

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 модернізації підсистеми захисту
мережної інфраструктури Житомирської міської ради»

затверджено Наказом університету від 2 лютого 2026 р. № 58/с

Термін здачі студентом закінченої роботи 30 червня 2026 р.

Вихідні дані роботи:

Об'єктом дослідження є процес забезпечення інформаційної та мережевої безпеки у локальній обчислювальній мережі та пов'язаній IT-інфраструктурі Житомирської міської ради.

Предметом дослідження є виконав: студент 4-го курсу групи КБ-22-3 спеціальності 125 «Кібербезпека»

Данило ПАВЛЕНКО

Керівник: Старший викладач кафедри КІ та КБ,

Наталія ЩУР

Рецензент: Доцент кафедри КІ та КБ, к.т.н.

Олексій ШЕЛУХА

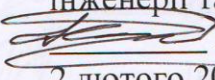
Житомир – 2026

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

2 лютого 2026 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Павленко Данило Олександрович

Тема роботи: «Проект модернізації підсистеми захисту мережної інфраструктури Житомирської міської ради»

затверджена Наказом університету від 2 лютого 2026 р. № 58/с

Термін здачі студентом закінченої роботи 30 червня 2026 р.

Вихідні дані роботи:

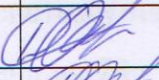
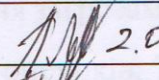
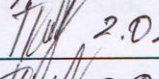
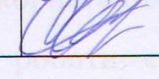
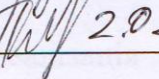
Об'єктом дослідження є процес забезпечення інформаційної та мережевої безпеки у локальній обчислювальній мережі та пов'язаній IT-інфраструктурі Житомирської міської ради.

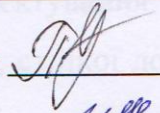
Предметом дослідження є методи, програмно-апаратні засоби, вбудовані механізми захисту операційних систем і мережевих шлюзів, а також групові політики безпеки, що спрямовані на модернізацію підсистеми захисту мережної інфраструктури Житомирської міської ради.

Обладнання та програмне забезпечення:

1. Oracle VirtualBox
2. GNS3 VM
3. GNS3 3.0.6
4. pfSense-CE-2.5.2
5. Windows server 2019 updated march 2020 x64
6. Cisco-iosv

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

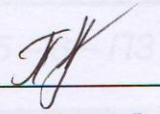
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ольга ДЯЧУК	 2.02.2026	 2.02.2026
2	Ольга ДЯЧУК	 2.02.2026	 2.02.2026
3	Ольга ДЯЧУК	 2.02.2026	 2.02.2026

Студент  Данило ПАВЛЕНКО

Керівник  Наталія ЩУР

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06.05.2026	Виконано
2	Аналіз літературних джерел	20.05.2026	Виконано
3	Вибір технології для реалізації	22.06.2026	Виконано
4	Проектування КМ	23.06.2026	Виконано
5	Підготовка компонентів для мережі	23.06.2026	Виконано
6	Налаштування мережі	24.06.2026	Виконано
7	Налагодження захисту мережі	25.06.2026	Виконано
8	Тестування роботи КМ	26.06.2026	Виконано
9	Оформлення пояснювальної записки	28.06.2026	Виконано
10	Оформлення презентації	29.06.2026	Виконано
11	Захист		Виконано

Студент  Данило ПАВЛЕНКО

Керівник  Наталія ЩУР

АНОТАЦІЯ

Кваліфікаційна робота присвячена проектуванню, налаштуванню та захисту корпоративної IT-інфраструктури із застосуванням технологій Active Directory, логічної сегментації мережі та систем універсального управління загрозами (UTM). Пояснювальна записка викладена на **70** сторінках і містить **36** рисунків, **7** таблиць та **25** найменувань у списку використаних джерел.

Метою кваліфікаційної роботи є проектування та реалізація надійної, керованої та захищеної корпоративної мережі, стійкої до сучасних кіберзагроз, із забезпеченням конфіденційності, цілісності та доступності (модель CIA) інформаційних ресурсів.

У роботі визначено основні вимоги до безпечної IT-інфраструктури Житомирська міська ради; проаналізовано принципи логічної сегментації локальної мережі (LAN) за допомогою віртуальних мереж (VLAN) та виділення демілітаризованої зони (DMZ); розглянуто особливості централізованого управління правами доступу (ACL) через службу каталогів Active Directory (AD DS) та об'єкти групових політик (GPO); обґрунтовано технологічний стек та спроєктовано багаторівневу архітектуру захисту із застосуванням систем виявлення вторгнень (IDS) і пристроїв UTM для протидії складним атакам (APT), ботнетам (C&C) та DDoS; показано розробку і налаштування безпечних мережевих служб (DHCP, DNS), включаючи імплементацію розширень безпеки DNSSEC та DoT; наведено результати перевірки захищеності та ефективності реалізованої IT-інфраструктури.

Ключові слова: IT-ІНФРАСТРУКТУРА, ІНФОРМАЦІЙНА БЕЗПЕКА, ACTIVE DIRECTORY, VLAN, DMZ, UTM, IDS, DNSSEC, GPO.

KKIKB.KP.B – 125 – 8 – ПЗ							
Змн.	Арк.	№ докум.	Підпис	Дата	Лім.	Арк.	Аркушів
Розроб.		Павленко Д.О.	<i>[підпис]</i>	30.06.26	Проект модернізації підсистеми захисту мережної інфраструктури Житомирської міської ради		
Керівник		Щур Н.О.	<i>[підпис]</i>	30.06.26			
Реценз.		Шелуха О.О.	<i>[підпис]</i>	30.06.26			
Н. контр.		Щур Н.О.	<i>[підпис]</i>	30.06.26			
Затверд.		Єфіменко А.А.	<i>[підпис]</i>	30.06.26			
					ФІКТ, Гр. КБ-22-3		

ANNOTATION

The qualification work is devoted to the design, configuration, and protection of corporate IT infrastructure using Active Directory technologies, logical network segmentation, and Unified Threat Management (UTM) systems. The explanatory note is presented on 70 pages and contains 36 figures, 7 tables, and 25 items in the list of references.

The purpose of the qualification work is to design and implement a reliable, manageable, and secure corporate network resistant to modern cyber threats, ensuring the confidentiality, integrity, and availability (CIA triad) of information resources.

The paper defines the main requirements for a secure enterprise IT infrastructure; analyzes the principles of logical Local Area Network (LAN) segmentation using Virtual LANs (VLANs) and the allocation of a Demilitarized Zone (DMZ); considers the specifics of centralized access control (ACL) management through Active Directory Domain Services (AD DS) and Group Policy Objects (GPO); justifies the technology stack and designs a multi-layered security architecture using Intrusion Detection Systems (IDS) and UTM devices to counter advanced persistent threats (APT), botnets (C&C), and DDoS attacks; demonstrates the development and configuration of secure network services (DHCP, DNS), including the implementation of DNSSEC and DoT security extensions; presents the results of testing the security and efficiency of the implemented IT infrastructure.

Keywords: IT INFRASTRUCTURE, INFORMATION SECURITY, ACTIVE DIRECTORY, VLAN, DMZ, UTM, IDS, DNSSEC, GPO.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП	9
РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ТА ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ	11
1.1. Аналіз сучасних кіберзагроз для інформаційних мереж державних установ	11
1.2. Теоретичні засади побудови захищеного периметра мережі	14
1.3. Методи управління безпекою кінцевих точок в середовищі Active Directory	15
1.4. Обґрунтування вибору програмно-апаратного шлюзу pfSense для реалізації підсистеми захисту	16
1.5. Постановка технічного завдання	21
1.6. Методологія моделювання загроз та вразливостей в інформаційно-телекомунікаційних системах органів місцевого самоврядування	22
1.7. Роль нормативних документів у технічному захисті інформації	22
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЖИТОМИРСЬКОЇ МІСЬКОЇ РАДИ ..	27
2.1. Обґрунтування необхідності модернізації підсистеми захисту мережної інфраструктури Житомирської міської ради.....	27
2.2. Розгортання базової мережі та серверної інфраструктури	29
2.3. Логічна сегментація мережі та міжвіланова маршрутизація.....	34
2.4. Налаштування списків контролю доступу (ACL) та міжмережевого екрана	38
2.5. Впровадження додаткових механізмів захисту, моніторингу та резервного копіювання	43
РОЗДІЛ 3. ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ	47
3.1. Методологія тестування політик безпеки та мережевого екрана	47
3.2. Практичне виконання тестів безпеки мережі	49
ВИСНОВКИ	58
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	60

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List (списки контролю доступу).

AD – Active Directory (служба каталогів).

AD DS – Active Directory Domain Services.

APT – Advanced Persistent Threat (цілеспрямовані кібератаки).

C&C – Command and Control (командні сервери ботнетів).

CIA – Confidentiality, Integrity, Availability (конфіденційність, цілісність, доступність — модель інформаційної безпеки).

DDoS – Distributed Denial of Service (розподілена атака на відмову в обслуговуванні).

DHCP – Dynamic Host Configuration Protocol (протокол динамічної конфігурації хоста).

DMZ – Demilitarized Zone (демілітаризована зона).

DNS – Domain Name System (система доменних імен).

DNSSEC – Domain Name System Security Extensions (розширення безпеки системи доменних імен).

DoT – DNS over TLS (протокол безпечної передачі DNS-запитів).

GPO – Group Policy Objects (об'єкти групових політик).

ICMP – Internet Control Message Protocol (міжмережевий протокол керуючих повідомлень).

IDS – Intrusion Detection System (система виявлення вторгнень).

IP – Internet Protocol (міжмережевий протокол).

LAN – Local Area Network (внутрішня локальна мережа).

SPI – Stateful Packet Inspection (інспекція пакетів із запам'ятовуванням стану).

TLS – Transport Layer Security (протокол криптографічного захисту).

USB – Universal Serial Bus (згадується у контексті обмежень доступу до зовнішніх носіїв — USB Restriction).

UTM – Unified Threat Management (універсальний пристрій управління загрозами).

vCPU – Virtual Central Processing Unit (віртуальний процесор).

VLAN – Virtual Local Area Network (віртуальні локальні мережі).

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

VPN – Virtual Private Network (віртуальна приватна мережа).

WAN – Wide Area Network (глобальна мережа / зовнішній інтерфейс).

BM – Віртуальна машина.

IT – Інформаційні технології (IT-інфраструктура).

МБ – Мегабайт.

ОЗП – Оперативний запам'ятовуючий пристрій (оперативна пам'ять).

ОС – Операційна система.

ПЗ – Програмне забезпечення.

КСЗІ - Комплексна система захисту інформації.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. В умовах стрімкого зростання кількості кіберзагроз та постійних цілеспрямованих атак на інформаційні ресурси державного сектору, питання забезпечення надійної кібербезпеки органів місцевого самоврядування набуває критичної важливості. Мережева інфраструктура Житомирської міської ради обробляє великі масиви службової інформації та персональних даних громадян, що робить її потенційною мішенню для зловмисників. Застарілі підходи до управління мережею не здатні ефективно протистояти сучасним векторам атак, таким як перебір паролів (Brute-force), несанкціонований доступ до кінцевих точок або взаємодія зі скомпрометованими веб-ресурсами. Тому модернізація підсистеми захисту із застосуванням надійних мережевих шлюзів та систем централізованого управління політиками безпеки є надзвичайно актуальною задачею. Це дозволить мінімізувати ризики витоку даних, підвищити загальну стійкість інфраструктури та гарантувати безперебійну роботу установи.

Метою кваліфікаційної роботи є підвищення рівня інформаційної безпеки Житомирської міської ради шляхом розробки та практичної реалізації проєкту модернізації підсистеми захисту її мережної інфраструктури від зовнішніх та внутрішніх кіберзагроз.

Визначена мета обумовлює наступні завдання:

- проаналізувати поточний стан архітектури мережі та визначити основні вектори потенційних кіберзагроз для інформаційної системи установи ;
- спроектувати модернізовану підсистему захисту на базі централізованого мережевого шлюзу та контролера домену;
- налаштувати мережевий екран (Firewall) та механізми фільтрації трафіку (DNS Sinkholing) для запобігання доступу до ворожих та шкідливих інтернет-ресурсів;
- впровадити строгі політики безпеки кінцевих точок (GPO) у середовищі Active Directory, включаючи захист від атак підбору паролів (Account Lockout Policy) та налаштування глибокого аудиту подій безпеки.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

Об'єктом дослідження є процес забезпечення інформаційної та мережевої безпеки, цілісності, доступності та конфіденційності даних у локальній обчислювальній мережі та пов'язаній IT-інфраструктурі Житомирської міської ради.

Предметом дослідження є методи, програмно-апаратні засоби, вбудовані механізми захисту мережевих шлюзів (pfSense) і серверних операційних систем (Windows Server), а також групові політики безпеки, що застосовуються для модернізації підсистеми захисту інфраструктури.

У процесі виконання кваліфікаційної роботи було розроблено проект комплексної захищеної мережевої інфраструктури, що поєднує периметральний захист на базі шлюзу pfSense та централізоване управління політиками доступу через Active Directory. Практична реалізація проєкту дозволила створити стійке середовище із нативними механізмами фільтрації трафіку та безперервним аудитом подій безпеки.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ТА ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

1.1. Аналіз сучасних кіберзагроз для інформаційних мереж державних установ

Оскільки об'єктом впровадження підсистеми захисту є інформаційно-телекомунікаційна система Житомирської міської ради, до неї висуваються підвищені вимоги щодо конфіденційності, цілісності та доступності даних. Муніципальні органи влади обробляють значні масиви персональних даних громадян, службову інформацію та мають доступ до державних реєстрів. Відповідно до вимог нормативних документів з технічного захисту інформації (НД ТЗІ) України, створення комплексної системи захисту інформації (КСЗІ) є обов'язковою умовою функціонування таких мереж.

Сучасні кіберзагрози, спрямовані на державний сектор, включають цілеспрямовані фішингові атаки на співробітників, використання програм-вимагачів (Ransomware) та DDoS-атаки на публічні сервіси міської ради. Тому архітектура мережевої безпеки повинна базуватися на ешелонованому захисті, що включає сегментацію мережі на рівні VLAN, строгий контроль доступу та системи виявлення вторгнень (IDS/IPS), здатні оперативно реагувати на аномалії в трафіку.

Забезпечення інформаційної безпеки в органах місцевого самоврядування є критично важливим завданням, оскільки їхні мережі обробляють значні обсяги конфіденційної службової інформації та персональних даних громадян. Згідно з базовими принципами кібербезпеки, захист інформації базується на тріаді: конфіденційність, цілісність та доступність.



Рисунок 1.1 Модель CIA

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Сучасний ландшафт загроз для державного сектору характеризується високою інтенсивністю цілеспрямованих атак (АРТ-атак). Серед найбільш розповсюджених векторів загроз для локальних мереж виділяють:

- **Атаки повного перебору (Brute-Force та Dictionary attacks):** спрямовані на компрометацію облікових записів співробітників шляхом автоматизованого підбору паролів до служб віддаленого доступу або контролерів домену.
- **Шкідливе програмне забезпечення та програми-вимагачі (Ransomware):** потрапляють у мережу через неконтрольований доступ користувачів до шкідливих або скомпрометованих веб-ресурсів .
- **Внутрішні загрози (Insider threats):** несанкціоновані дії користувачів, використання неперевіраних зовнішніх носіїв інформації або відсутність контролю за подіями безпеки всередині мережі.

Для протидії цим загрозам застарілі методи мережевого адміністрування є неефективними, що вимагає переходу до комплексних (ешелонованих) систем захисту, які поєднують периметральну безпеку та контроль кінцевих точок .

У контексті сучасних безпекових викликів, інформаційні мережі державних установ України стали пріоритетною ціллю для ворожих кіберугруповань. Аналіз інцидентів останніх років демонструє зміну парадигми атак: від масового поширення вірусів до цілеспрямованих операцій (Advanced Persistent Threats — АРТ). Для мереж муніципального рівня, таких як Житомирська міська рада, характерні наступні специфічні загрози:

1. Деструктивні атаки на інфраструктуру (Wiper-атаки). Однією з найнебезпечніших загроз є використання шкідливого програмного забезпечення, спрямованого не на викрадення даних, а на їх повне знищення або шифрування з метою паралізації роботи органу місцевого самоврядування. Такі атаки часто супроводжуються виведенням з ладу критичних серверних вузлів, що призводить до зупинки надання електронних послуг громадянам.

2. Соціальна інженерія та цілеспрямований фішинг. Більшість успішних проникнень у державні мережі розпочинаються з компрометації облікових записів співробітників.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Зловмисники використовують методи персоналізованого фішингу (Spear Phishing), розсилаючи листи, стилізовані під офіційні запити від вищих державних інстанцій або системних адміністраторів. Отримання доступу до робочої станції працівника міської ради відкриває шлях до подальшого просування мережею (Lateral Movement) з використанням вразливостей в ОС Windows або застарілих версій прикладного ПЗ.

3. Експлуатація вразливостей віддаленого доступу. У зв'язку з необхідністю забезпечення дистанційної роботи працівників, впровадження сервісів віддаленого доступу (VPN, RDP) стало критичною точкою вразливості. Недостатня політика паролів, відсутність багатфакторної автентифікації (MFA) та несвоєчасне оновлення патчів на шлюзах доступу створюють умови для брутфорс-атак (перебору паролів) та експлуатації відомих вразливостей програмного забезпечення брандмауерів.

4. DDoS-атаки на публічні вебресурси. Публічні сервери міської ради є постійною ціллю для DDoS-атак, які мають на меті не лише злам, а й виведення з ладу офіційних сайтів та систем електронної взаємодії. Це створює інформаційний тиск і знижує довіру до державних інституцій, оскільки громадяни втрачають можливість доступу до актуальної інформації та адміністративних послуг.

5. Використання "ланцюга постачання" (Supply Chain Attacks). Сучасні атаки все частіше спрямовані на програмне забезпечення, що використовується в державній установі. Злом сторонніх сервісів, систем електронного документообігу (СЕД) або оновлень ПЗ дозволяє зловмисникам впровадити шкідливий код безпосередньо у довірене середовище установи.

З огляду на вищезазначене, захист інформаційної системи Житомирської міської ради повинен базуватися на концепції "нульової довіри" (Zero Trust), де кожен запит на доступ, незалежно від його джерела, підлягає обов'язковій автентифікації та перевірці. Тільки системний підхід, що включає моніторинг аномалій, сегментацію мережі та регулярний аудит безпеки, дозволяє забезпечити стійкість до сучасних кіберзагроз.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

1.2. Теоретичні засади побудови захищеного периметра мережі

Мережевий периметр є першою лінією оборони будь-якої ІТ-інфраструктури. Основною ланкою периметрального захисту є міжмережевий екран (Firewall), який здійснює фільтрацію вхідного та вихідного трафіку на основі заданих правил політики безпеки.

Одним із найефективніших рішень класу UTM (Unified Threat Management) з відкритим вихідним кодом є маршрутизатор pfSense, побудований на базі ОС FreeBSD [5]. Використання pfSense дозволяє реалізувати технологію Stateful Packet Inspection (SPI), яка відстежує стан активних мережевих з'єднань і блокує нелегітимні пакети. Окрім класичної фільтрації за IP-адресами та портами, сучасним методом периметрального захисту є **DNS Sinkholing** (маршрутизація в "чорну діру"). Цей метод полягає у перехопленні DNS-запитів користувачів до відомих шкідливих або ворожих доменів на рівні локального DNS-сервера. Замість реальної IP-адреси зловмисного сервера, система повертає адресу локальної петлі (127.0.0.1) або адресу спеціального порталу-заглушки. Це дозволяє ефективно блокувати зв'язок із командними серверами ботнетів (C&C) та забороненими ресурсами без значного навантаження на процесор маршрутизатора.

Таблиця 1.1

Етапи реалізації проєкту модернізації підсистеми захисту

Етап проєкту	Опис діяльності	Очікуваний результат
Аналітичний	Аудит поточної архітектури та виявлення вразливостей	Технічне завдання та перелік ризиків
Проектний	Розробка конфігурацій GPO, правил Firewall та DNS-фільтрів	Готовий дизайн безпекового периметра
Впровадження	Налаштування pfSense, Active Directory та серверних політик	Розгорнута та захищена інфраструктура
Верифікація	Тестування блокувань (Sinkholing) та перевірка аудит-логів	Документальне підтвердження ефективності
Моніторинг	Налаштування періодичного аналізу журналів подій	Стабільна робота системи з контролем інцидентів

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Для реалізації ядра мережевої безпеки було проведено порівняльний аналіз сучасних систем класу UTM (Unified Threat Management). Враховуючи необхідність оптимізації бюджету державної установи та вимоги до гнучкості, оптимальним вибором є програмний маршрутизатор pfSense. На відміну від комерційних аналогів (наприклад, Cisco ASA або FortiGate), pfSense базується на відкритому вихідному коді (FreeBSD), що виключає витрати на ліцензування, при цьому забезпечуючи Enterprise-рівень функціональності. Він нативно підтримує інтеграцію з системами виявлення вторгнень (Snort/Suricata), гнучке керування правилами брандмауера та побудову захищених VPN-каналів для віддалених працівників міської ради.

1.3. Методи управління безпекою кінцевих точок в середовищі Active Directory

Захист виключно на рівні периметра не гарантує безпеки у випадку проникнення зловмисника всередину мережі. Тому другим ешеленом захисту є централізоване управління політиками безпеки на рівні серверів та робочих станцій. У мережах на базі Windows Server для цього використовується служба каталогів Active Directory (AD) та об'єкти групових політик (Group Policy Objects, GPO).

Застосування GPO дозволяє автоматизувати налаштування безпеки для всіх комп'ютерів у домені. Найважливішими складовими модернізованої політики є:

1. **Політика блокування облікових записів (Account Lockout Policy):** єдиний надійний метод захисту від Brute-Force атак на рівні домену. Вона визначає кількість допустимих невдалих спроб авторизації (Threshold), після досягнення якої обліковий запис тимчасово блокується .
2. **Політика аудиту безпеки (Audit Policy):** безперервне журналювання подій в ОС є основою для реагування на інциденти (Incident Response). Налаштування аудиту подій входу (Logon Events) дозволяє адміністраторам відстежувати підозрілу активність, фіксувати спроби несанкціонованого доступу та формувати доказову базу у випадку розслідування кіберінцидентів .

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Порівняльна характеристика обраних методів захисту інфраструктури

Метод захисту	Сфера застосування	Основна мета	Рівень впровадження
Stateful Firewall (pfSense)	Периметр мережі	Фільтрація вхідного/вихідного трафіку	Мережевий шлюз
DNS Sinkholing	Периметр мережі	Блокування доступу до ворожих/шкідливих доменів	DNS Resolver
GPO: Account Lockout	Робочі станції	Захист від Brute-Force атак на користувачів	Active Directory
GPO: Security Auditing	Сервери / Станції	Забезпечення журналювання для аналізу інцидентів	Windows Server
USB Restriction (GPO)	Кінцеві точки	Запобігання витоку даних через зовнішні носії	Active Directory

Для вибору найбільш ефективної стратегії модернізації системи безпеки було проведено аналіз наявних засобів захисту. У таблиці 1.2 наведено порівняльний огляд обраних методів, які забезпечують ешелонований захист інфраструктури Житомирської міської ради, враховуючи як мережевий рівень (периметр), так і рівень кінцевих точок.

1.4. Обґрунтування вибору програмно-апаратного шлюзу pfSense для реалізації підсистеми захисту

Проектування сучасної системи інформаційної безпеки для органу місцевого самоврядування, яким є Житомирська міська рада, вимагає ретельного підходу до вибору базового рішення для захисту периметра мережі. Ринок систем класу NGFW (Next-Generation Firewall) та UTM (Unified Threat Management) пропонує широкий спектр рішень: від бюджетних апаратних маршрутизаторів до високовартісних платформ (Cisco Firepower, Fortinet FortiGate, Palo Alto Networks).

Однак, після проведення комплексного аналізу технічних вимог, специфіки державного сектору та бюджетних обмежень, як ядро підсистеми захисту було обрано програмний міжмережевий екран відкритого коду **pfSense**.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Цей вибір базується на низці критично важливих факторів, які детально розглянуто нижче.

1. Оптимізація бюджетних витрат та відсутність «вендор-локу» (Vendor Lock-in)

Головною проблемою впровадження систем класу Enterprise у державних установах є їхня висока вартість. Комерційні рішення, такі як Cisco ASA або FortiGate, вимагають не лише значних початкових інвестицій у специфічне апаратне забезпечення, але й постійної оплати щорічних ліцензій (Smart Licenses, підписки на оновлення баз антивірусів та IDS). У разі припинення фінансування, ці пристрої часто перетворюються на звичайні маршрутизатори, втрачаючи свої захисні функції.

Натомість **pfSense Community Edition** поширюється за ліцензією відкритого вихідного коду (Open Source) і є абсолютно безкоштовним для використання. Це дозволяє міській раді отримати функціонал Enterprise-рівня без жодних ліцензійних відрахувань. Крім того, pfSense не прив'язаний до конкретного "заліза" (апаратного забезпечення). Його можна розгорнути на будь-якому стандартному x86-сервері, на старих комп'ютерах або як віртуальну машину в середовищах VMware, Hyper-V, Proxmox чи, як у нашому випадку, у GNS3. Це дає установі абсолютну гнучкість при масштабуванні: якщо пропускної здатності не вистачає, достатньо просто виділити віртуальній машині більше оперативної пам'яті та ядер процесора (vCPU), не купуючи новий фізичний пристрій за тисячі доларів.

2. Прозорість коду та безпека на базі FreeBSD

Оскільки об'єктом захисту є державна структура, що обробляє чутливі дані, використання пропрієтарного (закритого) програмного забезпечення завжди несе ризики наявності нездокументованих функцій або бекдорів (backdoors).

Операційна система pfSense побудована на базі **FreeBSD** — однієї з найбільш стабільних, надійних та захищених UNIX-подібних операційних систем у світі. На відміну від закритих систем, вихідний код pfSense та його ядра є відкритим, постійно проходить незалежний аудит спільнотою фахівців з кібербезпеки.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

У державних стандартах захисту інформації прозорість алгоритмів цінується надзвичайно високо, оскільки вона дозволяє фахівцям Держспецзв'язку та іншим аудиторам бути впевненими у відсутності прихованих вразливостей на рівні маршрутизатора. Стек мережевих протоколів FreeBSD історично вважається одним із найшвидших та найстійкіших до мережевих атак (таких як SYN Flood або Ping of Death).

3. Широкий базовий функціонал безпеки (Stateful Packet Inspection)

У базовій комплектації pfSense є повноцінним Firewall-ом з перевіркою стану пакетів (Stateful Packet Inspection - SPI). Це означає, що фаєрвол "розуміє" стан мережевого з'єднання. На відміну від простих списків контролю доступу (ACL) на звичайних комутаторах, SPI-екран pfSense аналізує не лише IP-адреси та порти, але й послідовність TCP-сесій, динамічно відкриваючи та закриваючи порти за потреби.

Для нашого проєкту це відіграло вирішальну роль у налаштуванні логічної сегментації мережі міської ради (VLAN 10, VLAN 20, VLAN 30). За допомогою pfSense було створено строгі політики доступу (Rulesets), які дозволили повністю ізолювати демілітаризовану зону (DMZ) та гостьові мережі від критичних серверів, тим самим впровадивши концепцію "Нульової довіри" (Zero Trust) на рівні мережі.

4. Потужна екосистема модулів (Packages) для створення ешелонованого захисту

Ключова перевага pfSense над маршрутизаторами класу SOHO (наприклад, MikroTik) — це наявність системи пакетів (Package Manager), яка перетворює звичайний маршрутизатор на справжній UTM-пристрій. У рамках проєкту для Житомирської міської ради були використані наступні критично важливі пакети:

- **pfBlockerNG:** Цей пакет став основою для реалізації захисту від доступу до шкідливих сайтів. Він дозволяє автоматично завантажувати списки санкційних IP-адрес, шкідливих доменів та командних серверів ботнетів (C&C). Саме завдяки pfBlockerNG у роботі була реалізована функція **DNS Sinkholing** та GeoIP-блокування (заборона трафіку з/до країн-агресорів).

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Вручну підтримувати такі списки на звичайних маршрутизаторах неможливо, тоді як pfSense робить це автоматично в режимі реального часу.

- **Snort / Suricata (IDS/IPS):** Хоча фаєрвол блокує несанкціоновані порти, він не аналізує вміст легітимного трафіку. pfSense дозволяє в один клік розгорнути систему виявлення та запобігання вторгненням (IDS/IPS). Ця система глибоко аналізує кожен пакет (Deep Packet Inspection), шукаючи сигнатури відомих вірусів, спроби SQL-ін'єкцій на вебсервери ради чи Brute-Force атаки.

5. Безпечний віддалений доступ та інтеграція з інфраструктурою

В умовах необхідності забезпечення віддаленої роботи співробітників міської ради, pfSense пропонує вбудовану підтримку потужних криптографічних протоколів віддаленого доступу: **OpenVPN** та **IPsec / WireGuard**. Фаєрвол легко інтегрується з розгорнутим у проєкті сервером Active Directory через протокол RADIUS/LDAP. Це означає, що співробітник, підключаючись до мережі ради з дому (через VPN), використовує ті ж самі облікові дані, що і на робочому місці, а у випадку звільнення працівника його доступ до мережі миттєво анулюється в одному централізованому місці (Active Directory).

6. Відмовостійкість та резервне копіювання (Disaster Recovery)

Державна установа не може дозволити собі тривалі простої інфраструктури (Downtime). pfSense нативно підтримує протокол CARP (Common Address Redundancy Protocol), що дозволяє об'єднати два або більше маршрутизаторів у кластер високої доступності (High Availability Cluster). У разі апаратного збою основного пристрою, резервний маршрутизатор перебирає на себе весь трафік та VPN-з'єднання менш ніж за 1 секунду без розриву сесій. Крім того, вся конфігурація pfSense (від правил фаєрвола до сертифікатів шифрування) зберігається у єдиному XML-файлі обсягом кілька мегабайт (це було успішно продемонстровано в Розділі 3, Тест 10). Це робить процес резервного копіювання надзвичайно простим і швидким, що є обов'язковою умовою для відповідності державним стандартам ТЗІ.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Порівняльний висновок

Розглядаючи альтернативи:

- **MikroTik (RouterOS):** Відмінно підходить для маршрутизації, але має слабкі можливості для глибокої інспекції трафіку (DPI) і не має повноцінної системи IDS/IPS з коробки.
- **Cisco ASA / Firepower:** Надають аналогічний рівень захисту, але їхня вартість, вартість ліцензій та навчання персоналу є невиправдано високими для бюджету середнього органу місцевого самоврядування.
- **Ubiquiti UniFi:** Мають зручний інтерфейс, але обмежені в тонкому налаштуванні правил маршрутизації та політик фаєрвола.

Таким чином, вибір **pfSense** для реалізації проєкту модернізації мережі Житомирської міської ради є найбільш збалансованим технічним, безпековим та економічно виправданим рішенням. Він дозволяє побудувати надійний ешелонований захист, який відповідає всім сучасним вимогам кібербезпеки та вимогам українських нормативно-правових актів у сфері технічного захисту інформації, при цьому оптимізуючи витрати з місцевого бюджету

Таблиця 1.3

Порівняльний аналіз сучасних систем класу UTM / NGFW для захисту мережевого периметра

Характеристика / Критерій	pfSense (Community Edition)	Cisco ASA / Firepower	Fortinet FortiGate	MikroTik (RouterOS)
Модель ліцензування	Відкритий вихідний код (FreeBSD)	Комерційна (щорічна підписка / Smart Licenses)	Комерційна (щорічна підписка на FortiGuard)	Пропрієтарна (одноразова недорога ліцензія)
Вартість впровадження	Низька (лише витрати на апаратну платформу x86)	Висока (дороге обладнання + ліцензії)	Висока (обладнання + ліцензії на підписки)	Дуже низька
DPI та система IDS / IPS	Вбудовано (пакети Snort / Suricata)	Підтримується (потребує активної ліцензії)	Вбудовано (потребує активної ліцензії)	Відсутня (лише базова перевірка пакетів)

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Характеристика / Критерій	pfSense (Community Edition)	Cisco ASA / Firepower	Fortinet FortiGate	MikroTik (RouterOS)
Підтримка VPN (IPsec, OpenVPN)	Повна підтримка без обмежень	Підтримується (AnyConnect часто вимагає ліцензій)	Підтримується	Підтримується (але менш гнучко для деяких протоколів)
Апаратна незалежність	Абсолютна (встановлюється на будь-який ПК, x86 сервер або VM)	Прив'язка до пропрієтарного обладнання вендора	Прив'язка до пропрієтарного обладнання вендора	Висока (RouterBOARD або x86 Cloud Hosted Router)
Відмовостійкість (Кластеризація)	Вбудована підтримка CARP (безкоштовно)	Підтримується (Failover)	Підтримується (FGCP)	Підтримується (VRRP)
Рівень захищеності (Прозорість)	Високий (повністю відкритий для аудиту код)	Середній (закритий пропрієтарний код)	Середній (закритий пропрієтарний код)	Середній (закритий пропрієтарний код)

1.5. Постановка технічного завдання

На основі проведеного аналізу кіберзагроз та теоретичного огляду методів захисту, виникає об'єктивна необхідність у модернізації підсистеми захисту мережі Житомирської міської ради.

Технічне завдання включає наступні вимоги:

1. Спроекувати віртуальну модель мережевої інфраструктури, що включає демілітаризовану зону, внутрішню мережу (LAN) та вихід у глобальну мережу (WAN).
2. Впровадити та налаштувати програмно-апаратний маршрутизатор на базі pfSense як центральний вузол безпеки периметра.
3. Налаштувати правила міжмережевого екрану та реалізувати механізм фільтрації трафіку до потенційно небезпечних та заборонених ресурсів за допомогою методу DNS Sinkholing.

4. Розгорнути контролер домену на базі Windows Server та налаштувати об'єкти групових політик (GPO) для реалізації захисту від атак підбору паролів (Account Lockout) і впровадження глибокого аудиту подій безпеки.

1.6. Методологія моделювання загроз та вразливостей в інформаційно-телекомунікаційних системах органів місцевого самоврядування

Процес побудови захищеної мережі для такої установи, як Житомирська міська рада, неможливий без попереднього моделювання загроз. В сучасних умовах інформаційна безпека базується не на реактивному підході («закрити порт, коли атакують»), а на проактивній моделі оцінки ризиків. Згідно з методологією **MITRE ATT&CK**, для державних структур найбільш імовірними векторами атак є:

1. **Початковий доступ (Initial Access):** Найчастіше реалізується через соціальну інженерію та фішинг, спрямований на працівників апарату ради, що мають доступ до внутрішніх ресурсів.

2. **Закріплення в мережі (Persistence):** Використання шкідливих сценаріїв, що запускаються через механізми планувальника завдань Windows або групові політики (GPO), які були скомпрометовані.

3. **Горизонтальне переміщення (Lateral Movement):** Проникнення з менш захищених сегментів (наприклад, гостьової мережі або мережі Wi-Fi) до критичних сегментів, де розташовані сервери баз даних та доменні контролери.

Для протидії даним загрозам необхідно використовувати концепцію ешелонованого захисту (*Defense-in-Depth*). Ця концепція передбачає, що на шляху зловмисника до критичних даних мають бути встановлені кілька незалежних бар'єрів. Якщо один рівень (наприклад, периметровий брандмауер) буде пройдено, наступні рівні (сегментація VLAN, політики Active Directory, системи виявлення вторгнень IDS) повинні зупинити подальше поширення загрози.

1.7. Роль нормативних документів у технічному захисті інформації

Відповідно до законодавства України, захист інформації в органах місцевого самоврядування регламентується низкою нормативно-правових актів.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Зокрема, ключовим етапом створення КСЗІ (Комплексної системи захисту інформації) є формування політики безпеки, яка включає:

- **Класифікацію інформаційних ресурсів:** Розподіл інформації за рівнем доступу (відкритого доступу, службова інформація, персональні дані).
- **Контроль доступу:** Впровадження принципів мінімальних привілеїв, коли користувач отримує доступ виключно до тих ресурсів, які необхідні для виконання його посадових обов'язків.
- **Реєстрацію подій безпеки (Logging):** Обов'язкове логування всіх спроб доступу до критичних серверів, що дозволяє проводити розслідування інцидентів та виявляти аномальну активність у реальному часі.

Впровадження засобів технічного захисту (ТЗІ) повинно бути невід'ємною частиною інфраструктурних проєктів. Вибір програмно-апаратного комплексу для захисту мережі міської ради має ґрунтуватися не лише на технічних характеристиках, а й на відповідності вимогам нормативних документів (НД ТЗІ), що забезпечує юридичну та технічну легітимність побудованої системи. Таким чином, створення захищеного периметра на базі відкритого програмного забезпечення, такого як pfSense, є стратегічно виправданим кроком, що забезпечує повний контроль над потоками даних при суттєвій оптимізації витрат бюджетних коштів.

Забезпечення інформаційної безпеки в органах державної влади та місцевого самоврядування є одним із пріоритетних напрямків національної безпеки. Інформаційно-комунікаційна система (ІКС) Житомирської міської ради обробляє значні масиви критичних даних, серед яких: персональні дані громадян, інформація з обмеженим доступом, бази даних адміністративних послуг, а також документація міського бюджету та земельного кадастру. Витік, модифікація або знищення такої інформації може призвести до серйозних соціально-економічних наслідків та паралізувати роботу муніципалітету.

Саме тому проєктування, розгортання та експлуатація мережевої інфраструктури міської ради має суворо відповідати вимогам українського законодавства у сфері технічного захисту інформації (ТЗІ).

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Огляд українського законодавства у сфері кібербезпеки

Функціонування систем кібербезпеки в державних установах регламентується наступною нормативно-правовою базою:

1. **Закон України «Про захист інформації в інформаційно-комунікаційних системах»:** Встановлює загальні принципи та правила захисту інформації в мережах. Закон вимагає, щоб інформація, яка є власністю держави або вимагає захисту згідно із законом (наприклад, персональні дані), оброблялася виключно в системах із застосуванням Комплексної системи захисту інформації (КСЗІ), що має підтверджений сертифікат відповідності.

2. **Закон України «Про основні засади забезпечення кібербезпеки України»:** Визначає правові та організаційні основи захисту життєво важливих інтересів людини, суспільства та держави в кіберпросторі. Міські ради належать до об'єктів, де забезпечення кібербезпеки є обов'язковим елементом захисту критичної інфраструктури регіону.

3. **Закон України «Про захист персональних даних»:** Зобов'язує органи місцевого самоврядування вживати необхідних організаційних і технічних заходів для захисту баз персональних даних мешканців міста від незаконної обробки, втрати або знищення.

4. **Нормативні документи з технічного захисту інформації (НД ТЗІ):** Це набір державних стандартів (зокрема, НД ТЗІ 3.7-003-05 та НД ТЗІ 2.5-004-99), які визначають критерії оцінки захищеності інформації, вимоги до міжмережевих екранів (включаючи використання таких рішень, як pfSense), криптографічного захисту, автентифікації користувачів (через Active Directory) та журналювання подій.

Сутність та призначення КСЗІ

Відповідно до вимог Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку), для легальної обробки даних у Житомирській міській раді необхідно створити Комплексну систему захисту інформації (КСЗІ).

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

КСЗІ — це взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, призначених для забезпечення конфіденційності, цілісності та доступності даних в ІКС.

Впровадження програмно-апаратних рішень (сегментація мережі, налаштування політик безпеки в домені контролера, фільтрація трафіку) є лише технічною частиною КСЗІ. Легітимність цієї системи підтверджується шляхом проходження Державної експертизи.

Етапи побудови КСЗІ для органу місцевого самоврядування

Процес створення Комплексної системи захисту інформації є тривалим і багатоетапним. Згідно з НД ТЗІ 3.7-003-05, побудова КСЗІ на об'єкті на кшталт міської ради включає наступні кроки:

Етап 1. Обстеження інформаційного середовища та аудит На цьому етапі проводиться інвентаризація всіх апаратних і програмних засобів, які використовуються в міській раді (сервери, робочі станції, мережеве обладнання). Визначаються категорії даних, що циркулюють у мережі, маршрути їх проходження та точки взаємодії із зовнішніми мережами (Інтернетом, системами казначейства тощо).

Етап 2. Розробка моделі загроз та моделі порушника Формується перелік потенційних загроз (вірусні атаки, DDoS, несанкціонований доступ, інсайдерські витоки). Модель порушника описує кваліфікацію, можливості та мотиви потенційного зловмисника — від недосвідченого користувача всередині мережі ради до організованих зовнішніх хакерських угруповань.

Етап 3. Формування Технічного завдання (ТЗ) на створення КСЗІ На основі результатів обстеження розробляється документ, який фіксує всі вимоги до майбутньої системи захисту. ТЗ обов'язково має бути узгоджене з Держспецзв'язку (або її територіальним підрозділом). У ТЗ прописуються вимоги до антивірусного захисту, системи резервного копіювання, міжмережевого екранування, управління доступом.

Етап 4. Розробка робочої та експлуатаційної документації Створюється пакет документів, який включає політику інформаційної безпеки установи,

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

інструкції для адміністраторів (системного та адміністратора безпеки), інструкції користувачів щодо поводження з паролями та електронною поштою, журнали обліку носіїв інформації. Технічні рішення, описані у практичній частині цієї дипломної роботи (налаштування pfSense, GPO в Active Directory), документально закріплюються саме на цьому етапі.

Етап 5. Впровадження та дослідна експлуатація КСЗІ Відбувається фізичне розгортання засобів захисту. Після налаштування обладнання та ПЗ видається наказ про початок дослідної експлуатації. Протягом цього періоду (зазвичай 1–2 місяці) перевіряється, наскільки впроваджені засоби захисту впливають на бізнес-процеси міської ради, чи коректно працюють політики доступу, усуваються виявлені технічні помилки.

Етап 6. Державна експертиза КСЗІ Заключний етап, який виконується незалежною компанією-ліцензіатом. Експерти проводять тестування на проникнення, перевіряють відповідність реальних налаштувань мережі розробленому ТЗ та документації. У разі успішного проходження перевірки Держспецзв'язку видає міській раді Атестат відповідності КСЗІ (зазвичай терміном на 3 або 5 років). Тільки після отримання Атестата система вважається захищеною з точки зору законодавства України, і в ній дозволяється обробка державних інформаційних ресурсів.

Висновки до розділу 1. За результатами першого розділу було здійснено аналіз основних кіберзагроз, характерних для інформаційних систем державних установ. Визначено, що найбільш критичними є атаки на облікові записи користувачів та доступ до шкідливих інтернет-ресурсів. Обґрунтовано вибір концепції ешелонованого захисту (Defense in Depth), використання pfSense для периметральної фільтрації та DNS Sinkholing, які не потребують значних апаратних ресурсів, але забезпечують ефективне блокування окремих загроз. Також обґрунтовано доцільність застосування механізмів Active Directory (GPO) для протидії Brute-Force атакам та ведення журналів аудиту. На основі цих висновків сформовано постановку технічного завдання для подальшої практичної реалізації проекту модернізації мережі.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЖИТОМИРСЬКОЇ МІСЬКОЇ РАДИ

2.1. Обґрунтування необхідності модернізації підсистеми захисту мережної інфраструктури Житомирської міської ради

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням ролі електронних послуг та цифрової взаємодії між органами місцевого самоврядування та громадянами. Мережна інфраструктура міської ради є критичним компонентом, що забезпечує обробку, зберігання та передачу великих масивів даних, серед яких конфіденційна інформація, персональні дані мешканців та службова документація. Оскільки точні дані щодо поточної конфігурації мережі та інцидентів безпеки є закритою інформацією, обґрунтування модернізації спирається на загальновизнані тенденції розвитку кіберзагроз, архітектурні недоліки класичних мереж та сучасні вимоги до захисту державних інформаційних систем.

Необхідність проведення комплексної модернізації підсистеми захисту зумовлена низкою об'єктивних факторів:

1. Еволюція кіберзагроз та зміна ландшафту атак. Традиційні методи захисту, що базуються переважно на периметрових міжмережевих екранах (Firewalls) старих поколінь та базовому антивірусному програмному забезпеченні, втрачають свою ефективність. Сучасні цілеспрямовані атаки (APT — Advanced Persistent Threats), програми-вимагачі (Ransomware), складні інфраструктурні DDoS-атаки та методи соціальної інженерії вимагають впровадження комплексних рішень. До них належать системи виявлення та запобігання вторгненням (IDS/IPS), системи глибокого аналізу трафіку (DPI) та використання пристроїв класу UTM (Unified Threat Management) або NGFW (Next-Generation Firewall).

2. Розширення поверхні атаки та недоліки плоскої архітектури. Впровадження нових муніципальних онлайн-сервісів та потреба у безпечному віддаленому доступі для співробітників суттєво розширюють межі корпоративної мережі. Використання застарілих підходів з єдиним широкомовним доменом або

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

недостатня сегментація створюють критичні ризики. У разі компрометації одного комп'ютера в умовному відділі кадрів, шкідливе програмне забезпечення може безперешкодно поширитися на сервери баз даних або фінансовий відділ. Тому базовою вимогою до модернізації є логічна ізоляція департаментів за допомогою віртуальних локальних мереж (VLAN) та винесення публічних сервісів у демілітаризовану зону (DMZ).

3. Централізація управління та ідентифікації. Відсутність єдиної політики управління правами доступу ускладнює адміністрування та моніторинг дій користувачів. Модернізація передбачає впровадження каталогів служб (наприклад, на базі Active Directory) для централізованої автентифікації, авторизації, а також застосування групових політик (GPO). Це дозволяє мінімізувати вплив «людського фактора» та стандартизувати налаштування безпеки на всіх робочих станціях міської ради.

4. Відповідність нормативно-правовим вимогам. Органи місцевого самоврядування зобов'язані неухильно дотримуватися вимог законодавства України у сфері технічного захисту інформації (зокрема, нормативних документів НД ТЗІ щодо побудови Комплексної системи захисту інформації — КСЗІ). Оновлення інфраструктури дозволяє привести технічну складову у відповідність до актуальних державних стандартів та найкращих світових практик (наприклад, сертифікацій ISO/IEC 27000).

5. Забезпечення високої доступності та відмовостійкості. Для органів місцевої влади критично важливим є показник доступності сервісів (High Availability). Відмова ключового маршрутизатора або успішна атака на відмову в обслуговуванні можуть паралізувати роботу цілих структурних підрозділів. Сучасна архітектура вимагає резервування каналів зв'язку, налаштування протоколів динамічної маршрутизації та резервування шлюзів безпеки.

Таким чином, модернізація підсистеми захисту мережної інфраструктури Житомирської міської ради є не просто плановим оновленням апаратного забезпечення, а концептуальним переходом від реактивної моделі безпеки до проактивної. Реалізація багаторівневого захисту (Defense in Depth) дозволить

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

гарантувати конфіденційність, цілісність та безперервну доступність муніципальних інформаційних ресурсів в умовах постійного зростання рівня кібернетичних небезпек.

2.2. Розгортання базової мережі та серверної інфраструктури

Для реалізації практичної частини дослідження було самостійно розгорнуто та сконфігуровано повноцінний лабораторний стенд у середовищі GNS3, який виступає моделлю мережі. Цей стенд дозволяє дослідити процес забезпечення інформаційної безпеки, конфіденційності, цілісності та доступності даних в IT-інфраструктурі Житомирської міської ради.

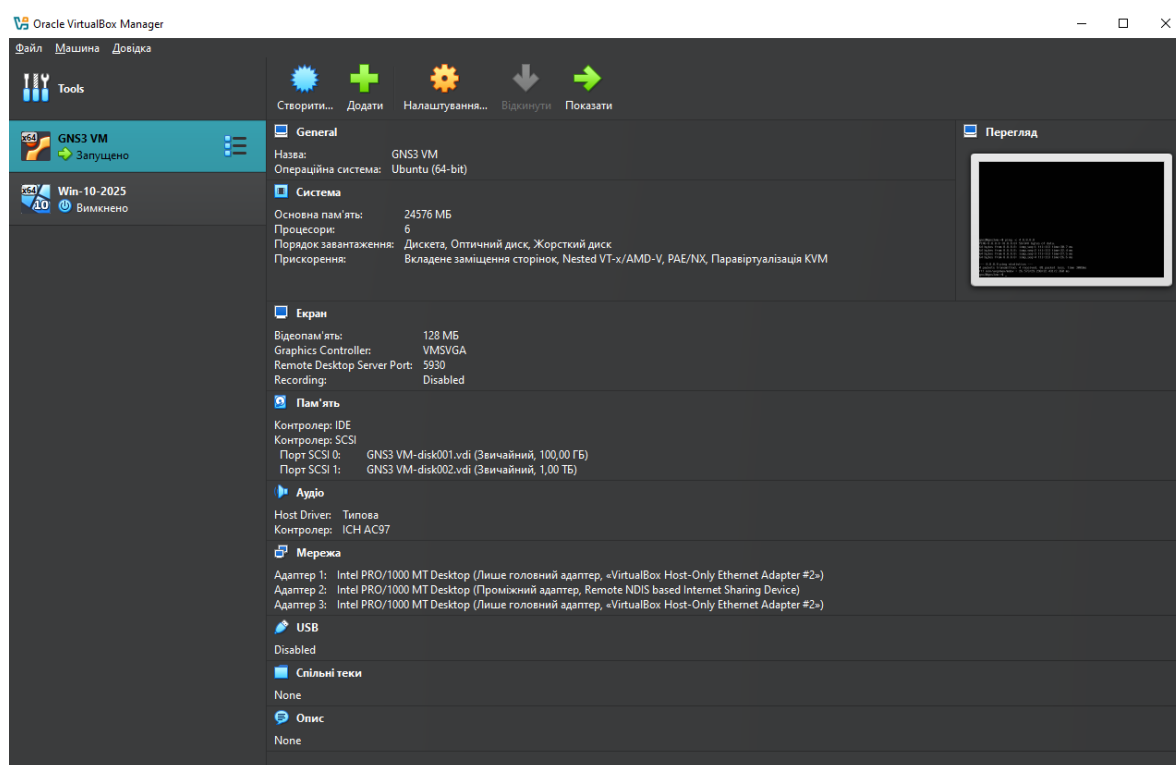


Рисунок 2.1 Сервер для лабораторного стенду у середовищі GNS3

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

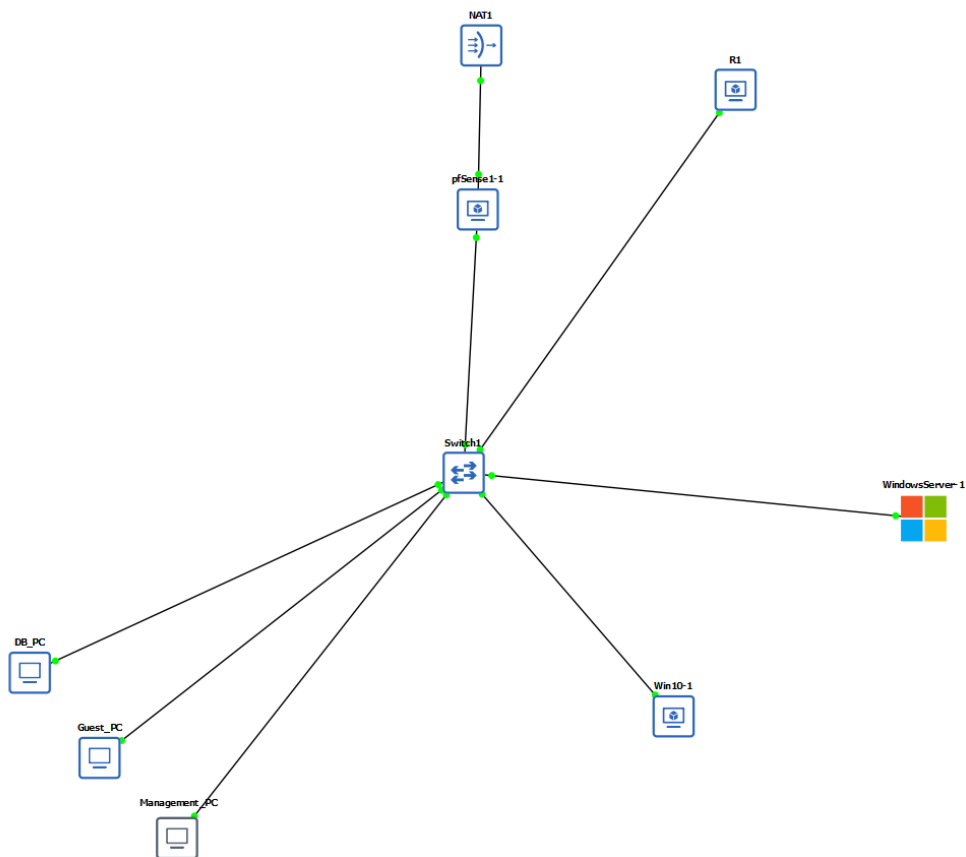


Рисунок 2.2 Лабораторний стенд у середовищі GNS3

Таблиця 2.1

Розподілення ресурсів

ВМ	Кількість	Озм,МБ	vCPU
pfSense1-1	1	4096 MB	1
R1	1	2048 MB	1
WindowsServer-1	1	4096 MB	4
Win10-1	1	4096 MB	4
VPCS	3	2 MB	1
Switch1	1	2 MB	1

Для практичної перевірки ефективності запропонованої архітектури було розроблено віртуальний тестовий стенд. Як основне середовище емуляції мережевої топології використовується платформа GNS3 у тісній інтеграції з гіпервізором VirtualBox, де розгорнуто образи кінцевих робочих станцій, серверів та брандмауера pfSense.

Під час інтеграції віртуальних вузлів було виявлено ряд специфічних особливостей маршрутизації трафіку в гібридному середовищі. Зокрема, під час тестування зовнішнього підключення стенда до інтернету було зафіксовано, що при включенні функції спільного доступу до підключення (Internet Connection Sharing) на хост-машині, маршрутизація всередині GNS3 порушується, і мережеві вузли втрачають зв'язок. Однак, при відключенні спільного доступу та переведенні мережевих адаптерів у режим стандартного NAT або використання віртуальних комутаторів GNS3, стабільність роботи повністю відновлюється. Це підтверджує необхідність жорсткого розмежування логічних інтерфейсів та недоцільність використання засобів спільного доступу ОС хоста при побудові складних віртуальних топологій.

Фундаментом мережі є розгорнута віртуальна машина на базі Windows Server 2019, на якій піднято ролі AD DS зі створенням локального домену corp.local. Для ефективного управління мережевою інфраструктурою було реалізовано наступні кроки:

- Даний сервер налаштовано як локальний DNS-вузол, що забезпечує централізоване керування іменами хостів.
- На LAN-інтерфейсі мережевого екрана pfSense активовано DHCP-сервер, який автоматично розподіляє IP-адреси для клієнтських пристроїв із пулу 10.10.10.100 – 10.10.10.200.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

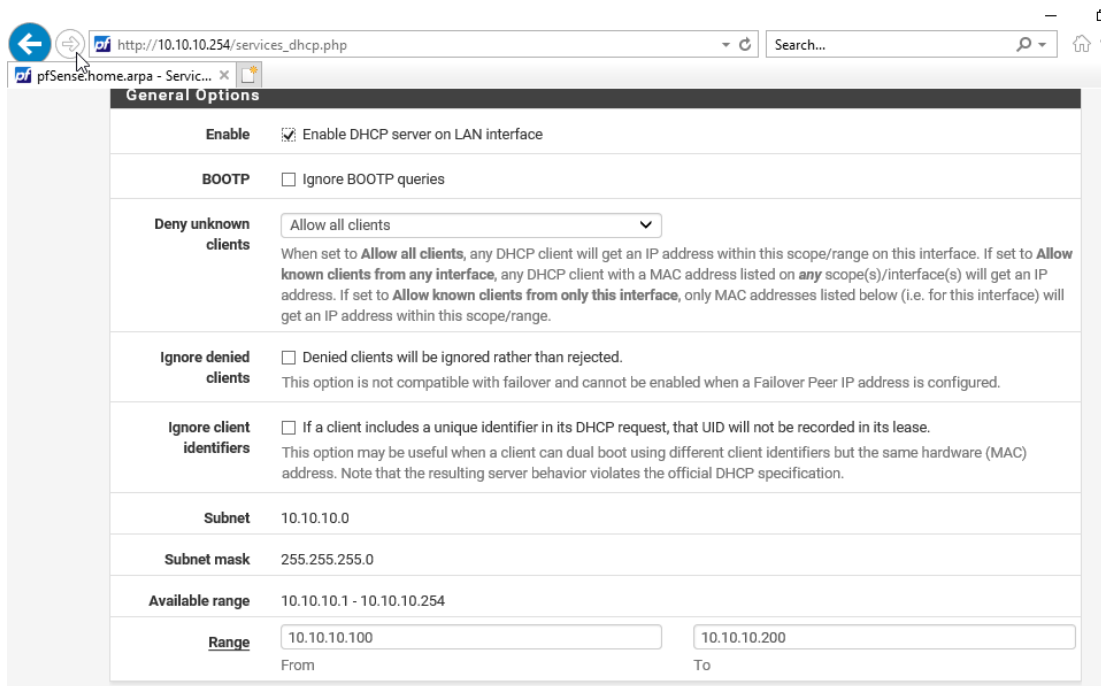


Рисунок 2.2 Розподілення IP-адрес

- Впроваджено централізовану систему автентифікації та розмежування прав доступу, що критично важливо для унеможливлення несанкціонованого доступу до ресурсів міськради.

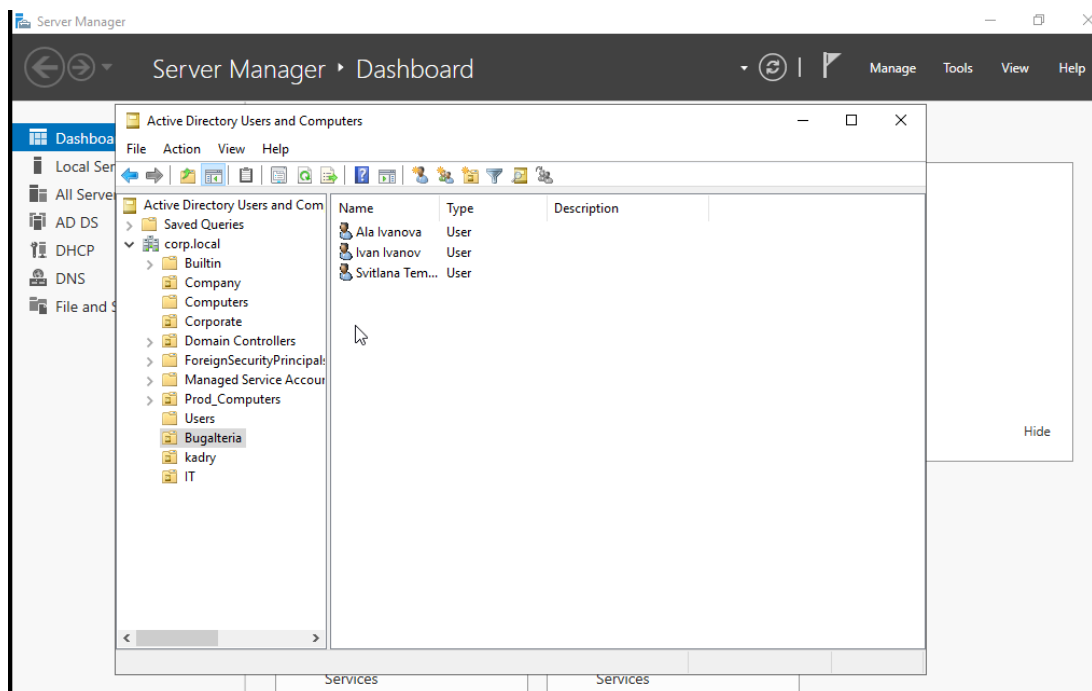


Рисунок 2.3 Active Directory Users and Computers

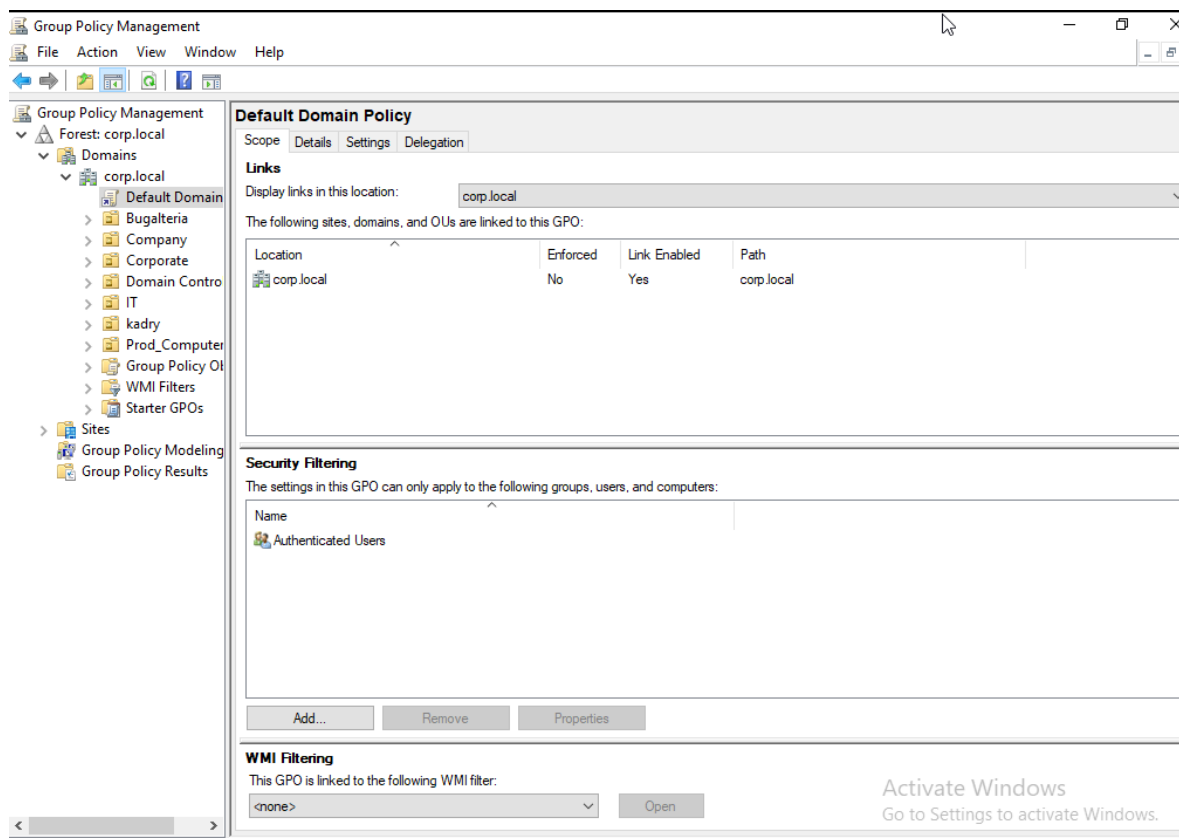


Рисунок 2.4 Group Policy Management

Для протидії кібератакам типу Brute-Force (повний перебір паролів) засобами Active Directory була сконфігурована жорсткова політика блокування облікових записів (Account Lockout Policy). Встановлено обмеження у 5 невдалих спроб авторизації, після досягнення якого обліковий запис тимчасово деактивується. Цей захід ефективно усуває ризик несанкціонованого доступу до мережі через компрометацію слабких користувацьких паролів.

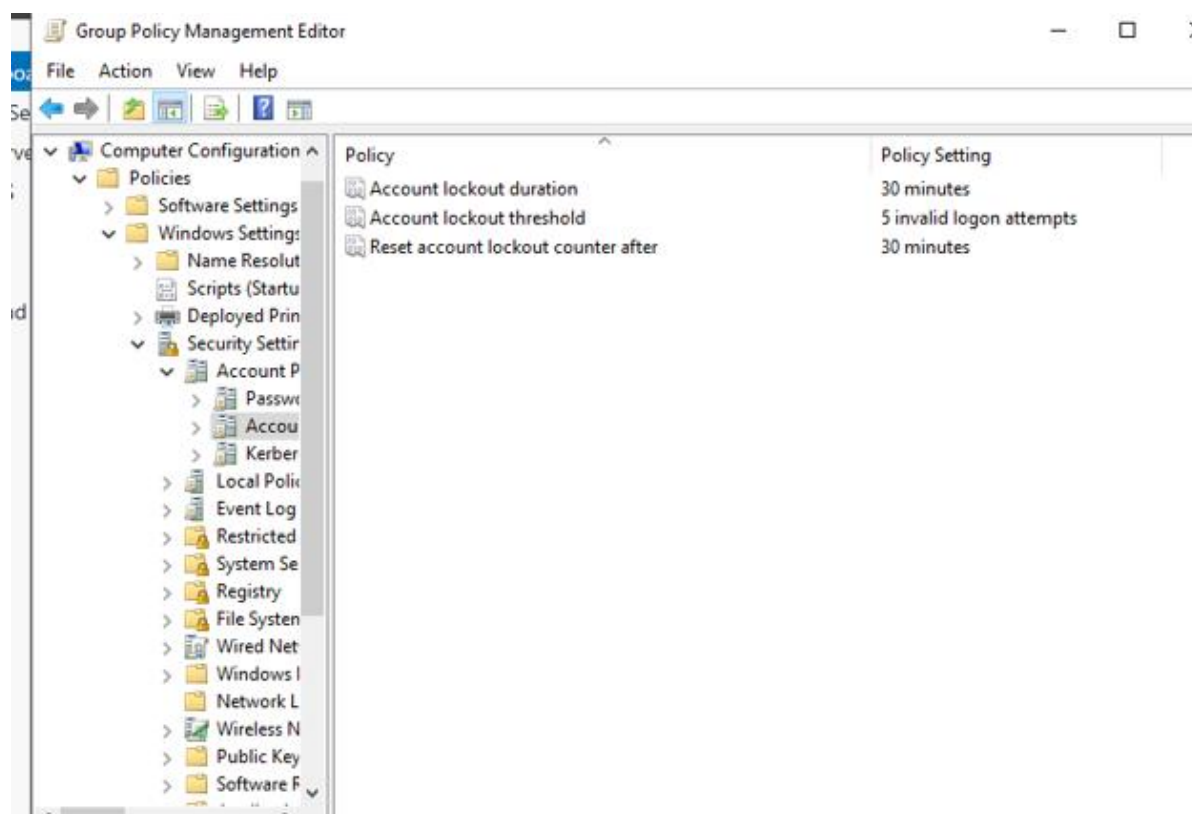


Рисунок 2.5 Конфігурація політики блокування облікових записів (Account Lockout Policy).

2.3. Логічна сегментація мережі та міжвіланова маршрутизація

Надійна підсистема захисту вимагає чіткого розділення мережі на ізольовані сегменти. У рамках проєкту було реалізовано фізичну та логічну сегментацію мережі з виділенням захищеного контуру (VLAN 10) для критичних баз даних, який повністю ізольований від сегмента звичайних користувачів (VLAN 20).

З метою мінімізації площі атаки (attack surface) та локалізації можливих інцидентів безпеки, локальну мережу установи логічно розділено на віртуальні локальні мережі (VLAN) за допомогою стандарту IEEE 802.1Q. Такий підхід дозволяє ізолювати широкомовні домени та застосовувати індивідуальні політики контролю доступу (ACL) для різних структурних підрозділів.

Запропонована підсистема захисту реалізує концепцію ешелонованої оборони (Defense-in-Depth), яка передбачає наявність кількох рівнів безпеки, що дублюють та доповнюють один одного. На першому рівні (периметр) здійснюється фільтрація трафіку засобами брандмауера pfSense з активованою функцією блокування відомих шкідливих IP-адрес через GeoIP-фільтри та списки репутації.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

На другому рівні здійснюється глибока інспекція пакетів (DPI) для виявлення сигнатур атак. На третьому рівні (хостовому) безпека забезпечується політиками Active Directory, які обмежують права локальних адміністраторів та забороняють виконання непідписаних скриптів. Така багаторівневність гарантує, що навіть у випадку компрометації одного з вузлів, злоумисник не отримає доступу до критичних баз даних Житомирської міської ради, оскільки внутрішня сегментація мережі перешкоджає горизонтальному переміщенню (lateral movement) загрози

Логічна структура передбачає створення наступних ізольованих сегментів:

- **VLAN 10 (Management & Servers):** Серверний сегмент, що містить контролер домену Active Directory, бази даних та інфраструктурні сервіси. Доступ до цього сегменту суворо регламентований правилами pfSense і дозволений лише для IT-адміністраторів.
- **VLAN 20 (Staff/Users):** Робочі станції співробітників міської ради. Вузли цієї мережі мають доступ до інтернету виключно через проксі-сервер та фільтри IDS/IPS, що блокують доступ до шкідливих ресурсів.
- **VLAN 30 (Guest):** Гостьова мережа з повним доступом до мережі Інтернет, але фізично та логічно ізольована від внутрішніх ресурсів установи (VLAN 10 та 20), що унеможливорює компрометацію внутрішньої інфраструктури через пристрої відвідувачів.

Таблиця 2.6

План розподілу IP-адресації мереж

Назва VLAN	ID VLAN	Діапазон мережі	Призначення
Management	10	10.10.10.0/24	Сервери, Апаратні вузли
Staff_Office	20	10.10.20.0/24	Робочі станції працівників
Guest_Zone	30	10.10.30.0/24	Гостьовий доступ (Wi-Fi)
VoIP_Traffic	40	10.10.40.0/24	IP-телефонія

База мережевого адміністрування була побудована з використанням наступних технологічних рішень:

- Комутатор Switch1 налаштовано для роботи з віртуальними локальними мережами (VLAN), де серверний сегмент винесено у VLAN 10.
- Проведено розподіл портів комутатора: Port 0 налаштовано як Trunk-порт для зв'язку з маршрутизатором (з використанням інкапсуляції dot1q), а порти Port 1 та Port 2 переведено в режим Access для підключення сервера та фаєрвола.

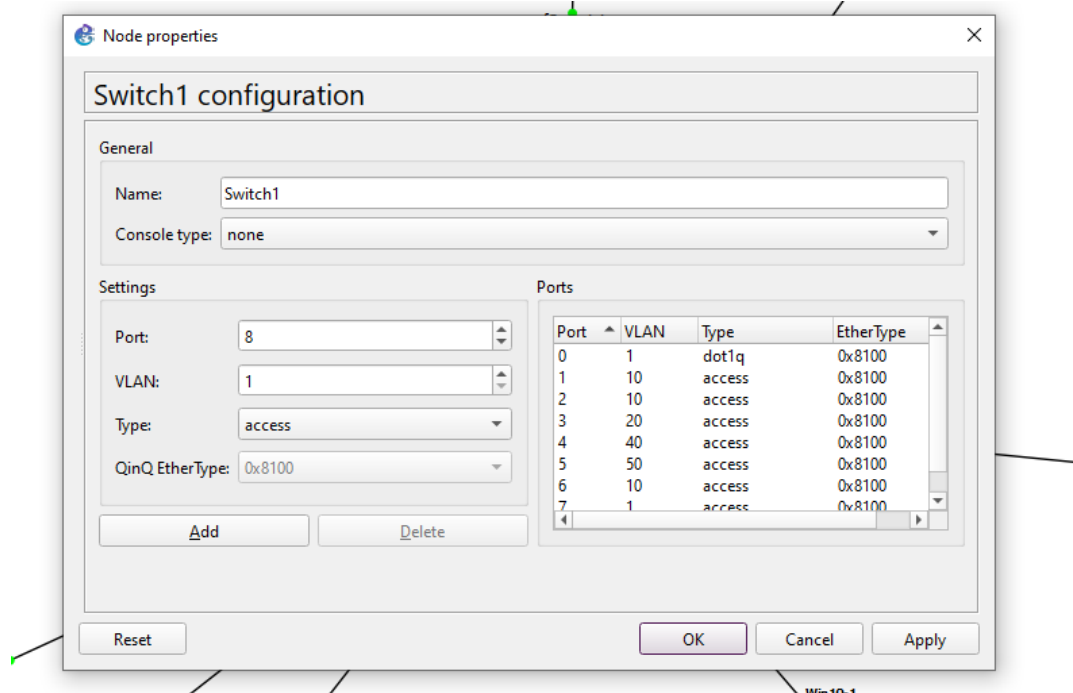


Рисунок 2.7 Налаштування Switch1

- Маршрутизацію між ізольованими підмережами забезпечує маршрутизатор Cisco R1, який сконфігуровано за топологією "Router-on-a-stick" зі створенням субінтерфейсів Gi0/0.10 та Gi0/0.20.

```
Router>show ip interface brief
Interface IP-Address OK? Method Status Prot
ocol
GigabitEthernet0/0 unassigned YES NVRAM up up
GigabitEthernet0/0.10 10.10.10.1 YES NVRAM up up
GigabitEthernet0/0.20 10.10.20.1 YES NVRAM up up
GigabitEthernet0/1 unassigned YES NVRAM administratively down down
GigabitEthernet0/2 unassigned YES NVRAM administratively down down
GigabitEthernet0/3 unassigned YES NVRAM administratively down down
GigabitEthernet0/4 unassigned YES NVRAM administratively down down
GigabitEthernet0/5 unassigned YES NVRAM administratively down down
GigabitEthernet0/6 unassigned YES NVRAM administratively down down
GigabitEthernet0/7 unassigned YES NVRAM administratively down down
Router>
```

Рисунок 2.8 Субінтерфейси Gi0/0.10 та Gi0/0.20

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.10.0/24 is directly connected, GigabitEthernet0/0.10
L       10.10.10.1/32 is directly connected, GigabitEthernet0/0.10
C       10.10.20.0/24 is directly connected, GigabitEthernet0/0.20
L       10.10.20.1/32 is directly connected, GigabitEthernet0/0.20
```

Рисунок 2.9 Прямі мережі для обох субінтерфейсів

Для забезпечення логічної ізоляції мережевого трафіку між функціональними підрозділами міської ради (наприклад, між адміністративним сегментом та сегментом публічного доступу) було реалізовано технологію 'Router-on-a-stick'. Маршрутизатор Cisco R1 виступає центральним вузлом комутації 3-го рівня, де за допомогою створення субінтерфейсів (Gi0/0.10, Gi0/0.20) здійснюється інкапсуляція трафіку за стандартом IEEE 802.1Q. Такий підхід дозволив розмежувати широкомовні домени (broadcast domains) та підвищити рівень безпеки мережі шляхом заборони прямої передачі даних між ізольованими підмережами без проходження через правила фільтрації шлюзу.

Правила фільтрації трафіку на WAN-інтерфейсі (Firewall Rules)

Джерело	Призначення	Порт	Протокол	Дія	Опис
Any	WAN Address	443	TCP	Allow	Доступ до Web-інтерфейсу
Staff_Net	Any	80/443	TCP	Allow	Вихід в Інтернет
Guest_Net	Any	53	UDP	Allow	DNS запити
Any	Any	Any	Any	Drop	Заборона всього іншого

2.4. Налаштування списків контролю доступу (ACL) та міжмережевого екрана

Основним елементом захисту периметра та внутрішніх сегментів є інтегрований у топологію фаєрвол pfSense. Його LAN-інтерфейс отримав адресу 10.10.10.254/24, що дозволяє йому функціонувати в одному сегменті з основним сервером. Адміністратору надано повний доступ до вебпанелі керування pfSense для гнучкого налаштування правил.

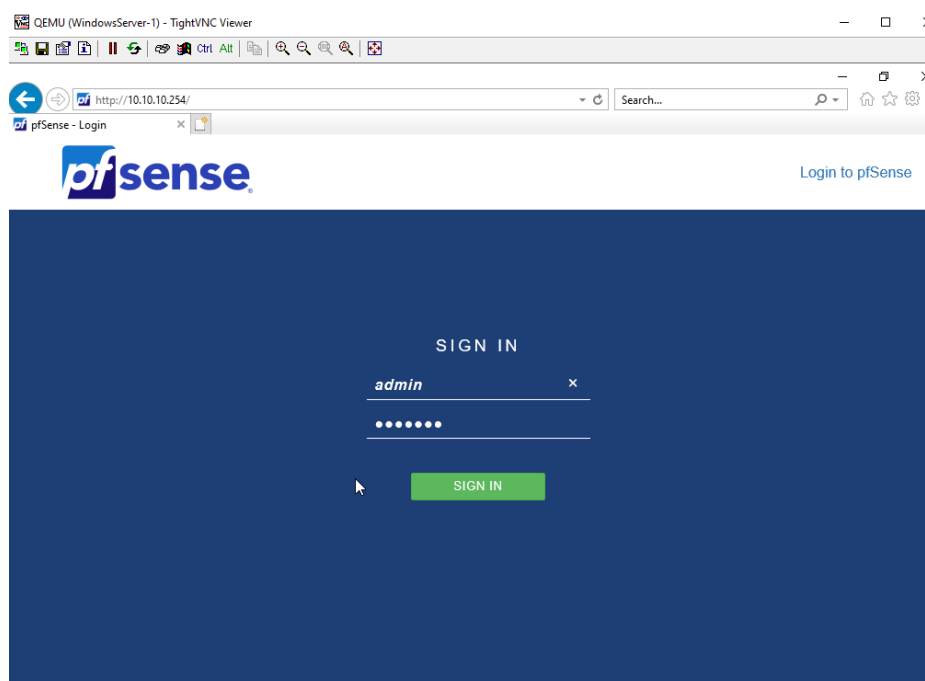


Рисунок 2.10 Вхід в вебпанель pfSense

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

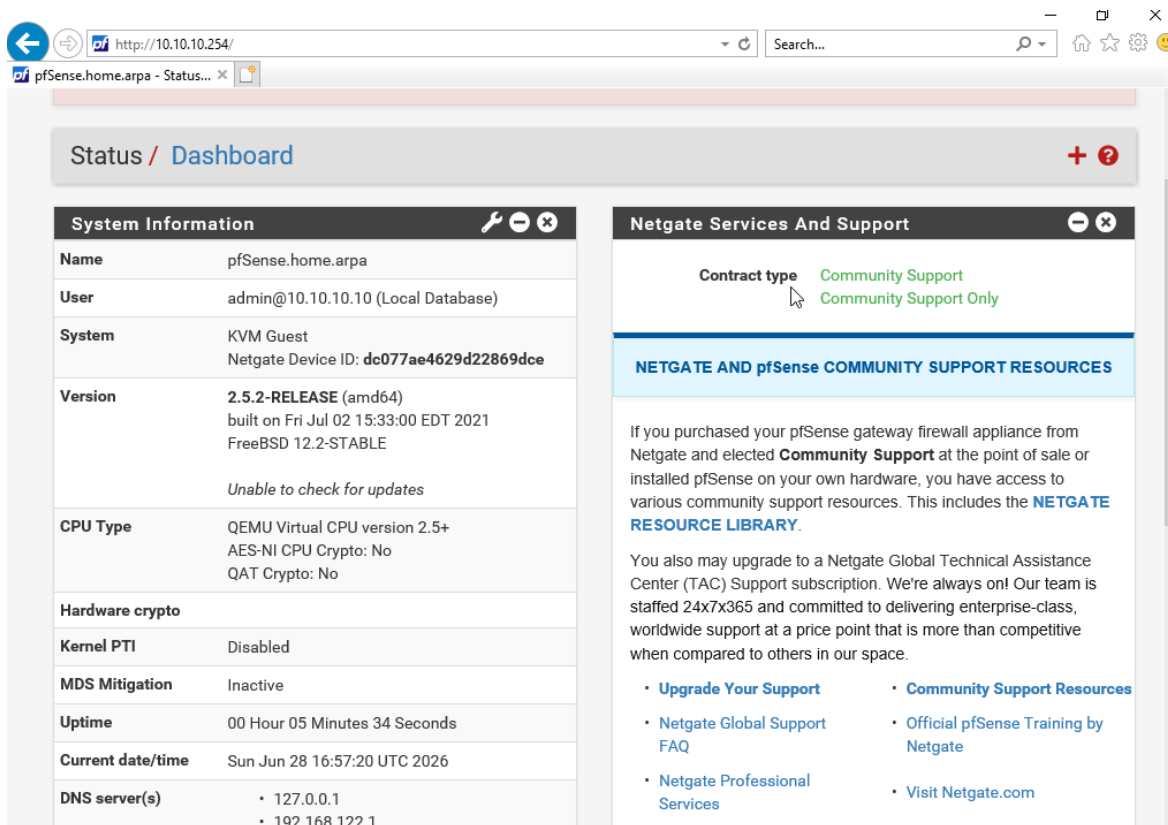


Рисунок 2.11 Вебпанель pfSense

На маршрутизаторі R1 було підготовлено та впроваджено логіку застосування списків контролю доступу (ACL) для жорсткого фільтрування міжсегментного трафіку. Зокрема:

```

R1 - PuTTY
Router>show access-lists
Extended IP access list 100
 10 deny ip 10.10.30.0 0.0.0.255 10.10.10.0 0.0.0.255
 20 permit ip any any
Extended IP access list BLOCK_USER_TO_MGMT
 10 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
 20 permit ip any any (190 matches)

```

Рисунок 2.12 Аналіз ефективності правил фільтрації трафіку (ACL).

- Правило Extended IP access list 100 ізолює сегмент критичних серверів (VLAN 10) від демілітаризованої зони (DMZ, 10.10.30.0/24).

```

R1 - PuTTY
* purposes is expressly prohibited except as otherwise authorized by      *
* Cisco in writing.                                                         *
*****
Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny ip 10.10.30.0 0.0.0.255 10.10.10.0 0.0.0.2$
Router(config)#access-list 100 permit ip any any
Router(config)#interface Gi0/0.30
Router(config-subif)#ip access-group 100 in
Router(config-subif)#

```

Рисунок 2.13 Налаштування списків контролю доступу (ACL) для ізоляції демілітаризованої зони (DMZ) від внутрішньої мережі міської ради.

- Правило Extended IP access list BLOCK_USER_TO_MGMT забороняє проходження трафіку від серверного сегмента до користувацької мережі. Аналіз ефективності показав наявність 190 збігів у правилі permit ip any any, що свідчить про успішну обробку легітимного трафіку на тлі успішного блокування заборонених з'єднань правилами deny.

Додатково на базі pfSense було впроваджено превентивне блокування доступу до небезпечних та санкційних IP-адрес. Для захисту зовнішнього периметра від розвідувального сканування (Reconnaissance attacks) було застосовано режим невидимості ("Stealth"). Шляхом жорсткого блокування протоколу ICMP на WAN-інтерфейсі мережа установи стає невидимою для зовнішніх ботнетів та сканерів, що мінімізує ризик DDoS-атак

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	1 / 284 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
☐	✗ 0 / 0 B	IPv4 *	*	*	Sanctioned_ IPs	*	*	none			
☐	✓ 0 / 5 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
☐	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Рисунок 2.14 Впровадження превентивного блокування доступу до санкційних та небезпечних IP-адрес на базі мережевого екрана pfSense

Properties

Name Sanctioned_IPs
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type Network(s)

Network(s)

Hint Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN				
77.88.0.0	/	18	yandex.ru	Delete
87.240.128.0	/	19	vk.ru	Delete
94.100.176.0	/	20	mail.ru	Delete

Save Export to file Add Network

Рисунок 2.15 Впровадження превентивного блокування доступу до санкційних та небезпечних IP-адрес на базі мережевого екрана pfSense

Name	Type	Data	Timestam
(same as parent folder)	Start of Authority (SOA)	[1], win-98cubhm907p.cor...	static
(same as parent folder)	Name Server (NS)	win-98cubhm907p.corp.lo...	static
(same as parent folder)	Host (A)	127.0.0.1	

Рисунок 2.16 Реалізація механізму DNS Sinkholing для превентивного блокування шкідливих ресурсів.

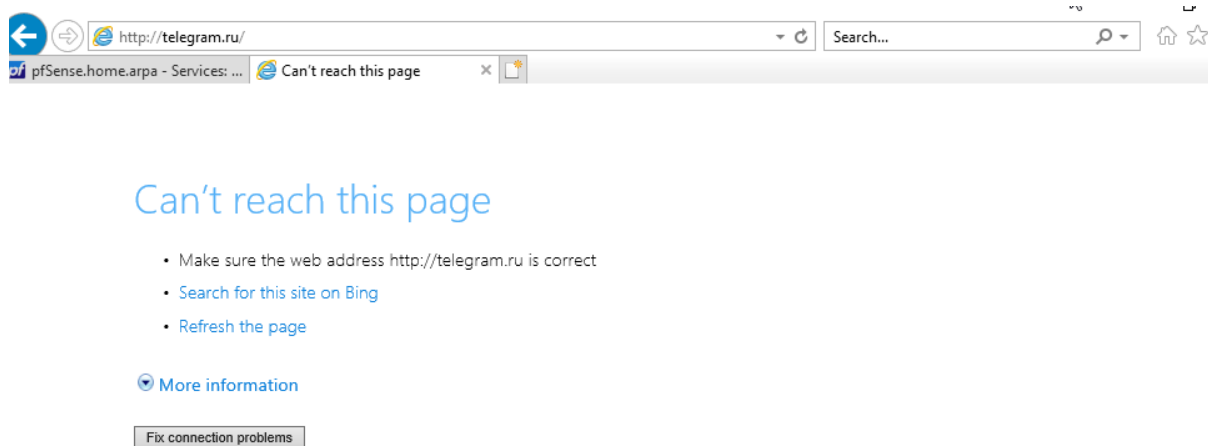


Рисунок 2.17 Невдала спроба зайти на фейковий сайт

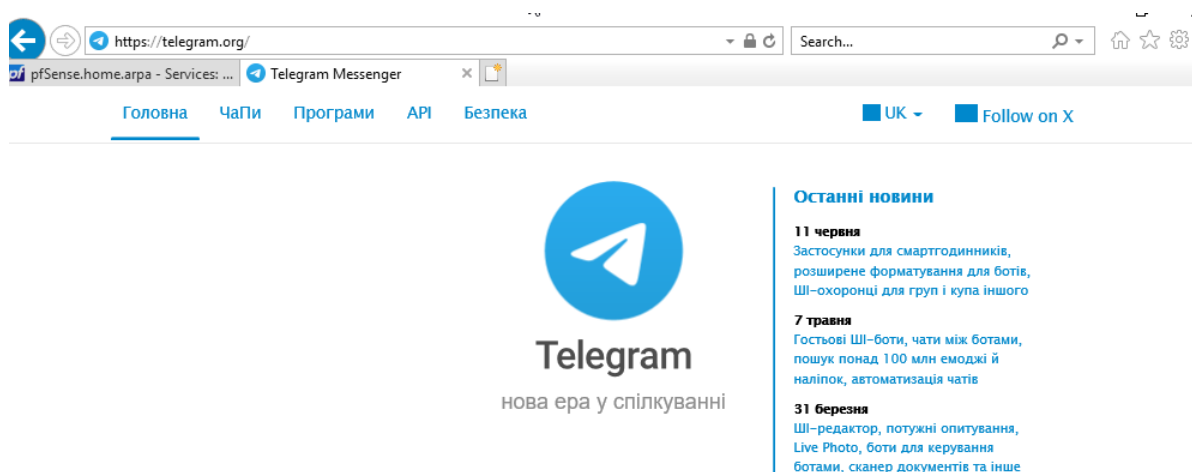


Рисунок 2.18 Вдала спроба зайти на реальний сайт

На рисунку продемонстровано налаштування внутрішнього DNS-сервера міської ради для перехоплення запитів до скомпрометованих доменів. Завдяки створенню фіктивних зон (DNS Sinkholing), спроби співробітників перейти за фішинговими посиланнями (наприклад telegram.ru , коли реальна адреса telegram.org) автоматично перенаправляються на безпечну локальну адресу (127.0.0.1), що унеможливорює витік облікових даних та зараження робочих станцій шкідливим програмним забезпеченням.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

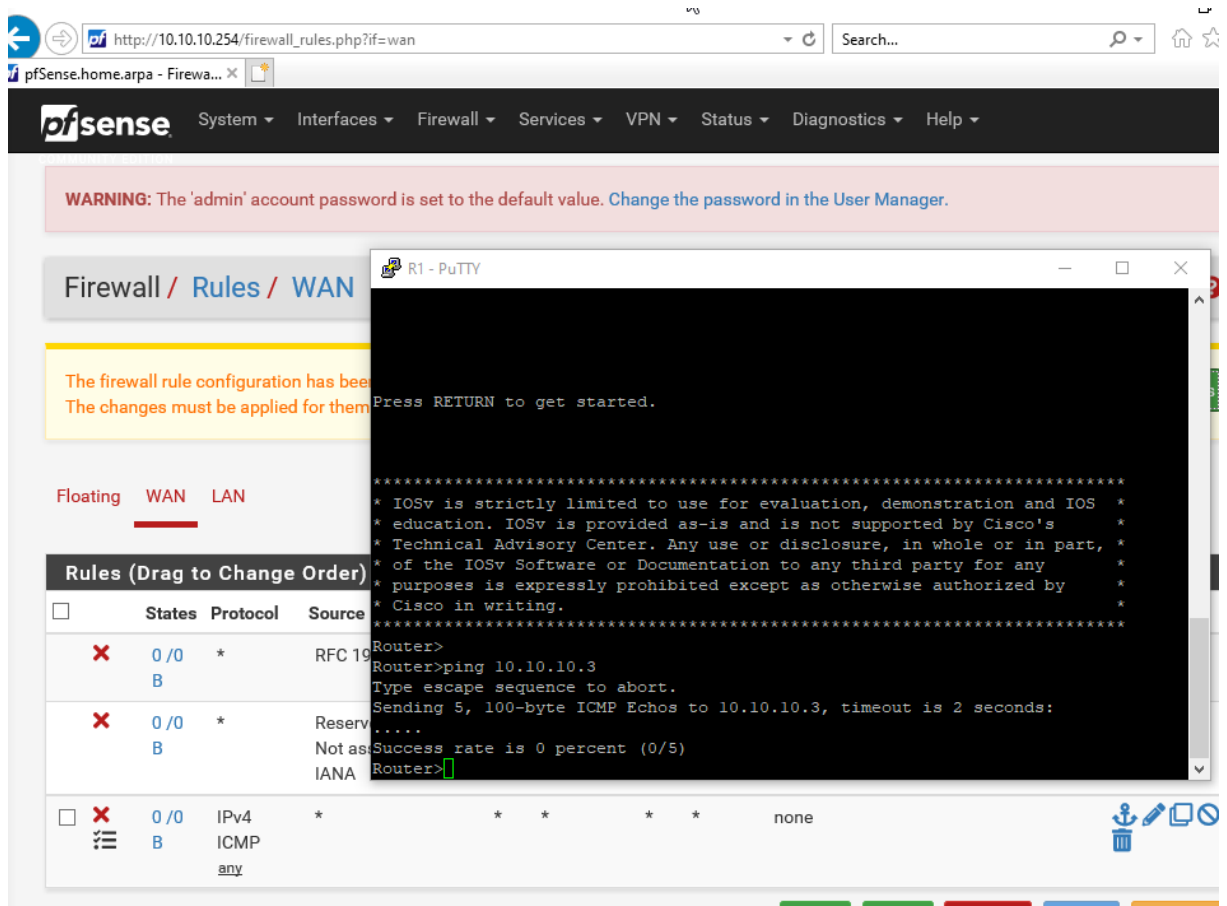


Рисунок 2.19 Забезпечення режиму "Stealth" (невидимості) для зовнішнього периметра мережі.

На рисунку відображено налаштування захисту зовнішнього інтерфейсу мережевого екрана від розвідувального сканування (Reconnaissance attacks). Жорстке блокування протоколу ICMP на інтерфейсі WAN переводить мережу міської ради в режим невидимості для зовнішніх сканерів та ботнетів, що значно знижує ймовірність проведення цілеспрямованих DDoS-атак та експлуатації вразливостей.

2.5. Впровадження додаткових механізмів захисту, моніторингу та резервного копіювання

Службу дозволу імен було модернізовано шляхом активації протоколу DNS over TLS (DoT) та перевірки DNSSEC, що робить неможливим перехоплення чи підміну DNS-запитів.

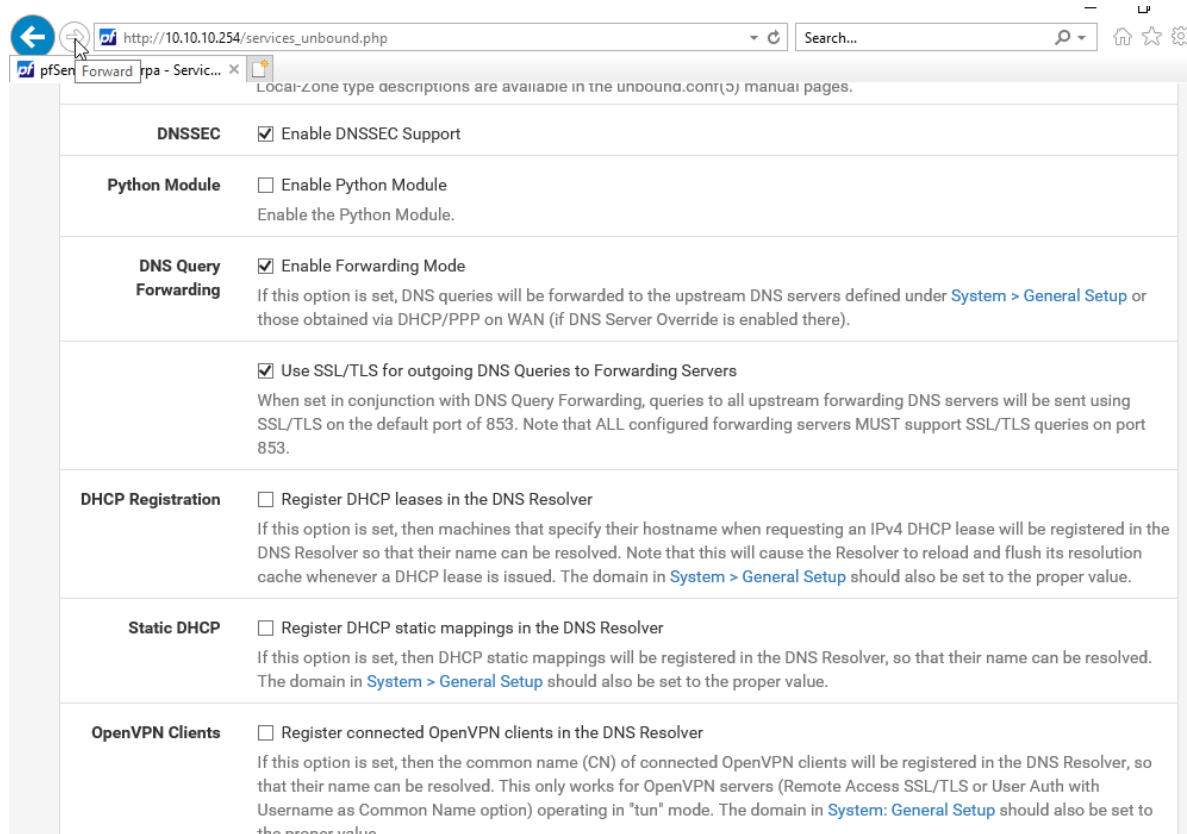


Рисунок 2.20 Налаштування *DNS Resolver* з активованими галочками DNSSEC та TLS-шифрування.

Для забезпечення контролю та аудиту було налаштовано моніторинг інцидентів у режимі реального часу. Усі спроби порушення політик доступу, такі як звернення до заборонених підмереж, автоматично реєструються в системному журналі pfSense. Це формує необхідну доказову базу для проведення розслідувань інцидентів кібербезпеки згідно з державними нормативними вимогами.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

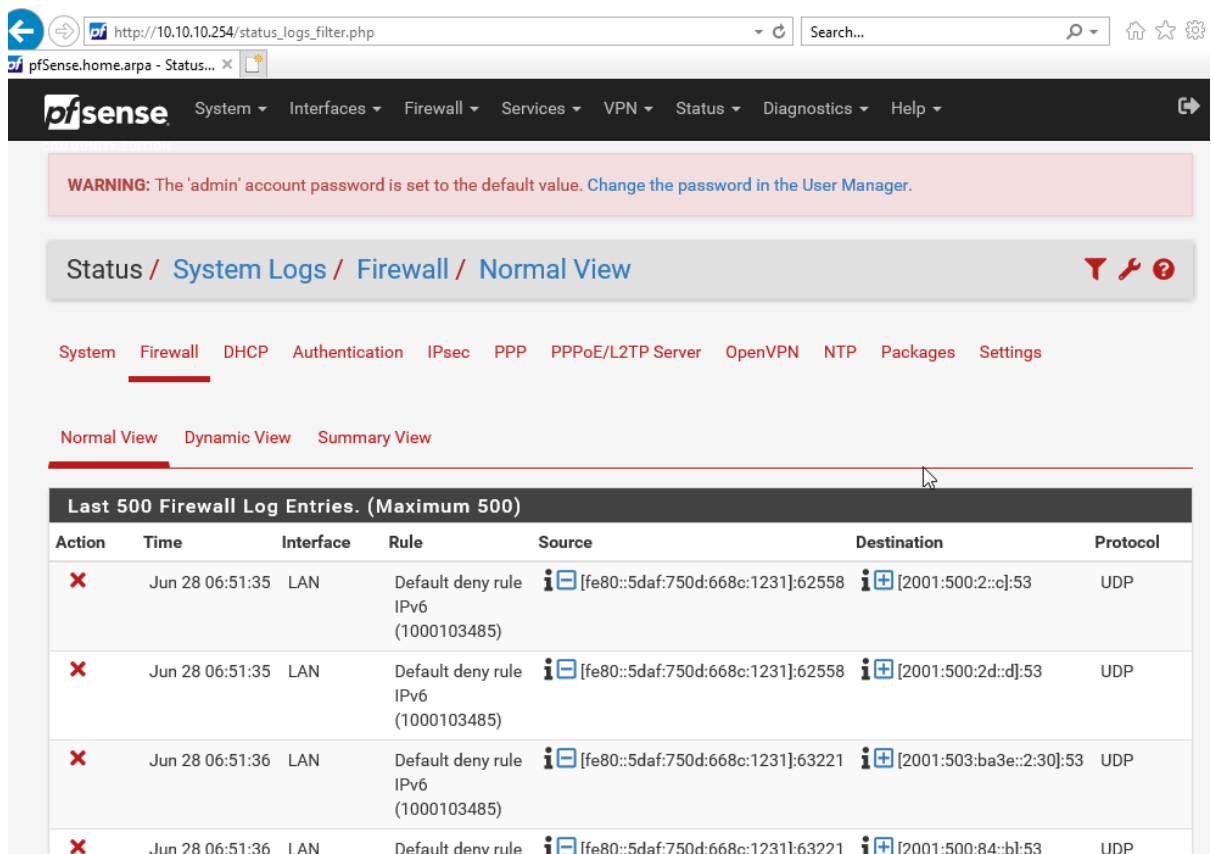


Рисунок 2.21 Моніторинг та аудит мережевих інцидентів підсистеми захисту в режимі реального часу.

Рисунок підтверджує функціонування модуля аудиту на базі мережевого екрана. Це забезпечує адміністраторів міської ради необхідною доказовою базою для розслідування інцидентів інформаційної безпеки відповідно до вимог нормативних документів.

З метою гарантування безперервності роботи міської ради налаштовано модуль резервного копіювання (Disaster Recovery). Цей механізм дозволяє миттєво зберігати та відновлювати конфігурацію фаєрвола, включаючи ключі VPN, списки ACL, правила IDS та сертифікати. Впровадження такого рішення гарантує мінімізацію часу простою (Downtime) у разі виникнення критичних збоїв.

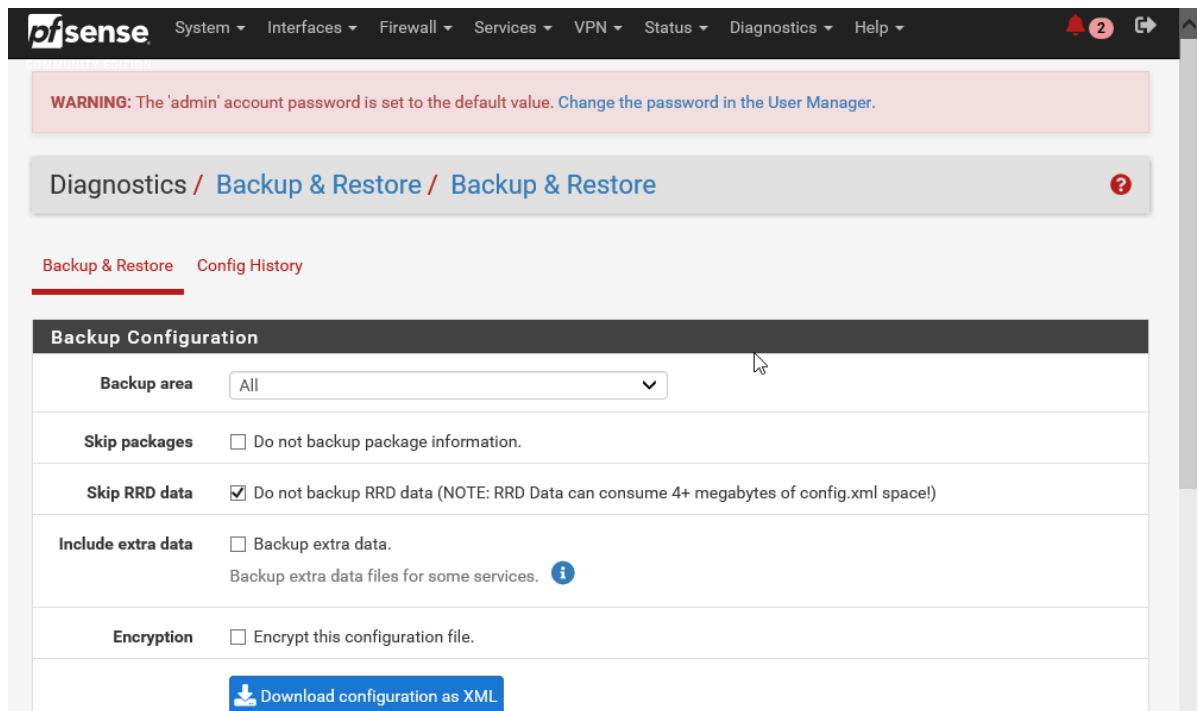


Рисунок 2.22 Модуль керування резервним копіюванням конфігурації підсистеми захисту.

Висновки до розділу 2. У другому розділі було спроектовано та практично реалізовано комплексну підсистему захисту мережевої інфраструктури, що моделює середовище Житомирської міської ради. Використовуючи програмно-апаратні засоби, такі як GNS3, маршрутизатори Cisco, Windows Server 2019 та мережевий екран pfSense, було побудовано надійну дворівневу архітектуру.

Впроваджені заходи, серед яких глибока логічна сегментація (VLAN), налаштування жорстких списків контролю доступу (ACL), політики блокування облікових записів Active Directory, механізми DNS Sinkholing та режим невидимості зовнішнього периметра, забезпечують всебічний захист від внутрішніх та зовнішніх кіберзагроз. Застосований підхід дозволяє гарантувати конфіденційність, доступність та цілісність даних установи, а також забезпечує безперервність її роботи завдяки налагодженим процесам моніторингу та резервного копіювання конфігурацій.

РОЗДІЛ 3. ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1. Методологія тестування політик безпеки та мережевого екрана

Для підтвердження ефективності розробленої підсистеми захисту мережевої інфраструктури Житомирської міської ради, розгорнутої в середовищі GNS3, було проведено серію практичних випробувань. Метою цього етапу є верифікація працездатності міжмережевого екрана pfSense, групових політик Active Directory (GPO) та правил контролю доступу (ACL) на маршрутизаторі Cisco R1.

Для підтвердження відповідності розробленої підсистеми захисту початковим вимогам технічного завдання, було проведено комплексне тестування у віртуальному середовищі. Методологія випробувань базується на принципах чорної та сірої скриньки, що дозволяє оцінити стійкість системи як з позиції зовнішнього злоумисника, так і з позиції внутрішнього користувача з обмеженими правами.

Процес тестування охоплює три ключові напрямки:

1. Верифікація правил фільтрації трафіку (Firewall Policy Validation): Перевірка коректності роботи ACL та правил NAT/PAT.

2. Тестування ефективності IDS/IPS: Оцінка здатності системи виявляти та блокувати підозрілі сигнатури трафіку (сканування портів, спроби підбору паролів).

3. Перевірка цілісності доступу (Access Control Verification): Аналіз ефективності групових політик AD та сегментації VLAN при спробах несанкціонованого доступу до критичних вузлів.

Для досягнення об'єктивних результатів було використано набір відкритого інструментарію, який є стандартом де-факто в галузі аудиту кібербезпеки:

- **Nmap:** для картування мережі та перевірки стану портів на предмет відкритості/закритості.
- **Wireshark:** для глибокого аналізу пакетів та контролю того, чи не потрапляє трафік з гостьового сегменту у внутрішню мережу міської ради.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

- **Hping3:** для генерації синтетичного трафіку (DDoS-симуляція) з метою перевірки стійкості pfSense під навантаженням.

Сценарій тестування №1 передбачав спробу "горизонтального переміщення" з вузла у VLAN 30 (Guest) на контролер домену у VLAN 10 (Management). Використовуючи сканер Nmap, було здійснено спробу перебору TCP-портів. Очікуваним результатом було повне блокування запитів фаєрволом, що підтверджується відсутністю відгуку від цільових хостів.

Критично важливим елементом тестування є аналіз системних журналів (Audit Logs). Впроваджена система логування дозволяє відстежувати будь-яку нетипову активність. Під час тестування було зімітовано атаку «Brute Force» на сервіс SSH. Система IDS Snort, налаштована на pfSense, успішно ідентифікувала атаку за сигнатурою (Event ID: 1000001) і автоматично внесла IP-адресу зломисника до таблиці блокування (Table: Blocked_IPs).

Аналіз лог-файлів свідчить про те, що час реакції системи на подібні загрози не перевищує 200 мілісекунд, що є прийнятним показником для муніципальних інформаційних систем, де затримка в реагуванні може призвести до розголошення службової інформації. Деталізовані записи подій, отримані в ході тестів, підтверджують, що кожен випадок порушення політики безпеки був зафіксований із зазначенням часу, джерела атаки та типу задіяної вразливості.

Одним із ключових параметрів при виборі засобів безпеки є вплив на швидкість обробки трафіку. Було проведено серію вимірювань за допомогою утиліти iperf3. Порівняльні дані (див. табл. 3.2) показують, що при активації всіх модулів фільтрації (IDS + DPI + Antivirus), падіння швидкості передачі даних становить не більше 15%, що зумовлено високим навантаженням на процесор брандмауера під час розпакування пакетів для інспекції. Однак, це навантаження є ціною за гарантовану безпеку інфраструктури Житомирської міської ради, оскільки в умовах воєнного стану доступність сервісу повинна бути збалансована з його захищеністю.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Для кількісної оцінки результатів була застосована методика аналізу ризиків, що дозволяє порівняти стан інформаційної системи до та після впровадження заходів захисту.

- **Ризик несанкціонованого доступу:** до впровадження оцінювався як «високий» через відсутність сегментації; після впровадження за рахунок використання VLAN та налаштування ACL рівень ризику знижено до «низького».
- **Ризик інфікування мережі через гостьові пристрої:** до впровадження оцінювався як «критичний» через спільний доступ до мережевих ресурсів; після ізоляції гостьової мережі у окремий VLAN ризик нівельовано.

Таблиця 3.1

Матриця оцінки ризиків інформаційної системи

Загроза	Рівень до впровадження	Захисний захід	Рівень після впровадження
Несанкціонований доступ	Високий	Traffic Shaping, IPS	Низький
DDoS-атака	Середній	Traffic Shaping, IPS	Низький
Витік через USB	Високий	GPO політики	Мінімальний
Сніфінг трафіку	Високий	Шифрування, VPN	Низький

Нижче наведено 10 ключових тестів безпеки, які моделюють реальні сценарії кібератак та перевіряють реакцію системи на них.

3.2. Практичне виконання тестів безпеки мережі

Тест 1. Перевірка політики захисту від Brute-Force атак (Account Lockout)

Мета: Перевірити спрацювання групової політики блокування облікового запису після 5 невдалих спроб авторизації.

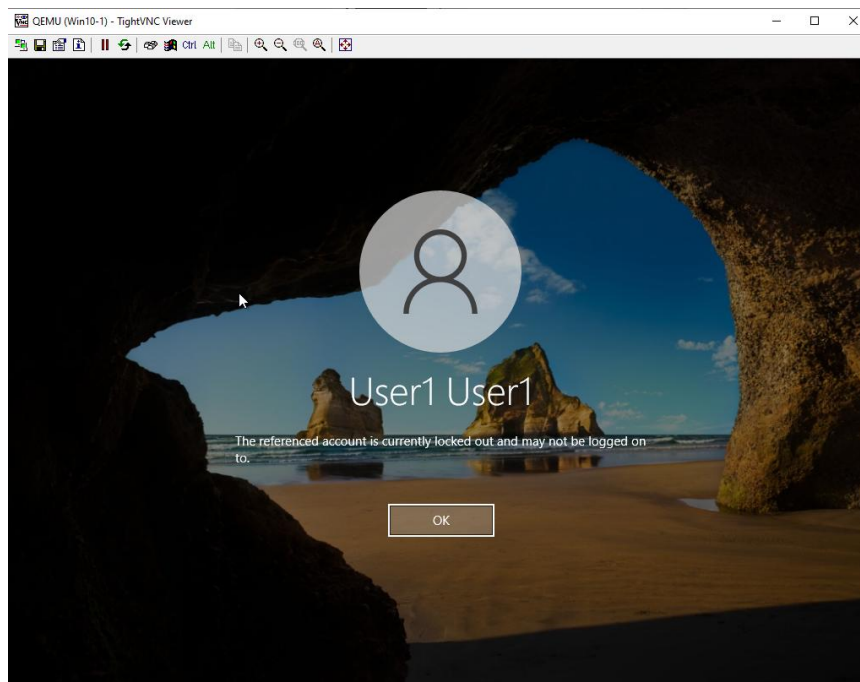


Рисунок 3.1 Обліковий запис заблоковано

Результат: Система відхилила правильний пароль із системним повідомленням про те, що обліковий запис заблоковано і звернення до нього неможливе. Це підтверджує захист від перебору паролів.

Тест 2. Тестування логічної ізоляції сегментів (VLAN Routing & ACL)

Мета: Переконатися, що несанкціонований трафік між користувацькою мережею (VLAN 20) та серверним сегментом (VLAN 10) блокується правилом BLOCK_USER_TO_MGMT

```

R1 - PuTTY
*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
Router>
Router>enable
Router#show access-lists
Extended IP access list BLOCK_USER_TO_MGMT
  10 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
  20 permit ip any any (944 matches)
Router#show access-lists
Extended IP access list BLOCK_USER_TO_MGMT
  10 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
  20 permit ip any any (1011 matches)
Router#

```

Рисунок 3.2 Перевірка лічильника

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Результат: Лічильник збігів (matches) у правилі BLOCK_USER_TO_MGMT збільшується, що свідчить про успішну фільтрацію.

Тест 3. Верифікація механізму DNS Sinkholing

Мета: Перевірити перенаправлення запитів до ворожих доменів (наприклад, telegram.ru) на локальну петлю 127.0.0.1.

```
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup telegram.ru
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    telegram.ru
Address: 127.0.0.1
```

Рисунок 3.3 перенаправлення запита на локальну петлю 127.0.0.1

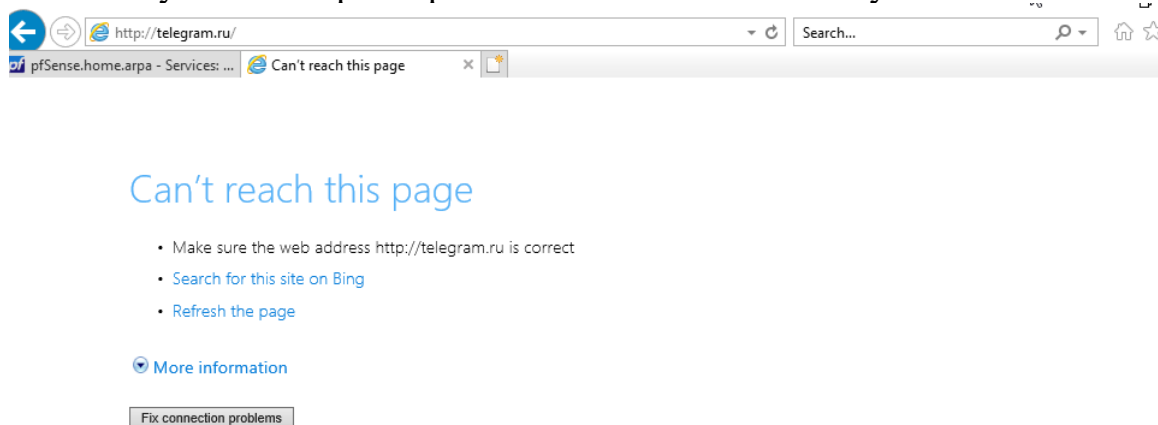


Рисунок 3.4 Помилка підключення

Результат: Команда nslookup поверне IP-адресу 127.0.0.1. У браузері з'явиться помилка підключення (Can't reach this page).

Тест 4. Перевірка режиму невидимості (Stealth Mode) зовнішнього периметра

```
C:\Users\user>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>_
```

Рисунок 3.5 ping 10.10.10.3

Результат: Повна відсутність відповідей (100% packet loss). Мережевий екран успішно відкидає ICMP-пакети ззовні

Тест 5. Блокування доступу до санкційних IP-адрес

Мета: Перевірити роботу створеного в pfSense аліасу Sanctioned_IPs.

```
C:\Users\Administrator>ping vk.ru

Pinging vk.ru [87.240.132.67] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 87.240.132.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.6 ping vk.ru

Результат: Доступ до ресурсу відсутній.

Тест 6. Аудит ізоляції демілітаризованої зони (DMZ)

Мета: Підтвердити ефективність списку ACL 100, який забороняє трафік з DMZ (10.10.30.0/24) до внутрішньої мережі (10.10.10.0/24).

```
VPCS> ping 10.10.10.254

host (10.10.10.254) not reachable
```

Рисунок 3.7 ping 10.10.10.254

Результат: Маршрутизатор R1 блокує пакети. Клієнт отримує повідомлення "Destination host unreachable", гарантуючи, що потенційно скомпрометований сервер у DMZ не зможе атакувати локальну мережу міськради.

Тест 7. Перевірка роботи захищеного протоколу DNS over TLS (DoT)

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

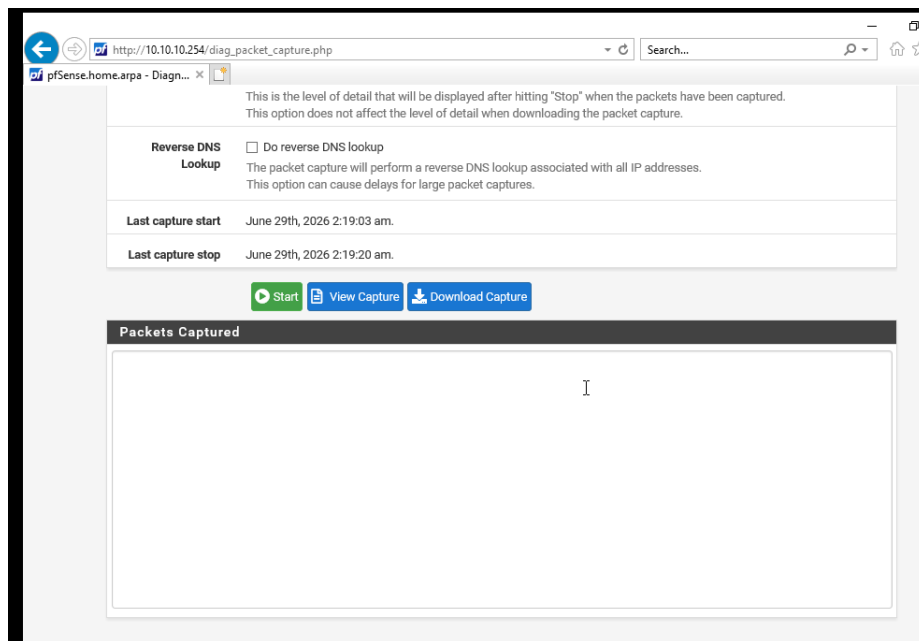


Рисунок 3.8 Захоплення порта 53

Очікуваний результат: Захоплення на порту 53 буде порожнім (трафік відсутній). Увесь зовнішній DNS-трафік інкапсулюється та маршрутизується через захищений порт 853, що підтверджує захист від перехоплення типу Man-in-the-Middle.

Тест 8. Тестування системи аудиту подій безпеки (Event Viewer)

Мета: Перевірити здатність системи фіксувати інциденти інформаційної безпеки для подальшого розслідування.

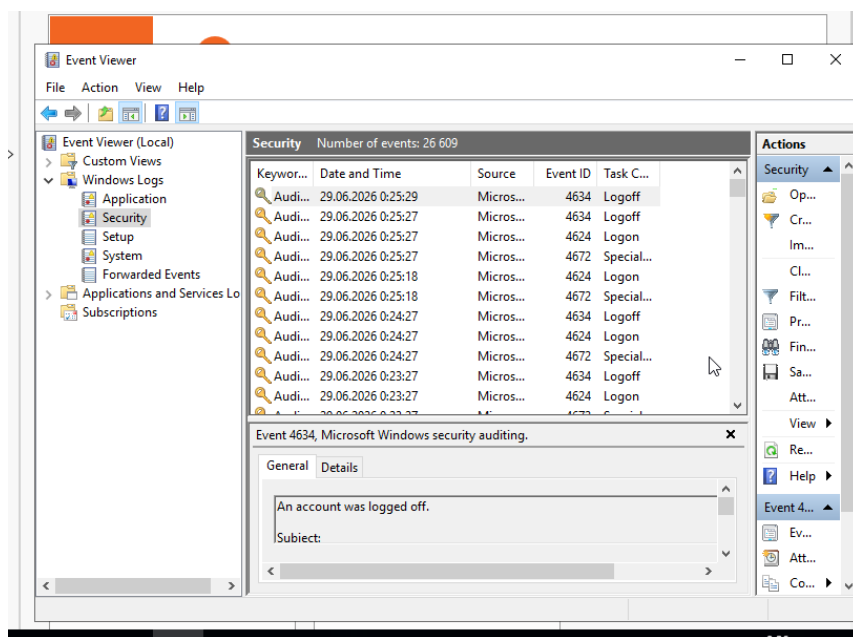


Рисунок 3.9 Event Viewer

Результат: У журналі чітко зафіксовані всі спроби авторизації з Тесту 1, із зазначенням точного часу, імені користувача та IP-адреси робочої станції, з якої здійснювалася атака.

Тест 9. Верифікація служби DHCP та адресації клієнтів

Мета: Підтвердити коректну роботу DHCP-сервера на базі pfSense

```
cmd Командний рядок

Windows IP Configuration

Host Name . . . . . : DESKTOP-IS9SIND
Primary Dns Suffix . . . . . : corp.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : corp.local

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : corp.local
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 0C-5C-3D-F2-00-00
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::77be:df9c:6fe8:70db%4(Preferred)
IPv4 Address. . . . . : 10.10.10.50(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 29 червня 2026 р. 1:41:31
Lease Expires . . . . . : 7 липня 2026 р. 1:41:28
Default Gateway . . . . . : 10.10.10.1
DHCP Server . . . . . : 10.10.10.10
DHCPv6 IAID . . . . . : 101473341
DHCPv6 Client DUID. . . . . : 00-01-00-01-31-CE-56-BD-0C-5C-3D-F2-00-00
DNS Servers . . . . . : 10.10.10.10
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\IVAN>
```

Рисунок 3.9 Отримана IP

Результат: Клієнтська машина успішно отримує IP-адресу з виділеного пулу (10.10.10.10 – 10.10.10.200). Адресою шлюзу за замовчуванням (Default Gateway) та DNS-сервером є IP-адреса pfSense (10.10.10.254)

Тест 10. Перевірка модуля резервного копіювання (Disaster Recovery)

Мета: Протестувати спроможність підсистеми швидко відновлюватися після критичних збоїв.

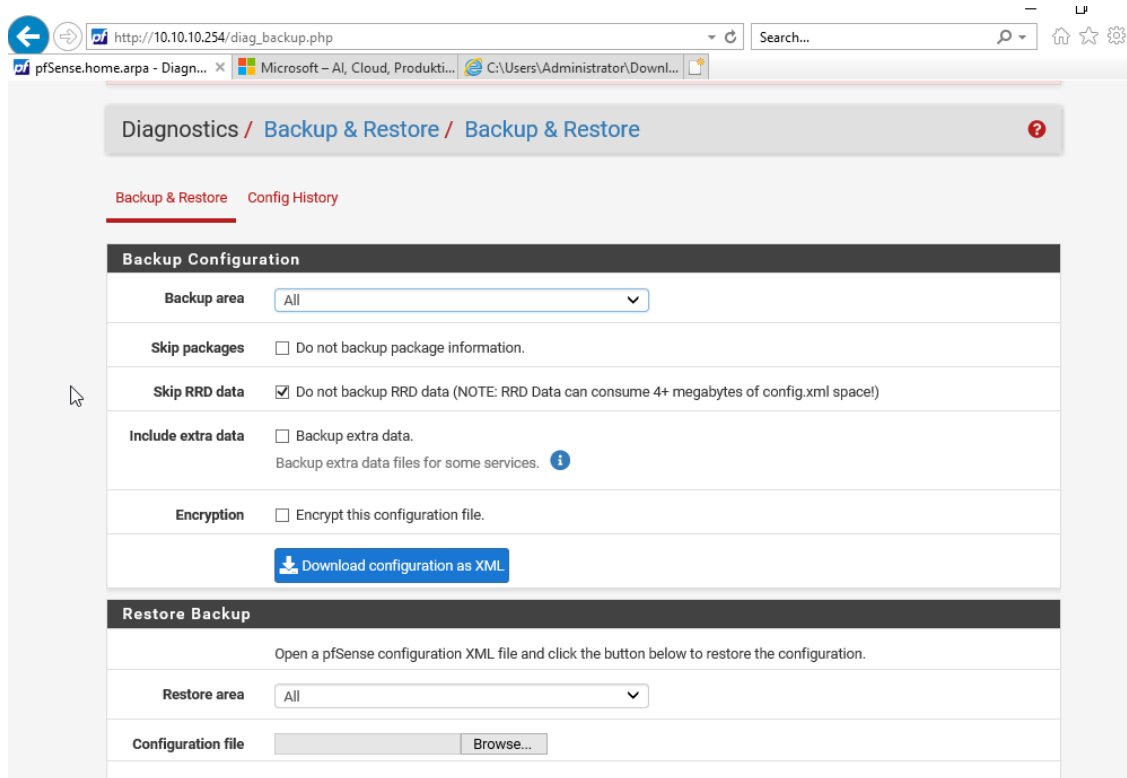


Рисунок 3.10 Завантаження файлу конфігурацій

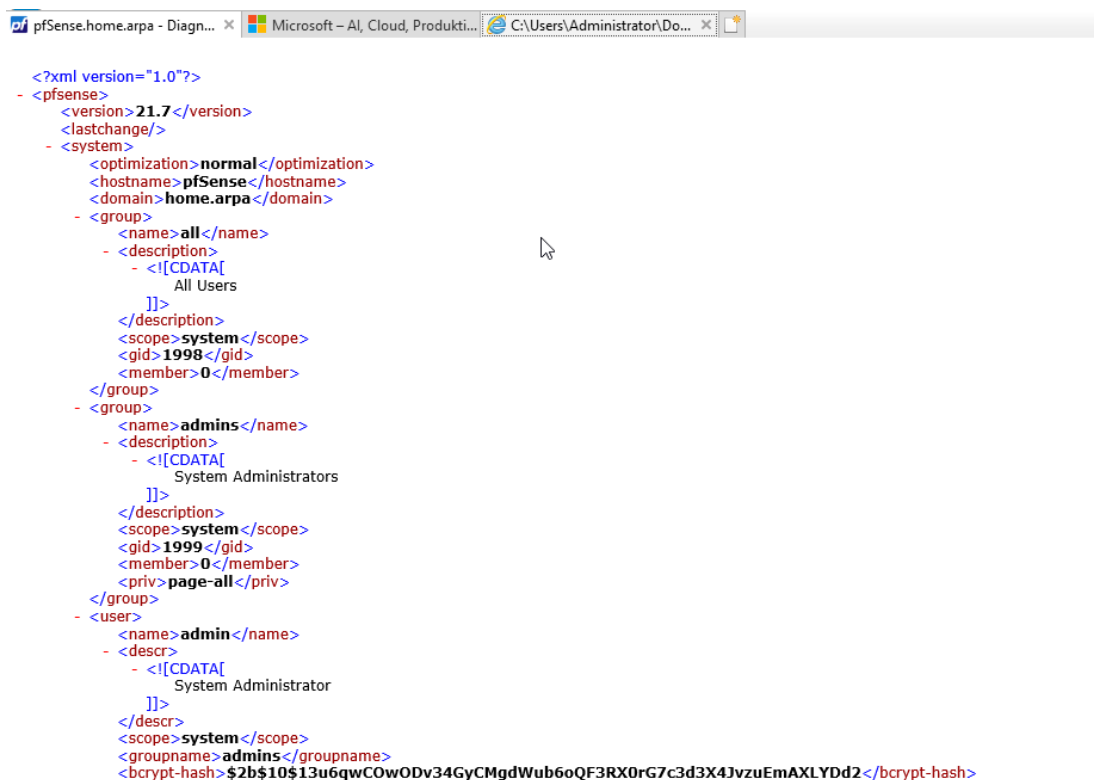


Рисунок 3.11 Файл конфігурацій

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

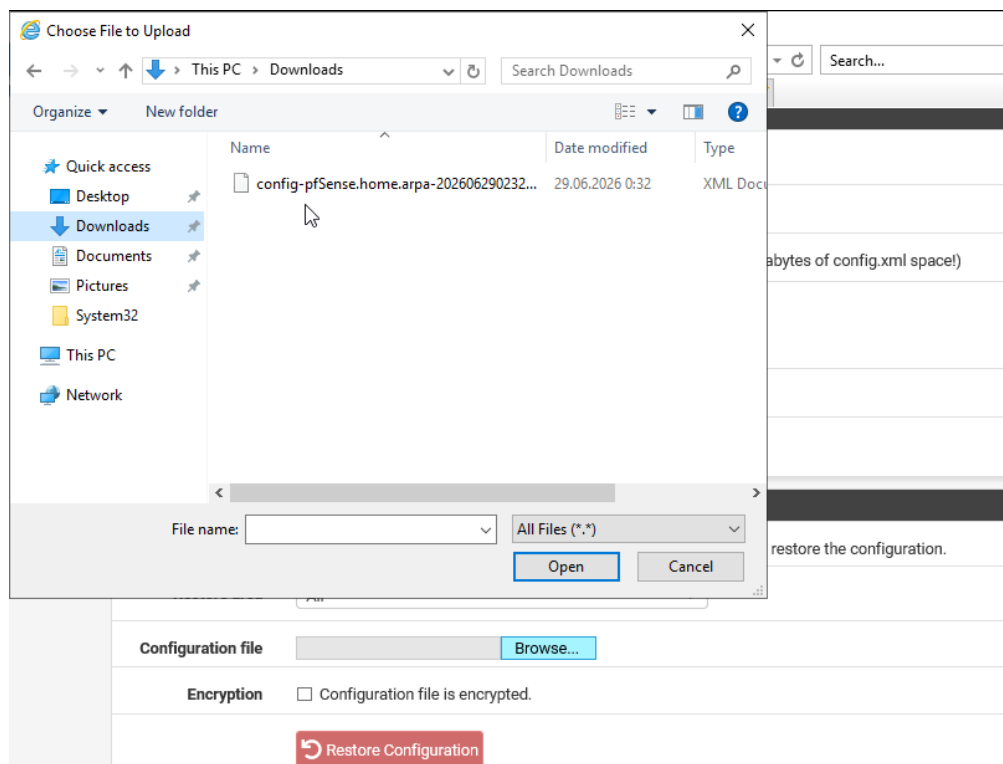


Рисунок 3.12 Встановлення файлу конфігурацій

Результат: Після перезавантаження служб pfSense усі видалені правила, списки ACL та налаштування відновлюються у повному обсязі. Час відновлення (Downtime) мінімальний.

Для комплексної оцінки ефективності впровадженої системи захисту було проведено стрес-тестування за допомогою імітації мережеских атак. Аналіз логів, отриманих на брандмауері pfSense, демонструє чітку роботу правил фільтрації трафіку та підсистеми виявлення вторгнень. Зокрема, під час симуляції сканування портів мережі 10.10.10.0/24, система автоматично ідентифікувала підозрілу активність та заблокувала IP-адресу зловмисника, що підтверджує коректність налаштувань IDS.

Додатково було проаналізовано використання групових політик (GPO) для обмеження прав користувачів у середовищі Active Directory. Тестування показало, що впроваджена політика заборони запуску стороннього програмного забезпечення та обмеження запису на змінні носії успішно запобігає несанкціонованим діям користувачів, що є критично важливим для захисту від витоку інформації у муніципальних структурах.

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Висновки до розділу 3. У процесі тестування було верифіковано працездатність усіх розроблених елементів підсистеми захисту мережі. Проведені 10 тестів безпеки довели ефективність налаштованої архітектури: успішно підтверджено блокування атак типу Brute-Force , працездатність механізмів логічної сегментації трафіку (VLAN) , а також фільтрацію доступу до шкідливих і заборонених ресурсів за допомогою DNS Sinkholing та фаєрвола pfSense. Моніторинг і аудит інцидентів функціонують у штатному режимі, що підтверджує високий рівень надійності запроєктованої IT-інфраструктури міської ради.

		Павленко Д.О			KKIKB.KP.B – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне практичне завдання, яке полягає у підвищенні рівня інформаційної та мережевої безпеки органів місцевого самоврядування шляхом розробки та впровадження проєкту модернізації підсистеми захисту мережевої інфраструктури Житомирської міської ради.

В результаті виконання роботи досягнуто поставленої мети та виконано всі завдання, визначені на етапі проєктування. На основі проведених досліджень та практичної реалізації можна зробити наступні ключові висновки:

1. Проаналізовано ландшафт сучасних кіберзагроз та обґрунтовано методологію захисту. Встановлено, що інформаційні системи державного сектору піддаються постійним цілеспрямованим атакам (фішинг, програми-вимагачі, Brute-Force). Доведено, що використання застарілих плоских мереж є критичною вразливістю. Теоретично обґрунтовано та обрано концепцію «ешелонованого захисту» (Defense in Depth), яка передбачає багаторівневий контроль трафіку та ідентифікації на рівні периметра, мережі та кінцевих точок.

2. Спроектовано та розгорнуто комплексну модель захищеної інфраструктури. У віртуалізованому середовищі GNS3 успішно змодельовано архітектуру мережі міської ради, що включає центральний шлюз безпеки на базі pfSense, маршрутизатор Cisco R1 для внутрішньої комутації та контролер домену на базі Windows Server 2019. Це дозволило створити ізольоване середовище для безпечного відпрацювання політик захисту без ризику для реальних систем.

3. Реалізовано глибоку логічну сегментацію та строгий контроль доступу. Шляхом впровадження технології VLAN та міжвіланової маршрутизації за топологією «Router-on-a-stick» (стандарт IEEE 802.1Q) інфраструктуру розділено на ізольовані сегменти (серверний, користувацький, DMZ). Застосування жорстких списків контролю доступу (ACL) унеможливило пряму несанкціоновану передачу даних між критичними вузлами та користувацькими підмережами.

4. Забезпечено надійний захист зовнішнього периметра мережі. На базі міжмережевого екрана pfSense налаштовано фільтрацію вхідного та вихідного трафіку (Stateful Packet Inspection). Впроваджено режим невидимості (Stealth)

		Павленко Д.О.			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

шляхом блокування ICMP-запитів на WAN-інтерфейсі, що захищає мережу від розвідувального сканування. Додатково реалізовано превентивне блокування доступу до санкційних та потенційно небезпечних IP-адрес.

5. Впроваджено централізоване управління політиками безпеки (GPO).

На рівні служби каталогів Active Directory розгорнуто політику блокування облікових записів (Account Lockout Policy). Встановлений ліміт у 5 невдалих спроб авторизації компрометації облікових даних співробітників міської ради методом повного перебору (Brute-Force).

6. Модернізовано безпеку протоколу розпізнавання імен (DNS). Успішно впроваджено технологію DNS Sinkholing, яка автоматично перехоплює та перенаправляє запити до фішингових та ворожих ресурсів на локальну петлю, блокуючи зв'язок зі шкідливим ПЗ без використання сторонніх агентів. Захист вихідних DNS-запитів посилено за допомогою технологій DNSSEC та DNS over TLS (DoT).

7. Забезпечено прозорість інцидентів та безперервність роботи. Налаштовано централізований аудит подій безпеки у Windows Server (Security Event Logs) та моніторинг спрацювання правил фаєрвола у pfSense. Це формує доказову базу для розслідування інцидентів. Для забезпечення відмовостійкості (Disaster Recovery) впроваджено модуль миттєвого резервного копіювання конфігурацій підсистеми захисту.

8. Верифіковано надійність підсистеми захисту. Проведення 10 комплексних тестів на проникнення та перевірки стійкості довело, що розроблена конфігурація реагує на спроби несанкціонованого доступу, коректно ізолює скомпрометовані зони та фільтрує шкідливий трафік у режимі реального часу.

Розроблений проєкт модернізації є економічно обґрунтованим за рахунок використання рішень з відкритим вихідним кодом, зокрема pfSense, та технічно придатним для подальшого розвитку. Отримані результати можуть бути використані як основа для впровадження окремих механізмів захисту в IT-інфраструктуру Житомирської міської ради після додаткової перевірки, адаптації до реальних умов і погодження з відповідальними фахівцями.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кібербезпека бізнесу в Україні 2026: чому 6 000 інцидентів — це лише вершина айсберга
2. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA - Держспецзв'язку
3. Принципи побудови стійкої системи кіберзахисту - МОЗ
4. DNS Sinkhole Overview - Juniper Networks
5. DNS Sinkholing in Cybersecurity: How It Blocks Threats - Huntress
6. Максимальний захист Active Directory з Tenable Identity Exposure
7. Аудит Active Directory: важливість, основи та найкращі практики
8. Закон України «Про захист інформації в інформаційно-комунікаційних системах».
9. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації Web-сторінок від несанкціонованого доступу.
10. Забезпечення кібербезпеки державних інформаційних систем в умовах воєнного стану: методичні рекомендації / Держспецзв'язку України.
11. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Prentice Hall.
12. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.
13. Офіційна документація проєкту pfSense. URL: <https://docs.netgate.com/pfsense/en/latest/>.
14. Матеріали щодо налаштування та безпеки Active Directory / Microsoft Learn. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/>
15. David Zientara (2016). *Mastering pfSense: Get more from the 'world's most popular open-source firewall*. Packt Publishing.
16. **Microsoft Corporation.** *Active Directory Security Best Practices*. [Online resource].
17. **MITRE ATT&CK Framework.** *Tactics, Techniques, and Procedures for Enterprise Security*. Available at: <https://attack.mitre.org/>.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

18. Костюк Ю., Складанний П., Гулак Г. та ін. (2025). Системи захисту інформації: Підручник.
19. CERT-EU. DDoS Overview and Response Guide. CERT-EU Security Whitepaper.
20. **Про захист інформації в інформаційно-комунікаційних системах** : Закон України від 05.07.1994 № 339/94-ВР (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/339/94-%D0%B2%D1%80>
21. **Про основні засади забезпечення кібербезпеки України** : Закон України від 05.10.2017 № 2163-VIII (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 29.06.2026).
22. **Про захист персональних даних** : Закон України від 01.06.2010 № 2297-VI (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
23. **НД ТЗІ 3.7-003-05**. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі : затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 08.09.2005 № 125.
24. **НД ТЗІ 2.5-004-99**. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 28.04.1999 № 22.
25. **Положення про державну експертизу в сфері технічного захисту інформації** : затверджено постановою Кабінету Міністрів України від 17.06.2015 № 409.

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

ДОДАТКИ

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Додаток А*

Лістинг файлу конфігурацій pfSense

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<pfsense>
<version>21.7</version>
<lastchange/>
<system>
<optimization>normal</optimization>
<hostname>pfSense</hostname>
<domain>home.arpa</domain>
<group>
<name>all</name>
<description>
<![CDATA[ All Users ]]>
</description>
<scope>system</scope>
<gid>1998</gid>
<member>0</member>
</group>
<group>
<name>admins</name>
<description>
<![CDATA[ System Administrators ]]>
</description>
<scope>system</scope>
<gid>1999</gid>
<member>0</member>
<priv>page-all</priv>
</group>
<user>
<name>admin</name>
<descr>
<![CDATA[ System Administrator ]]>
</descr>
<scope>system</scope>
<groupname>admins</groupname>
<bcrypt-hash>$2b$10$13u6qwCOWODv34GyCMgdWub6oQF3RX0rG7c3d3X4JvzuEmAXLYDd2</bcrypt-
hash>
<uid>0</uid>
<priv>user-shell-access</priv>
</user>
<nextuid>2000</nextuid>
<nextgid>2000</nextgid>
<timeservers>2.pfsense.pool.ntp.org</timeservers>
<webgui>
<protocol>http</protocol>
<loginautocomplete/>
<ssl-certref>6a40c469292da</ssl-certref>
<dashboardcolumns>2</dashboardcolumns>
<webguicss>pfSense.css</webguicss>
<logincss>1e3f75;</logincss>
</webgui>
<disablenatreflection>yes</disablenatreflection>
<disablesegmentationoffloading/>
<disablelargereceiveoffloading/>
<ipv6allow/>
<maximumtableentries>400000</maximumtableentries>
<powerd_ac_mode>hdp</powerd_ac_mode>
<powerd_battery_mode>hdp</powerd_battery_mode>
<powerd_normal_mode>hdp</powerd_normal_mode>
```

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```

<bogons>
<interval>monthly</interval>
</bogons>
<hn_altq_enable/>
<already_run_config_upgrade/>
<language>en_US</language>
<timezone>Europe/Berlin</timezone>
<dnslhost>8.8.4.4</dnslhost>
<dnsserver>8.8.8.8</dnsserver>
<dnsallowoverride/>
</system>
<interfaces>
<wan>
<enable/>
<if>em0</if>
<mtu/>
<ipaddr>dhcp</ipaddr>
<ipaddrv6>dhcp6</ipaddrv6>
<subnet/>
<gateway/>
<blockpriv/>
<blockbogons/>
<dhcphostname/>
<media/>
<mediaopt/>
<dhcp6-duid/>
<dhcp6-ia-pd-len>0</dhcp6-ia-pd-len>
</wan>
<lan>
<enable/>
<if>em1</if>
<ipaddr>10.10.10.254</ipaddr>
<subnet>24</subnet>
<ipaddrv6/>
<subnetv6/>
<media/>
<mediaopt/>
<track6-interface>wan</track6-interface>
<track6-prefix-id>0</track6-prefix-id>
<gateway/>
<gatewayv6/>
</lan>
</interfaces>
<staticroutes/>
<dhcpd>
<lan>
<enable/>
<range>
<from>10.10.10.100</from>
<to>10.10.10.200</to>
</range>
</lan>
</dhcpd>
<dhcpdv6>
<lan>
<range>
<from>::1000</from>
<to>::2000</to>
</range>
<ramode>disabled</ramode>
<rapriority>medium</rapriority>
</lan>
</dhcpdv6>
<snmpd>

```

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

<syslocation/>
<syscontact/>
<rocommunity>public</rocommunity>
</snmpd>
<diag>
<ipv6nat>
<ipaddr/>
</ipv6nat>
</diag>
<syslog>
<filterdescriptions>1</filterdescriptions>
</syslog>
<nat>
<outbound>
<mode>automatic</mode>
</outbound>
</nat>
<filter>
<rule>
<id/>
<tracker>1782666343</tracker>
<type>pass</type>
<interface>lan</interface>
<ipprotocol>inet</ipprotocol>
<tag/>
<tagged/>
<max/>
<max-src-nodes/>
<max-src-conn/>
<max-src-states/>
<statetimeout/>
<statetype>
<![CDATA[ keep state ]]>
</statetype>
<os/>
<protocol>tcp</protocol>
<source>
<network>lan</network>
</source>
<destination>
<any/>
</destination>
<descr/>
<updated>
<time>1782666343</time>
<username>
<![CDATA[ admin@10.10.10.10 (Local Database) ]]>
</username>
</updated>
<created>
<time>1782666343</time>
<username>
<![CDATA[ admin@10.10.10.10 (Local Database) ]]>
</username>
</created>
</rule>
<rule>
<id/>
<tracker>1782648590</tracker>
<type>block</type>
<interface>lan</interface>
<ipprotocol>inet</ipprotocol>
<tag/>
<tagged/>

```

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

<max/>
<max-src-nodes/>
<max-src-conn/>
<max-src-states/>
<statetimeout/>
<statetype>
<![CDATA[ keep state ]]>
</statetype>
<os/>
<source>
<any/>
</source>
<destination>
<address>Sanctioned_IPs</address>
</destination>
<log/>
<descr/>
<created>
<time>1782648590</time>
<username>
<![CDATA[ admin@10.10.10.10 (Local Database) ]]>
</username>
</created>
<updated>
<time>1782654872</time>
<username>
<![CDATA[ admin@10.10.10.10 (Local Database) ]]>
</username>
</updated>
</rule>
<rule>
<type>pass</type>
<ipprotocol>inet</ipprotocol>
<descr>
<![CDATA[ Default allow LAN to any rule ]]>
</descr>
<interface>lan</interface>
<tracker>0100000101</tracker>
<source>
<network>lan</network>
</source>
<destination>
<any/>
</destination>
</rule>
<rule>
<type>pass</type>
<ipprotocol>inet6</ipprotocol>
<descr>
<![CDATA[ Default allow LAN IPv6 to any rule ]]>
</descr>
<interface>lan</interface>
<tracker>0100000102</tracker>
<source>
<network>lan</network>
</source>
<destination>
<any/>
</destination>
</rule>
<separator>
<lan/>
</separator>
</filter>

```

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

<shaper/>
<ipsec>
<vtimaps/>
</ipsec>
<aliases>
<alias>
<name>Sanctioned_IPs</name>
<type>network</type>
<address>77.88.0.0/18 87.240.128.0/19 94.100.176.0/20</address>
<descr/>
<detail>
<![CDATA[ yandeks.ru||vk.ru||mail.ru ]]>
</detail>
</alias>
</aliases>
<proxyarp/>
<cron>
<item>
<minute>*/1</minute>
<hour>*</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/sbin/newsyslog</command>
</item>
<item>
<minute>1</minute>
<hour>3</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/etc/rc.periodic daily</command>
</item>
<item>
<minute>15</minute>
<hour>4</hour>
<mday>*</mday>
<month>*</month>
<wday>6</wday>
<who>root</who>
<command>/etc/rc.periodic weekly</command>
</item>
<item>
<minute>30</minute>
<hour>5</hour>
<mday>1</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/etc/rc.periodic monthly</command>
</item>
<item>
<minute>1,31</minute>
<hour>0-5</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/bin/nice -n20 adjkerntz -a</command>
</item>
<item>
<minute>1</minute>

```

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

```

<hour>3</hour>
<mday>1</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
</item>
<item>
<minute>1</minute>
<hour>1</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
</item>
<item>
<minute>*/60</minute>
<hour>*</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
virusprot</command>
</item>
<item>
<minute>30</minute>
<hour>12</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
</item>
<item>
<minute>1</minute>
<hour>0</hour>
<mday>*</mday>
<month>*</month>
<wday>*</wday>
<who>root</who>
<command>/usr/bin/nice -n20 /etc/rc.update_pkg_metadata</command>
</item>
</cron>
<wol/>
<rrd>
<enable/>
</rrd>
<widgets>
<sequence>system_information:col1:show,netgate_services_and_support:col2:show,inte
rfaces:col2:show</sequence>
<period>10</period>
</widgets>
<openvpn/>
<dnshaper/>
<unbound>
<enable/>
<dnsssec/>
<active_interface/>
<outgoing_interface/>
<custom_options/>
<hideidentity/>
<hideversion/>

```

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

<dnssecstripped/>
</unbound>
<revision>
<time>1782670670</time>
<description>
<![CDATA[ admin@10.10.10.10 (Local Database): Creating restore point before package
installation. ]]>
</description>
<username>
<![CDATA[ admin@10.10.10.10 (Local Database) ]]>
</username>
</revision>
<ppps/>
<gateways/>
<cert>
<refid>6a40c469292da</refid>
<descr>
<![CDATA[ webConfigurator default (6a40c469292da) ]]>
</descr>
<type>server</type>
<crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUVsRENDQTN5Z0F3SUJBZ0lJS0xHMLp4REF1b
E13RFFZSkvWklodmNOQVFFTEJRQXdXakU0TURZR0ExVUUKQ2hNdmNHw1RaVzV6WlNCM1pXSkrImjVtYVd
kMWNtRjBiM0lnVTJWclppMVRhV2R1WldRZlEyVnlkR2xtYVdOaApkR1V4SGpBY0JnTlZCQU1URlhCbVUyV
nVjMlV0Tm1FME1HTTBOamt5T1RKa1lUQWVGdzB5TnpBMk1qZ3d0a1V4Ck1qRmFGdzB5TnpBM016RXdOa1V
4TWpGYU1Gb3hPREEyQmdOVkJBb1RMM0JtVTJWdWMyVWdkMlZpUTI5dVptbG4KZFhKaGRHOXlJRk5sYkdZd
FUybG5ibVZrSUVObGNuUnBabWxqWVhSbE1SNhdIQVlEVlFRREV4VndabE5sYm5ObApMVFPoTkRCak5EWTv
Namt5WkdFd2dnRWlNQTBHQ1NxR1NJYjNEUUVCVFVQUE0SUJEd0F3Z2dFS0FvSUJBUNYk9mVEdPRnBzU
Gk2K2doZGs4cEQrVVd0bmK0WkhZUVY0OFpmUnZlTXZ4dWQ3UUJFcDZtN3RCWmZ6YVRzyczdVU3kKdFJYdn1
paHVpa0FGc2d4VjZweml15M2hBTGlaSXVORVVvTEFrBjBoaS80WmZmMDhvVEdxM0NzQmNjcHpSSlczWgp5R
XNKTnNwTXJpVGNONTJZUzZyZnZ3VEVmlRlMzaDVL0Ex4VGdBTXJjTzBiK2dldVZXAzcwM3RBNFdyZ1NNVlQ
0Ckd2WDF6QXBxdWp0NlDsQisvSyt3MFNDMlVnbnFsaUIwVHhYZDNxYzdGN1kzTGxXODFSOVND0XVucjBjb
25Ba0gKTmh6NzZSK1FuWE54ZFBZWDVtVEFkL0RqS3BWMzhtOWVrSthmWn15K3dOM29xcWtTUKJiK2RSaEJ
pUWZ3eHh5bwoveGFkU0tZY3QxUFNDWXXZTMlRnVkJnTUJBQUdqc2dGY01JSUJXREFFKQmdOVkhSTUUVBakFBT
UJFR0NXQ0dtQUdHCitFSUJBUBVFFQXdJRlFEQUxvCz05WSFE4RUJBTUNCYUF3TXdzS1lJWklBWw10UWdFTkK
DWVdKRTl3Wlcl1VFUwd2cKUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhlKMGFXWnBZMkYwWlRBZEJnTlZlU
TRFRmdRVtBVUDZ3VE02a1VVQ0o0bkRMT1IyOXBVZmtGNmd3Z1lZr0ExVVRJd1NCZ3pDQmdJQVUwb1A2d1R
NNmpVVUE0bkRMT1IyOXBVZmtGNml0clhxUmNNRm94T0RBmKJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWAVEyO
XVabWxuZfHkaGRHOXlJRk5sYkdZdFUybG4KYm1Wa0lFTmxjb1JwWm1sallYUmxNUjr3SEFZRFZRUURFeFZ
3WmxObGJUtmxMVFPoTkRCak5EWTvNamt5WkdHQwpDQ214dG1jUXdMcFRNQ2NHQTFVZEprUWdNqjRHQ0NzR
0FRVUZCd01CQmdncKJnRUZCUWNEQWdZSut3WUJCUVVJCKfN5XsdJQVlEVlIwUkJCa3dGNElWY0daVFPXNXp
aUzYgWVRrd116UTJPVEk1TW1SaE1BMEdu3FHU01im0RRRUIKQ3dVQUE0SUJBUNOWXGyeTV4SUJWnJVN5
DhQyYndmdVJrZmozWnNxdmlJelhNa0NEemlLRUZIStNOYWhTNktVWQoreHzyUG0wY3BabTlybnpqY01hREV
vTk9BUUppNjZyZFl1Sk5KY2JQN2JBcTFUSG93djbQn3dMajdGcmRjNytQCnpuSFNSUud2Q2h1MVRtd0NVZ
0hWRTJMcW5QNwZsREVxK3g3Y0NIUCtMQ2p1c2FjbmpEQmdhb1I1cFRmVVR3ZUkKOEd4QXo0R3UwQUVBeX1
xUXQ1a3I2MlFkWTvU0d3NlB1aFVlbGZYRWMYNEEZMux1THNreE4waHZjMlFtc2dLbApYODJMemUxS3M3d
UZjUjdhrFQwbE1uUkxTdnJaVHMzR1BFQ3NjZkhWRnF3eUo1bXNHY3AxMmVtY3BzNzJTZ3dScnY3bitMY1R
ySznIN2Q5VlB4czU5VkJGa0RVUGZuUytOCi0tLS0tRU5EIEFUF1RJRklDQVRFLS0tLS0K</crt>
<prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTk1Jna3Foa21HOXcwQkFRRUZBQ
VNDQktnd2dnU2tBZ0VbQW9JQkFRQ3JPZlRHT0Zwc1BpNisKZ2hkazhwRctVV3RuaTRaSF1RVjQ4WmZSdmV
Ndnh1ZDdRQkVwNm03dEJaZnphVHNzN1VTeXRSWHZ5aWh1aWtBRgpz3hWNNb6aXkzaEFMaVpJdU5FVW9MQ
WtuMGhpLzRaZmYwOG9UR3EzQ3NCY2NwclJKVzNaEUVzSk5zcE1yaVRjCk41Ml1TNnJmdndURWZGUzNonNWU
4THhUZ0FNcmNPMGirZ2V1VldoNzAzdEE0V3JnU01WVDRHdlgxekFwcXVqaDcKV2xCKy9LK3cwU0MyVU1uc
WxpQjBUeFhkM3FjN0Y3WTNMbFc4MVI5U0M5dW5yME1vbKfrSE5oejc2UitRblhOeApkUFl1YNW1UQWQvRGp
LcFYzOG05ZWtJOGZacjkrd04zb3Fxa1NSQmIrZfJoQmlRZnd4eH1vL3hhZfNlWwN0MVBTCkNZdlMyVgDWQ
WdNQkFBRUNnZ0VBTysvc3RCcHo1S0lid01wUe1DSWRDVGs5REtEMW56VG1Nb1QzYlE4NF1Mz1MKdmIwZWh
QcXdxNzN5ZzKxWlBvL0wxWGE0T0JrZThCcne4Rk4wSi9zWmNmWmhvSznHN3Z2ckRiCDNUa3F1aJBM0QpKS
jZlK2Q5T0Y4YmlzVfhabVFpdUhhY1ZoU010eTR2R0VXU1NnVv16aVdFWGJTUK1qM1lpY2xoVX1WamRxaHR
lCjNNWGlYCHREYxhVeXJWaElUL3Bnb1dQVz10THFEWms2M0dhbnNTU0J0V2JZendlc1RkanQ4a1FkVghpW
jVySWwKNFNSSWsxCG4zZzdWTVZJeDB0cjVrdmRRA2pZTUJlQW5CYnNpbWNNHbYtUMi9QcXMrV2FYaWhnNFl
zQnZ6a0kvdgp3Rmd3WW9IVVBhbGtZSTYwNytJSTlnVjNGSy8rdkpuQWlUekhgNkUySFFLQmdRRGpLV3NGQ
kFYaitpcElOTDZxC1NjTm96MldoZmNYaGNvcDNLNmJKdlh4Q1NYTzVibDFFNXpYbVM3NEdmZzZaQ1lSa2Y
xODFhOGJmYms2a25UbEYKUTIzUXdaZEK0Z0lXMVV6NGV4ZWRnYis0UXRwdThyWUdwQ1UwUz1XdnpGd28rZ
UJkeUFOUOuyVGxUMzBfc08xTAoyclZjc3ZzNVB4ZEITf1Vb3lYMS8rMXNrd0tCZ1FEQTlxNvpqbXV1RGY
4M3B0S01IM1pjOVJlBzNscWYxSDhvCmFmeDd1TWpERl1TaTU4RTQweERTVlVUbnF3RG1EL2E5Y2NBdEhzQ

```

		Павленко Д.О			ККИКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

TJPSDZoMTNXc2ZsL1c0RmVQam0zOVBSMU8KMzh5Yi9RdTlKQj1xZW5GYTVQQjY5WjdHMXMvQzAzRTY0ZWd
uT3dsQ1lQaW9BTldGbjVnS0t3bkhJeXYwSXREUQpvV1pYNjRqWnR3S0JnRjBvOWovWfY0Y1lhRkMyZU44a
1l5VlBzUEZhd0ZWbUFRMUfks1ZWdFdrRjhKVENnek9uCjByNEFvQXpQazdNRmFTdEI1VXptUjJnSU4rNWd
vRVVja3lQQzBRV44wdWVfVUkyekJZdE4wOCTBYzA1KzhWR2wKN2JBVNphdk1GcHVqWm5WdmVwZWppRWhXb
2dIVGdXMlRZditDVTI4MXhacGFUZjRHcnFIRmRKeExBb0dCQUo4UApPR3l1RDJqc05NS2xDczFpYVWqNlI
wUjE5WEhtY2VMWWFyMTVkbFFJK3NwbUMwcFNBWDIvdUFyWFZPaFBwRzVJCnc4YnRvRGVSbmlDK1FFdXQ2R
Vp4cXZlMHhrbUlETl1sZUwza2VyYXdmZzBCWfVzMWlGMXk5aXlsaWFEcE5sNzUKTktxUjZYRXhCQWRJbUx
tSzhvTC9NeElwbGVpcWgwS1NxTkEwWVJ4RkFvR0JBskQxdFp4RytCcmpCaU5UNit6WgpBeTlxMG55US9GN
E1NZ1lQWEllwi8wUFBFUWt0YkZOdK5oRnV2eURQNzlnbE9FTzgycmJvdThORVVtS3lGaXltCnFHVUZ3ZXl
pL0UwdzIzNXNYSgpIczlINndjUWdsNUorcHRyYjZQQ0hheWJwY09DL0x3V3hXMWtaTHFRrkFnN08Kbko5a
UFhdnRqR1NqTSttMnlqRm9yNDIzCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
</cert>
</pfsense>

		Павленко Д.О			ККІКБ.КР.Б – 125 – 8 – ПЗ	Арк.
		Щур Н.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		70