

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної гетерогенної мережі організації з впровадженням архітектури Zero Trust»

Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Олександр КОСТЕНКО

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

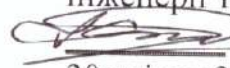
 Андрій ЄФІМЕНКО

Рецензент: професор кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Володимир ВОРОТНИКОВ

Житомир – 2025

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
30 квітня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Костенко Олександр Вячеславович

Тема роботи: «Проект захищеної гетерогенної мережі організації з впровадженням архітектури Zero Trust»

затверджена Наказом університету від 3 березня 2025 р. № 80/с.

Термін здачі студентом закінченої роботи 25 червня 2025 р.

Вихідні дані роботи:

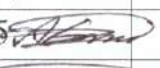
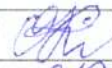
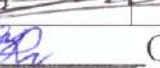
Вимоги до безпеки, масштабованості та керованості гетерогенної мережі сучасної організації з гібридною моделлю роботи, специфіка архітектури Zero Trust, а також функціональні можливості програмного та апаратного забезпечення (Cisco IOS, pfSense, FreeRADIUS), що моделюється у середовищі GNS3.

Обладнання та програмне забезпечення:

GNS3 (Graphical Network Simulator 3): використовується як основне середовище для моделювання та тестування захищеної гетерогенної мережі з реалізацією принципів архітектури Zero Trust.

Microsoft Windows: використовується як операційна система на робочій станції, де встановлені програмні засоби GNS3, pfSense та інші інструменти конфігурації мережі.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	20.05.2025 	20.05.2025 
2	Єфіменко А.А.	30.05.2025 	30.05.2025 
3	Єфіменко А.А.	04.06.2025 	04.06.2025 

Студент  Олександр КОСТЕНКО
Керівник  Андрій ЄФІМЕНКО

Календарний план

№	Назви етапів випускної кваліфікаційної робо-ти	Термін вико- нання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Формулювання технічного завдання	14.03.2025	Виконано
3	Проведення аналізу літературних джерел	18.03.2025	Виконано
4	Розробка плану	06.05.2025	Виконано
5	Проектування структури системи	14.05.2025	Виконано
6	Побудова локальної мережі в програмному додатку	26.05.2025	Виконано
7	Проведення тестувань побудованої мережі	02.06.2025	Виконано
8	Оформлення пояснювальної записки	12.06.2025	Виконано
9	Підготовка доповіді та створення презентації	20.06.2025	Виконано
10	Захист		Виконано

Студент  Олександр КОСТЕНКО

Керівник  Андрій ЄФІМЕНКО

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з проєкту захищеної гетерогенної мережі організації, розробленого в середовищі моделювання, та пояснювальної записки. Пояснювальна записка до кваліфікаційної роботи містить текстову частину обсягом 71 сторінок друкованого тексту. Список використаних джерел складається з 15 найменування і займає 2 сторінки. У роботі подано 46 рисунків та 6 таблиць. Загальний обсяг роботи — 93 сторінки.

Метою роботи є розробка комплексного проєкту захищеної гетерогенної мережевої інфраструктури організації з впровадженням принципів архітектури Zero Trust, що передбачає відмову від неявної довіри, мікросегментацію, централізований контроль доступу та дотримання політики найменших привілеїв.

Проектування мережі включало аналіз сучасних загроз, оцінку вихідного середовища, логічну сегментацію за допомогою VLAN, створення DMZ, впровадження списків контролю доступу (ACL), а також реалізацію централізованої автентифікації адміністраторів за допомогою RADIUS. Для побудови периметру було використано фаєрвол pfSense, а міжvlanову маршрутизацію реалізовано на маршрутизаторах Cisco. Уся топологія моделювалась у середовищі GNS3.

Розроблена мережа пройшла тестування на працездатність, ізоляцію сегментів, коректну маршрутизацію, автентифікацію та фільтрацію трафіку відповідно до обраної моделі безпеки.

Ключові слова: ZERO TRUST, ГЕТЕРОГЕННА МЕРЕЖА, VLAN, ACL, RADIUS, PFSense, МАРШРУТИЗАЦІЯ, СЕГМЕНТАЦІЯ, GNS3, БЕЗПЕКА ІНФРАСТРУКТУРИ.

					KKIKB.KP.B – 125 – 09 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Костенко О.В.		25.06.25	Проект захищеної гетерогенної мережі організації з впровадженням архітектури Zero Trust	Літ.	Арк.
Керівник		Сфіменко А.А.		25.06.25			4
Реценз.		Воротніков В.В.		25.06.25		ФІКТ, Гр. КБ-21-1	
Н. контр.		Сфіменко А.А.		25.06.25			
Затверд.		Сфіменко А.А.		25.06.25			

ANNOTATION

The final bachelor's thesis consists of a project of a secure heterogeneous network of an organization developed in a simulation environment and an explanatory note. The explanatory note to the qualification work contains a text part of 71 pages of printed text. The list of references consists of 15 titles and occupies 2 pages. The work contains 46 figures and 6 tables. The total volume of the work is 93 pages.

The purpose of the work is to develop a comprehensive project of a secure heterogeneous network infrastructure of an organization with the implementation of the principles of Zero Trust architecture, which involves the rejection of implicit trust, micro-segmentation, centralized access control, and compliance with the policy of least privilege.

The network design included analysis of modern threats, assessment of the source environment, logical segmentation using VLANs, creation of DMZs, implementation of access control lists (ACLs), and implementation of centralized administrator authentication using RADIUS. The pfSense firewall was used to build the perimeter, and inter-VLAN routing was implemented on Cisco routers. The entire topology was modeled in the GNS3 environment.

The developed network has been tested for operability, segment isolation, correct routing, authentication, and traffic filtering in accordance with the chosen security model.

Keywords: ZERO TRUST, HETEROGENEOUS NETWORK, VLAN, ACL, RADIUS, PFSense, ROUTING, SEGMENTATION, GNS3, INFRASTRUCTURE SECURITY.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1. ТЕОРЕТИКО-АНАЛІТИЧНІ ОСНОВИ ЗАХИСТУ	
ГЕТЕРОГЕННИХ МЕРЕЖ НА БАЗІ АРХІТЕКТУРИ ZERO TRUST	11
1.1. Характеристика сучасних гетерогенних мереж організацій	11
1.2. Архітектура безпеки Zero Trust як сучасний підхід до захисту інформаційних систем	16
1.3. Переваги та недоліки впровадження архітектури Zero Trust	21
1.4. Адаптація та застосування принципів Zero Trust для захисту гетерогенних мереж	25
Висновки до розділу 1	32
Розділ 2. Проєктування захищеної гетерогенної мережі організації з використанням архітектури Zero Trust	
33	
2.1. Аналіз мережної інфраструктури організації для формування вимог щодо захисту на базі архітектури Zero Trust	33
2.2. Проєктування удосконаленої ІТ-інфраструктури організації	42
2.3. Проєктування підсистеми захисту гетерогенної мережі з використанням принципів Zero Trust	47
Висновки до розділу 2	52
Розділ 3. Моделювання, реалізація архітектури Zero Trust, аналіз результатів та рекомендації	
54	
3.1. Вибір середовища моделювання та обладнання	54
3.2. Налаштування базової мережевої інфраструктури у середовищі моделювання	57
3.3. Впровадження компонентів архітектури Zero Trust	64
3.4. Тестування функціональності та ефективності захисту	72
Висновки до розділу 3	76
ВИСНОВКИ	78
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	80
ДОДАТКИ	82

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List, список контролю доступу

AAA – Authentication, Authorization, Accounting, автентифікація, авторизація та облік

AD – Active Directory, служба каталогів користувачів у середовищі Windows

BYOD – Bring Your Own Device, політика використання особистих пристроїв співробітників

DMZ – Demilitarized Zone, демілітаризована зона

DNS – Domain Name System, система доменних імен

DHCP – Dynamic Host Configuration Protocol, протокол динамічної конфігурації хоста

Entra ID – Microsoft Entra ID, хмарна служба ідентичностей

GNS3 – Graphical Network Simulator 3, середовище моделювання мереж

HTTP – HyperText Transfer Protocol, протокол прикладного рівня

HTTPS – HyperText Transfer Protocol Secure, захищений протокол прикладного рівня

ICMP – Internet Control Message Protocol, протокол діагностики мережі

IoT – Internet of Things, Інтернет речей

IP – Internet Protocol, протокол міжмережевої взаємодії

LAN – Local Area Network, локальна мережа

NAT – Network Address Translation, трансляція мережевих адрес

NAS – Network Attached Storage, мережеве сховище даних

pfSense – Platform FreeBSD Sense, програмний фаєрвол з відкритим кодом

RADIUS – Remote Authentication Dial-In User Service, віддалена служба автентифікації

SSH – Secure Shell, захищений протокол доступу до пристроїв

STP – Spanning Tree Protocol, протокол запобігання петлям у мережі

VLAN – Virtual Local Area Network, віртуальна локальна мережа

VPN – Virtual Private Network, віртуальна приватна мережа

Wi-Fi – Wireless Fidelity, бездротова мережа

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ZTNA – Zero Trust Network Access, модель доступу у парадигмі Zero Trust

Zero Trust – Архітектура нульової довіри, концепція безпеки без неявного довір'я

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В умовах стрімкої цифрової трансформації, зростання використання хмарних технологій, віддаленого доступу та розширення спектру мережевих пристроїв (включаючи IoT), корпоративна мережева інфраструктура перестає бути лише технічним елементом і стає ключовим компонентом стратегії інформаційної безпеки організації. Гетерогенні мережі, що поєднують різні типи пристроїв, операційних систем та топологій, стають все більш поширеними через потребу в гнучкості та масштабованості. Проте така різноманітність підвищує ризики несанкціонованого доступу, горизонтального переміщення атак та ускладнює контроль за поведінкою користувачів.

Традиційні моделі безпеки, що базуються на захисті периметра, поступово втрачають ефективність у контексті сучасних загроз. Зловмисники дедалі частіше отримують початковий доступ до внутрішніх сегментів і далі вільно переміщуються мережею, використовуючи недоліки у довірчих зонах. За таких умов виникає потреба у впровадженні нової парадигми безпеки — Zero Trust, яка базується на принципі «нікому не довіряй, завжди перевіряй» та передбачає жорсткий контроль доступу, мікросегментацію і постійну верифікацію дій користувачів і пристроїв.

Таким чином, задача проєктування захищеної гетерогенної мережі з вбудованими механізмами Zero Trust є надзвичайно актуальною. Поєднання класичних технологій маршрутизації, сегментації та управління доступом із сучасними підходами безпеки дозволяє створити інфраструктуру, що здатна протистояти складним та цілеспрямованим кіберзагрозам.

Метою даної кваліфікаційної роботи є розробка комплексного проєкту захищеної гетерогенної мережі організації з впровадженням архітектури Zero Trust, що передбачає ізоляцію критичних ресурсів, централізовану автентифікацію, контроль доступу та сегментацію мережевих взаємодій.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Для досягнення поставленої мети необхідно вирішити наступні основні завдання: Провести системний аналіз теоретичних основ побудови гетерогенних мереж і концепції Zero Trust. Дослідити архітектурні підходи до ізоляції сегментів, контролю доступу, мікросегментації та централізованої автентифікації. Спроектувати логічну структуру мережі з поділом на VLAN-сегменти, виділенням зон довіри, периметру та DMZ. Вибрати необхідне мережеве обладнання та програмне забезпечення для реалізації маршрутизації, фільтрації, NAT, AAA. Реалізувати функціональну модель інфраструктури у середовищі моделювання GNS3 з використанням Cisco IOS, pfSense, FreeRADIUS. Провести тестування мережі з перевіркою доступності сервісів, ефективності політик безпеки та ізоляції сегментів.

Об’єктом дослідження є процес проектування, моделювання та забезпечення захисту корпоративних гетерогенних мереж.

Предметом дослідження є моделі, технології та інструменти, які використовуються для реалізації архітектури Zero Trust у мережевій інфраструктурі організації.

У процесі виконання кваліфікаційної роботи було розроблено проєкт гнучкої, масштабованої та захищеної гетерогенної мережі, в основі якої лежать принципи Zero Trust. Побудована модель включає логічну сегментацію, контроль доступу за допомогою ACL, централізовану автентифікацію через RADIUS, фільтрацію міжзонного трафіку на фаєрволі pfSense та структуровану маршрутизацію, що забезпечує надійну та контрольовану взаємодію мережевих компонентів.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИКО-АНАЛІТИЧНІ ОСНОВИ ЗАХИСТУ ГЕТЕРОГЕННИХ МЕРЕЖ НА БАЗІ АРХІТЕКТУРИ ZERO TRUST

1.1. Характеристика сучасних гетерогенних мереж організацій

1.1.1. Поняття, структура та ключові особливості гетерогенних мереж

Сучасні організації все частіше стикаються з необхідністю інтеграції різноманітних технологій та пристроїв у свої корпоративні мережі, що призводить до формування складних гетерогенних ІТ-середовищ. Такі середовища, хоча й надають значні переваги у гнучкості та функціональності, водночас створюють нові виклики для забезпечення інформаційної безпеки. Традиційні моделі захисту, орієнтовані на периметр, виявляються недостатньо ефективними в умовах розмитих меж корпоративної мережі. У відповідь на ці виклики набуває популярності архітектура безпеки Zero Trust («Нульова Довіра»), яка пропонує кардинально інший підхід до захисту інформаційних активів.

Гетерогенна мережа організації – це інформаційно-комунікаційна система, яка об'єднує апаратні та програмні компоненти, що відрізняються за своїми архітектурами, виробниками, операційними системами, протоколами взаємодії та іншими технічними характеристиками. На відміну від гомогенних мереж, де переважно використовуються рішення одного вендора або стандартизовані технології, гетерогенні мережі є результатом поєднання різнорідних елементів.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Typical Heterogeneous Network Structure

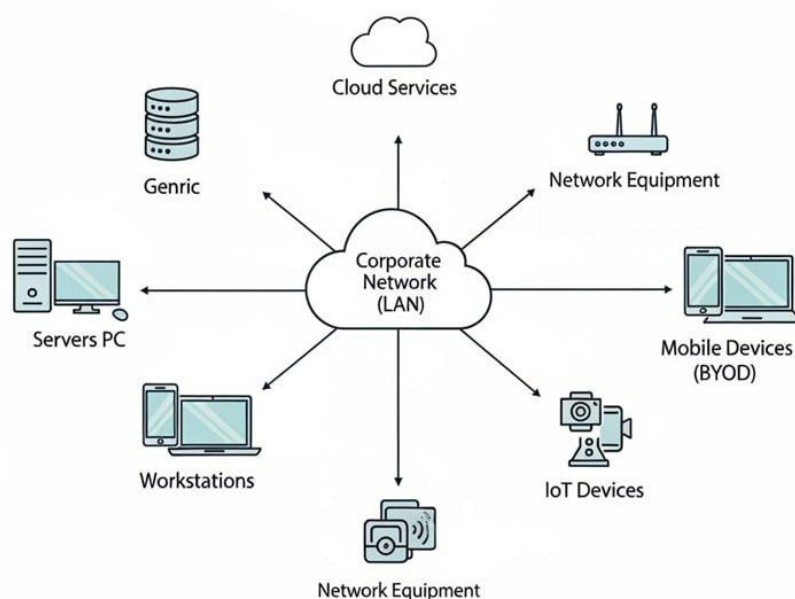


Рисунок 1.1 – Типова гетерогенна мережа організації

До типових компонентів сучасних гетерогенних мереж належать:

- Серверне обладнання під управлінням різних ОС (Windows Server, Linux-дистрибутиви, UNIX-системи).
- Робочі станції та персональні комп'ютери з різними версіями настільних ОС (Windows, macOS, Linux).
- Мобільні пристрої співробітників (смартфони, планшети) на базі Android, iOS (концепція BYOD – Bring Your Own Device).
- Пристрої Інтернету речей (IoT), такі як сенсори, камери, промислове обладнання, які часто мають власні специфічні протоколи та обмежені можливості захисту.
- Мережеве обладнання (маршрутизатори, комутатори, міжмережеві екрани, точки доступу Wi-Fi) від різних виробників.
- Хмарні сервіси та ресурси (IaaS, PaaS, SaaS), що інтегруються з локальною інфраструктурою.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

— Спеціалізоване програмне забезпечення та застарілі (legacy) системи, які можуть бути несумісними з сучасними засобами безпеки.

Ключовими особливостями гетерогенних мереж є їхня підвищена гнучкість, здатність адаптуватися до специфічних завдань бізнесу та можливість використання найкращих у своєму класі рішень від різних постачальників. Однак, ця різноманітність породжує і значні складності.

1.1.2. Специфічні виклики та загрози безпеці в гетерогенних мережах

Гетерогенність IT-інфраструктури створює низку унікальних викликів та загроз інформаційній безпеці:



Рисунок 1.2 – Ключові виклики безпеці в гетерогенних мережах

- Розширена поверхня атаки.
- Складність управління та адміністрування.
- Проблеми сумісності та інтероперабельності
- Низька прозорість та видимість
- Тіньове IT (Shadow IT)
- Обмежені ресурси безпеки на деяких пристроях

Розширена поверхня атака має на увазі, що кожен новий тип пристрою, ОС або додатку додає потенційні точки входу для зломисників. Різноманітність систем

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

означає більшу кількість потенційних вразливостей, які потрібно відстежувати та усувати.

Складність управління та адміністрування має на увазі, управління різнорідними системами вимагає від ІТ-персоналу ширших знань та навичок. Застосування єдиних політик безпеки та стандартів конфігурації стає складним завданням.

Проблеми сумісності та інтеоперабельності має на увазі, засоби безпеки, розроблені для однієї платформи, можуть бути несумісними з іншими. Інтеграція рішень від різних вендорів для створення комплексної системи захисту може бути технічно складною.

Низька прозорість та видимість – це отримання повної картини стану безпеки всієї гетерогенної мережі, моніторинг активності та виявлення аномалій ускладнюються через різноманітність форматів логів та протоколів.

Тіньове ІТ (Shadow IT) це означає, що співробітники можуть використовувати не-санкціоновані пристрої та сервіси, що ще більше ускладнює контроль над мережею та її безпекою.

Обмежені ресурси безпеки на деяких пристроях це – Багато IoT-пристроїв та деякі мобільні платформи мають обмежені обчислювальні ресурси, що не дозволяє встановлювати на них повноцінні засоби захисту.

1.1.3. Недоліки традиційних підходів до безпеки в контексті гетерогенних інфраструктур

Традиційні моделі безпеки, які значною мірою покладаються на концепцію захисту периметра, виявляються все менш ефективними в умовах сучасних гетерогенних мереж. Основні недоліки таких підходів:

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14



Рисунок 1.3 – Порівняння традиційної моделі безпеки та сучасного гетерогенного середовища

1. Розмитий периметр
2. Припущення про "довірену" внутрішню мережу
3. Недостатня гранулярність контролю доступу
4. Складність адаптації до змін

Розмитий периметр має на увазі, що використання мобільних пристроїв, хмарних сервісів, віддалений доступ співробітників та наявність IoT-пристроїв призводять до того, що чітко визначений периметр безпеки практично зникає.

Припущення про "довірену" внутрішню мережу має на увазі, що класичний підхід часто передбачає, що все, що знаходиться всередині корпоративної мережі, є довіреним. Однак, у гетерогенних мережах внутрішні загрози (наприклад, скомпрометовані пристрої, інсайдери) становлять значний ризик. Як тільки зломисник долає периметр, він часто отримує відносну свободу дій у внутрішній мережі.

Недостатня гранулярність контролю доступу має на увазі, що політики доступу часто застосовуються на рівні мережових сегментів, а не окремих користувачів чи ресурсів, що є недостатнім для гетерогенних середовищ.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Складність адаптації до змін має на увазі, що традиційні системи безпеки можуть повільно адаптуватися до швидких змін у гетерогенній інфраструктурі (додавання нових типів пристроїв, сервісів).

Ці недоліки зумовлюють необхідність переходу до більш сучасних та адаптивних моделей безпеки, однією з яких є архітектура Zero Trust.

1.2. Архітектура безпеки Zero Trust як сучасний підхід до захисту інформаційних систем

1.2.1. Передумови виникнення та еволюція концепції Zero Trust

Концепція Zero Trust (ZT), або "Нульова Довіра", не є новою технологією, а скоріше стратегічним підходом до проєктування та реалізації систем інформаційної безпеки. Вона почала формуватися на початку XXI століття у відповідь на зростаючу неефективність традиційних моделей безпеки, заснованих на периметрі. Усвідомлення того, що зловмисники можуть перебувати як ззовні, так і всередині мережі, а також те, що довіра до будь-якого суб'єкта чи об'єкта в мережі є потенційною вразливістю, стало ключовою передумовою для розвитку ZT.

Концепція нульової довіри була присутня в кібербезпеці ще до того, як з'явився сам термін «нульова довіра». Агентство оборонних інформаційних систем (DISA) і Міністерство оборони США опублікували свою роботу над більш безпечною корпоративною стратегією, яка отримала назву «чорне ядро» [BCORE]. Чорне ядро передбачало перехід від моделі безпеки, що базується на периметрі, до моделі, яка зосереджується на безпеці окремих транзакцій. Робота Єрихонського форуму в 2004 році оприлюднила ідею депериметризації - обмеження неявної довіри, заснованої на розташуванні мережі, і обмежень, пов'язаних з покладанням на окремі статичні засоби захисту у великому сегменті мережі [JERICHO]. Концепція депериметризації розвинулася і вдосконалилася в більш широку концепцію нульової довіри, яку пізніше запропонував Джон Кіндерваг, працюючи в компанії Forrester.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

The Evolutionary Path to Zero Trust

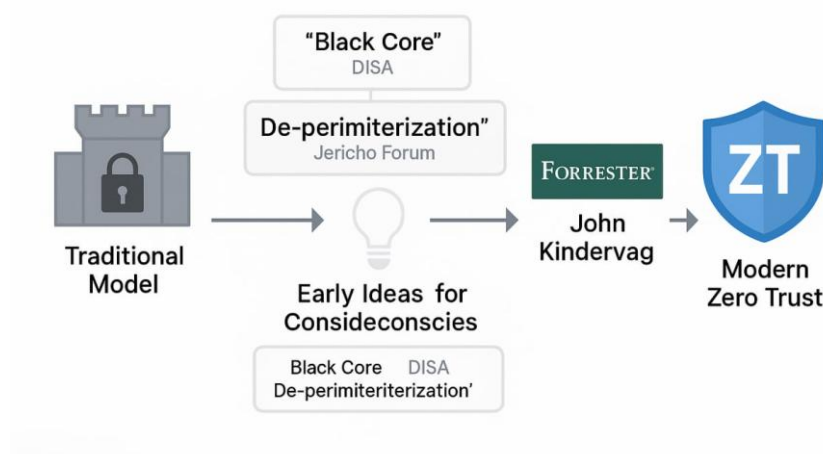


Рисунок 1.4 – Еволюційний шлях до концепції Zero Trust

Нульова довіра стала терміном, що використовується для опису різних рішень з кібербезпеки, які відійшли від неявної довіри, заснованої на розташуванні мережі, і натомість зосередилися на оцінці довіри на основі кожної транзакції. Приватний сектор і вища освіта також пройшли цей шлях від безпеки на основі периметра до стратегії безпеки, заснованої на принципах нульової довіри.

Еволюція Zero Trust триває, і сьогодні вона охоплює широкий спектр технологій та методологій, спрямованих на забезпечення гранулярного контролю доступу та мінімізацію поверхні атаки.

1.2.2. Основні принципи та філософія Zero Trust

Філософія Zero Trust базується на припущенні, що загрози можуть існувати як ззовні, так і всередині мережі, тому жодному суб'єкту (користувачу, пристрою, додатку) чи об'єкту (данам, сервісу) не можна довіряти за замовчуванням. Доступ надається на основі суворої перевірки та за принципом мінімальних привілеїв.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.5 – Основні принципи архітектури Zero Trust

Ключові принципи Zero Trust включають:

- 1. Ідентифікація та автентифікація всіх суб'єктів та об'єктів**
- 2. Мікросегментація мережі**
- 3. Принцип мінімальних привілеїв**
- 4. Всебічний моніторинг та аналіз безпеки**
- 5. Динамічний контроль доступу**
- 6. Захист даних**

Ідентифікація та автентифікація всіх суб'єктів та об'єктів має на увазі, що кожен користувач, пристрій, додаток та потік даних повинен бути однозначно ідентифікований та автентифікований перед наданням доступу. Багатофакторна автентифікація (MFA) є обов'язковою.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Мікросегментація мережі має на увазі, що мережа розділяється на невеликі, ізольовані сегменти (мікропериметри) для обмеження можливості горизонтального переміщення злоумисника у випадку компрометації одного із сегментів. Доступ між сегментами суворо контролюється.

Принцип мінімальних привілеїв має на увазі, що користувачам, пристроям та додаткам надається лише той рівень доступу, який є абсолютно необхідним для виконання їхніх функцій (Just-Enough Access, JEA) і лише на необхідний час (Just-in-Time Access, JIT).

Всебічний моніторинг та аналіз безпеки має на увазі здійснення безперервного збору, аналізу та кореляції даних про події безпеки з усіх джерел (мережеві пристрої, сервери, кінцеві точки, додатки). Це дозволяє виявляти аномалії, потенційні загрози та інциденти в режимі реального часу.

Динамічний контроль доступу має на увазі, що рішення про надання доступу приймаються не лише на основі статичних правил, а й з урахуванням контексту: стану пристрою, поведінки користувача, геолокації, часу доби та інших факторів ризику. Захист даних має на увазі, що дані мають бути захищені незалежно від їхнього місцезнаходження (в стані спокою, при передачі, при обробці) за допомогою шифрування, класифікації та політик запобігання витокам (DLP)[1][2][11].

1.2.3. Ключові компоненти (стовпи) архітектури Zero Trust

Реалізація архітектури Zero Trust зазвичай спирається на декілька взаємопов'язаних компонентів або "стовпів":

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Ключові компоненти архітектури Zero Trust

ВИДИМІСТЬ ТА АНАЛИТИКА

ІДЕНТИЧНІСТЬ

КІНЦЕВІ ТОЧКИ

МЕРЕЖА

ДОДАТКИ / РОБОЧІ
НАВАНТАЖЕННЯ

ДАНІ

АВТОМАТИЗАЦІЯ ТА ОРКЕСТРАЦІЯ

Рисунок 1.6 – Ключові компоненти (стовпи) архітектури Zero Trust

1. Ідентичність (Identity)
2. Кінцеві точки (Endpoints/Devices)
3. Мережа (Network)
4. Додатки (Applications/Workloads)
5. Дані (Data)
6. Видимість та аналітика (Visibility and Analytics)
7. Автоматизація та оркестрація (Automation and Orchestration)

Ідентичність (Identity) стосується користувачів, сервісних акаунтів та ключів API. Передбачає надійну автентифікацію (включаючи MFA), управління життєвим циклом ідентичностей та авторизацію на основі ролей та атрибутів.

Кінцеві точки (Endpoints/Devices) — це будь-які пристрої, що запитують доступ до корпоративних ресурсів (комп'ютери, мобільні пристрої, сервери, IoT-пристрої).

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Передбачає перевірку стану безпеки пристрою (наявність оновлень, антивірусу, відсутність шкідливого ПЗ) перед наданням доступу.

Мережа (Network) включає локальні мережі, глобальні мережі, хмарні мережі. Передбачає сегментацію та мікросегментацію, контроль трафіку між сегментами, запобігання вторгненням та захист від DDoS-атак.

Додатки (Applications/Workloads) — це корпоративні додатки, як локальні, так і хмарні. Передбачає безпечну розробку (DevSecOps), контроль доступу до API, захист від веб-атак.

Дані (Data) — це інформаційні активи організації. Передбачає класифікацію даних, шифрування, контроль доступу до даних на основі їхньої чутливості, моніторинг використання даних та запобігання витокам (DLP).

Видимість та аналітика (Visibility and Analytics) — це збір та аналіз логів

Автоматизація та оркестрація (Automation and Orchestration) — це автоматизація рутинних завдань безпеки та оркестрація реагування на інциденти.

1.3. Переваги та недоліки впровадження архітектури Zero Trust

1.3.1. Позитивні аспекти застосування Zero Trust

Впровадження архітектури Zero Trust надає організаціям низку суттєвих переваг:

1. Покращений захист від сучасних загроз
2. Зменшення поверхні атаки
3. Краща видимість та контроль
4. Підтримка сучасних ІТ-середовищ
5. Захист даних
6. Спрощення дотримання нормативних вимог
7. Зниження ризиків, пов'язаних з інсайдерами

Покращений захист від сучасних загроз означає, що завдяки принципу "ніколи не довіряй, завжди перевіряй" та мікросегментації значно ускладнюється проникнення злоумисників у мережу та їхнє горизонтальне переміщення у випадку компрометації одного компонента.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Зменшення поверхні атаки має на увазі, що гранулярний контроль доступу та мінімальні привілеї обмежують потенційний вплив атаки.

Краща видимість та контроль — це безперервний моніторинг та аналітика, які надають повне уявлення про те, хто, що, коли, де і як отримує доступ до ресурсів.

Підтримка сучасних ІТ-середовищ означає, що Zero Trust добре адаптується до хмарних та гібридних інфраструктур, підтримує концепцію BYOD та віддалену роботу співробітників [13].

Захист даних має на увазі акцент на захисті даних на всіх етапах їхнього життєвого циклу.

Спрощення дотримання нормативних вимог — це те, що багато принципів Zero Trust (наприклад, контроль доступу, моніторинг, захист даних) допомагають відповідати вимогам різних стандартів безпеки (наприклад, GDPR, PCI DSS).

Зниження ризиків, пов'язаних з інсайдерами означає, що сувора автентифікація та контроль дій користувачів допомагають мінімізувати загрози з боку внутрішніх порушників.

1.3.2. Потенційні виклики, складності та обмеження при реалізації Zero Trust

Незважаючи на значні переваги, впровадження архітектури Zero Trust є складним, багатогранним процесом і може супроводжуватися низкою суттєвих викликів, труднощів та обмежень, які організаціям необхідно враховувати та заздалегідь планувати їх подолання:

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Ключові виклики при впровадженні Zero Trust



Рисунок 1.7 – Ключові виклики при впровадженні архітектури Zero Trust

1. Комплексність реалізації
2. Вартість
3. Вплив на користувацький досвід
4. Сумісність із застарілими системами (Legacy Systems)
5. Необхідність у кваліфікованих фахівцях
6. Культурні зміни в організації

Комплексність реалізації полягає в тому, що перехід на Zero Trust – це не просто встановлення нового програмного забезпечення, а фундаментальна зміна підходу до безпеки, що вимагає:

- Ретельного планування, з аналізом існуючої інфраструктури та потоків даних.
- Значних змін в інфраструктурі, таких як редизайн мережі, впровадження MFA, IAM, тощо.
- Інтеграції різних технологій, включаючи EDR/XDR, NAC, DLP та інші.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

- Підходу як до безперервного процесу, а не одноразового проєкту.

Вартість включає фінансові інвестиції у технології, послуги впровадження, навчання персоналу та підтримку:

- Закупівля технологій: нове ПЗ, ліцензії.
- Послуги впровадження: консалтинг, інтеграція.
- Навчання персоналу: як IT-фахівців, так і кінцевих користувачів.
- Операційні витрати: підтримка та обслуговування систем.

Вплив на користувацький досвід означає необхідність балансу між безпекою та зручністю:

- Ризик надмірної суворості політик: надто часті перевірки, складність у роботі.
- Негативний досвід: може знизити продуктивність та викликати обхід політик.
- Пошук балансу: адаптивна MFA, прозора автентифікація, комунікація з користувачами.

Сумісність із застарілими системами (Legacy Systems) створює технічні труднощі:

- Обмеження legacy-систем: відсутність підтримки сучасних протоколів, відсутність API.
- Ризики: складність реалізації контролю доступу.
- Складність інтеграції: потреба в проксі, ізоляції або спеціальних рішеннях.

Необхідність у кваліфікованих фахівцях означає потребу у працівниках із широким набором знань:

- Спектр навичок: від ідентифікації та мереж до хмар і автоматизації.
- Дефіцит кадрів: високий попит, висока вартість, особливо складно для малих компаній.

Культурні зміни в організації необхідні для трансформації мислення:

- Зміна парадигми: від довіри до постійної перевірки.
- Опір змінам: спротив з боку користувачів.
- Роль керівництва: комунікація, навчання, залучення бізнес-підрозділів.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

1.4. Адаптація та застосування принципів Zero Trust для захисту гетерогенних мереж

1.4.1. Обґрунтування релевантності Zero Trust для гетерогенних середовищ

Перехід до архітектури Zero Trust є особливо виправданим та ефективним у контексті гетерогенних мереж, які за своєю природою містять значну кількість різноманітних елементів та створюють унікальні виклики для традиційних моделей безпеки. Адаптація ZT дозволяє нівелювати багато з цих викликів, пропонуючи більш гранулярний, динамічний та орієнтований на дані підхід до захисту.

Архітектура Zero Trust є особливо актуальною та ефективною для захисту саме гетерогенних мереж з огляду на виклики, які вони створюють. Основні причини релевантності:



Рисунок 1.8 – Відповідність принципів Zero Trust викликам гетерогенних мереж

1. Управління різноманітністю
2. Мікросегментація як відповідь на розширену поверхню атаки
3. Контроль доступу в умовах розмитого периметра
4. Динамічна адаптація політик
5. Фокус на захисті даних

Управління різноманітністю означає, що принципи Zero Trust дозволяють застосовувати уніфіковані підходи до контролю доступу незалежно від типу пристрою, ОС чи місцезнаходження ресурсу. Ідентифікація та сувора автентифікація кожного запиту допомагає керувати довірою в середовищі з великою кількістю неконтрольованих або малоконтрольованих елементів. Наприклад, незалежно від пристрою або місця користувача, доступ до корпоративної бази даних буде надаватися лише після перевірки ідентичності, стану пристрою та контексту запиту.

Мікросегментація як відповідь на розширену поверхню атаки забезпечує ізоляцію критичних ресурсів та обмеження поширення атаки. У гетерогенних мережах, де є пристрої з обмеженим захистом (наприклад, IoT), мікросегментація створює логічно ізольовані зони, що дозволяє уникнути компрометації критичних систем, навіть якщо інший пристрій зламано.

Контроль доступу в умовах розмитого периметра означає, що ZT розглядає кожен ресурс як окремий об'єкт захисту. Це дозволяє надати доступ лише до конкретних ресурсів після перевірки через механізми ZTNA, що замінює традиційні VPN. Такий підхід знижує ризик несанкціонованого доступу, навіть якщо облікові дані чи пристрій скомпрометовано.

Динамічна адаптація політик дозволяє змінювати рівень доступу в реальному часі залежно від контексту (геолокація, стан пристрою, поведінка користувача). Це забезпечує високий рівень гнучкості у гетерогенних середовищах, де сценарії використання постійно змінюються.

Фокус на захисті даних передбачає, що незалежно від місця зберігання чи передачі (локально, у хмарі, на мобільних пристроях) застосовуються заходи шифрування, класифікації, DLP та доступу за мінімальними привілеями. Це гарантує, що лише уповноважені користувачі можуть взаємодіяти з чутливою інформацією.

1.4.2. Огляд моделей та стандартів реалізації Zero Trust

Для практичної реалізації архітектури Zero Trust існує низка моделей та стандартів, які надають керівні принципи та рекомендації.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Одним з найвпливовіших документів є **NIST Special Publication 800-207 "Zero Trust Architecture"**[1]. Цей стандарт визначає абстрактну модель Zero Trust, її логічні компоненти (Policy Engine, Policy Administrator, Policy Enforcement Point), а також різні підходи до проєктування та сценарії розгортання.

Logical Components of the a Zero Trust Architecture according to NIST SP 800-207

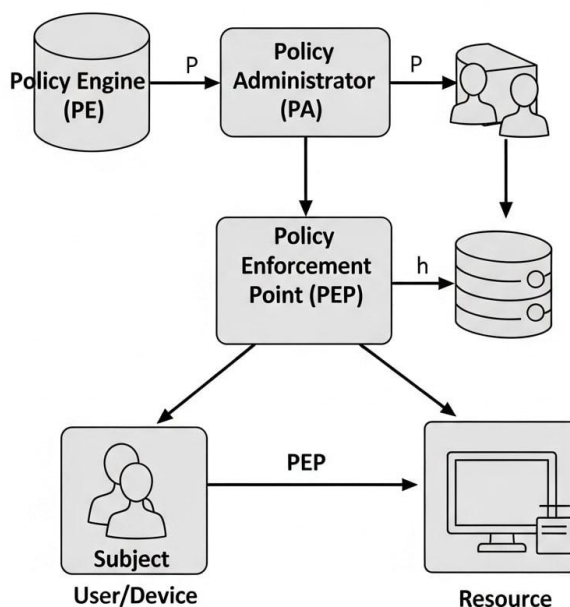


Рисунок 1.9 – Логічні компоненти архітектури Zero Trust

Окрім NIST, існують інші моделі та концептуальні підходи, які часто використовуються при побудові ZT:

1. Zero Trust Network Access (ZTNA)
2. Identity-Defined Security
3. Software-Defined Perimeter (SDP)
4. Мікросегментація на основі програмного забезпечення (Software-Based Microsegmentation)

Zero Trust Network Access (ZTNA) фокусується на наданні захищеного доступу до конкретних додатків та сервісів на основі ідентифікації користувача та стану пристрою, замінюючи традиційні VPN. ZTNA перевершує VPN у гетерогенних кон-

текстах, оскільки забезпечує гранулярний доступ "додаток-до-додатку" або "користувач-до-додатку", а не широкий доступ до всієї мережі. Це зменшує поверхню атаки й краще підходить для хмарних сервісів і сценаріїв BYOD [2][3].

Identity-Defined Security розглядає ідентичність (користувача, пристрою, сервісу, додатку) як новий периметр безпеки. У гетерогенних мережах, де неможливо довіряти фізичному розташуванню або типу пристрою, ключовим фактором для надання доступу є підтверджена ідентичність. Підхід вимагає використання SSO, MFA та ефективного управління життєвим циклом ідентичностей.

Software-Defined Perimeter (SDP) створює логічно ізольовані мережі, у яких ресурси залишаються невидимими для неавторизованих користувачів. SDP працює за принципом "спочатку автентифікація, потім доступ", що унеможливорює навіть виявлення ресурсів без попередньої перевірки. Це особливо ефективно для ізоляції чутливих IoT-пристроїв або захисту застарілих систем [11].

Мікросегментація на основі програмного забезпечення (Software-Based Microsegmentation) дозволяє створювати детальні політики безпеки для окремих додатків або робочих навантажень, незалежно від фізичної топології мережі. Вона є більш гнучкою, ніж традиційна VLAN-сегментація, і підходить для захисту динамічних середовищ: віртуальних машин, контейнерів, хмарних сервісів — навіть в межах одного сервера або середовища.

Вибір конкретної моделі або комбінації підходів залежить від специфіки організації, її IT-інфраструктури, наявних ресурсів, бізнес-цілей та цілей безпеки. Часто ефективна реалізація Zero Trust вимагає поєднання елементів з різних моделей.

1.4.3 Стратегії практичного впровадження Zero Trust в гетерогенних мережах.

Впровадження архітектури Zero Trust у складних гетерогенних середовищах — це не одномоментна задача, а довготривалий процес, що вимагає стратегічного планування та поетапної реалізації.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Поетапний підхід (Phased Approach): Спроба одночасно трансформувати всю ІТ-інфраструктуру за принципами Zero Trust (підхід "big bang") є надзвичайно ризикованою, дорогою та може призвести до значних збоїв у роботі бізнес-процесів, особливо в гетерогенних мережах з великою кількістю взаємозалежних компонентів. Натомість рекомендується поетапний підхід. Починати варто з ідентифікації найбільш критичних активів, процесів або зон з високим ризиком. Це можуть бути пілотні проєкти, наприклад, впровадження ZTNA для захисту віддаленого доступу до ключових додатків, мікросегментація навколо баз даних з чутливою інформацією, або посилення контролю доступу для привілейованих користувачів. Успішна реалізація таких пілотних проєктів дозволить отримати практичний досвід, продемонструвати переваги підходу та поступово розширювати застосування принципів ZT на інші частини інфраструктури.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Етапи впровадження архітектури Zero Trust

ІДЕНТИФІКАЦІЯ ПОВЕРХНІ
ЗАХИСТУ (ДАНІ, АКТИВИ,
ДОДАТКИ, СЕРВІСИ)



МАПУВАННЯ ПОТОКІВ
ТРАНЗАКЦІЙ



ПРОЄКТУВАННЯ
АРХІТЕКТУРУ ZT



ВИЗНАЧЕННЯ
ПОЛІТИК ZT



ВИБІР ТА ВПРОВАДЖЕННЯ
ТЕХНОЛОГІЙ



МОНІТОРИНГ
ТА ПІДТРИМКА

Рисунок 1.10 – Етапи впровадження архітектури Zero Trust

1. Інвентаризація та класифікація активів
2. Управління ідентифікацією як центральний елемент
3. Інтеграція з існуючими системами (включно із застарілими – Legacy Systems)
4. Забезпечення всебічної видимості та аналітики
5. Автоматизація політик безпеки та реагування

Інвентаризація та класифікація активів — це основа для будь-якої ініціативи Zero Trust, що полягає у повному розумінні того, що саме потрібно захищати. В гетерогенних мережах це завдання ускладнюється через різноманітність пристроїв, операційних систем і додатків. Необхідно провести ретельну інвентаризацію всіх апаратних та програмних активів, користувачів та потоків даних, а також класифікувати їх за ступенем критичності.

Управління ідентифікацією як центральний елемент означає, що оскільки Zero Trust базується на принципі "ніколи не довіряй, завжди перевіряй", надійна ідентифікація та автентифікація є наріжним каменем. Це передбачає впровадження сильної багатофакторної автентифікації (MFA), технологій єдиного входу (SSO) та управління привілейованим доступом (PAM) для суворого контролю над усіма типами користувачів та пристроїв.

Інтеграція з існуючими системами (включно із застарілими – Legacy Systems) передбачає застосування стратегій, що дозволяють "обгорнути" ці системи шаром безпеки Zero Trust, оскільки їх повна заміна часто є неможливою. Це може включати ізоляцію систем у мікросегментах або використання шлюзів доступу та проксі-серверів, які виступають посередниками і застосовують політики безпеки до запитів, адресованих до застарілих систем.

Забезпечення всебічної видимості та аналітики являє собою критично важливий процес для ефективної роботи моделі Zero Trust. Він полягає у впровадженні інструментів (таких як SIEM, UEBA, NDR) для централізованого збору, агрегації та аналізу подій безпеки з різноманітних джерел. Це надає інформацію, необхідну для прийняття обґрунтованих рішень щодо політик доступу та виявлення потенційних атак.

Автоматизація політик безпеки та реагування допомагає забезпечити послідовне, своєчасне та масштабоване застосування політик Zero Trust, оскільки ручне управління політиками безпеки для кожного користувача, пристрою та ресурсу в масштабній гетерогенній мережі є практично неможливим та схильним до помилок. Автоматизація допомагає забезпечити послідовне, своєчасне та масштабоване застосування політик Zero Trust. Це може включати автоматичне призначення прав

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

доступу на основі атрибутів користувача та пристрою, динамічну зміну політик залежно від контексту та рівня ризику, а також автоматизоване реагування на виявлені інциденти безпеки. Наприклад, при виявленні шкідливого програмного забезпечення на кінцевій точці система може автоматично ізолювати цей пристрій від мережі або відкликати його права доступу до критичних ресурсів до усунення загрози..

Реалізація цих стратегій дозволить організації поступово та ефективно трансформувати свою систему безпеки відповідно до принципів Zero Trust, значно підвищивши рівень захищеності своєї гетерогенної мережі.

Висновки до розділу 1

У першому розділі було проведено аналіз концептуальних засад побудови захищених гетерогенних мереж з використанням архітектури Zero Trust. Розглянуто сутність, структуру та специфічні виклики безпеки гетерогенних ІТ-середовищ, а також обмеження традиційних підходів до їх захисту.

Детально проаналізовано філософію, ключові принципи та компоненти архітектури Zero Trust, яка пропонує парадигму "ніколи не довіряй, завжди перевіряй". Оцінено переваги такого підходу, серед яких покращений захист від сучасних загроз, зменшення поверхні атаки та краща адаптивність до динамічних ІТ-ландшафтів. Водночас визначено потенційні складності та недоліки, пов'язані з комплексністю реалізації, вартістю та необхідністю культурних змін в організації.

Обґрунтовано високу релевантність застосування принципів Zero Trust саме для гетерогенних мереж, оскільки цей підхід дозволяє ефективно управляти різноманітністю компонентів, контролювати доступ в умовах розмитого периметра та обмежувати поширення загроз за допомогою мікросегментації. Наведено огляд ключових стандартів, зокрема NIST SP 800-207, та моделей реалізації Zero Trust.

Отримана теоретична база створює необхідне підґрунтя для переходу до наступних етапів дипломної роботи, а саме – проєктування конкретної моделі захищеної гетерогенної мережі організації та її практичного моделювання з впровадженням елементів архітектури Zero Trust.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Розділ 2. Проектування захищеної гетерогенної мережі організації з використанням архітектури Zero Trust

2.1. Аналіз мережної інфраструктури організації для формування вимог щодо захисту на базі архітектури Zero Trust

2.1.1. Опис організації та її IT-інфраструктури

Для розробки проекту захищеної гетерогенної мережі на базі архітектури Zero Trust обрана організація «DataSecure Group». Це комерційна структура, яка спеціалізується на наданні послуг у сфері обробки великих даних, консалтингу з кібербезпеки, а також розробки та підтримки внутрішніх інформаційних систем для клієнтів корпоративного сегменту.

Організація має один центральний офіс, розташований у багатоповерховій будівлі, і підтримує гібридну модель роботи, яка передбачає можливість як локального, так і віддаленого доступу співробітників до корпоративних ресурсів. Частина персоналу працює безпосередньо в офісі, інші — з використанням захищених каналів зв'язку із зовнішніх локацій. Загальна чисельність співробітників складає приблизно 120 осіб, серед яких:

1. IT-відділ: адміністратори, розробники, технічна підтримка;
2. Аналітики, що працюють із чутливою інформацією клієнтів;
3. Бухгалтери: фінансовий та юридичний відділи;
4. Адміністративно-керівний персонал;
5. Тимчасові підрядники, гостьові користувачі та аудитори.
6. IoT пристрої

Інформаційна інфраструктура організації є гетерогенною, тобто включає різні типи пристроїв, платформ, операційних систем, мережевих технологій і сервісів. Її побудовано з урахуванням потреб масштабованості, продуктивності, гнучкості доступу та підвищених вимог до безпеки.

Основними компонентами IT-інфраструктури є:

1. Клієнтські пристрої.
2. Серверна інфраструктура.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

3. Мережеве обладнання.
4. Хмарні сервіси.
5. IoT-інфраструктура.
6. Підключення до Інтернету.

До клієнтських пристроїв входить:

- Робочі станції з ОС Windows 10 у бухгалтерії, юридичному відділі, керівництві;
- Лаптопи розробників та аналітиків із Linux/Windows;
- Особисті мобільні пристрої співробітників (BYOD), що використовують захищене підключення до Wi-Fi.

До серверної інфраструктури входить:

- Веб-сервери для розміщення внутрішніх і клієнтських порталів;
- Бази даних PostgreSQL/MySQL для зберігання фінансової, аналітичної та внутрішньої інформації;
- Файлові сервери для спільного доступу до проєктних матеріалів;
- Сервер резервного копіювання, налаштований на створення регулярних бекапів;
- Служби каталогів (Active Directory) для централізованої автентифікації та авторизації користувачів.

До мережного обладнання входить:

- L2-комутатори доступу з підтримкою 802.1Q (VLAN);

До хмарних сервісів входить:

- Microsoft 365 (Exchange Online, OneDrive, Teams, Entra ID);
- Хмарне сховище Amazon S3 для архівних та резервних даних;
- VPN-служба з двофакторною автентифікацією для безпечного віддаленого підключення.

До IoT-інфраструктури входить:

- Камери відеоспостереження із записом на внутрішній NAS;
- Сенсори температури, вологості та руху в серверній кімнаті;

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

- Електронна система контролю доступу до приміщень на основі смарт-карт.

До підключення до інтернету входить:

- Два надійних інтернет-провайдери із виділеним каналом зв'язку;
- Комунікація з глобальною мережею здійснюється через маршрутизатор ядра;
- Використання UPS (джерел безперебійного живлення) для підтримки стабільної роботи основних вузлів;
- Створено окрему DMZ-зону для розміщення публічних сервісів (API, зовнішній портал клієнтів) з можливістю доступу з Інтернету під контролем міжмережевого екрану.

Інфраструктура компанії перебуває на етапі модернізації, яка здійснюється паралельно з впровадженням архітектури Zero Trust. Такий підхід передбачає не лише оновлення технічної бази, а й повну реконцепцію моделей доступу, перевірки довіри, сегментації ресурсів та централізованого контролю над користувачами, пристроями й мережевим трафіком.

Для ефективного функціонування IT-інфраструктури «DataSecure Group», забезпечення її масштабованості, керованості та високого рівня безпеки, необхідно обрати архітектурну модель побудови корпоративної мережі. Типовим для побудови IT-інфраструктур є застосування 3-и рівневої ієрархічної моделі Cisco та моделі Spine-Leaf.

У моделі Cisco виділяють три рівні: Access (доступ), Distribution (розподіл), Core (ядро), що дає такі переваги як чіткий розподіл функцій, легкість управління, масштабованість, можливість впровадження політик безпеки на різних рівнях. Водночас ця модель має певні недолік, а саме: відносно більша вартість у порівнянні з простішими моделями.

У моделі Spine-Leaf мережа складається з двох рівнів: Spine (хребет) та Leaf (листки). Така структура забезпечує рівномірний розподіл навантаження, низьку затримку передачі даних та високу пропускну здатність, що особливо ефективно

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

для горизонтального трафіку між серверами. Водночас модель має і певні обмеження: складність впровадження, потреба у значній кількості портів та не повна оптимальність для традиційних офісних середовищ, де переважає трафік "клієнт–сервер".

Беручи до уваги масштаби та завдання організації, змішаний характер трафіку (клієнт-сервер, хмара, віддалений доступ), а також гетерогенне середовище з різними типами клієнтських пристроїв, операційних систем та сервісів, було прийнято рішення використовувати трирівневу ієрархічну модель Cisco. Вона забезпечує гнучкість, надійність, безпечну маршрутизацію між сегментами мережі та ефективну сегментацію на основі VLAN.

Опис рівнів обраної топології

- **Рівень ядра (Core):** високошвидкісна маршрутизація, мінімізація затримок, з'єднання з провайдером, резервування.
- **Рівень розподілу (Distribution):** маршрутизація між VLAN, застосування політик безпеки (ACL), агрегація трафіку з комутаторів доступу.
- **Рівень доступу (Access):** підключення кінцевих пристроїв, призначення VLAN, реалізація Port Security, 802.1X, DHCP тощо.

У рамках дипломної роботи для аналізу рівня захисту і подальшого впровадження архітектури Zero Trust було змодельовано спрощену базову мережу організації, яка умовно відображає один із поверхів офісу або початковий варіант мережевої інфраструктури до етапу модернізації. У цій конфігурації відсутні мікросегментація, централізований контроль доступу та міжмережеве зонування, що дозволяє виявити основні вразливості, які мають бути усунуті під час переходу до нової архітектури безпеки.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

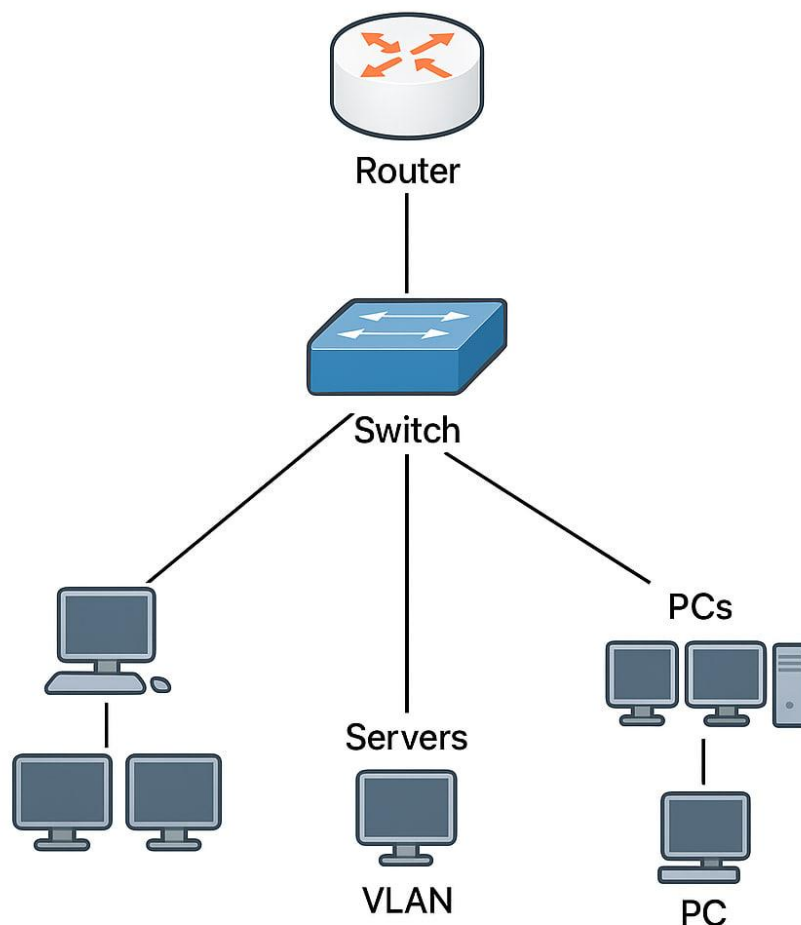


Рисунок 2.1 – Спрощена модель базової мережі організації до модернізації

2.1.2. Визначення активів, що підлягають захисту, та потенційних векторів атак

В межах проектування захищеної гетерогенної мережі організації «DataSecure Group» одним з ключових етапів є виявлення інформаційних активів, що потребують захисту, а також аналіз потенційних векторів атак, які можуть бути використані для їх компрометації.

Критичні активи організації класифіковано за кількома категоріями, відповідно до їхнього значення для бізнес-процесів та рівня конфіденційності оброблюваних даних:

1. Інформаційні активи:

- Бази даних клієнтів, фінансова інформація, внутрішня документація

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

(PostgreSQL, MySQL).

- Внутрішні портали та CRM-системи, доступні через веб-інтерфейс.
- Корпоративна електронна пошта, хмарне сховище з конфіденційними файлами (Microsoft 365, OneDrive).
- Аналітичні звіти, які формуються аналітиками на основі конфіденційних даних клієнтів.

2. Інфраструктурні активи:

- Сервери, на яких розгорнуті внутрішні сервіси, сервіси зберігання та резервного копіювання.
- Засоби ідентифікації та автентифікації (Active Directory, Entra ID).
- Комутатори та маршрутизатори, що забезпечують маршрутизацію та VLAN-сегментацію.
- Система відеоспостереження, сенсори безпеки та контролю доступу.

3. Користувачі та їхні пристрої:

- Постійні працівники (офісні та віддалені), які мають доступ до чутливих систем.
- Підрядники та тимчасові користувачі.
- Особисті мобільні пристрої співробітників (BYOD).

4. Хмарні сервіси та віддалений доступ:

- VPN-інфраструктура з двофакторною автентифікацією.
- Веб-інтерфейси до внутрішніх систем (портали клієнтів).
- Хмарні сховища, API-доступ до систем для зовнішніх клієнтів.

З урахуванням гетерогенного характеру мережі та багаторівневого доступу, можливі такі основні вектори атак:

1. Фішингові атаки та крадіжка облікових даних:

- Спрямовані на користувачів з доступом до критичних сервісів (аналітики, IT-персонал).
- Можуть призвести до отримання доступу до корпоративних ресурсів через компрометацію облікових записів.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

2. Використання незахищених або неконтрольованих пристроїв (BYOD, IoT):

- Мобільні пристрої, що підключаються до корпоративної Wi-Fi-мережі.
- IoT-пристрої з базовим або відсутнім захистом, які можуть бути використані як точка входу в мережу.

3. Атаки на віддалений доступ:

- Зловмисники можуть спробувати обійти VPN або скомпрометувати канали віддаленого з'єднання.
- Потенційна експлуатація слабких політик автентифікації або відсутність перевірки стану клієнтських пристроїв.

4. Внутрішні загрози (insider threats):

- Несанкціоноване використання прав доступу або спроби передачі даних стороннім особам.
- Навмисні або випадкові дії працівників, що можуть поставити під загрозу цілісність або конфіденційність даних.

5. Недоліки в сегментації мережі:

- Недостатньо ізольовані VLAN-сегменти можуть дозволити переміщення зловмисника мережею (lateral movement) після первинного проникнення.
- Відсутність мікросегментації на рівні сервісів і даних.

6. Атаки на служби автентифікації та директорії:

- Наприклад, спроби компрометації Active Directory або Entra ID.
- Pass-the-hash, Golden Ticket або brute-force атаки.

7. Зовнішні DDoS-атаки на публічні сервіси:

- Напади на зовнішній портал замовника або відкриті API з метою виведення з ладу сервісів або витоку даних.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

2.1.3. Формулювання політик безпеки на основі принципів Zero Trust

Впровадження архітектури Zero Trust в організації «DataSecure Group» потребує чіткого визначення та формалізації політик безпеки, які регламентують доступ до інформаційних ресурсів на основі концепції «ніколи не довіряй, завжди перевіряй». Ці політики мають враховувати контекст запиту, мінімізацію привілеїв, перевірку стану пристрою та контроль активностей користувачів.

Основні принципи формування політик

1. Аутентифікація та ідентифікація

- Усі суб'єкти (користувачі, пристрої, додатки) повинні проходити **багатофакторну автентифікацію (MFA)**.
- Ідентифікація базується на унікальних облікових даних, сертифікатах або токенах.
- Підтримка єдиного входу (SSO) через Entra ID для підвищення зручності без зниження рівня безпеки.

2. Принцип мінімальних привілеїв (Least Privilege Access)

- Доступ надається виключно до тих ресурсів, які потрібні для виконання посадових обов'язків.
- Усі політики побудовані за принципом "**Just Enough Access**" і, де можливо, "**Just-in-Time Access**".
- Для адміністративного доступу впроваджуються тимчасові права з автоматичним відкликанням.

3. Контекстно-залежний доступ

- Рішення про надання доступу враховує:
 1. Геолокацію користувача
 2. Тип та стан пристрою (наявність оновлень, антивірусу, шифрування)
 3. Час доби та частоту доступу
 4. Поведінкові аномалії
- Доступ із підозрілих середовищ (публічні Wi-Fi, нетипові країни) обмежується або потребує додаткової перевірки.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Мікросегментація

- Всі VLAN розділені логічно за функціональними групами (аналітики, розробники, керівництво, IoT).
- Доступ між сегментами контролюється за допомогою **ACL, фаєрволів**, а згодом — через **програмно-визначені політики (SDP)**.
- Усі критичні сервери (бази даних, AD, NAS) — ізольовані у власних мікросегментах з обмеженим доступом.

5. Моніторинг, аналітика та аудит

- Усі дії користувачів та системних процесів логуються в **SIEM-систему**.
- Реалізовано виявлення аномальної поведінки через **UEBA**, що дозволяє виявляти потенційно шкідливу активність навіть за наявності валідних облікових даних.
- Політики щоквартально переглядаються з урахуванням інцидентів і змін у структурі організації.

6. Політики захисту даних

- Уся конфіденційна інформація класифікується за рівнем чутливості.
- Для даних високої чутливості застосовується:
 1. **Шифрування** (на диску, при передачі, у хмарі)
 2. **Політики DLP** (Data Loss Prevention)
 3. Обмеження на копіювання, друк, пересилання даних зовнішнім користувачам

7. Доступ третіх сторін та підрядників

- Гостьовий доступ реалізується через сегментовану мережу з чіткими часовими рамками.
- Всі підрядники автентифікуються через тимчасові акаунти з обмеженням прав доступу.
- Зовнішній доступ до ресурсів дозволяється виключно через шлюз ZTNA з перевіркою пристрою.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2. Проектування удосконаленої IT-інфраструктури організації

2.2.1. Проектування фізичної та логічної топології мережі

Проектування фізичної та логічної структури мережі є базовим етапом при побудові захищеної IT-інфраструктури організації в контексті архітектури Zero Trust.

Для реалізації моделі обрано топологію із **одним маршрутизатором, шістьма комутаторами, одним фаєрволом pfSense**, а також **віртуальними машинами**, що емулюють користувачів і сервери:

- **Маршрутизатор (R1)** — виконують функції міжвланової маршрутизації та реалізації ACL.
- **Комутатори L2 (SW1–SW6)** — об'єднують кінцеві пристрої в окремі VLAN та передають трафік до маршрутизаторів через trunk-з'єднання.
- **pfSense** — розміщується між сегментами з різним рівнем довіри та виконує функції фільтрації.
- **Клієнтські машини (PC1–PC15)** — розміщуються у різних VLAN (аналітики, бухгалтерія, керівництво, IoT, гостьова зона).
- **Ubuntu** — емуляція звичайного користувача або адміністратора.
- **Windows** — емуляція звичайного користувача або адміністратора.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

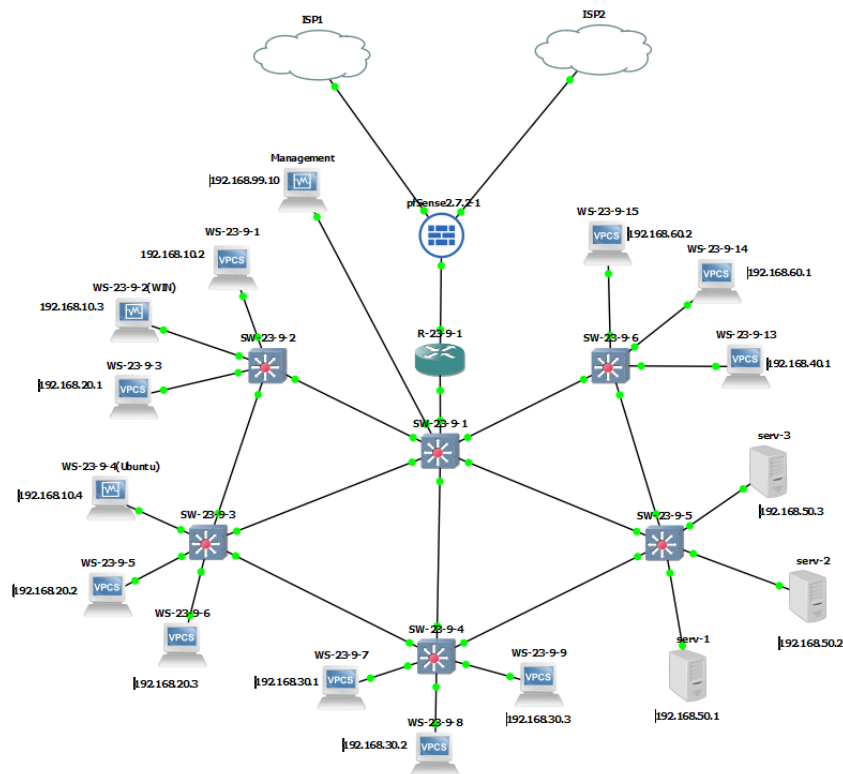


Рисунок 2.2 – Загальна топологія спроектованої мережі

Логічна мережа базується на мікросегментації та поділі на **зони довіри**. Кожен функціональний підрозділ організації ізольований в межах окремого VLAN:

Усі VLAN передаються через trunk-інтерфейси до маршрутизаторів, де створено підінтерфейси з відповідними IP-адресами. Міжвлановий трафік дозволяється лише згідно з ACL, визначеному на маршрутизаторі R1.

1. **Ізоляція сегментів:** у базовій конфігурації трафік між VLAN заблокований.
2. **Міжсегментна маршрутизація:** дозволяється лише через фаєрвол pfSense, який розміщений між маршрутизатором і Інтернетом.
3. **Наявність DMZ-зони:** можлива симуляція доступу до умовних публічних сервісів (веб-сайтів, API) через окремий сегмент.
4. **Інтеграція RADIUS:** для централізованої автентифікації користувачів.
5. **Гнучкість:** топологію легко масштабувати — можна додавати нові VLAN, вузли або сервіси.

З метою реалізації концепції Zero Trust, топологія мережі умовно представляє частину офісу компанії, імітуючи різні сегменти, пристрої та міжмережеві взаємодії.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2.2. Проектування схеми VLAN-сегментації

Одним із базових технічних механізмів реалізації принципів Zero Trust у корпоративній мережі є **логічне розділення мережевого трафіку на сегменти** за допомогою технології **VLAN (Virtual Local Area Network)**. Мікросегментація дозволяє мінімізувати взаємодію між пристроями різного призначення, обмежити зону поширення потенційних атак та реалізувати диференційовані політики доступу на міжсегментному рівні.

В рамках моделі, для організації «DataSecure Group», було спроектовано чітку схему VLAN-сегментації з урахуванням структурної організації компанії, ролей користувачів та рівня довіри до пристроїв.

Таблиця 2.1.

Схема VLAN-сегментації

VLAN ID	Назва сегмента	IP-підмережа	Призначення	Рівень довіри
10	Аналітика	192.168.10.0/24	Робочі станції аналітиків	Середній
20	Бухгалтерія	192.168.20.0/24	ПК фінансового відділу	Середній
30	Керівництво	192.168.30.0/24	Директор, топменеджмент	Високий
40	Гостьова зона	192.168.40.0/24	Тимчасові користувачі, Wi-Fi	Низький
50	Серверна зона	192.168.50.0/24	Веб-сервери, БД, DNS, AD	Високий
60	ІоТ-пристрої	192.168.60.0/24	Камери, сенсори, пристрої контролю	Низький
99	Менеджмент	192.168.99.0/24	Адміністративний доступ до обладнання	Високий

1. Функціональна ізоляція
2. Розмежування рівнів довіри
3. Обмеження широкомовного трафіку
4. Маршрутизація між VLAN
5. Обслуговування через trunk-з'єднання

Функціональна ізоляція передбачає, що кожен VLAN створено відповідно до логічної структури організації — відділи, серверні служби, IoT, гостьовий доступ. Це дозволяє накладати окремі політики контролю доступу для кожного типу трафіку.

Розмежування рівнів довіри означає, що високочутливі ресурси (сервери, AD, фінансові ПК) відокремлені від нестабільних або відкритих зон (гостьові, IoT), що повністю відповідає моделі зонування Zero Trust.

Обмеження широкомовного трафіку — це важлива перевага VLAN, яка дозволяє зменшити кількість широкомовних запитів (broadcast), що позитивно впливає на продуктивність та зменшує ризики атаки.

Маршрутизація між VLAN являє собою процес, за якого усі міжвланові з'єднання проходять через маршрутизатор. На ньому реалізовано підінтерфейси зі списками контролю доступу (ACL), що дозволяють або блокують доступ між сегментами згідно з політиками безпеки.

Обслуговування через trunk-з'єднання — це механізм, за допомогою якого трафік усіх VLAN передається до маршрутизатора або фаєрвола через спеціальні trunk-порти комутаторів. Такий підхід дозволяє централізовано обробляти та фільтрувати весь трафік.

2.2.3. Розробка схеми IP-адресації

Схема IP-адресації є важливим елементом проєктування мережі, що впливає на її масштабованість, керованість і безпеку. У контексті архітектури Zero Trust адресація також слугує засобом логічної ідентифікації зон довіри, а також спрощує застосування міжсегментних політик контролю доступу.

Для моделі, реалізованої в середовищі GNS3, застосовано приватну IP-адресацію в межах діапазону **192.168.0.0/16**, із поділом на підмережі для кожного VLAN-сегмента. Префікс кожної підмережі логічно відповідає номеру VLAN, що підвищує зручність адміністрування, підтримку структури зон довіри, а також спрощує налагодження та аудит.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Таблиця 2.2.

Принципи адресації

VLAN ID	Назва сегмента	IP-підмережа	Приклад шлюзу	Маска	Призначення
10	Аналітика	192.168.10.0/24	192.168.10.1	/24	Робочі станції аналітиків
20	Бухгалтерія	192.168.20.0/24	192.168.20.1	/24	ПК фінансового відділу
30	Керівництво	192.168.30.0/24	192.168.30.1	/24	Директор, топменеджмент
40	Гостьова зона	192.168.40.0/24	192.168.40.1	/24	Тимчасові користувачі, Wi-Fi
50	Серверна зона	192.168.50.0/24	192.168.50.1	/24	Веб-сервери, БД, DNS, AD
60	IoT-пристрої	192.168.60.0/24	192.168.60.1	/24	Камери, сенсори, пристрої контролю
99	Management	192.168.99.0/24	192.168.99.1	/24	Доступ до маршрутизатора, pfSense

Для всіх VLAN обрано уніфіковану маску /24, що надає до 254 доступних IP-адрес у кожному сегменті. Хоча для деяких зон (наприклад, керівництво або IoT-пристрої) це перевищує поточні потреби, уніфікація забезпечує простоту налаштування, стандартизацію політик контролю (ACL, фаєрвол) і значний резерв для подальшого масштабування без необхідності редизайну мережі.

Номер VLAN логічно співпадає з третім октетом IP-адреси (наприклад, VLAN 10 → 192.168.10.0/24). Такий підхід спрощує розпізнавання трафіку, створення політик безпеки та трасування маршрутів у процесі обслуговування та моніторингу мережі

Для кожного сегмента перша доступна IP-адреса (192.168.x.1) зарезервована для шлюзу за замовчуванням. Цей шлюз реалізується як підінтерфейс маршрутизатора або фаєрволу pfSense з підтримкою 802.1Q. Така стандартизація прискорює конфігурацію та знижує ймовірність помилок.

Адресна схема дозволяє швидко визначати джерело трафіку, зону, роль і привілейований рівень пристрою. Це критично важливо для реалізації Zero Trust, де

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

доступ залежить не лише від VLAN або імені користувача, але й від IP-адреси, контексту пристрою й мережевого середовища. У моделі використовується змішаний підхід:

- Динамічна адресація (DHCP) застосовується для клієнтських сегментів: серверів, аналітики, бухгалтерії та гостьовій зоні. DHCP-сервер може бути реалізований на маршрутизаторі або окремому сервері.
- Статичні IP-адреси використовуються на шлюзах на роутері і на pfSense. Ці адреси виключені з діапазонів DHCP.

Хоча у проєкті реалізовано IPv4 через його простоту у лабораторному середовищі GNS3, запропонована адресна структура логічно готова до впровадження IPv6 за моделлю dual-stack. У разі переходу організації на нову адресацію впровадження IPv6 можливе без змін у структурі VLAN або зонуванні, що забезпечує довгострокову актуальність архітектури.

2.3. Проєктування підсистеми захисту гетерогенної мережі з використанням принципів Zero Trust

2.3.1. Вибір моделі реалізації Zero Trust

З урахуванням особливостей IT-інфраструктури організації «DataSecure Group», а також виявлених загроз і політик безпеки, доцільно впроваджувати **комбіновану модель архітектури Zero Trust**, яка інтегрує елементи кількох підходів: **ZTNA (Zero Trust Network Access)**, **SDP (Software-Defined Perimeter)** та **Identity-Based Security**.

1. Гібридна модель роботи (офіс + віддалений доступ):

- Потребує динамічного контролю доступу, що змінюється залежно від геолокації, пристрою та ризиків.
- Традиційні VPN не забезпечують достатнього контролю після встановлення з'єднання.
- **ZTNA** дозволяє забезпечити доступ лише до визначених ресурсів після автентифікації та перевірки стану пристрою.

2. Високий ступінь гетерогенності середовища:

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

- Присутні різні ОС (Windows, Linux), особисті мобільні пристрої (BYOD), IoT-компоненти.
- Вимагає однакового рівня контролю для різнорідних об'єктів доступу — як для серверів, так і для пристроїв користувачів.
- **Identity-Based Security** дозволяє керувати доступом через атрибути користувача, роль, тип пристрою, контекст.

3. Потреба у мікросегментації:

- Розподіл на VLAN та логічні сегменти вже реалізовано, але не вистачає засобів ізоляції критичних ресурсів.
- **SDP** дозволяє зробити системи «невидимими» для неавторизованих користувачів навіть усередині корпоративної мережі.

2.3.2. Паралельне впровадження архітектури Zero Trust під час модернізації мережевої інфраструктури

З метою забезпечення високого рівня інформаційної безпеки в умовах гетерогенного середовища організації «DataSecure Group», в рамках даної дипломної роботи впроваджено архітектуру Zero Trust як частину загальної модернізації мережевої інфраструктури, яка раніше не забезпечувала належного рівня ізоляції, автентифікації та контролю доступу. Її впровадження передбачає повну реконцепцію механізмів довіри, контролю доступу та сегментації корпоративної мережі.

1. «Ніколи не довіряй, завжди перевіряй»
2. Мінімізація привілеїв (Least Privilege Access)
3. Мікросегментація
4. Постійний моніторинг і аудит

«Ніколи не довіряй, завжди перевіряй» — це фундаментальний принцип, який означає, що жоден пристрій або користувач не вважається надійним за замовчуванням, незалежно від його фізичного чи логічного розташування в мережі.

Мінімізація привілеїв (Least Privilege Access) передбачає, що доступ до ресурсів надається користувачам виключно в межах, необхідних для виконання їхньої визначеної ролі, завдання та з урахуванням поточного контексту.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Мікросегментація являє собою підхід, за якого мережа логічно поділена на невеликі, ізольовані сегменти (в нашому випадку — VLAN) із суворим контролем трафіку між ними.

Постійний моніторинг і аудит — це процес, за якого усі запити до ресурсів та дії користувачів безперервно реєструються й підлягають аналізу з метою своєчасного виявлення потенційних аномалій та загроз безпеці.

1. Маршрутизатор Cisco (IOS)
2. Комутатори L2
3. pfSense
4. FreeRADIUS
5. Клієнтські машини (VPCS, QEMU-VM)

Маршрутизатор Cisco (IOS) відповідає за реалізацію міжвланової маршрутизації та фільтрацію внутрішнього трафіку за допомогою списків контролю доступу (ACL).

Комутатори L2 слугують для моделювання мікросегментації на рівні доступу, розділяючи мережу на логічно ізольовані домени за допомогою технології VLAN.

pfSense виконує роль фаєрвола, периметрового міжмережевого екрана, шлюзу в Інтернет та NAT.

FreeRADIUS забезпечує централізовану автентифікацію пристроїв.

Клієнтські машини (VPCS, QEMU-VM) емулюють робочі місця користувачів з різними ролями — аналітики, розробники, гостьові користувачі, адміністратори, а також імітують роботу серверів.

2.3.3. Забезпечення безпеки взаємодії між сегментами мережі в контексті Zero Trust

У межах архітектури Zero Trust важливим елементом є не лише ізоляція ресурсів, але й **контроль взаємодії між окремими сегментами мережі**. Така взаємодія повинна відбуватися виключно на основі чітко визначених політик до-

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

ступу, контекстної перевірки, автентифікації та моніторингу. У моделі корпоративної мережі організації «DataSecure Group», побудованій у середовищі GNS3, реалізовано низку технічних рішень, що забезпечують безпечну взаємодію між сегментами згідно з принципами Zero Trust.

Основні механізми контролю міжсегментної взаємодії

1. Міжвланова маршрутизація з ACL

- Усі міжсегментні з'єднання реалізуються через маршрутизатор, на якому налаштовані **списки контролю доступу (ACL)**.

- За замовчуванням між VLAN-комунікація заборонена; дозволи надаються **точково**, наприклад:

1. бухгалтерія може звертатися до серверу звітності (ця політика реалізована у списку доступу ZT_VLAN20_ACCOUNTANTS, де за допомогою правила `permit ip 192.168.20.0 0.0.0.255 host 192.168.50.2` надається доступ з усього VLAN 20 лише до одного конкретного сервера 192.168.50.2, що є прямою реалізацією принципу мінімальних привілеїв);

2. аналітики — до БД із клієнтськими даними;

3. гостьові VLAN — взагалі не мають доступу до внутрішніх сегментів.

2. Зонування та логічна ізоляція

- Усі сегменти мережі розподілено на **зони довіри**, кожна з яких має власні правила доступу.

- Приклад зон:

1. **високої довіри** (сервери БД, AD),

2. **контрольованої довіри** (внутрішні користувачі),

3. **низької довіри** (гостьова мережа, IoT-пристрої).

- Міжзонна взаємодія дозволена лише через фаєрвол pfSense з фільтрацією трафіку за IP, портами та додатковими умовами (час, тип запиту).

3. Логування та моніторинг міжсегментної активності

- Усі міжмережеві запити логуються та передаються до syslog-сервера.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

- Логи дозволяють виявляти спроби несанкціонованого доступу або відхилення від стандартної поведінки.

Приклад сценарію міжсегментної взаємодії

Користувач-аналітик (VLAN 10) виконує запит до **серверу БД (VLAN 50)**.
Запит проходить через:

- ACL на маршрутизаторі → дозволено звертатися лише до TCP-порту
- Логи → записуються в syslog для аудита

Особливу увагу в моделі було приділено протидії горизонтальному переміщенню зловмисника (lateral movement) — одній із найбільш поширених технік у складних цільових атаках. У традиційних корпоративних мережах компрометація одного вузла, особливо в периферійному сегменті (наприклад, гостьовому або IoT), часто дає зловмиснику змогу здійснювати сканування внутрішньої мережі, переміщуватися між сегментами та поступово отримувати доступ до критичних систем.

У впровадженій моделі архітектури Zero Trust така можливість суттєво обмежується завдяки поєднанню декількох захисних механізмів:

- **Мікросегментація** ізолює трафік в межах окремих VLAN, зводячи до мінімуму поверхню взаємодії.

- **Списки контролю доступу (ACL)** на маршрутизаторах блокують будь-яку міжсегментну комунікацію, яка не була явно дозволена відповідно до політик доступу.

- **Зонування мережі** із поділом на сегменти різного рівня довіри (висока, контрольована, низька) дозволяє диференційовано підходити до регулювання доступу між компонентами системи.

- **Модель Software Defined Perimeter (SDP)** унеможливорює видимість критичних ресурсів (наприклад, серверів баз даних або внутрішніх порталів) до моменту успішної автентифікації та авторизації користувача.

- **Межсегментний трафік додатково фільтрується фаєрволом pfSense** з урахуванням IP-адреси, протоколу, часу, ролі користувача та інших факторів.

Завдяки цим заходам навіть у разі успішної атаки на окремий пристрій у менш захищеному сегменті подальше поширення зловмисника мережею (так зване lateral

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

movement) стає технічно складним або повністю заблокованим. Такий підхід відповідає принципу Zero Trust щодо мінімізації довіри, ізоляції доступу та обмеження потенційного впливу інциденту.

Висновки до розділу 2

У другому розділі було виконано комплексне проектування захищеної гетерогенної мережі для умовної організації «DataSecure Group» з імплементацією ключових принципів архітектури Zero Trust. Роботу було проведено у кілька логічних етапів, від аналізу вимог до розробки конкретних технічних рішень та їх моделювання.

На першому етапі було сформульовано вимоги до мережі: детально описано IT-інфраструктуру організації, її гетерогенний характер, визначено критичні інформаційні та інфраструктурні активи. Аналіз потенційних векторів атак, таких як фішинг, компрометація незахищених пристроїв та ризики горизонтального переміщення, дозволив обґрунтувати необхідність переходу від традиційної моделі безпеки до Zero Trust та сформулювати відповідні політики безпеки, що базуються на принципах тотальної перевірки, мінімізації привілеїв та контекстно-залежного доступу.

На основі цих вимог було спроектовано фізичну та логічну топологію мережі, обравши за основу надійну та масштабовану трирівневу ієрархічну модель. Було розроблено детальну схему VLAN-сегментації, яка логічно ізолює функціональні підрозділи та ресурси відповідно до їх ролей та рівнів довіри. Створена схема IP-адресації забезпечила не лише керованість та простір для масштабування, але й стала інструментом для ідентифікації та контролю трафіку між сегментами.

На завершальному етапі було спроектовано підсистему захисту. Обґрунтовано вибір комбінованої моделі реалізації Zero Trust (ZTNA, SDP, Identity-Based Security), яка найкраще відповідає потребам організації з гібридною моделлю роботи. Було описано, як ці принципи реалізовано у віртуальній моделі GNS3 за допомогою таких інструментів, як фаєрвол pfSense для інспекції трафіку,

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

FreeRADIUS для централізованої автентифікації, а також списків контролю доступу (ACL) для жорсткої фільтрації. Особливу увагу було приділено механізмам протидії горизонтальному переміщенню, що є однією з ключових переваг впровадженої архітектури.

Таким чином, у другому розділі було створено комплексну модель захищеної мережі, яка демонструє практичне застосування архітектури Zero Trust для підвищення рівня безпеки, контролю та видимості у складному гетерогенному середовищі. Результати цього проєктування є основою для подальшого аналізу та тестування ефективності запропонованих рішень.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

Розділ 3. Моделювання, реалізація архітектури Zero Trust, аналіз результатів та рекомендації

3.1. Вибір середовища моделювання та обладнання

Вибір обладнання для побудови захищеної корпоративної мережі є критичним етапом, що визначає її продуктивність, надійність та здатність підтримувати сучасні політики безпеки. Нижче наведено вибір конкретних моделей реального обладнання, яке відповідає вимогам проєкту гетерогенної мережі з архітектурою Zero Trust для середньої за розміром організації.

1. Маршрутизатор

Для виконання функцій між-VLAN'ної маршрутизації, яка є центральною точкою застосування політик мікросегментації, а також для реалізації сервісів DHCP та підтримки протоколу RADIUS, необхідний функціональний та гнучкий маршрутизатор.

Обрана модель: Cisco ISR 4331 (Integrated Services Router).

Обґрунтування вибору: Цей маршрутизатор є сучасним рішенням для корпоративних мереж. Його операційна система IOS XE підтримує розширені списки контролю доступу (ACL), необхідні для гранулярної фільтрації трафіку між сегментами. Достатня продуктивність дозволяє обробляти трафік кількох VLAN без затримок, а вбудовані функції безпеки та підтримка AAA роблять його ідеальним кандидатом для реалізації принципів Zero Trust.



Рисунок 3.1 – Маршрутизатор Cisco ISR 4331

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Основні характеристики маршрутизатора Cisco ISR 4331

Категорія	Характеристика	Значення
Продуктивність	Пропускна здатність	100 Мбіт/с - 300 Мбіт/с (з ліцензією)
	Кількість підтримуваних VLAN	до 1000
Інтерфейси	Вбудовані порти	2 x GE (RJ45), 1 x GE (SFP), 1 x GE (RJ45/SFP)
	Слоти розширення	2 x NIM (Network Interface Modules)
Протоколи	Безпека	ACL, Zone-Based Firewall, RADIUS, TACACS+
	Маршрутизація	OSPF, EIGRP, BGP, статична маршрутизація
Функції	Сервіси	DHCP, NAT, Syslog, SSH

2. Комутатори

Комутатори є першою лінією підключення для кінцевих пристроїв та відіграють ключову роль у сегментації мережі та застосуванні початкових політик безпеки.

Обрана модель: Cisco Catalyst 2960-X Series.

Обґрунтування вибору: Це надійна та перевірена часом серія керованих L2-комутаторів, яка є галузевим стандартом для рівня доступу. Вони забезпечують повну підтримку стандарту 802.1Q для створення VLAN, а також мають широкий набір функцій безпеки на портах, таких як Port Security, DHCP Snooping, BPDU Guard, що є необхідним для захисту від атак на каналному рівні.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55



Рисунок 3.2 – L2-комутатор

Таблиця 3.2

Основні характеристики комутатора Cisco Catalyst 2960-X

Категорія	Характеристика	Значення
Продуктивність	Комутаційна ємність	до 216 Гбіт/с
	Швидкість пересилання	до 71.4 Mpps
Інтерфейси	Порти доступу	24 або 48 портів 10/100/1000BASE-T (часто з PoE+)
	Аплінк-порти	2 або 4 порти 1G/10G SFP/SFP+
Протоколи	Стандарти	802.1Q (VLAN), 802.1D (STP), 802.1w (RSTP), 802.1s (MSTP)
	Безпека	Port Security, DHCP Snooping, Dynamic ARP Inspection, BPDU Guard

3. Центральний вузол безпеки (апаратна платформа для pfSense)

Для реалізації багатофункціонального вузла безпеки, який виконуватиме роль міжмережевого екрана, RADIUS-сервера, проксі-сервера та Syslog-сервера, доцільно використовувати спеціалізований апаратний пристрій (appliance) з встановленим ПЗ pfSense.

Обрана модель: Netgate 6100 Security Gateway Appliance.

Обґрунтування вибору: Пристрої від Netgate є офіційною апаратною платформою для pfSense, що гарантує оптимальну сумісність та продуктивність. Модель 6100 має достатню обчислювальну потужність та кількість мережевих інтерфейсів для обробки трафіку середньої компанії та одночасної роботи кількох сервісів безпеки, що є центральним елементом нашої моделі Zero Trust.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.3 – Апаратна платформа для pfSense Netgate 6100 Security Gateway Appliance

Таблиця 3.3

Основні характеристики Netgate 6100

Категорія	Характеристика	Значення
Продуктивність	Процесор	Intel Atom C3558 @ 2.2 GHz
	Пропускна здатність (Firewall)	до 18.6 Гбіт/с
Інтерфейси	Мережеві порти	2 x 10GbE (SFP+), 2 x 2.5GbE (RJ45), 4 x 1GbE (RJ45)
ПЗ та сервіси	Операційна система	pfSense Plus
	Ключові ролі	Firewall, NAT, VPN, RADIUS, Syslog, Squid Proxy

Для практичної реалізації, налаштування та тестування спроектованої мережі в рамках даної кваліфікаційної роботи буде використано програмний емулятор GNS3. Обрані вище моделі реального обладнання будуть змодельовані за допомогою відповідних віртуальних образів:

3.2. Налаштування базової мережевої інфраструктури у середовищі моделювання

3.2.1. Конфігурація інфраструктури комутації та забезпечення стабільності L2

На першому етапі практичної реалізації потрібно було створити стійку та керовану інфраструктуру комутації рівня L2, яка забезпечує передачу VLAN-трафіку

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

між різними частинами мережі без петель та колізій. Також необхідно було закласти фундамент для подальшої сегментації.

Цілі:

- Визначити root-комутатор для побудови STP-дерева.
- Створити необхідні VLAN відповідно до проєктної таблиці.
- Налаштувати trunk-порти для передачі трафіку між комутаторами.
- Захистити порти доступу від потенційних атак на канальному рівні.

У середовищі GNS3 було змодельовано шість комутаторів Cisco IOS. Один із них — SW-23-9-1 — виконує роль центрального вузла (distribution layer). На всіх комутаторах було активовано протокол Rapid PVST (Rapid Per VLAN Spanning Tree) для швидкої конвергенції:

```
SW-23-9-5(config)#spanning-tree mode rapid-pvst
```

Рисунок 3.4 – Активація протоколу Rapid PVST на комутаторі

Для забезпечення стабільної топології мережі центральний комутатор **SW-23-9-1** був призначений **root primary** для всіх VLAN завдяки зниженому пріоритету:

```
SW-23-9-1(config)#spanning-tree vlan 1-4094 root primary
```

Рисунок 3.5 – Призначення центрального комутатора кореневим (root primary)

А всі інші комутатори були призначені як root secondary:

```
SW-23-9-5(config)#spanning-tree vlan 1-4094 root secondary
```

Рисунок 3.6 – Налаштування резервного кореневого комутатора (root secondary)

Міжкомутаторні з'єднання та зв'язки з маршрутизатором були налаштовані як trunk-порти з інкапсуляцією 802.1Q:

```
SW-23-9-1(config)#int e0/0  
SW-23-9-1(config-if)#switchport trunk encapsulation dot1q  
SW-23-9-1(config-if)#switchport mode trunk
```

Рисунок 3.7 – Налаштування trunk-порту на комутаторі

Кінцеві порти були налаштовані в режимі **access** з прив'язкою до відповідного VLAN. Наприклад:

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

```
SW-23-9-2(config)#int e0/2
SW-23-9-2(config-if)#switchport mode access
SW-23-9-2(config-if)#switchport access vlan 10
```

Рисунок 3.8 – Налаштування access-порту з прив'язкою до VLAN 10

Для забезпечення безпеки канального рівня та запобігання петель використувалися:

```
SW-23-9-5(config)#int range e0/3, e1/0-1
SW-23-9-5(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 3 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW-23-9-5(config-if-range)#spanning-tree bpduguard enable
```

Рисунок 3.9 – Налаштування PortFast та BPDU Guard для безпеки L2

Ці налаштування забезпечують швидке включення кінцевих пристроїв та захист від несанкціонованого підключення мережевих пристроїв.

3.2.2. Реалізація між-VLAN'ної маршрутизації та базових сервісів L3

Після побудови канального рівня мережі необхідно було реалізувати маршрутизацію між VLAN для забезпечення взаємодії окремих сегментів, які перебувають у різних підмережах. Крім цього, потрібно було забезпечити базову службу DHCP, щоб автоматично роздавати IP-адреси кінцевим пристроям у кожному сегменті.

Цілі:

- Здійснити маршрутизацію між VLAN (інтер-VLAN routing) на маршрутизаторі Cisco.
- Реалізувати сабінтерфейси з теговою інкапсуляцією dot1Q для кожного VLAN.
- Призначити шлюзові IP-адреси для кожної підмережі.
- Налаштувати DHCP-пули для кожного VLAN з відповідними параметрами.

Маршрутизатор R-23-9-1 було підключено до центрального комутатора через trunk-лінію, що дозволило передавати тегований VLAN-трафік. На інтерфейсі

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

FastEthernet3/0 було створено сабінтерфейси для кожного VLAN з відповідною інкапсуляцією:

```
R-23-9-1(config)#int fa3/0.10
R-23-9-1(config-subif)#encapsulation dot1Q 10
R-23-9-1(config-subif)#ip address 192.168.10.1 255.255.255.0
R-23-9-1(config-subif)#ip access-group ZT VLAN10 ANALYSTS in
```

Рисунок 3.10 – Конфігурація сабінтерфейсу для між-VLAN маршрутизації

Усього було налаштовано 7 підінтерфейсів для VLAN 10–60 та 99, кожен з яких має свою адресу шлюзу. До кожного з них прив'язано ACL, які реалізують політику мінімальних привілеїв між сегментами.

Для кожного VLAN також було реалізовано DHCP-пул з унікальною IP-підмережею та вказаним шлюзом (default-router) і DNS-сервером (Google DNS 8.8.8.8):

```
R-23-9-1(config)#ip dhcp pool VLAN10
R-23-9-1(dhcp-config)#network 192.168.10.0 255.255.255.0
R-23-9-1(dhcp-config)#default-router 192.168.10.1
R-23-9-1(dhcp-config)#dns-server 8.8.8.8
```

Рисунок 3.11 – Налаштування DHCP-пулу для VLAN 10

Крім того, було зарезервовано IP-адреси, які не повинні видаватися DHCP (наприклад, шлюзи та сервери):

```
R-23-9-1(config)#ip dhcp excluded-address 192.168.10.1
```

Рисунок 3.12 – Резервування IP-адреси шлюзу з DHCP-пулу

На маршрутизаторі також було додано маршрут за замовчуванням до pfSense:

```
R-23-9-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Рисунок 3.13 – Додавання статичного маршруту за замовчуванням на маршрутизаторі

Цей рівень функціональності є критично важливим для подальшої реалізації контролю доступу між сегментами згідно з Zero Trust.

3.2.3. Побудова периметра та забезпечення доступу до Інтернету

Після конфігурації внутрішньої маршрутизації наступним критичним етапом є побудова захищеного периметра мережі, який слугуватиме точкою контролю всього

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

трафіку, що надходить іззовні та прямує в Інтернет. В рамках моделі Zero Trust периметр не є єдиною лінією захисту, але залишається важливим компонентом для фільтрації,

Цілі:

- Розгорнути центральний міжмережевий екран для інспекції всього вхідного та вихідного трафіку.
- Налаштувати трансляцію мережевих адрес (NAT) для приховування внутрішньої IP-структури від зовнішнього світу.
- Налаштувати статичну маршрутизацію для забезпечення зв'язності між зовнішнім світом та внутрішніми VLAN.
- Створити базові правила фаєрвола, які дозволяють легітимний трафік та блокують небажаний.

В якості центрального пристрою безпеки було обрано відкрите програмне рішення pfSense, розгорнуте як віртуальна машина. Воно було розміщене між внутрішнім маршрутизатором R-23-9-1 та мережею Інтернет.

3. Конфігурація інтерфейсів: На pfSense було налаштовано три ключові інтерфейси:

- WAN – зовнішній інтерфейс, що отримує IP-адресу від умовного провайдера (в моделі GNS3 це реалізовано через NAT-хмару).
- LAN – внутрішній інтерфейс із статичною IP-адресою 192.168.1.1/24, який є шлюзом для внутрішнього маршрутизатора.

4. Налаштування маршрутизації: Щоб pfSense знав, як досягти внутрішніх сегментів (VLAN 10, 20, 30 тощо), були створені статичні маршрути. Для кожної підмережі 192.168.X.0/24 було вказано, що наступним переходом (gateway) є внутрішній маршрутизатор R-23-9-1 з IP-адресою 192.168.1.2.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

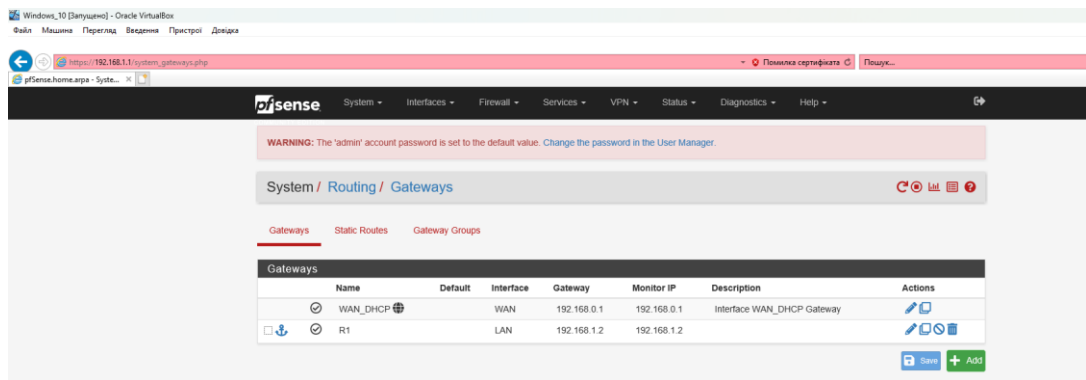


Рисунок 3.14 – Налаштування шлюзів у pfSense

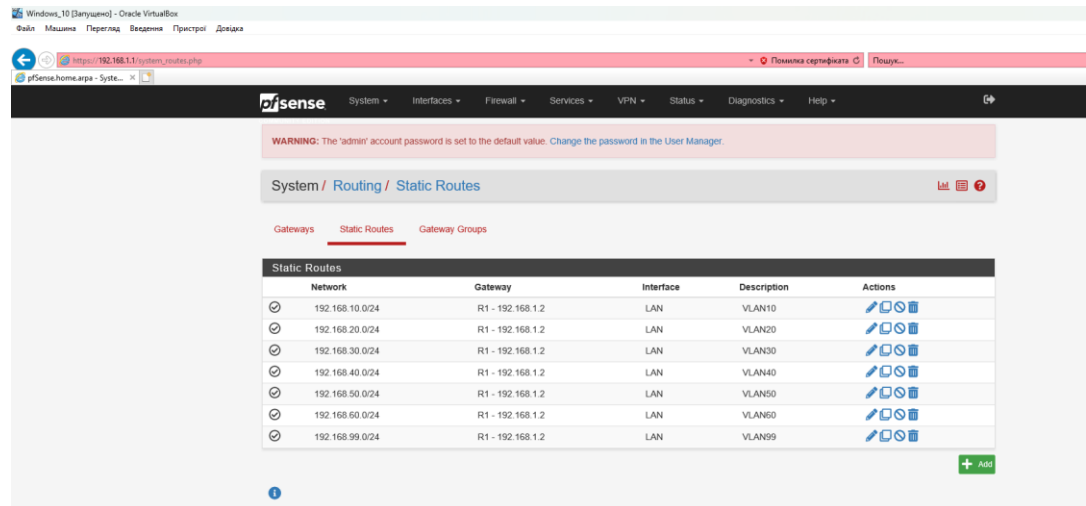


Рисунок 3.15 – Конфігурація статичних маршрутів у pfSense

3. Конфігурація правил NAT: Було налаштовано вихідний NAT (Outbound NAT) в автоматичному режимі. Це правило забезпечує трансляцію приватних IP-адрес усіх внутрішніх VLAN в єдину публічну IP-адресу WAN-інтерфейсу pfSense. Таким чином, для зовнішнього світу вся внутрішня мережа виглядає як один пристрій, що відповідає базовим принципам безпеки.

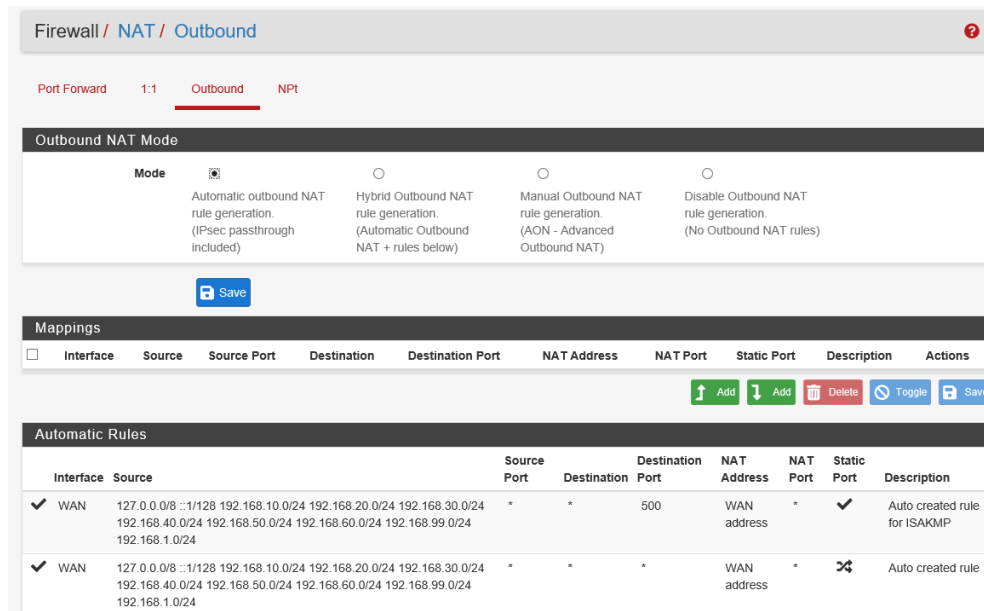


Рисунок 3.16 – Налаштування автоматичної трансляції мережних адрес (Outbound NAT) у pfSense

4. Базові правила міжмережевого екрана: На LAN-інтерфейсі було створено правила, що дозволяють трафік із внутрішніх підмереж до будь-якої точки призначення (any). На WAN-інтерфейсі за замовчуванням усі вхідні з'єднання блокуються, що унеможливорює несанкціонований доступ з Інтернету до внутрішніх ресурсів.

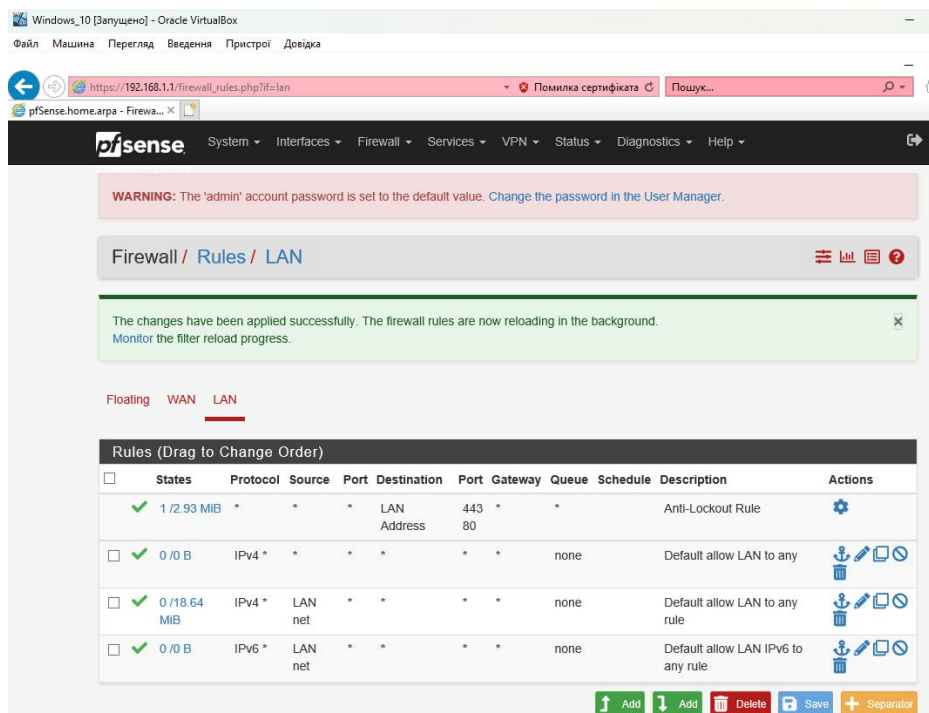


Рисунок 3.17 – Правила міжмережевого екрана для LAN-інтерфейсу в pfSense

Ці кроки дозволили створити функціональну базову інфраструктуру, на якій можна розгорнути більш складні механізми захисту відповідно до стратегії Zero Trust.

3.3. Впровадження компонентів архітектури Zero Trust

3.3.1. Реалізація політик мікросегментації за допомогою списків доступу (ACL)

Zero Trust — це не просто набір інструментів, а стратегія, що передбачає відсутність довіри до будь-якого пристрою чи користувача за замовчуванням, незалежно від його розташування у мережі. У цьому розділі описано реалізацію ключових механізмів безпеки, які були впроваджені поверх базової інфраструктури з метою формування багаторівневої моделі захисту.

Мікросегментація була реалізована шляхом застосування розширених списків контролю доступу (ACL) до сабінтерфейсів маршрутизатора Cisco (Fa3/0.X). Кожен ACL був створений на основі заздалегідь визначеної матриці доступу, яка базувалася на ролях користувачів, мінімально необхідному функціоналі та зоні довіри.

Приклади логіки ACL:

- VLAN 10 – Аналітики (ZT_VLAN10_ANALYSTS):
 1. Доступ до серверної зони (VLAN 50).
 2. Відкритий доступ до Інтернету.
 3. Заборона на ICMP-запити до інших користувацьких VLAN.
- VLAN 20 – Бухгалтерія (ZT_VLAN20_ACCOUNTANTS):
 - Доступ лише до одного сервера (host 192.168.50.2).
 - Блокування горизонтального доступу до інших VLAN.
 - Відкритий доступ до Інтернету.
- VLAN 30 – Керівництво (ZT_VLAN30_MANAGEMENT):
 - Повний доступ до всіх сегментів, окрім IoT і гостей.
 - Відкритий доступ до Інтернету
- VLAN 40 – Гості (ZT_VLAN40_GUESTS):
 1. Доступ виключно до публічних Інтернет-ресурсів.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

2. Всі внутрішні ресурси повністю заблоковані.
- VLAN 50 – Серверна зона (ZT_VLAN50_SERVERS):
 1. Вихід у мережу Інтернет (для оновлень).
 2. Прийом з'єднань лише від дозволених VLAN (10, 20, 30, 60).
 3. Заборона ініціювання нових з'єднань із серверної до клієнтів:
 - VLAN 60 – IoT-пристрої (ZT_VLAN60_IOT):
 1. Обмежений доступ до одного внутрішнього сервера.
 2. Доступ до DNS і HTTP.
 3. Відсутність горизонтального доступу.
 - VLAN 99 – Адміністративна зона (ZT_VLAN99_MANAGEMENT):
 1. Доступ до pfSense (Web UI), RADIUS і SSH на маршрутизаторі.
 2. Повна прозорість для адміністрування та моніторингу.

Приклад налаштувань:

```
R-23-9-1(config)#ip access-list extended ZT_VLAN10_ANALYSTS
R-23-9-1(config-ext-nacl)#92.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
R-23-9-1(config-ext-nacl)#permit udp 192.168.10.0 0.0.0.255 any eq 53
R-23-9-1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R-23-9-1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit tcp any any established
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
R-23-9-1(config-ext-nacl)#ex
R-23-9-1(config)#ip access-list extended ZT_VLAN20_ACCOUNTANTS
R-23-9-1(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 host 192.168.50.2
R-23-9-1(config-ext-nacl)#permit udp 192.168.20.0 0.0.0.255 any eq 53
R-23-9-1(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 any eq 80
R-23-9-1(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit tcp any any established
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
R-23-9-1(config-ext-nacl)#ex
R-23-9-1(config)#ip access-list extended ZT_VLAN30_MANAGEMENT
R-23-9-1(config-ext-nacl)#92.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
R-23-9-1(config-ext-nacl)#92.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
R-23-9-1(config-ext-nacl)#92.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
R-23-9-1(config-ext-nacl)#permit udp 192.168.30.0 0.0.0.255 any eq 53
R-23-9-1(config-ext-nacl)#permit tcp 192.168.30.0 0.0.0.255 any eq 80
R-23-9-1(config-ext-nacl)#permit tcp 192.168.30.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit tcp any any established
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
R-23-9-1(config-ext-nacl)#ex
R-23-9-1(config)#ip access-list extended ZT_VLAN40_GUESTS
R-23-9-1(config-ext-nacl)#permit udp 192.168.40.0 0.0.0.255 any eq 53
R-23-9-1(config-ext-nacl)#permit tcp 192.168.40.0 0.0.0.255 any eq 80
R-23-9-1(config-ext-nacl)#permit tcp 192.168.40.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit tcp any any established
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
R-23-9-1(config-ext-nacl)#ex
R-23-9-1(config)#ip access-list extended ZT_VLAN50_SERVERS
R-23-9-1(config-ext-nacl)#permit udp 192.168.50.0 0.0.0.255 any eq 53
R-23-9-1(config-ext-nacl)#permit tcp 192.168.50.0 0.0.0.255 any eq 80
R-23-9-1(config-ext-nacl)#permit tcp 192.168.50.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit tcp any any established
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
R-23-9-1(config-ext-nacl)#ex
R-23-9-1(config)#ip access-list extended ZT_VLAN60_IOT
R-23-9-1(config-ext-nacl)#permit ip 192.168.60.0 0.0.0.255 host 192.168.50.60
R-23-9-1(config-ext-nacl)#permit udp 192.168.60.0 0.0.0.255 any eq 53
R-23-9-1(config-ext-nacl)#permit tcp 192.168.60.0 0.0.0.255 any eq 80
R-23-9-1(config-ext-nacl)#permit tcp 192.168.60.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit tcp any any established
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.18 – Приклад конфігурації списків доступу (ACL) для реалізації мікро-сегментації

```
R-23-9-1(config)#ip access-list extended ZT_VLAN99_MANAGEMENT
R-23-9-1(config-ext-nacl)#192.168.99.0 0.0.0.255 host 192.168.1.1 eq www
R-23-9-1(config-ext-nacl)#192.168.99.0 0.0.0.255 host 192.168.1.1 eq 443
R-23-9-1(config-ext-nacl)#permit udp 192.168.99.0 0.0.0.255 any eq domain
R-23-9-1(config-ext-nacl)#permit tcp 192.168.99.0 0.0.0.255 any eq www
R-23-9-1(config-ext-nacl)#permit tcp 192.168.99.0 0.0.0.255 any eq 443
R-23-9-1(config-ext-nacl)#permit icmp 192.168.99.0 0.0.0.255 any echo
R-23-9-1(config-ext-nacl)#permit icmp any any echo-reply
R-23-9-1(config-ext-nacl)#permit tcp any any established
```

Рисунок 3.19 – Приклад конфігурації списків доступу (ACL) для реалізації мікро-сегментації

Усі ACL були застосовані до відповідних сабінтерфейсів маршрутизатора у напрямку in, що дозволяє контролювати міжвланову маршрутизацію на точці входу до кожного сегмента.

VLAN	Роль / Сегмент	Доступ до VLAN	Призначення до-стupu	Служби / Прото-коли
10	Аналітики	50	Доступ до серверів	HTTP, HTTPS, DNS, ICMP
		Інтернет	Загальний доступ	HTTP, HTTPS, DNS
		20, 30, 40, 60	Заборонено	—
20	Бухгалтерія	50 (host .2)	Доступ до бух. сер-вера	HTTP, HTTPS, DNS, ICMP
		Інтернет	Загальний доступ	HTTP, HTTPS, DNS
		10, 30, 40, 60	Заборонено	—
30	Керівництво	10, 20, 50	Повний доступ	IP, ICMP, DNS, HTTP, HTTPS
		Інтернет	Загальний доступ	HTTP, HTTPS, DNS
		40, 60	Заборонено	—
40	Гості	Інтернет	Дозволено	HTTP, HTTPS, DNS
		—	Повна ізоляція	—
50	Сервери	—	Прийом з'єднань	established, ICMP-reply
		Інтернет	Для оновлень	HTTP, HTTPS, DNS
60	ІоТ	50 (host .2)	Передача даних	HTTP, HTTPS

		Інтернет	Загальний доступ	HTTP, HTTPS, DNS
		10–40	Заборонено	—
99	Адміністративна зона	1.1 (pfSense), 1.2 (R)	Керування інфра-структурою	HTTPS, SSH, DNS
		Інтернет	Загальний доступ	HTTP, HTTPS, DNS

3.3.2 Впровадження централізованого управління ідентифікацією (RADIUS)

В архітектурі Zero Trust ідентичність є новим периметром. Тому централізоване та надійне управління автентифікацією адміністраторів є обов'язковим. Для цього було реалізовано автентифікацію через RADIUS-сервер.

Налаштування на pfSense:

- FreeRADIUS було встановлено як плагін.

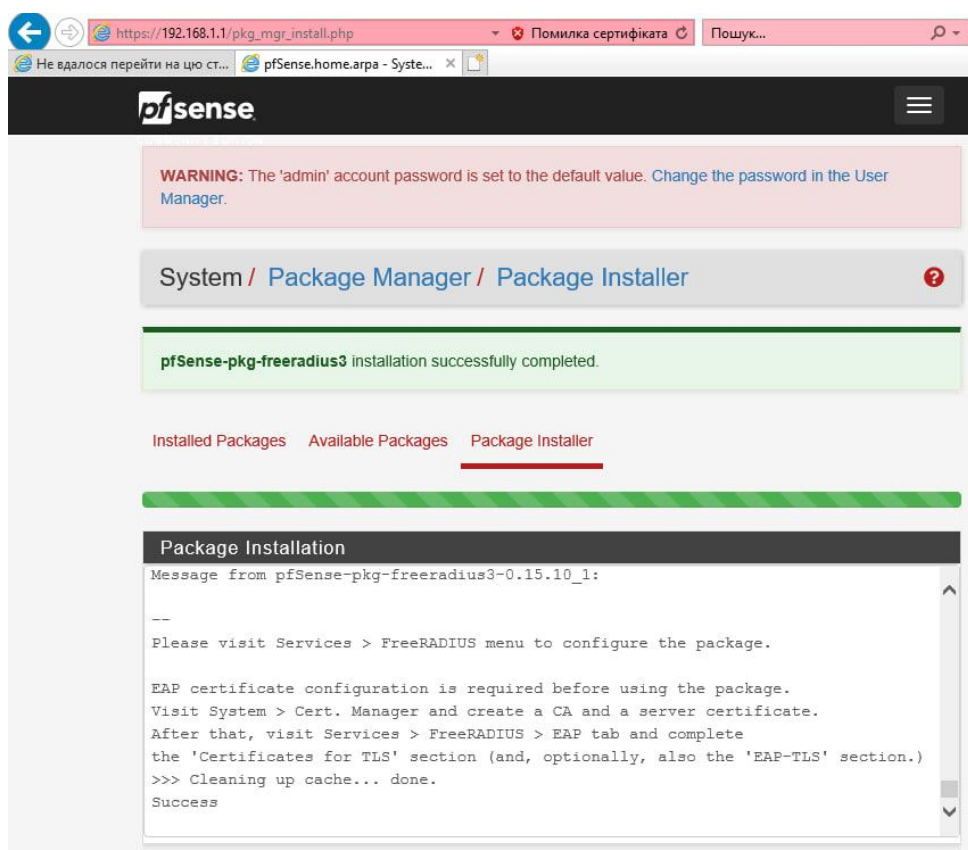


Рисунок 3.20 – Встановлення пакета FreeRADIUS у pfSense

- У налаштуваннях FreeRADIUS було додано маршрутизатор R-23-9-1 як клієнта (NAS/Client), вказавши його IP-адресу 192.168.1.2 та спільний секретний ключ (shared secret).

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

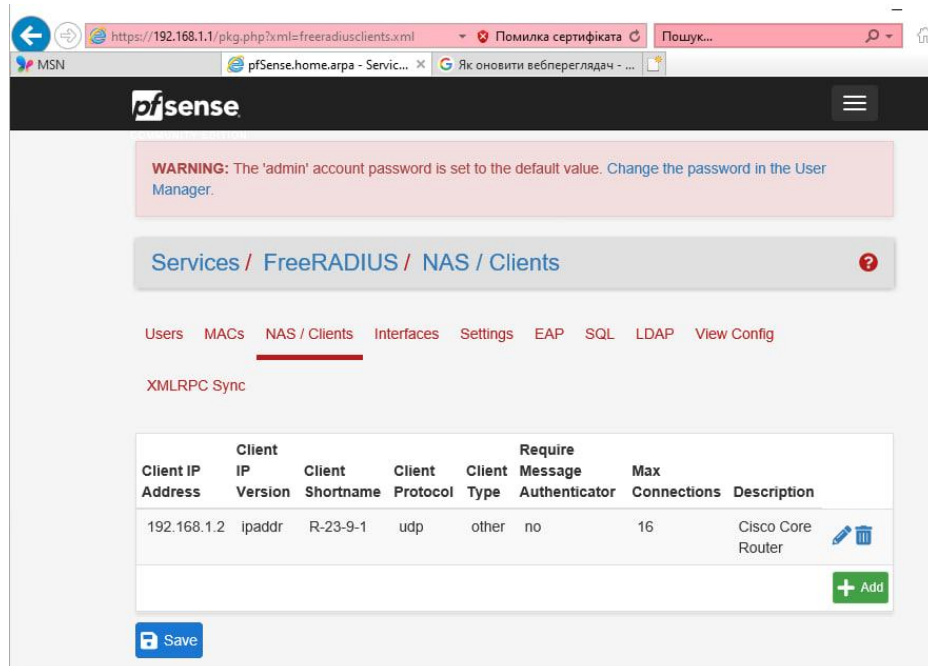


Рисунок 3.21 – Додавання RADIUS-клієнта (маршрутизатора) у pfSense

– У розділі Users було створено облікові записи для адміністраторів з пароллями.

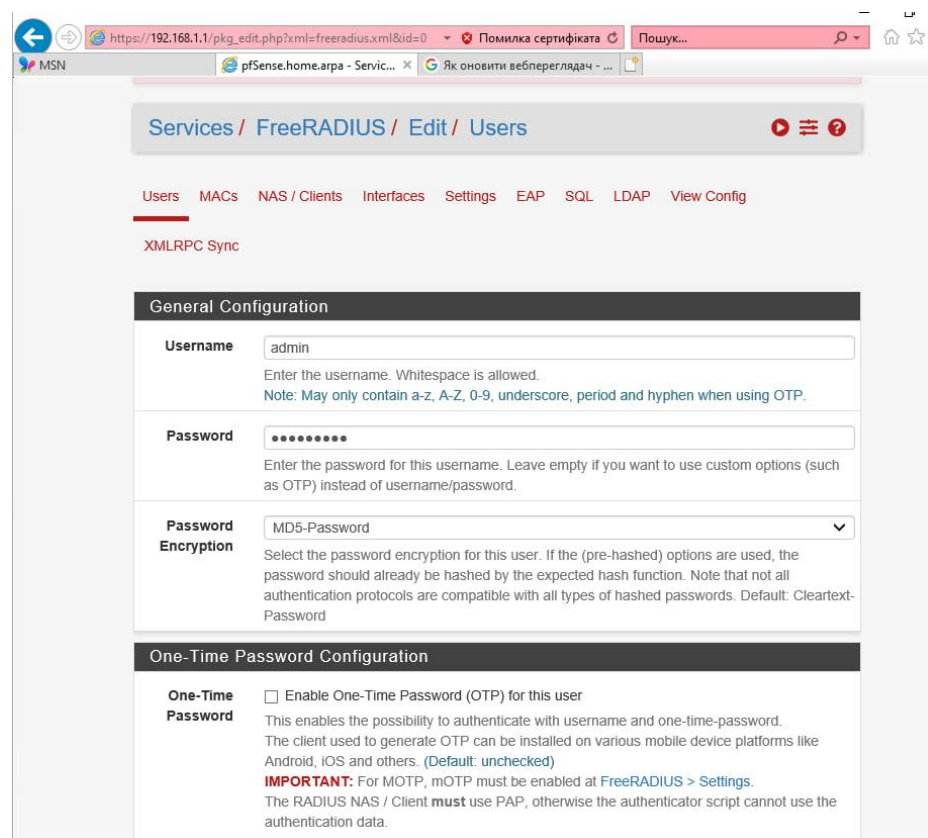


Рисунок 3.22 – Створення облікового запису користувача у FreeRADIUS

– Активовано служби Authentication, Accounting на портах 1812/1813.

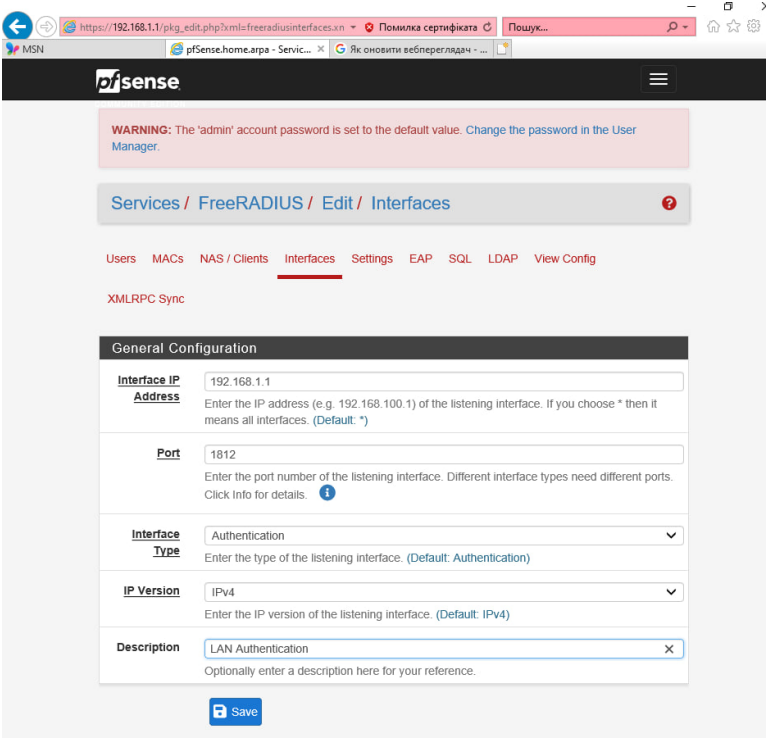


Рисунок 3.23 – Налаштування інтерфейсу для сервісу Authentication у FreeRADIUS

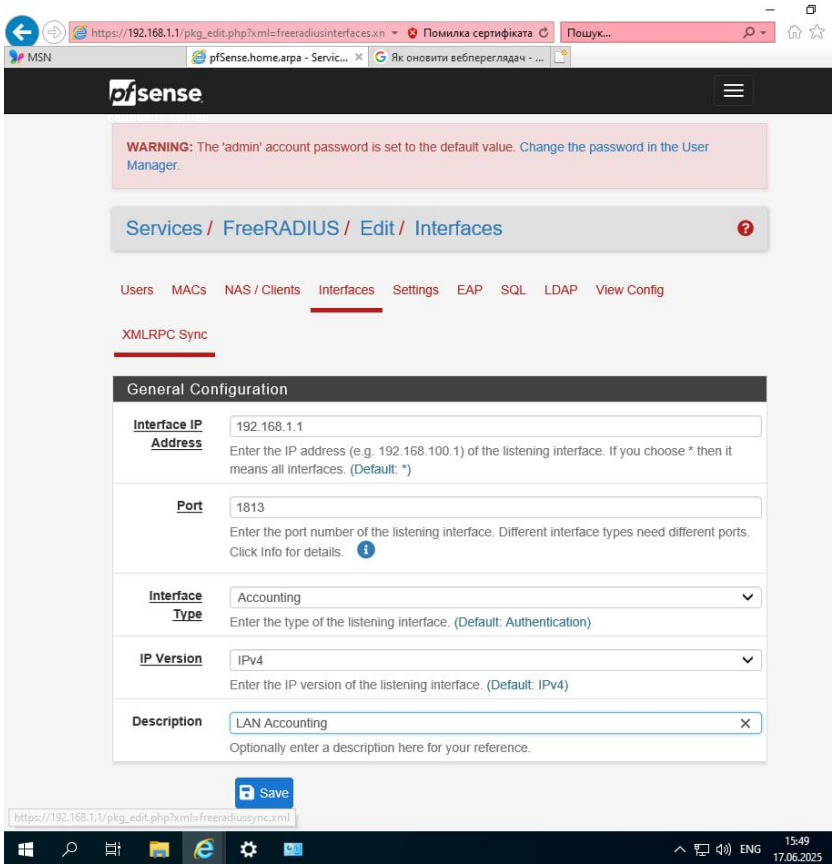


Рисунок 3.24 – Налаштування інтерфейсу для сервісу Accounting у FreeRADIUS

Налаштування AAA на маршрутизаторі Cisco:

- Було увімкнено нову модель AAA (Authentication, Authorization, and Accounting)
- Маршрутизатор був налаштований на використання RADIUS-сервера 192.168.1.1 із тим самим секретним ключем.
- Було створено списки методів автентифікації, які вказують, що при спробі входу (login) система спочатку звертається до групи RADIUS-серверів, і лише у випадку їх недоступності використовує локальну базу даних
- Ці списки були застосовані до віртуальних термінальних ліній

```
R-23-9-1(config)#aaa new-model
R-23-9-1(config)#2.168.1.1 auth-port 1812 acct-port 1813 key cisco123!
R-23-9-1(config)#aaa authentication login default group radius local
R-23-9-1(config)#aaa authorization exec default group radius local
R-23-9-1(config)#line vty 0 4
R-23-9-1(config-line)#login authentication default
```

Рисунок 3.25 – Налаштування AAA для автентифікації через RADIUS на маршрутизаторі Cisco

Завдяки цьому механізму адміністратори, які підключаються через SSH, проходять централізовану перевірку на сервері, що відповідає принципам динамічної перевірки довіри до користувача.

3.3.3. Розгортання розширених сервісів безпеки та моніторингу

Без всебічної видимості та моніторингу неможливо підтримувати архітектуру Zero Trust. Необхідно збирати, аналізувати та реагувати на події безпеки з усієї інфраструктури. Через це було прийняте рішення по впровадженню наступних інструментів:

1. Централізоване логування (Syslog)
2. Контентна фільтрація (Squid Proxy)

На pfSense було налаштовано як Syslog-сервер, який отримує повідомлення від маршрутизатора. Таким чином, на pfSense збираються всі події ACL, DHCP, підключення по SSH тощо. Логи доступні для подальшого аналізу у Splunk / Graylog або базовому інтерфейсі pfSense.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Package / Services: Syslog-ng / General

General Advanced Log Viewer

General Options

Enable ☒ Select this option to enable syslog-ng

Interface Selection LAN
WAN
loopback
Select interfaces you want to listen on

Default Protocol UDP
Select the default protocol you want to listen on

CA FreeRADIUS CA
Select Certificate Authority for TLS protocol.
You can use it in your object definition as ca-dir('/var/etc/syslog-ng/ca.d') option of tls().

Certificate GUI default (6851a500e46db)
Select server certificate for TLS protocol.
You can use it in your object definition as key-file('/var/etc/syslog-ng/syslog-ng.key') and cert-file('/var/etc/syslog-ng/syslog-ng.cert') options of tls().

Default Port 8514
Enter default port number you want to listen on

Default Log Directory /var/syslog-ng
Enter default log directory (no trailing slash)

Default Log File default.log
Enter default log file

Archive Frequency Daily

Рисунок 3.26 – Конфігурація Syslog-сервера у pfSense

```
R-23-9-1(config)#logging on
R-23-9-1(config)#logging host 192.168.1.1
R-23-9-1(config)#logging trap informational
```

Рисунок 3.27 – Налаштування відправки логів з маршрутизатора на Syslog-сервер

Showing 50 of 100 messages				
Jun 18 15:36:57	192.168.1.2	%SNMP-5-COLDSTART:	SNMP agent on host R-23-9-1 is undergoing a cold start	
Jun 18 15:36:57	192.168.1.2	%SSH-5-ENABLED:	SSH 1.99 has been enabled	
Jun 18 15:36:57	192.168.1.2	%SYS-5-CONFIG_1:	Configured from memory by console	
Jun 18 15:36:57	192.168.1.2	%SYS-5-RESTART:	System restarted --	
Jun 18 15:36:57	192.168.1.2	%SYS-6-LOGGINGHOST_STARTSTOP:	Logging to host 192.168.1.1 port 8514 started - CLI initiated	
Jun 18 15:36:58	192.168.1.2	%LINK-5-CHANGED:	Interface ATM1/0, changed state to administratively down	
Jun 18 15:36:58	192.168.1.2	%LINK-5-CHANGED:	Interface ATM2/0, changed state to administratively down	
Jun 18 15:36:59	192.168.1.2	%LINK-5-CHANGED:	Interface FastEthernet4/0, changed state to administratively down	
Jun 18 15:36:59	192.168.1.2	%LINK-5-CHANGED:	Interface FastEthernet5/0, changed state to administratively down	
Jun 18 15:36:59	192.168.1.2	%LINK-5-CHANGED:	Interface FastEthernet5/1, changed state to administratively down	
Jun 18 15:36:59	192.168.1.2	%LINK-5-CHANGED:	Interface FastEthernet5/0, changed state to administratively down	
Jun 18 15:36:59	192.168.1.2	%LINK-5-CHANGED:	Interface FastEthernet6/1, changed state to administratively down	
Jun 18 16:09:54	192.168.1.2	%PLATFORM-3-PACONFIG:	Exceeds 600 bandwidth points for slots 0, 1, 3 & 5	
Jun 18 16:09:54	192.168.1.2	%PLATFORM-3-PACONFIG:	Exceeds 600 bandwidth points on both odd & even numbered slots	
Jun 18 16:10:03	192.168.1.2	%LINEPROTO-5-UPDOWN:	Line protocol on Interface VoIP-Null0, changed state to up	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface ATM1/0, changed state to up	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface ATM2/0, changed state to up	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface FastEthernet0/0, changed state to up	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface FastEthernet3/0, changed state to up	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface FastEthernet4/0, changed state to down	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface FastEthernet5/0, changed state to up	
Jun 18 16:10:03	192.168.1.2	%LINK-3-UPDOWN:	Interface FastEthernet5/1, changed state to up	

Рисунок 3.28 – Перегляд логів з маршрутизатора в інтерфейсі pfSense

На pfSense також було розгорнуто Squid Proxu для фільтрації HTTP/HTTPS трафіку. Налаштовані ACL для обмеження доступу до категорій сайтів (в моєму випадку Wikipedia).

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

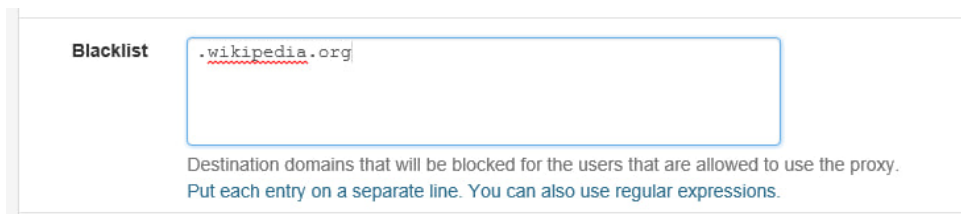


Рисунок 3.29 – Налаштування чорного списку (Blacklist) у проксі-сервері Squid

Ці сервіси забезпечують прозорість, відстежуваність дій користувачів та контроль контенту, що є ключовими вимогами у Zero Trust-підході.

Компоненти аналітики безпеки (SIEM, UEBA) не впроваджувалися через обмеження моделювання, однак їх використання є рекомендованим на етапі продуктивного розгортання системи в реальному середовищі.

3.4. Тестування функціональності та ефективності захисту

3.4.1. Валідація політик контролю доступу між сегментами

Для підтвердження правильності реалізації архітектури Zero Trust у змодельованому середовищі було проведено серію тестів, що демонструють коректну роботу механізмів контролю доступу, автентифікації та фільтрації.

Була проведена перевірка мікросегментації, реалізованої за допомогою ACL на маршрутизаторі. Зокрема, з робочої станції у VLAN 10 (аналітики) здійснювались запити до інших VLAN.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

```

WS-23-9-1 - PuTTY
WS-23-9-1> ip dhcp
DDORA IP 192.168.10.2/24 GW 192.168.10.1

WS-23-9-1> ping 192.168.10.3
84 bytes from 192.168.10.3 icmp_seq=1 ttl=128 time=0.948 ms
84 bytes from 192.168.10.3 icmp_seq=2 ttl=128 time=0.892 ms

WS-23-9-1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=113 time=39.232 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=113 time=38.184 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=113 time=37.640 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=113 time=37.910 ms

WS-23-9-1> ping 192.168.20.2
*192.168.10.1 icmp_seq=1 ttl=255 time=7.577 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.10.1 icmp_seq=2 ttl=255 time=8.962 ms (ICMP type:3, code:13, Communication administratively prohibited)

WS-23-9-1> ping 192.168.50.2
192.168.50.2 icmp_seq=1 timeout
192.168.50.2 icmp_seq=2 timeout
84 bytes from 192.168.50.2 icmp_seq=3 ttl=63 time=16.438 ms
84 bytes from 192.168.50.2 icmp_seq=4 ttl=63 time=15.324 ms
84 bytes from 192.168.50.2 icmp_seq=5 ttl=63 time=16.532 ms

WS-23-9-1> ping 192.168.30.2
*192.168.10.1 icmp_seq=1 ttl=255 time=6.434 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.10.1 icmp_seq=2 ttl=255 time=4.577 ms (ICMP type:3, code:13, Communication administratively prohibited)

WS-23-9-1> ping 192.168.40.2
*192.168.10.1 icmp_seq=1 ttl=255 time=10.671 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.10.1 icmp_seq=2 ttl=255 time=5.792 ms (ICMP type:3, code:13, Communication administratively prohibited)

WS-23-9-1> ping 192.168.60.2
*192.168.10.1 icmp_seq=1 ttl=255 time=2.146 ms (ICMP type:3, code:13, Communication administratively prohibited)

WS-23-9-1>

```

Рисунок 3.30 – Результати тестування політик доступу між VLAN

Для прикладу на скріншоті видно повідомлення, що при спробі доступу з хоста у VLAN 10 до 192.168.20.2, його шлюз 192.168.10.1 повернув ICMP-повідомлення Communication administratively prohibited. Це однозначно вказує на те, що доступ було заблоковано на рівні ACL маршрутизатора".

Це вказує на те, що доступ було заблоковано на рівні ACL. Аналогічні результати отримані при перевірці інших VLAN, зокрема:

- VLAN 30 має доступ до VLAN 10 та 20.

```

WS-23-9-7 - PuTTY

WS-23-9-7> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=63 time=18.951 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=63 time=11.718 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=63 time=17.544 ms

WS-23-9-7> ping 192.168.20.2
192.168.20.2 icmp_seq=1 timeout
192.168.20.2 icmp_seq=2 timeout
192.168.20.2 icmp_seq=3 timeout
192.168.20.2 icmp_seq=4 timeout
192.168.20.2 icmp_seq=5 timeout

WS-23-9-7> ping 192.168.30.3
84 bytes from 192.168.30.3 icmp_seq=1 ttl=64 time=0.621 ms
84 bytes from 192.168.30.3 icmp_seq=2 ttl=64 time=0.748 ms

WS-23-9-7> ping 192.168.40.3
*192.168.30.1 icmp_seq=1 ttl=255 time=8.554 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)
*192.168.30.1 icmp_seq=2 ttl=255 time=8.061 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)

WS-23-9-7> ping 192.168.50.3
192.168.50.3 icmp_seq=1 timeout
192.168.50.3 icmp_seq=2 timeout
84 bytes from 192.168.50.3 icmp_seq=3 ttl=63 time=17.442 ms
84 bytes from 192.168.50.3 icmp_seq=4 ttl=63 time=17.535 ms

WS-23-9-7> ping 192.168.60.2
*192.168.30.1 icmp_seq=1 ttl=255 time=7.543 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)
*192.168.30.1 icmp_seq=2 ttl=255 time=6.886 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)
*192.168.30.1 icmp_seq=3 ttl=255 time=6.246 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)
*192.168.30.1 icmp_seq=4 ttl=255 time=6.875 ms (ICMP type:3, code:13, Communicat
ion administratively prohibited)

WS-23-9-7> ping 192.168.20.2
192.168.20.2 icmp_seq=1 timeout
192.168.20.2 icmp_seq=2 timeout
192.168.20.2 icmp_seq=3 timeout
192.168.20.2 icmp_seq=4 timeout

WS-23-9-7> ping 192.168.20.3
84 bytes from 192.168.20.3 icmp_seq=1 ttl=63 time=23.641 ms
84 bytes from 192.168.20.3 icmp_seq=2 ttl=63 time=14.763 ms
84 bytes from 192.168.20.3 icmp_seq=3 ttl=63 time=17.386 ms

WS-23-9-7> █

```

Рисунок 3.31 – Результат тестування доступу з VLAN 30 (Керівництво)
 Це підтверджує коректну реалізацію принципу least privilege і мікросегмен-
 тації.

3.4.2. Перевірка роботи централізованої автентифікації адміністративного доступу

Для перевірки централізованого управління доступом адміністратор виконав SSH-підключення до маршрутизатора R-23-9-1 з машини у VLAN 99.

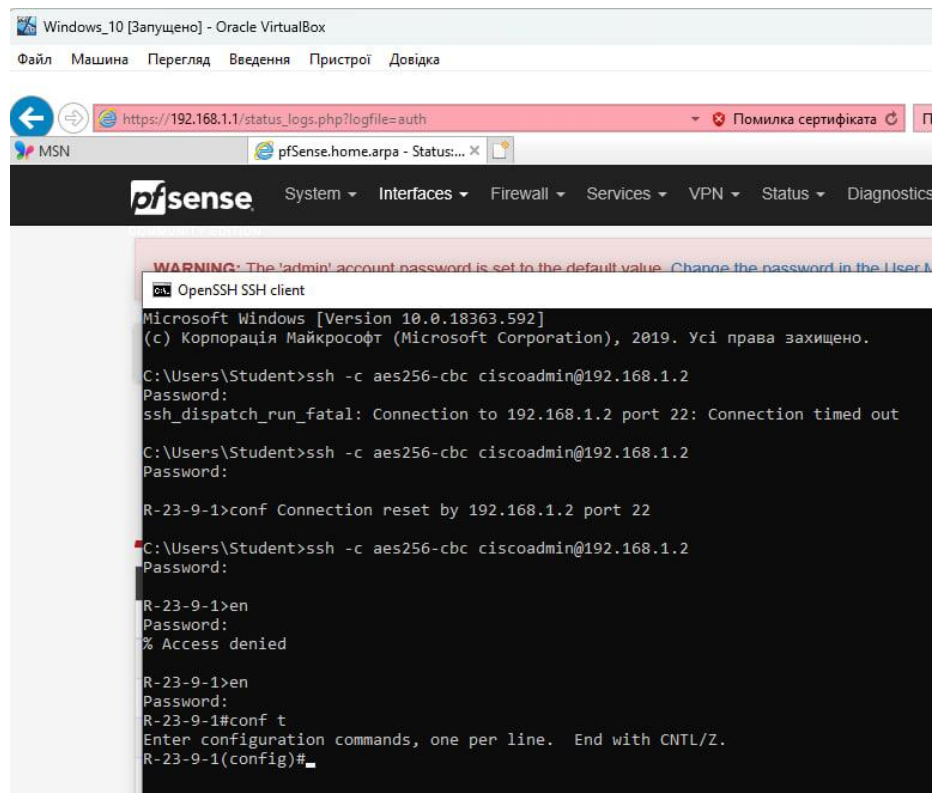


Рисунок 3.32 – Тестування централізованої автентифікації адміністративного доступу через SSH та RADIUS

Це підтверджує, що працює повний ланцюг AAA → RADIUS → User access, що є ключовим елементом Zero Trust у контексті контролю адміністративного доступу.

3.4.3. Перевірка ефективності контентної фільтрації

Було протестовано функціонування проксі-сервера Squid, налаштованого на pfSense, з політиками блокування за категоріями сайтів.

При спробі доступу до сайту wikipedia.org з клієнта у VLAN 10, у браузері відобразилась сторінка з повідомленням ‘Гм. Ніяк не вдається знайти цей сайт.’

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

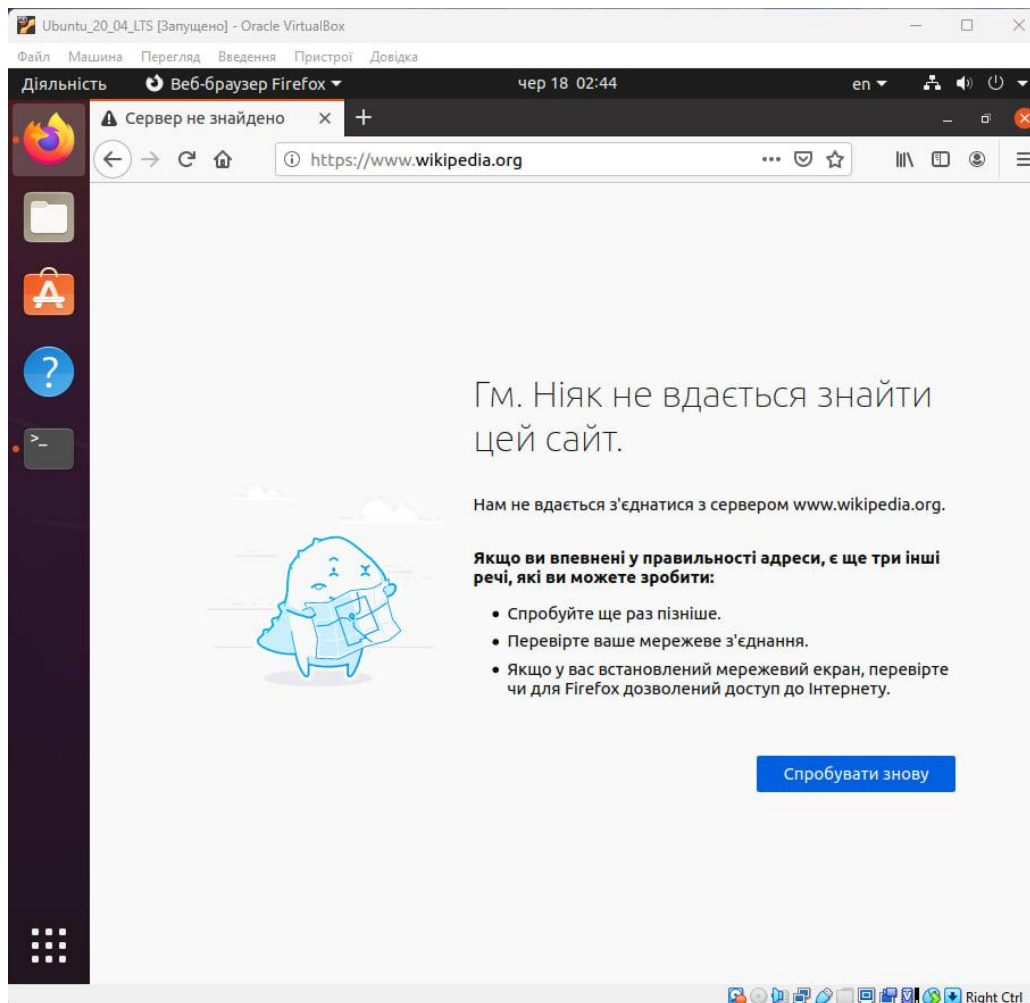


Рисунок 3.33 – Результат блокування доступу до ресурсу з чорного списку проксі-сервером Squid

Це підтверджує, що фільтрація працює, і трафік контролюється за допомогою політик проксі-сервера, що дозволяє дотримуватись політики захисту контенту та мінімізації ризиків витоку інформації через небажані ресурси.

Висновки до розділу 3

У даному розділі було реалізовано та протестовано ключові компоненти архітектури Zero Trust у рамках змодельованої гетерогенної мережі. Побудована інфраструктура охоплює як базові рівні L2/L3, так і розширені засоби контролю доступу, автентифікації та моніторингу.

Було здійснено повноцінну реалізацію міжвланової маршрутизації з мікросегментацією на основі списків контролю доступу (ACL), що забезпечило ізоляцію та захист між сегментами мережі відповідно до ролей користувачів. Централізована ав-

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

тентифікація на основі RADIUS-сервера дозволила керувати адміністративним доступом до обладнання з дотриманням принципу "нікому не довіряй за замовчуванням". Реалізовані сервіси фільтрації трафіку та логування забезпечили високий рівень прозорості та можливість аналізу активності у мережі.

Проведене тестування підтвердило коректність реалізації кожного з компонентів:

- політики доступу обмежують трафік відповідно до визначеної матриці взаємодій;
- автентифікація адміністраторів проходить через зовнішній сервер із логуванням спроб;
- трафік небажаного змісту блокується згідно з заданими проксі-правилами.

Отже, реалізована модель демонструє ефективність архітектури Zero Trust у гетерогенному середовищі. Такий підхід дозволяє побудувати стійку до загроз мережу, яка відповідає сучасним вимогам безпеки і може бути масштабована у майбутньому для реального корпоративного середовища.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

ВИСНОВКИ

У межах кваліфікаційної роботи було розроблено, спроектовано та змодельовано захищену гетерогенну мережеву інфраструктуру організації з урахуванням вимог сучасної кібербезпеки. Основною метою проєкту стало впровадження архітектури Zero Trust, яка передбачає повну відмову від неявної довіри в корпоративних мережах, постійну перевірку користувачів і пристроїв, а також мінімізацію привілеїв у доступі до ресурсів.

У першому розділі було розглянуто теоретичні засади побудови гетерогенних інформаційних систем, охарактеризовано їхню структуру, ризики та обмеження традиційного perimeter-based підходу. Значну увагу приділено архітектурі Zero Trust, її ключовим принципам, компонентам та практикам впровадження, що дозволило обґрунтувати доцільність її застосування в сучасних мережах.

На основі цих теоретичних положень у другому розділі було виконано аналіз вихідних умов, сформовано модель загроз та спроектовано захищену інфраструктуру організації. Розроблено логічну топологію з поділом на VLAN-сегменти, реалізовано маршрутизацію, визначено зони довіри та DMZ, сформовано політики контролю доступу. У проєкті враховано потреби в сегментації, резервуванні та масштабованості, що дозволяє адаптувати мережу до реальних умов організаційного середовища.

У третьому розділі реалізовано практичну модель у середовищі GNS3 із використанням маршрутизаторів Cisco, фаєрвола pfSense, віртуальних серверів і клієнтських машин. Було реалізовано такі компоненти:

- інфраструктура L2 з підтримкою VLAN і STP,
- міжвланова маршрутизація та IP-адресація,
- політики мікросегментації за допомогою ACL,
- фаєрвол з NAT, DMZ і міжзонною фільтрацією,
- централізована автентифікація доступу через RADIUS,
- базовий моніторинг та контроль трафіку.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

Кожен етап конфігурування супроводжувався перевіркою досягнення функціональних та безпекових цілей, включно з тестуванням доступу, фільтрації та відмовостійкості.

Результатом роботи є цілісне рішення з побудови захищеної мережевої інфраструктури, що відповідає сучасним стандартам інформаційної безпеки. Впроваджені технології дозволяють досягти ізоляції критичних сегментів, обмеження доступу за принципом найменших привілеїв, підвищеної прозорості дій користувачів і масштабованості рішення. Реалізована модель може слугувати основою для реального впровадження Zero Trust у мережах малого або середнього підприємства.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. NIST. Zero Trust Architecture. NIST Special Publication 800-207. URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf>.
2. Microsoft Security. What is Zero Trust Architecture?. URL: <https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture>.
3. 10Guards. Zero Trust: переваги та недоліки архітектури. URL: <https://10guards.com/ua/blog/2023/06/30/zero-trust-security-benefits-and-disadvantages/>.
4. Csecurity Journal. Перспективи Zero Trust в Україні. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/508>.
5. Geeksforgeeks. Difference Between Two-Tier And Three-Tier Database Architecture. URL: <https://www.geeksforgeeks.org/dbms/difference-between-two-tier-and-three-tier-database-architecture>.
6. Practical Networking. Routing Between VLANs & Layer 3 Switches. URL: <https://www.practicalnetworking.net/stand-alone/routing-between-vlans/>.
7. pfSense Documentation. Introduction and Configuration Guide. URL: <https://docs.netgate.com/pfsense/en/latest/>.
8. FreeRADIUS. The FreeRADIUS Server Project. URL: <https://wiki.freeradius.org/>.
9. Cisco. Configure RADIUS Authentication for CLI Access. URL: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/116058-config-radius-00.html>.
10. GNS3. Official Documentation. URL: <https://docs.gns3.com/docs/>.
11. OWASP. Zero Trust Cheat Sheet. URL: https://cheatsheet-series.owasp.org/cheatsheets/Zero_Trust_Cheat_Sheet.html.
12. Cisco. Understanding VLANs. URL: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/white-paper-c11-740756.html>.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

13. Cybersecurity & Infrastructure Security Agency (CISA). Zero Trust Maturity Model. URL: <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>.

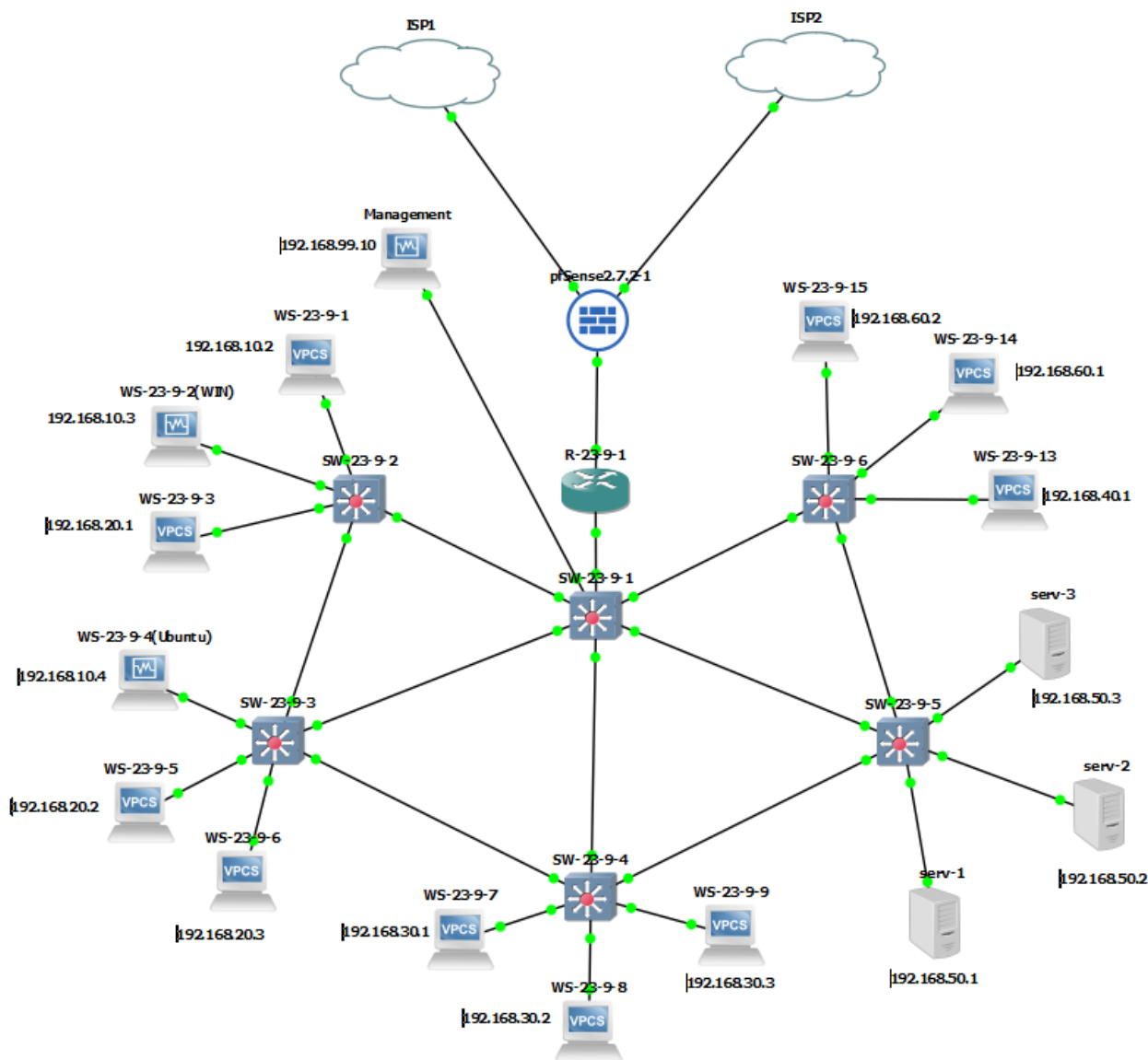
14. Журавська І. Гетерогенні комп'ютерні мережі критичного застосування на основі роїв та зграй БПЛА : монографія. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2019. –192 с.

15. Stallings W. Cryptography and Network Security: Principles and Practice (8th Edition). Hoboken, NJ : Pearson, 2020. С. 621–654.

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		



R-23-9-1

```
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 8.8.8.8
!
ip dhcp pool VLAN60
    network 192.168.60.0 255.255.255.0
    default-router 192.168.60.1
    dns-server 8.8.8.8
!
!
no ip domain lookup
ip domain name secure-network.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$LtUr$aSr2wvnoap/5bmly5hfPK1
username ciscoadmin secret 5
$1$hL7Y$gCy7sL7S7CuOMwKrNL4SW.
archive
log config
hidekeys
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 192.168.1.2 255.255.255.0
duplex half
!
interface ATM1/0
no ip address
shutdown
no atm ilmi-keepalive
!
interface ATM2/0
no ip address
shutdown
```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no atm ilmi-keepalive
!
interface FastEthernet3/0
no ip address
duplex half
!
interface FastEthernet3/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
ip access-group ZT_VLAN10_ANALYSTS in
!
interface FastEthernet3/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
ip access-group ZT_VLAN20_ACCOUNTANTS in
!
interface FastEthernet3/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
ip access-group ZT_VLAN30_MANAGEMENT in
!
interface FastEthernet3/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
ip access-group ZT_VLAN40_GUESTS in
!
interface FastEthernet3/0.50
encapsulation dot1Q 50
ip address 192.168.50.1 255.255.255.0
ip access-group ZT_VLAN50_SERVERS in
!
interface FastEthernet3/0.60
encapsulation dot1Q 60
ip address 192.168.60.1 255.255.255.0
ip access-group ZT_VLAN60_IOT in
!
interface FastEthernet3/0.99
encapsulation dot1Q 99
ip address 192.168.99.1 255.255.255.0
ip access-group ZT_VLAN99_MANAGEMENT in
!
interface FastEthernet4/0
no ip address
shutdown
duplex half
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet6/0
no ip address
shutdown
duplex auto
speed auto

```

```

!
interface FastEthernet6/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.1
no ip http server
no ip http secure-server
!
!
!
ip access-list extended ZT_VLAN10_ANALYSTS
permit ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
permit udp 192.168.10.0 0.0.0.255 any eq domain
permit tcp 192.168.10.0 0.0.0.255 any eq www
permit tcp 192.168.10.0 0.0.0.255 any eq 443
permit tcp any any established
permit icmp any any echo-reply
permit icmp 192.168.10.0 0.0.0.255 192.168.50.0
0.0.0.255 echo
deny icmp 192.168.10.0 0.0.0.255 192.168.20.0
0.0.0.255
deny icmp 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
deny icmp 192.168.10.0 0.0.0.255 192.168.40.0
0.0.0.255
deny icmp 192.168.10.0 0.0.0.255 192.168.60.0
0.0.0.255
permit icmp 192.168.10.0 0.0.0.255 any echo
ip access-list extended ZT_VLAN20_ACCOUNTANTS
permit ip 192.168.20.0 0.0.0.255 host 192.168.50.2
permit udp 192.168.20.0 0.0.0.255 any eq domain
permit tcp 192.168.20.0 0.0.0.255 any eq www
permit tcp 192.168.20.0 0.0.0.255 any eq 443
permit tcp any any established
permit icmp any any echo-reply
permit icmp 192.168.20.0 0.0.0.255 host 192.168.50.2
echo
deny icmp 192.168.20.0 0.0.0.255 192.168.10.0
0.0.0.255
deny icmp 192.168.20.0 0.0.0.255 192.168.30.0
0.0.0.255
deny icmp 192.168.20.0 0.0.0.255 192.168.40.0
0.0.0.255
deny icmp 192.168.20.0 0.0.0.255 192.168.60.0
0.0.0.255
permit icmp 192.168.20.0 0.0.0.255 any echo
ip access-list extended ZT_VLAN30_MANAGEMENT
permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
permit udp 192.168.30.0 0.0.0.255 any eq domain
permit tcp 192.168.30.0 0.0.0.255 any eq www
permit tcp 192.168.30.0 0.0.0.255 any eq 443
permit tcp any any established
permit icmp any any echo-reply
permit icmp 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255 echo
permit icmp 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255 echo

```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

```

permit icmp 192.168.30.0 0.0.0.255 192.168.50.0
0.0.0.255 echo
deny icmp 192.168.30.0 0.0.0.255 192.168.40.0
0.0.0.255
deny icmp 192.168.30.0 0.0.0.255 192.168.60.0
0.0.0.255
permit icmp 192.168.30.0 0.0.0.255 any echo
ip access-list extended ZT_VLAN40_GUESTS
permit udp 192.168.40.0 0.0.0.255 any eq domain
permit tcp 192.168.40.0 0.0.0.255 any eq www
permit tcp 192.168.40.0 0.0.0.255 any eq 443
permit tcp any any established
permit icmp any any echo-reply
ip access-list extended ZT_VLAN50_SERVERS
permit udp 192.168.50.0 0.0.0.255 any eq domain
permit tcp 192.168.50.0 0.0.0.255 any eq www
permit tcp 192.168.50.0 0.0.0.255 any eq 443
permit tcp any any established
permit icmp any any echo-reply
ip access-list extended ZT_VLAN60_IOT
permit udp 192.168.60.0 0.0.0.255 any eq domain
permit tcp 192.168.60.0 0.0.0.255 any eq www
permit tcp 192.168.60.0 0.0.0.255 any eq 443
permit tcp any any established
permit icmp any any echo-reply
permit ip 192.168.60.0 0.0.0.255 host 192.168.50.2
ip access-list extended ZT_VLAN99_MANAGEMENT
permit tcp 192.168.99.0 0.0.0.255 host 192.168.1.1 eq
www
permit tcp 192.168.99.0 0.0.0.255 host 192.168.1.1 eq
443
permit udp 192.168.99.0 0.0.0.255 any eq domain
permit tcp 192.168.99.0 0.0.0.255 any eq www
permit tcp 192.168.99.0 0.0.0.255 any eq 443
permit icmp 192.168.99.0 0.0.0.255 any echo
permit icmp any any echo-reply
permit tcp any any established

permit tcp 192.168.99.0 0.0.0.255 host 192.168.1.2 eq
22
!
logging host 192.168.1.1 transport udp port 8514
no cdp log mismatch duplex
!
!
!
!
!
radius-server host 192.168.1.1 auth-port 1812 acct-port
1813 key 7 09784B1A0D5445415F
!
control-plane
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
transport input ssh
!
end

```

SW-23-9-1

```

SW-23-9-1#show run
Building configuration...

Current configuration : 1475 bytes
!
! Last configuration change at 16:36:12 UTC Wed Jun
18 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-23-9-1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!

```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

!
!
!
!
!
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/2
 switchport access vlan 99
 switchport mode access
!
interface Ethernet1/3
!

```

```

interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end

```

SW-23-9-2

```

SW-23-9-2#show run
Building configuration...

Current configuration : 1889 bytes
!
! Last configuration change at 15:27:01 UTC Wed Jun
18 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-23-9-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000

```

```

logging console discriminator EXCESS
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 28672
!
vlan internal allocation policy ascending

```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				87
Змн.	Арк.	№ докум.	Підпис	Дата		


```

!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 28672
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/3
switchport access vlan 10
switchport mode access
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/0
switchport access vlan 20
switchport mode access
spanning-tree portfast edge
spanning-tree bpduguard enable

```

SW-23-9-4#show run
Building configuration...

Current configuration : 1926 bytes

```

!
interface Ethernet1/1
switchport access vlan 20
switchport mode access
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

SW-23-9-4

```

!
! Last configuration change at 15:27:06 UTC Wed Jun
18 2025
!

```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-23-9-4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 28672
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
```

```

switchport mode trunk
!
interface Ethernet0/3
switchport access vlan 30
switchport mode access
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/0
switchport access vlan 30
switchport mode access
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/1
switchport access vlan 30
switchport mode access
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0

```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-23-9-5

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
control-plane
!
!

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

SW-23-9-6

SW-23-9-6#show run
Building configuration...

Current configuration : 1682 bytes
!
! Last configuration change at 15:27:09 UTC Wed Jun 18 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-23-9-6
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 28672
!
vlan internal allocation policy ascending
!

ip tcp synwait-time 5
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/2
switchport access vlan 40
switchport mode access
!
interface Ethernet0/3
switchport access vlan 60
switchport mode access
!
interface Ethernet1/0
switchport access vlan 60
switchport mode access
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

```

!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!

```

```

!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

		Костенко О.В.			ККІКБ.КР.Б – 125 – 09 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		93