторгнень, включаючи IDS/IPS, SNMP-моніторинг для збору інформації про стан мережевих пристроїв та використання систем аналізу логів та поведінки мережі для виявлення аномалій.

У рамках цього проекту розроблено комплексний підхід до забезпечення безпеки PON-мережі підприємства критичної інфраструктури. Розроблена допоміжна інфраструктура та підсистеми захисту враховують специфіку PON-технології та забезпечують високий рівень захисту від найпоширеніших методів атак. Впроваджені механізми дозволяють не лише захистити мережу, але й забезпечити її надійне функціонування та можливість моніторингу для своєчасного виявлення та реагування на потенційні загрози.

Висновки до другого розділу

Спроектовано схему підприємства критичної інфраструктури. Виділено зони, зокрема зону виробництва, офісних приміщень, периметру, демітаризовану зону, а центр обробки даних та зону управління мережею. Розроблено топологію мережі на основі прийнятих проєктних рішень.

Визначено адреси для обладнання та виділено діапазони IP адрес для спроектованих зон. Розроблено допоміжну сервісну інфраструктуру та запропоновані підсистеми захисту. Проведені дії дозволять управляти мережею за рахунок її впорядкування.

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ

3.1 Вибір обладнання та програмного забезпечення для розробки проєкту

При розгортанні захищеної PON-мережі підприємства критичної інфраструктури необхідно ретельно підійти до вибору обладнання від перевірених виробників. Провідними компаніями в цій галузі є Cisco Systems, Juniper Networks, Huawei Technologies, D-Link Systems, Inc, Mikrotik, BDCOM.

Cisco є беззаперечним лідером в області мережевих технологій. Їхні рішення охоплюють магістральну маршрутизацію, комутацію, віртуалізацію центрів обробки даних, відеотехнологію та архітектури для цифрової трансформації бізнесу.

Juniper Networks спеціалізується на високопродуктивних маршрутизаторах, комутаторах, міжмережевих екранах та магістральному обладнанні для дата-центрів. Їхні продукти відрізняються високими показниками безпеки, надійності та масштабованості.

Huawei пропонує новітні телекомунікаційні мережі наступного покоління з широким спектром індивідуальних рішень для клієнтів.

Компанії MikroTik та D-Link відомі своїми якісними маршрутизаторами та точками доступу з підтримкою PoE за доступною ціною.

BDCOM є постачальником економічно-ефективних мережевих рішень, орієнтованих на провайдерів, великі підприємства та державні структури.

Для зони обробки даних візьмемо SRX4100 Firewall (рисунок 3.1). Брандмауер нового покоління (NGFW) SRX4100 захищає невеликі та середні кампуси, центри обробки даних і мережі регіональних штаб-квартир. Енергоефективний пристрій розміром 1 U забезпечує пропускну здатність брандмауера до 90 Гбіт/с на стійку та підтримує інтерфейси 100 Гбіт/с із шифруванням MACsec на швидкості з'єднання для захисту даних у русі.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

SRX4100 об'єднує мережу та безпеку в одній платформі. Він має вбудовані можливості нульової довіри, інтеграцію EVPN-VXLAN і AI Predictive Threat Prevention для надвисокої ефективності безпеки. Централізовано керований Juniper Security Director Cloud, SRX4100 забезпечує високопродуктивну IPsec VPN і єдине керування політикою для надійного захисту вашої мережі.

Брандмауер SRX4100 є невід'ємною частиною архітектури розподілених послуг Connected Security від Juniper і дає можливість організаціям запровадити нульову довіру в своїх мережах.



Рисунок 3.1 – Зовнішній вигляд SRX4100

Як ОЛТ візьмемо термінал BDCOM P3600-08E (рисунок 3.2). BDCOM P3600-08E - це керований комутатор рівня 2+, призначений для використання в корпоративних мережах та мережах провайдерів. Ось його основні характеристики:

1. Порти:
 - 8 портів 10/100/1000Base-T (гігабітні Ethernet порти);
 - 2 комбо-порти SFP для підключення оптичних модулів.
2. Продуктивність:
 - Пропускна здатність: 20 Gbps;
 - Швидкість пересилання пакетів: 14.88 Mpps;

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

- Таблиця MAC-адрес: 8K записів.



Рисунок 3.2 – Зовнішній вигляд BDCOM P3600-08E

3. Функції Layer 2+:

- Підтримка VLAN (802.1Q, до 4K VLAN ID);
- Spanning Tree Protocol (STP, RSTP, MSTP);
- Link Aggregation (LACP);
- IGMP Snooping для multicast.

4. Якість обслуговування (QoS):

- 4 черги пріоритетів на порт;
- Підтримка 802.1p CoS та DSCP.

5. Безпека:

- Port Security;
- 802.1X аутентифікація;
- ACL (Access Control Lists).

6. Управління:

- Web-інтерфейс;
- CLI (Command Line Interface)№
- SNMP v1/v2c/v3№
- RMON.

7. Фізичні характеристики:

- Форм-фактор: настільний або для монтажу в стійку;
- Розміри: 440 мм x 180 мм x 44 мм (ШxГxВ);
- Живлення: AC 100-240V, 50/60Hz.

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

8. Додаткові функції:

- Підтримка Jumbo frames до 9К байт;
- DHCP Snooping;
- Дзеркалювання портів.

Цей комутатор підходить для створення надійних та ефективних локальних мереж, забезпечуючи високу продуктивність та гнучкість налаштування для різноманітних мережевих сценаріїв.

У випадку, якщо необхідно забезпечити маршрутизацію та безпеку у одному пристрої, або фінансова спроможність дозволяє можна використати Juniper ACX5448- AC (рисунок 3.3).



Рисунок 3.3 – Зовнішній вигляд Juniper ACX5448-AC

Оптичний модуль можна обрати Picotel EPON OLT SFP PX20 (рисунок 3.4) він має наступні характеристики:

- Технологія: EPON.
- Довжина хвилі передавача: 1490 nm.
- Довжина хвилі приймача 1310 nm.
- Форм-фактор: SFP (Small Form-factor Pluggable).
- Оптичний роз'єм: SC/UPC.
- Потужність передавача (TX): +5 dBm ~ +8 dBm.
- Чутливість приймача (RX): -33 dBm.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43



Рисунок 3.4 – Зовнішній вигляд Picotek EPON OLT SFP PX20

Оптичний термінал бажано обирати від виробника OLT як приклад Оптичний термінал BDCOM GP1702-1G 1x10/100/1000M (рисунок 3.5).



Рисунок 3.5 – Зовнішній вигляд BDCOM GP1702-1G 1x10/100/1000M
Проведемо базове налаштування обраного обладнання.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

3.2 Базове налагодження мережних пристроїв

Для початку налаштуємо базову маршрутизацію на рівні ОЛТ за схемою на рисунку 3.6

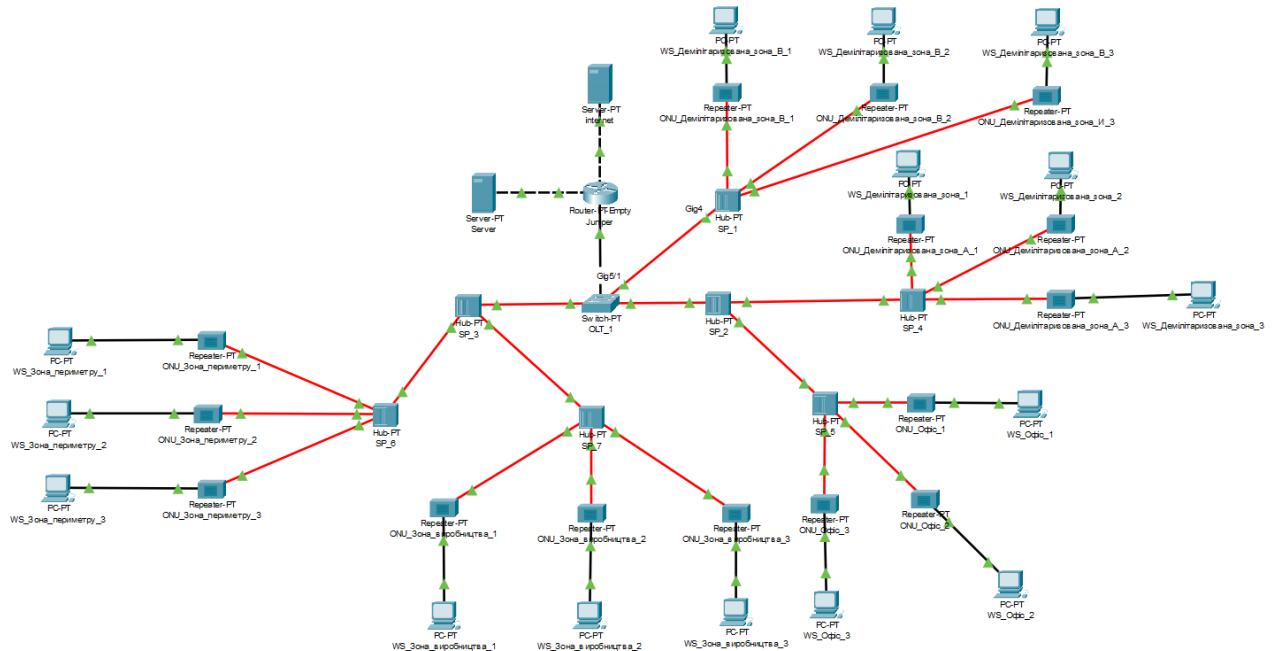


Рисунок 3.6 – Схема мережі підприємства критичної інфраструктури.

Базове налагодження пристроїв включає налаштування основних протоколів та технологій обладнання для забезпечення передачі інформації у мережі. Це критичний етап, який забезпечує основну функціональність та безпеку мережі.

Розглянемо налаштування маршрутизатора Juniper:

1. Налаштування інтерфейсів:

```
Juniper>enable
```

```
Juniper#configure terminal
```

```
Juniper(config)#interface GigabitEthernet6/0.1
```

```
Juniper(config-subif)#encapsulation dot1Q 111
```

```
Juniper(config-subif)#ip address 192.168.111.1 255.255.255.0
```

```
Juniper(config-subif)#exit
```

```
Juniper(config)#interface GigabitEthernet6/0.2
```

```
Juniper(config-subif)#encapsulation dot1Q 100
```

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Juniper(config-subif)#ip address 192.168.100.1 255.255.255.0
Juniper(config-subif)#exit
Juniper(config)#interface GigabitEthernet6/0.3
Juniper(config-subif)#encapsulation dot1Q 102
Juniper(config-subif)#ip address 192.168.102.1 255.255.255.0
Juniper(config-subif)#exit
Juniper(config)#interface GigabitEthernet7/0
Juniper(config-if)#ip address 8.8.4.5 255.0.0.0
Juniper(config-if)#exit

```

Ці налаштування створюють підінтерфейси на GigabitEthernet6/0, кожен з яких відповідає окремій VLAN. Це дозволяє логічно розділити мережу на сегменти, покращуючи керованість та безпеку. Використання dot1Q енкапсуляції забезпечує сумісність з IEEE 802.1Q стандартом, що важливо для взаємодії з іншими мережевими пристроями.

Перевага: Сегментація мережі покращує продуктивність, спрощує управління та підвищує безпеку, дозволяючи ізолювати різні типи трафіку.

2. Налаштування віддаленого доступу:

```

Juniper(config)#aaa new-model
Juniper(config)#aaa authentication login default group radius local
Juniper(config)#aaa authentication enable default group radius local
Juniper(config)#username admin secret 5
$1$mERr$hwZUBIE0HdnNjuMKaBA400
Juniper(config)#ip ssh version 1
Juniper(config)#ip domain-name google.com
Juniper(config)#radius-server host 192.168.20.1 auth-port 1645
Juniper(config)#radius-server key Juniper123
Juniper(config)#line vty 0 4
Juniper(config-line)#password Juniper
Juniper(config-line)#login authentication default
Juniper(config-line)#transport input ssh

```

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Juniper(config-line)#exit

Ці налаштування забезпечують безпечний віддалений доступ до пристрою:

- AAA (Authentication, Authorization, and Accounting) модель забезпечує централізоване управління доступом.

- RADIUS сервер використовується для аутентифікації, що дозволяє централізовано керувати обліковими записами користувачів.

- SSH (Secure Shell) забезпечує шифрований зв'язок для віддаленого доступу.

Перевага: Централізоване управління доступом підвищує безпеку та спрощує адміністрування, особливо у великих мережах.

Тепер розглянемо налаштування комутатора OLT_1:

1. Налаштування VLAN та інтерфейсів:

OLT_1>enable

OLT_1#configure terminal

OLT_1(config)#interface GigabitEthernet3/1

OLT_1(config-if)#switchport access vlan 111

OLT_1(config-if)#switchport trunk allowed vlan 100,111

OLT_1(config-if)#switchport mode access

OLT_1(config-if)#switchport port-security

OLT_1(config-if)#switchport port-security maximum 64

OLT_1(config-if)#switchport port-security mac-address sticky

OLT_1(config-if)#exit

OLT_1(config)#interface GigabitEthernet4/1

OLT_1(config-if)#switchport access vlan 100

OLT_1(config-if)#switchport mode access

OLT_1(config-if)#switchport port-security

OLT_1(config-if)#switchport port-security maximum 64

OLT_1(config-if)#switchport port-security mac-address sticky

OLT_1(config-if)#exit

OLT_1(config)#interface GigabitEthernet5/1

OLT_1(config-if)#switchport access vlan 102

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

```

OLT_1(config-if)#switchport mode access
OLT_1(config-if)#switchport port-security
OLT_1(config-if)#switchport port-security maximum 64
OLT_1(config-if)#switchport port-security mac-address sticky
OLT_1(config-if)#exit

```

Ці налаштування конфігурують порти комутатора для роботи з різними VLAN та встановлюють базові параметри безпеки портів:

- Призначення портів до конкретних VLAN ізолює трафік різних сегментів мережі.

- Port security обмежує кількість MAC-адрес, які можуть використовувати порт, захищаючи від MAC-флудингу та несанкціонованого доступу.

Перевага: Ці налаштування значно підвищують безпеку на рівні доступу, запобігаючи несанкціонованому підключенню пристроїв та обмежуючи можливості атак.

2. Налаштування DHCP:

```

OLT_1(config)#ip dhcp pool vlan100
OLT_1(dhcp-config)#network 192.168.100.0 255.255.255.0
OLT_1(dhcp-config)#default-router 192.168.100.1
OLT_1(dhcp-config)#dns-server 8.8.8.8
OLT_1(dhcp-config)#exit
OLT_1(config)#ip dhcp pool vlan111
OLT_1(dhcp-config)#network 192.168.111.0 255.255.255.0
OLT_1(dhcp-config)#default-router 192.168.111.1
OLT_1(dhcp-config)#dns-server 8.8.8.8
OLT_1(dhcp-config)#exit
OLT_1(config)#ip dhcp pool vlan102
OLT_1(dhcp-config)#network 192.168.102.0 255.255.255.0
OLT_1(dhcp-config)#default-router 192.168.102.1
OLT_1(dhcp-config)#dns-server 8.8.8.8
OLT_1(dhcp-config)#exit

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Далі налаштуємо маршрутизацію на Juniper SRX. Варто зазначити, що комутатори Juniper притримуються політики не дозволено отже заборонено. Тому частина налаштувань систем захисту є обов'язковими для роботи маршрутизації.

1. Налаштуємо базові функції для комутатора, та створимо користувача:

```
set system host-name Juniper_SRX_100
set system time-zone Europe/Kiev
set system root-authentication encrypted-password
set system login user admin uid 2001
set system login user admin class super-user
set system login user admin authentication encrypted-password
set system services ssh
set system services telnet
set system services xnm-clear-text
set system services web-management http interface vlan.0
set system services web-management https system-generated-certificate
set system services web-management https interface vlan.0
set system syslog archive size 100k files 3
set system syslog user * any emergency
set system syslog file messages any critical
set system syslog file messages authorization info
set system syslog file interactive-commands error
set system max-configurations-on-flash 5
set system max-configuration-rollbacks 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set system ntp server 192.168.201.100
```

2. Налаштуємо інтерфейси, призначимо їм зони та vlan:

```
set interfaces fe-0/0/1 unit 0 family ethernet-switching port-mode trunk
set interfaces fe-0/0/1 unit 0 family ethernet-switching vlan members [ 7 40 ]
set interfaces fe-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/2 unit 0 family ethernet-switching vlan members vlan-trust
```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

set interfaces fe-0/0/3 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/3 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces fe-0/0/4 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/4 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces fe-0/0/5 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/5 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces fe-0/0/6 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/6 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces fe-0/0/7 unit 0 family ethernet-switching port-mode access
set interfaces fe-0/0/7 unit 0 family ethernet-switching vlan members vlan-trust
set interfaces vlan unit 0
set interfaces vlan unit 7 family inet address 192.168.167.100/24
set interfaces vlan unit 40 family inet
set routing-options static route 0.0.0.0/0 next-hop 192.168.167.254
set protocols stp
set vlans vlan-trust vlan-id 3
set vlans vlan-trust l3-interface vlan.0
set vlans vlan40 vlan-id 40
set vlans vlan40 l3-interface vlan.40
set vlans vlan7 vlan-id 7
set vlans vlan7 l3-interface vlan.7

```

На наступному етапі проведемо налаштування підсистеми захисту.

3.3 Налагодження засобів підсистем захисту

У цьому пункті розглянемо налаштування додаткових засобів безпеки, які значно підвищують захищеність мережі. Почнемо з налаштувань OLT_1:

1. Налаштування port-security:

```

interface GigabitEthernet3/1
switchport port-security
switchport port-security maximum 64

```

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

```

switchport port-security mac-address sticky
interface GigabitEthernet4/1
switchport port-security
switchport port-security maximum 64
switchport port-security mac-address sticky
interface GigabitEthernet5/1
switchport port-security
switchport port-security maximum 64
switchport port-security mac-address sticky

```

Ці налаштування обмежують кількість MAC-адрес, які можуть бути вивчені на порту, та зберігають дозволені MAC-адреси в конфігурації.

Перевага: Захист від MAC-флудингу та несанкціонованого підключення пристроїв. Це значно ускладнює проведення атак, пов'язаних з підміною MAC-адрес.

2. Налаштування захисту від ARP-атак:

```

ip arp inspection vlan 100,102,111
ip dhcp snooping vlan 100,102,111
ip dhcp snooping
interface GigabitEthernet3/1
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 250
interface GigabitEthernet4/1
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 250
interface GigabitEthernet5/1
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 250

```

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Ці налаштування активують Dynamic ARP Inspection (DAI) та DHCP snooping:

- DAI перевіряє ARP-пакети на відповідність запису в DHCP snooping базі даних, запобігаючи ARP-спуфінгу.
- DHCP snooping запобігає атакам з використанням підробних DHCP-серверів.

Перевага: Суттєво підвищує безпеку мережі, запобігаючи поширеним атакам на канальному рівні.

3. Налаштування STP захисту:

spanning-tree mode pvst

spanning-tree extend system-id

interface GigabitEthernet3/1

spanning-tree portfast

spanning-tree bpduguard enable

interface GigabitEthernet6/1

spanning-tree guard root

Ці налаштування покращують роботу протоколу Spanning Tree:

- PVST (Per-VLAN Spanning Tree) забезпечує окреме дерево STP для кожної VLAN.
- PortFast дозволяє порту швидко перейти в стан пересилання.
- BPDU Guard захищає від несанкціонованого підключення комутаторів.
- Root Guard запобігає зміні кореневого комутатора STP.

Перевага: Підвищує стабільність та безпеку мережі, запобігаючи атакам на протокол STP та прискорюючи конвергенцію мережі.

Далі налаштуємо захист на комутаторі Juniper. Налаштуємо захист (IDP, intrusion detection prevention):

set security screen ids-option untrust-screen icmp ping-death

set security screen ids-option untrust-screen ip source-route-option

set security screen ids-option untrust-screen ip tear-drop

set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024

set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200

set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

set security screen ids-option untrust-screen tcp syn-flood destination-threshold 2048

set security screen ids-option untrust-screen tcp syn-flood timeout 20

set security screen ids-option untrust-screen tcp land

Налаштування NAT для забезпечення підключення користувачів з локальної мережі до глобальної:

set security nat source rule-set trust-to-untrust from zone trust

set security nat source rule-set trust-to-untrust to zone untrust

set security nat source rule-set trust-to-untrust rule source-nat-rule match source-address 0.0.0.0/0

set security nat source rule-set trust-to-untrust rule source-nat-rule then source-nat interface

Далі налаштуємо зони та політику переходу між зонами:

set security policies from-zone trust to-zone untrust policy trust-to-untrust match source-address any

set security policies from-zone trust to-zone untrust policy trust-to-untrust match destination-address any

set security policies from-zone trust to-zone untrust policy trust-to-untrust match application any

set security policies from-zone trust to-zone untrust policy trust-to-untrust then permit

set security policies from-zone trust to-zone untrust policy our-internet-policy match source-address any

set security policies from-zone trust to-zone untrust policy our-internet-policy match destination-address any

set security policies from-zone trust to-zone untrust policy our-internet-policy match application any

set security policies from-zone trust to-zone untrust policy our-internet-policy then permit

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

set security policies from-zone untrust to-zone trust policy our-deny-policy match source-address any

set security policies from-zone untrust to-zone trust policy our-deny-policy match destination-address any

set security policies from-zone untrust to-zone trust policy our-deny-policy match application any

set security policies from-zone untrust to-zone trust policy our-deny-policy then deny

set security zones security-zone trust host-inbound-traffic system-services all

set security zones security-zone trust host-inbound-traffic protocols all

Додаємо відповідні vlan та інтерфейси до відповідних зон trust і untrust.

set security zones security-zone untrust interfaces vlan.7

set security zones security-zone untrust interfaces vlan.40

set security zones security-zone trust interfaces vlan.0

set security zones security-zone trust interfaces fe-0/0/2.0

set security zones security-zone trust interfaces fe-0/0/3.0

set security zones security-zone trust interfaces fe-0/0/4.0

set security zones security-zone trust interfaces fe-0/0/5.0

set security zones security-zone trust interfaces fe-0/0/6.0

set security zones security-zone trust interfaces fe-0/0/7.0

Налаштуємо додаткові дозволи для використання окремих додаткових протоколів та функцій:

set security zones security-zone untrust screen untrust-screen

set security zones security-zone untrust host-inbound-traffic system-services all

set security zones security-zone untrust host-inbound-traffic protocols all

set security zones security-zone untrust interfaces fe-0/0/0.0 host-inbound-traffic system-services dhcp

set security zones security-zone untrust interfaces fe-0/0/0.0 host-inbound-traffic system-services tftp

set security zones security-zone untrust interfaces fe-0/0/0.0 host-inbound-traffic system-services telnet

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

set security zones security-zone untrust interfaces fe-0/0/1.0 host-inbound-traffic system-services ping

set security zones security-zone untrust interfaces fe-0/0/1.0 host-inbound-traffic system-services telnet

На цьому ми завершили базове налаштування безпека для комутатора Juniper. Варто зазначити, що при наявності ліцензій можна додатково налаштувати антивірус, аналіз трафіку та інше.

Загалом, ці налаштування створюють багаторівневу систему захисту, яка значно підвищує безпеку мережі, зменшуючи ризики несанкціонованого доступу та різних типів мережеских атак.

3.4 Тестування складових елементів захищеної мережі

Перевіримо налаштування маршрутизації мережі почнемо з рівня комутаторів та серверів, рис.3.7.

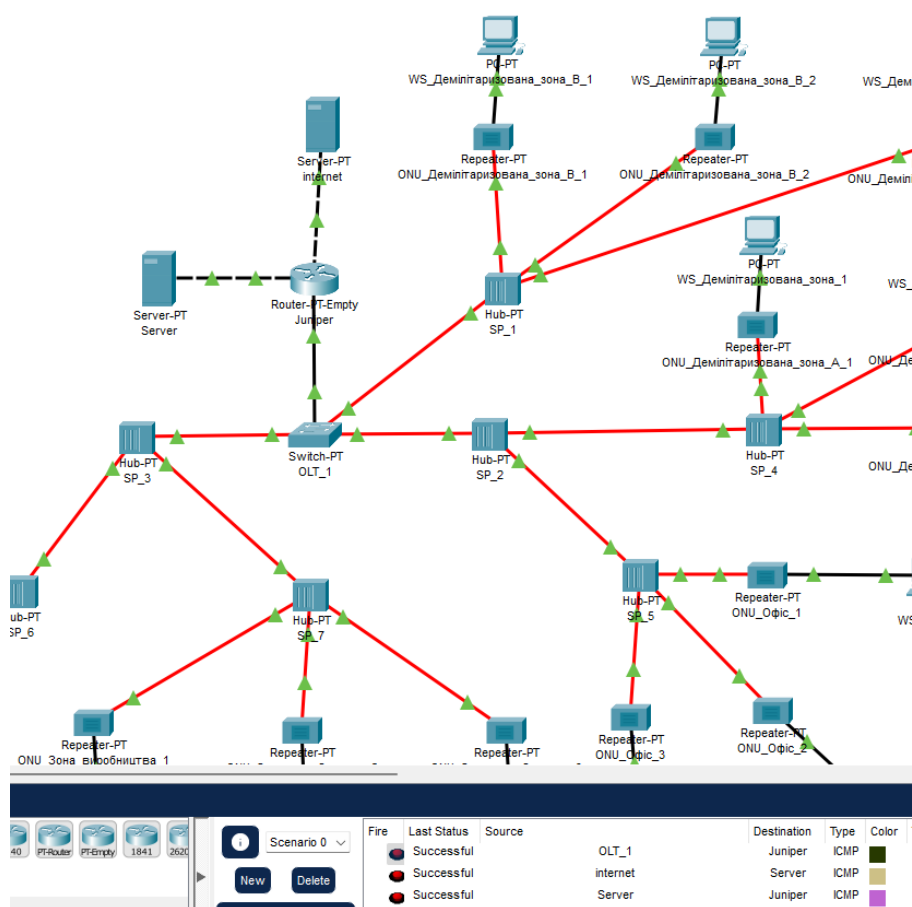


Рисунок 3.7 – Перевірка роботи маршрутизаторів

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі перевіримо чи отримали робочі станції динаміку та доступ до серверу, рис.3.8 та рис.3.9.

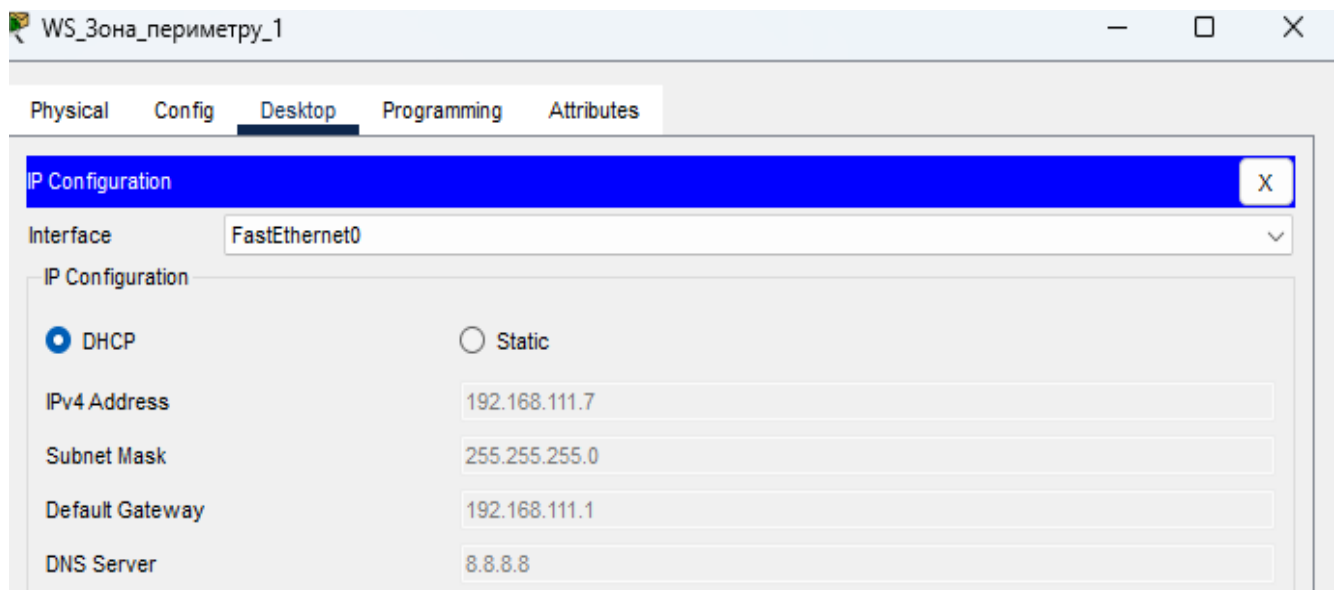


Рисунок 3.8 – Динамічна адреса яку отримала станція

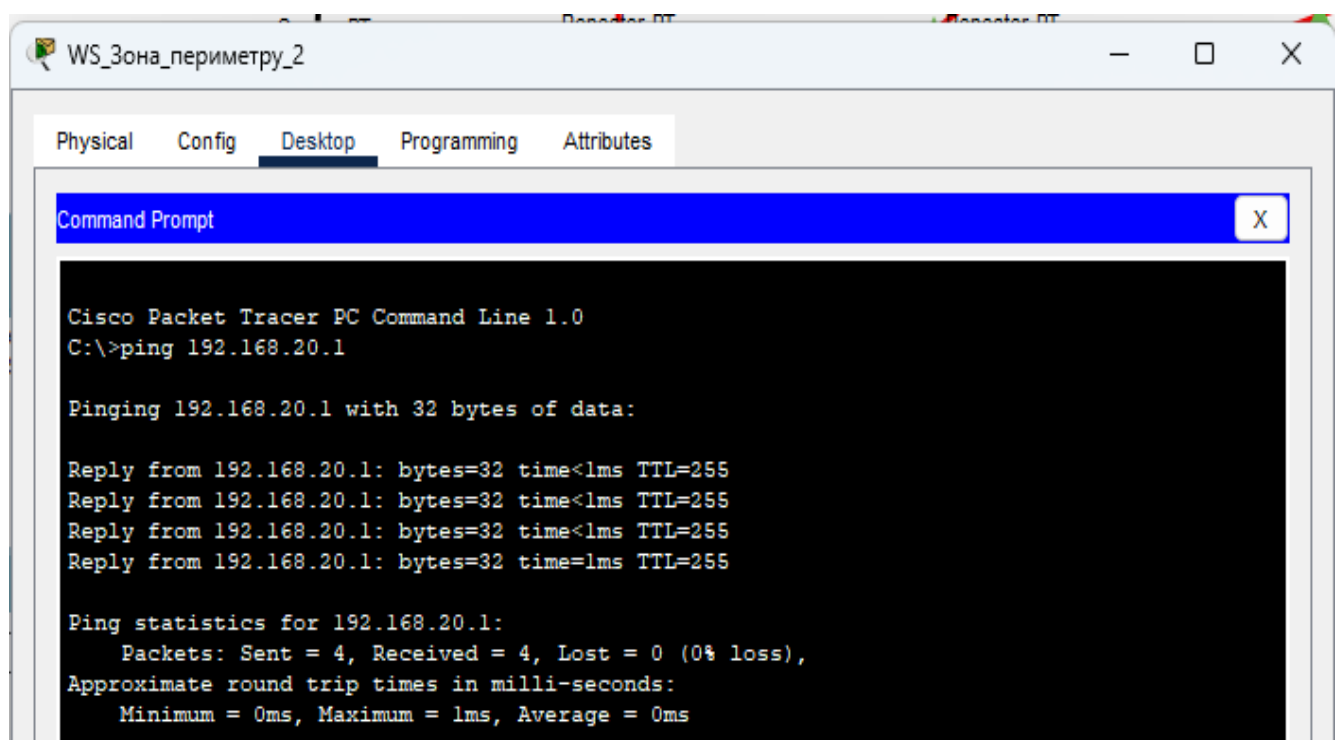


Рисунок 3.9 – Перевірка доступу на сервер

Далі перевіримо віддалений доступ, рис.3.10.

		Корень Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

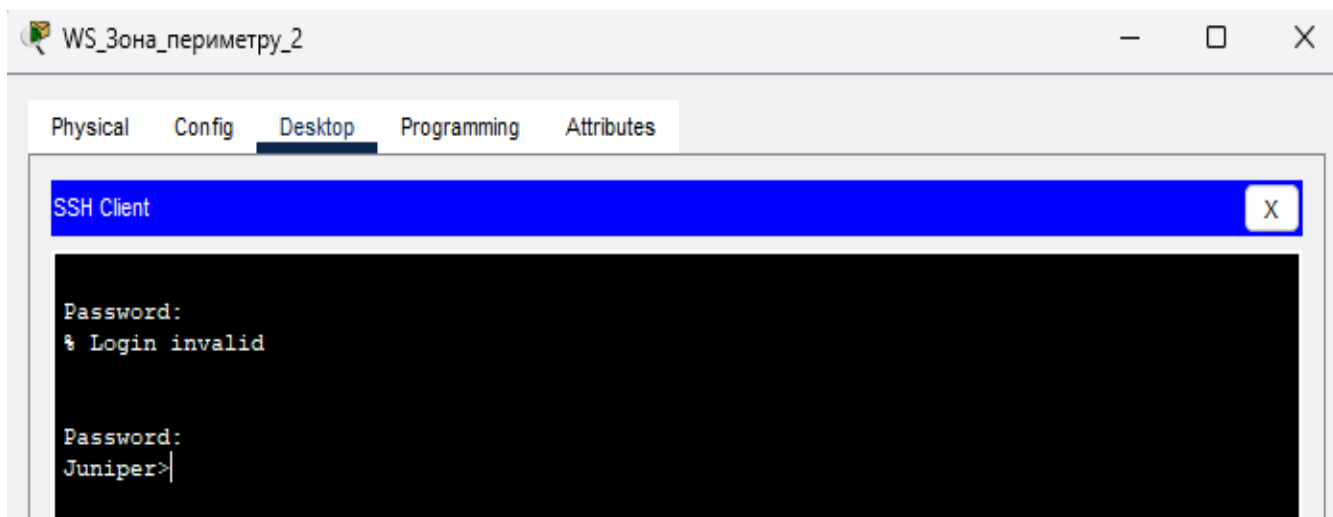


Рисунок 3.10 – Перевірка віддаленого доступу

Перевіримо налаштування Juniper, рис.3.11.

```
admin@Juniper_SRX_100> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes

^C
— 8.8.8.8 ping statistics —
10 packets transmitted, 0 packets received, 100% packet loss

admin@Juniper_SRX_100> ping 192.168.167.254
PING 192.168.167.254 (192.168.167.254): 56 data bytes
64 bytes from 192.168.167.254: icmp_seq=0 ttl=255 time=2.994 ms
64 bytes from 192.168.167.254: icmp_seq=1 ttl=255 time=3.162 ms
64 bytes from 192.168.167.254: icmp_seq=2 ttl=255 time=2.669 ms
64 bytes from 192.168.167.254: icmp_seq=3 ttl=255 time=2.615 ms
64 bytes from 192.168.167.254: icmp_seq=4 ttl=255 time=2.773 ms
^C
— 192.168.167.254 ping statistics —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.615/2.843/3.162/0.206 ms

admin@Juniper_SRX_100> █
```

Рисунок 3.11 – Перевірка роботи маршрутизації на Juniper

Як ми бачимо комутатор не зміг виконати команду ping 8.8.8.8. Це пов'язано з налаштуванням безпеки, а саме зони untrust . Як ми переконаємося далі вихід у глобальну мережу є. Далі виконаємо підключення по telnet, рис.3.12.

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

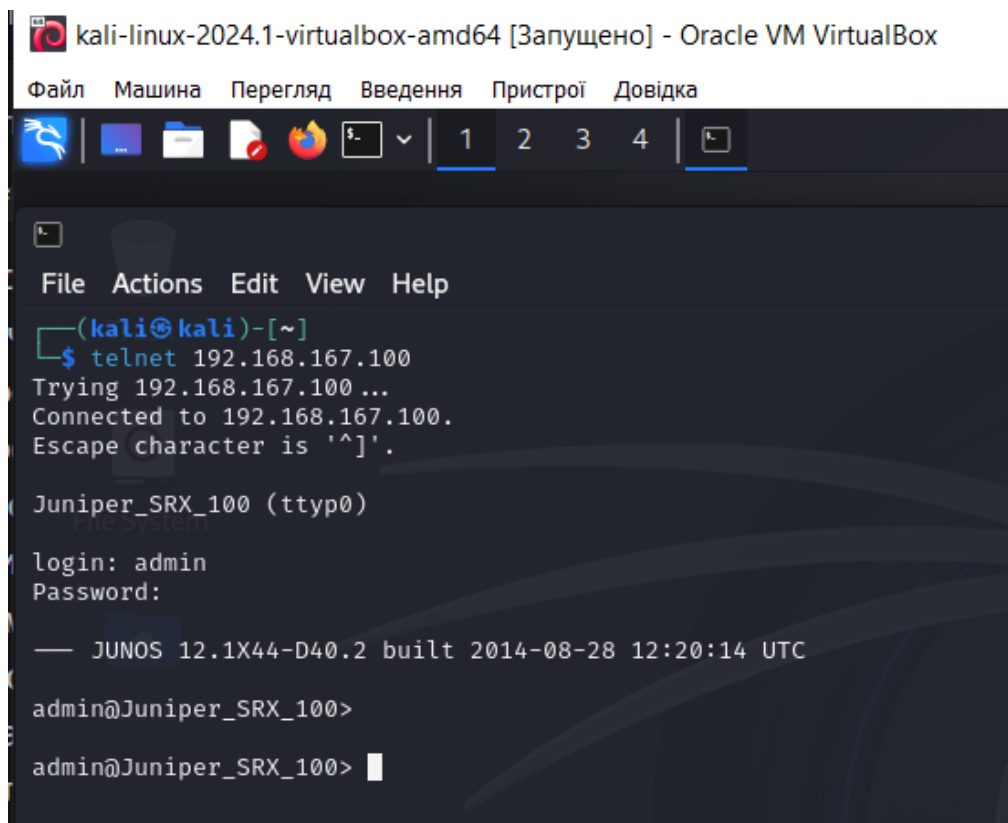


Рисунок 3.12 – Перевірка віддаленого доступу до Juniper

Не дивлячись на те, що порт 0/0/0 і vlan 7 належать до зони untrust підключення по telnet можливе, так як telnet був дозволений для зони untrust. Щоб переконатися в роботі маршрутизатора виконаємо команду ping з зони trust, рис.3.13.

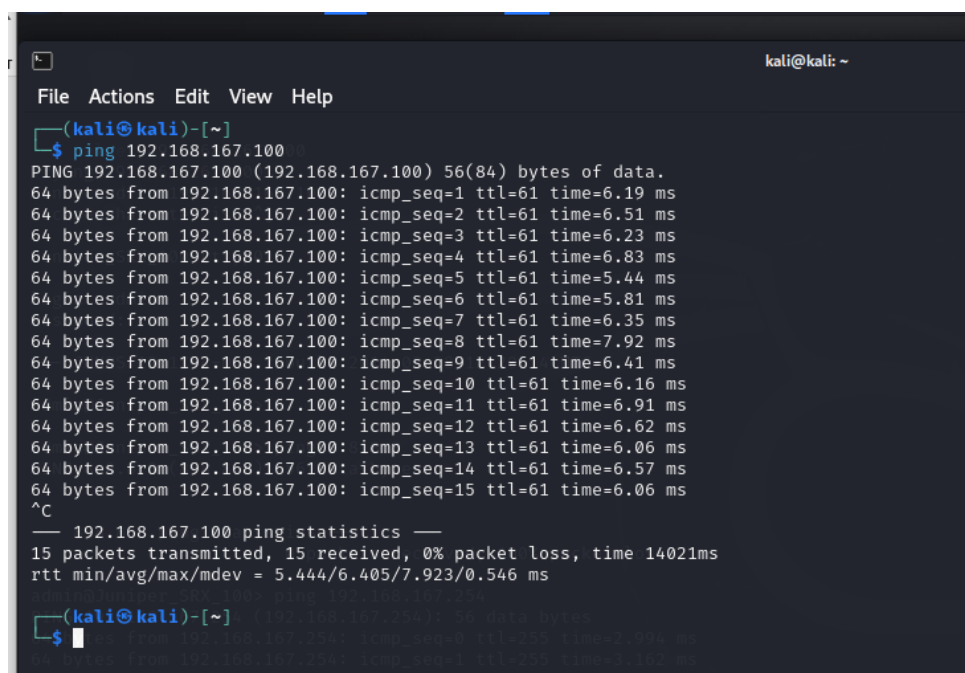


Рисунок 3.13 – Перевірка трафіку з зони trust

		Корень Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Також спробуємо виконаємо команду ping з зони untrust та підключитися віддалено, але будемо використовувати адресу з іншого vlan рис.3.14.

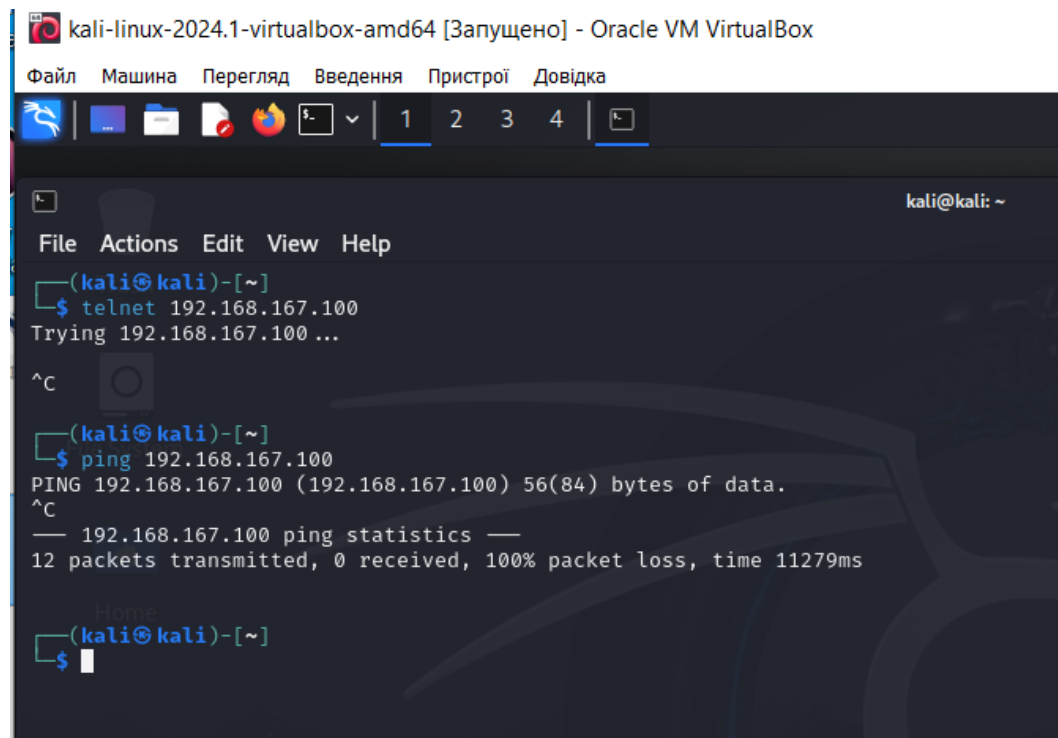


Рисунок 3.14 – Спроба несанкціонованого підключення

Як ми бачимо не вдалося виконати підключення по telnet, команда ping також не виконалась. Причина цьому, що адреса з якої ми намагалися зайти не належала діапазону адрес vlan 7.

Висновки до третього розділу

Проведено вибір та обґрунтування обладнання для забезпечення працездатності спроектованої мережі. Здійснено базове налагодження мережних пристроїв та засобів підсистеми захисту.

Здійснено тестування спроектовано та налагодженої мережі, зокрема здійснено перевірку налаштування рівня комутаторів та серверів, наявність доступу до серверів з робочих станцій, у тому числі віддалених.

ВИСНОВКИ

Проект захищеної PON-мережі для підприємства критичної інфраструктури спрямований на створення надійної та безпечної телекомунікаційної системи, що відповідає сучасним вимогам до захисту інформації.

У ході розробки були детально розглянуті ключові аспекти PON-технології та методи її захисту, включаючи шифрування даних, автентифікацію користувачів та моніторинг мережі. Особлива увага приділялась забезпеченню безперервності роботи та стійкості до кібератак, що є критично важливим для підприємств, які відіграють стратегічну роль у функціонуванні держави та суспільства. Запропоноване рішення дозволяє досягти високого рівня захищеності при збереженні переваг PON-технології, таких як висока пропускна здатність, економічність та масштабованість.

Хоча впровадження такої системи може зіткнутися з певними викликами, зокрема, необхідністю навчання персоналу та інтеграції з існуючими системами, ці питання можуть бути ефективно вирішені за допомогою ретельного планування та поетапного впровадження. Загалом, розроблений проект демонструє високу ефективність та доцільність застосування для підвищення безпеки та надійності комунікаційної інфраструктури критично важливих об'єктів, що сприятиме загальному зміцненню національної безпеки та стійкості держави до сучасних загроз.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Архітектура мережі або мережева архітектура [Електронний ресурс] – Режим доступу: <https://nettech.ua/news/arxitektura-seti-ili-setevaja-arxitektura>.
2. Oleksandr O. Nonik, Nadiia M. Lobanchykova, Tetiana A. Vakaliuk, Viacheslav V. Osadchyi and Oleksandr V. Farrakhov. Approaches to solving proxy performance problems for HTTP and SOCKS5 protocols for the case of multi-port passwordless access. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems. Kyiv, Ukraine, February 28, 2024. Edited by Volodymyr Sokolov, Vasyl Ustimenko, Tamara Radivilova, Mariya Nazarkevych. CEUR Workshop Proceedings, 2024. Vol. 3654. Pp. 189–200. – Режим доступу: <https://ceur-ws.org/Vol-3654/paper16.pdf>
3. Lobanchykova, N., Pilkevych, I., Korchenko, O. Analysis of attacks on components of IoT systems and cybersecurity technologies. Joint Proceedings of the Workshops on Quantum Information Technologies and Edge Computing (QuaInT+doors 2021), Zhytomyr, Ukraine, April 11, 2021. Edited by Serhiy O. Semerikov. (CEUR-WS.org). pp. 83-96.
4. Pilkevych I., Boychenko O., Lobanchykova N., Vakaliuk T., Semerikov S. Method of Assessing the Influence of Personnel Competence on Institutional Information Security. Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, Khmelnytskyi, Ukraine, March 24–26, 2021. Edited by Tetiana Hovorushchenko, Oleg Savenko, Peter Popov, Sergii Lysenko. CEUR Workshop Proceedings, 2021. Vol. 2853. pp. 266-275. – Режим доступу: <http://ceur-ws.org/Vol-2853/paper33.pdf>
5. Andrii Morozov, Nadiia Lobanchykova, Halyna Tarasiuk, Tetiana Vakaliuk. Methods of information protection of electronic data. Digitalization of economics: interdisciplinary and inter-branch approach: manual. Zhytomyr: Publishing House “Book-Druk”, 2023. P. 310-394
6. Лобанчикова Н.М., Серденюк Б.О. Дослідження процесів захисту інформації в IoT. Тези доповідей X Міжнародної науково-технічної конференції

		Коренев Р.П.		
		Єфіменко А.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 11 – КБ

Арк.

61

«Інформаційно-комп'ютерні технології – 2019», 18-20 квітня 2019 року. Житомир: ЖДТУ, 2019. С. 80-83.

7. CLI User Guide Junos OS:
<https://www.juniper.net/documentation/us/en/software/junos/cli/index.html>.

8. GPON-концентратор BDCOM GP3600-08 [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/katalog/concentrators-olt/bdcom-gp3600-08.html>.

9. Juniper Networks [Електронний ресурс] – Режим доступу: <https://omnilink.ua/juniper/>.

10. Маршрутизатори Juniper ACX5400 Metro Router: <https://stack-systems.com.ua/marshrutizator-juniper-acx5448-ac-afo>.

11. Мережа Gigabit Ethernet [Електронний ресурс] – Режим доступу: <https://ua5.org/lan/141-merezha-gigabit-ethernet.html>.

12. Міжмережевого екрану Juniper SRX4100: <https://stack-systems.com.ua/mezhsetevoj-jekran-juniper-srx4100-sys-jb-ac>.

13. Навчальний курс CCNA Cybersecurity Operations [Електронний ресурс] – Режим доступу: www.netacad.com.

14. Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

15. Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

16. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: www.netacad.com.

17. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.

18. Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

19. Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

20. Навчальний курс CCNP Enterprise: Core Networking [Електронний ресурс] – Режим доступу: www.netacad.com.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

21. Опис технології Fast Ethernet [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/opisanie-tehnologii-fast-ethernet.html>.

22. Побудова мереж GPON на базі обладнання ТМ BDcom (практична частина) (семінар по обладнанню BDcom) [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/ua-equipment-gpon-bdcom-seminar-3.html>.

23. Побудова мережевої та локальної системи безпеки [Електронний ресурс] - <https://www.telesphera.net/blog/network-and-local-security-system.html>.

24. Принципи роботи PON мережі: <https://homenet.online/shcho-take-pon-tehnologiya/>.

25. Технологія PON [Електронний ресурс] – Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/66122.html>.

26. Що таке IPv4? [Електронний ресурс] – Режим доступу: <https://uk.education-wiki.com/6575994-what-is-ipv4>.

27. Що таке SSH і як він працює? [Електронний ресурс] – Режим доступу: <https://instagalleryapp.com/informacijna-bezpeka/shho-take-ssh-i-jak-vin-pracjue/>.

28. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO [Електронний ресурс] – Режим доступу: <https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco>.

		Коренів Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

ДОДАТКИ

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Файл конфігурації маршрутизатора Juniper

```
Juniper#show running-config
Building configuration...

Current configuration : 1899 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Juniper
!
!
!
enable secret 5 $1$mERr$hwZUBIE0HdnNjuMKaBA400
!
!
!
!
!
aaa new-model
!
aaa authentication login default group radius local
aaa authentication enable default group radius local
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin secret 5 $1$mERr$hwZUBIE0HdnNjuMKaBA400
!
!
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name google.com
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
```

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

speed auto
!
interface GigabitEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet2/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet3/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet4/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet5/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet6/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet6/0.1
encapsulation dot1Q 111
ip address 192.168.111.1 255.255.255.0
!
interface GigabitEthernet6/0.2
encapsulation dot1Q 100
ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet6/0.3
encapsulation dot1Q 102
ip address 192.168.102.1 255.255.255.0
!
interface GigabitEthernet7/0
ip address 8.8.4.5 255.0.0.0
duplex auto
speed auto
!
interface GigabitEthernet8/0
ip address 192.168.20.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet9/0
no ip address
duplex auto

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

speed auto
!
ip classless
!
ip flow-export version 9
!
!
!
!
radius-server host 192.168.20.2 auth-port 1645
radius-server key Juniper123
!
!
!
line con 0
password Juniper
!
line aux 0
!
line vty 0 4
password Juniper
login authentication default
transport input ssh
line vty 5 15
password Juniper
!
!
!
end

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Файл конфігурації комутатора OLT_1

OLT_1#show running-config

Building configuration...

Current configuration : 3402 bytes

!

version 12.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname OLT_1

!

enable secret 5 \$1\$mERr\$hwZUBIE0HdnNjuMKaBA400

!

!

ip dhcp excluded-address 192.168.100.1

ip dhcp excluded-address 192.168.11.1

ip dhcp excluded-address 192.168.111.1

ip dhcp excluded-address 192.168.102.1

!

ip dhcp pool vlan100

network 192.168.100.0 255.255.255.0

default-router 192.168.100.1

dns-server 8.8.8.8

ip dhcp pool vlan111

network 192.168.111.0 255.255.255.0

default-router 192.168.111.1

dns-server 8.8.8.8

ip dhcp pool vlan102

network 192.168.102.0 255.255.255.0

default-router 192.168.102.1

dns-server 8.8.8.8

!

ip arp inspection vlan 100,102,111

!

ip dhcp snooping vlan 100,102,111

ip dhcp snooping

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface GigabitEthernet0/1

switchport mode trunk

!

interface GigabitEthernet1/1

switchport mode trunk

!

interface GigabitEthernet2/1

switchport mode trunk

!

interface GigabitEthernet3/1

switchport access vlan 111

switchport trunk allowed vlan 100,111

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 250

switchport mode access

switchport port-security

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

switchport port-security maximum 64
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0000.0C85.7C24
switchport port-security mac-address sticky 0002.17EE.93BC
switchport port-security mac-address sticky 0030.F2B8.87C4
switchport port-security mac-address sticky 0090.0C34.7029
switchport port-security mac-address sticky 0090.0CDD.BA9D
switchport port-security mac-address sticky 00D0.58B6.37C2
spanning-tree portfast
spanning-tree bpduguard enable
!
interface GigabitEthernet4/1
switchport access vlan 100
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 250
switchport mode access
switchport port-security
switchport port-security maximum 64
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.4373.20BA
switchport port-security mac-address sticky 0006.2A70.2E15
switchport port-security mac-address sticky 000C.8522.9D01
switchport port-security mac-address sticky 0060.4760.DE91
switchport port-security mac-address sticky 00D0.D317.CEBB
switchport port-security mac-address sticky 00D0.D3E7.BC7C
!
interface GigabitEthernet5/1
switchport access vlan 102
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 250
switchport mode access
switchport port-security
switchport port-security maximum 64
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.97E5.8430
switchport port-security mac-address sticky 000D.BD10.3133
switchport port-security mac-address sticky 00D0.D3AC.826E
!
interface GigabitEthernet6/1
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet7/1
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan11
no ip address
!
interface Vlan100
ip address 192.168.100.254 255.255.255.0
!
interface Vlan102
ip address 192.168.102.254 255.255.255.0
!
interface Vlan111
ip address 192.168.111.254 255.255.255.0

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

!
ip default-gateway 192.168.21.8
!
!
!
!
line con 0
password 7 080B594000090005
login
!
line vty 0 4
password 7 080B594000090005
login
line vty 5 15
password 7 080B594000090005
login
!
!
!
!
end

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Файл конфігурації Junipere SRX100

```
admin@Juniper_SRX_100# show
## Last changed: 2024-06-23 19:33:14 EEST
version 12.1X44-D40.2;
system {
    host-name Juniper_SRX_100;
    time-zone Europe/Kiev;
    root-authentication {
        encrypted-password "$1$aw1p4A89$rKSiSM7fnPscybQwXmqAI0"; ## SECRET-DATA
    }
    login {
        user admin {
            uid 2001;
            class super-user;
            authentication {
                encrypted-password "$1$QU2F7V8E$QOU3X1d2AI/1H2PIB/Zt50"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh;
        telnet;
        xnm-clear-text;
        web-management {
            http {
                interface vlan.0;
            }
            https {
                system-generated-certificate;
                interface vlan.0;
            }
        }
    }
    syslog {
```

		Коренєв Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

archive size 100k files 3;

user * {
    any emergency;
}

file messages {
    any critical;
    authorization info;
}

file interactive-commands {
    interactive-commands error;
}

}

max-configurations-on-flash 5;
max-configuration-rollback 5;

license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}

ntp {
    server 192.168.210.100;
}

}

interfaces {
    fe-0/0/0 {
        unit 0;
    }

    fe-0/0/1 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [ 7 40 ];
                }
            }
        }
    }
}

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

    }
}
fe-0/0/2 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/3 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/4 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vlan-trust;
            }
        }
    }
}
fe-0/0/5 {
    unit 0 {
        family ethernet-switching {

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

    port-mode access;

    vlan {
        members vlan-trust;
    }
}

fe-0/0/6 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vlan-trust;
            }
        }
    }
}

fe-0/0/7 {
    unit 0 {
        family ethernet-switching {
            port-mode access;
            vlan {
                members vlan-trust;
            }
        }
    }
}

vlan {
    unit 0;
    unit 7 {
        family inet {
            address 192.168.167.100/24;
        }
    }
    unit 40 {

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

        family inet;
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.168.167.254;
    }
}
protocols {
    stp;
}
security {
    screen {
        ids-option untrust-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
            }
            land;
        }
    }
}
nat {

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

source {
    rule-set trust-to-untrust {
        from zone trust;
        to zone untrust;
        rule source-nat-rule {
            match {
                source-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    interface;
                }
            }
        }
    }
}

policies {
    from-zone trust to-zone untrust {
        policy trust-to-untrust {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
        policy our-internet-policy {
            match {
                source-address any;
                destination-address any;
                application any;
            }

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

    then {
        permit;
    }
}
}

from-zone untrust to-zone trust {
    policy our-deny-policy {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}

zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            vlan.0;
            fe-0/0/2.0;
            fe-0/0/3.0;
            fe-0/0/4.0;
            fe-0/0/5.0;
            fe-0/0/6.0;

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

```

        fe-0/0/7.0;
    }
}

security-zone untrust {
    screen untrust-screen;
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
}

interfaces {
    fe-0/0/0.0 {
        host-inbound-traffic {
            system-services {
                dhcp;
                tftp;
                telnet;
            }
        }
    }

    fe-0/0/1.0 {
        host-inbound-traffic {
            system-services {
                ping;
                telnet;
            }
        }
    }

    vlan.7;
    vlan.40;
}
}

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

```

    }
}
vlangs {
    vlan-trust {
        vlan-id 3;
        l3-interface vlan.0;
    }
    vlan40 {
        vlan-id 40;
        l3-interface vlan.40;
    }
    vlan7 {
        vlan-id 7;
        l3-interface vlan.7;
    }
}

```

		Коренев Р.П.			КІК.КР.Б – 125 – 11 – КБ	Арк.
		Єфіменко А.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця адрес маршрутизаторів

Назва пристрою	Інтерфейс	Адреса	Маска	Префікс
interner	GigE0	8.8.4.4	255.0.0.0	/8
server	GigE0	192.168.20.2	255.255.255.0	/24
Juniper	GigE6/0.1	192.168.111.1	255.255.255.0	/24
	GigE6/0.2	192.168.100.1	255.255.255.0	/24
	GigE6/0.3	192.168.102.1	255.255.255.0	/24
	GigE7/0	8.8.4.5	255.0.0.0	/8
	GigE8/0	192.168.20.2	255.255.255.0	/24
OLT_1	GigE3/1	192.168.111.254	255.255.255.0	/24
	GigE4/1	192.168.100.254	255.255.255.0	/24
	GigE5/1	192.168.102.254	255.255.255.0	/24