ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ПІДСИСТЕМА КЕРУВАННЯ ПРАВАМИ ДОСТУПУ ДО ДАНИХ У ВІРТУАЛІЗОВАНЕ СЕРЕДОВИЩЕ НА ПЛАТФОРМІ PROXMOX»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Ілля ШКОЛЬНИЙ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КСДМ-62
Ілля ШКОЛЬНИЙ
Ім'я, ПРІЗВИЩЕ
Керівник: Людмила АСЄЄВА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ

«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Школьний Ілля Михайлович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Підсистема керування правами доступу до даних у віртуалізоване середовище на платформі Proxmox
керівник кваліфікаційної роботи Людмила АСЄЄВА,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10 2025р. № 467
2. Строк подання кваліфікаційної роботи «_____» _____ 2025р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, методи системного аналізу, порівняльного аналізу програмно-апаратних засобів, методи віртуалізації та експериментального моделювання мережевих процесів.
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Базові теоретичні аспекти регулювання доступу до інформаційних ресурсів
2. Практична реалізація та архітектурне проєктування інфраструктури ad rms у корпоративному сегменті мережі
3. Практична реалізація проєкту та верифікація системи захисту інформації
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «_____» _____ 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.09-24.10.2025	Виконано
2	Обробка матеріалу	25.10-05.11.2025	Виконано
3	Розробка теоретичної частини	06.11-10.11.2025	Виконано
4	Розробка підсистеми	11.11-15.11.2025	Виконано
5	Висновки за результатами аналізу	15.11-19.11.2025	Виконано
6	Оформлення пояснювальної записки	19.11-21.11.2025	Виконано
7	Розробка презентації	21.11-29.11.2025	Виконано
8	Передзахист	01.12-02.12.2025	Виконано
9	Здача в деканат	15.12-18.12.2025	Виконано

Здобувач вищої освіти _____ Ілля ШКОЛЬНИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Людмила АСЄЄВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 68 стор., 7 рис., 18 джерел.

Мета дослідження – підвищення рівня інформаційної безпеки корпоративної мережі шляхом проєктування та імплементації системи управління цифровими правами AD RMS у віртуальному середовищі Proxmox VE.

Об'єкт дослідження – архітектура, методи розгортання та налаштування служби Active Directory Rights Management Services та засобів віртуалізації.

Предмет дослідження – архітектурні рішення, програмно-апаратні засоби та політики безпеки для побудови корпоративної мережі на базі технологій Cisco та Microsoft.

Короткий зміст роботи: У кваліфікаційній роботі проведено аналіз теоретичних основ управління доступом, розглянуто моделі DAC, MAC, RBAC та ABAC. Обґрунтовано вибір програмного забезпечення для віртуалізації, надано перевагу гіпервізору KVM у складі Proxmox VE. Спроєктовано мережеву топологію та розраховано необхідні апаратні ресурси. Виконано практичне розгортання служби каталогів Active Directory, налаштовано сервери інфраструктури та систему резервного копіювання Proxmox Backup Server. Реалізовано захист даних за допомогою AD RMS, створено спеціалізовані шаблони політик прав та проведено тестування обмежень функціональності на клієнтських місцях.

Результати: Побудовано відмовостійку систему, яка забезпечує персистентний захист документів. Реалізовано механізми суворої аутентифікації та авторизації, що унеможливлюють несанкціонований доступ до даних навіть при їх витоку за межі організації..

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, ACTIVE DIRECTORY, AD RMS, PROXMOX VE, ВІРТУАЛІЗАЦІЯ, КОНТРОЛЬ ДОСТУПУ, ПОЛІТИКИ ПРАВ, ШИФРУВАННЯ, РЕЗЕРВНЕ КОПІЮВАННЯ.

ABSTRACT

Textual part of the Master's qualification paper: 68 pages, 7 figures, 18 references.

The purpose of the research is to increase the level of information security in a corporate network by designing and implementing the AD RMS digital rights management system within the Proxmox VE virtual environment.

The object of the research is the architecture, deployment methods, and configuration of the Active Directory Rights Management Services (AD RMS) and virtualization tools.

The subject of the research is the architectural solutions, software and hardware tools, and security policies for building a corporate network based on Cisco and Microsoft technologies.

Summary of the work: The qualification paper analyzes the theoretical foundations of access control and examines the DAC, MAC, RBAC, and ABAC models. The choice of virtualization software is substantiated, with preference given to the KVM hypervisor within Proxmox VE. The network topology is designed, and the necessary hardware resources are calculated. Practical deployment of the Active Directory service is performed, and infrastructure servers and the Proxmox Backup Server system are configured. Data protection using AD RMS is implemented, specialized rights policy templates are created, and functionality restrictions are tested on client workstations.

Results: A fault-tolerant system has been built that ensures persistent document protection. Strict authentication and authorization mechanisms have been implemented, preventing unauthorized access to data even if it leaks outside the organization.

KEYWORDS: INFORMATION SECURITY, ACTIVE DIRECTORY, AD RMS, PROXMOX VE, VIRTUALIZATION, ACCESS CONTROL, RIGHTS POLICIES, ENCRYPTION, BACKUP.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Школьний І. М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)
на тему: «Підсистема керування правами доступу до даних у віртуалізоване середовище на платформі Proxmox».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Школьний І. М. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Школьний Ілля Михайлович на оцінку «відмінно», та присвоїти їй кваліфікацію «магістр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Людмила АСЄЄВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«_» _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Школьний І. М.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Школьний Ілля Михайлович
(прізвище, ім'я, по батькові)
на тему: «Підсистема керування правами доступу до даних у віртуалізоване середовище на платформі Proxmox»

Актуальність:

Кваліфікаційна магістерська робота присвячена вирішенню одного з найгостріших питань сучасної кібербезпеки — захисту корпоративних даних від внутрішніх загроз та витоків. В умовах розмивання мережевого периметра класичні засоби захисту стають недостатніми. Робота пропонує комплексний підхід до впровадження системи Active Directory Rights Management Services (AD RMS), яка забезпечує захист інформації на рівні самого файлу. Такий підхід дозволяє організації контролювати використання інтелектуальної власності незалежно від місця її знаходження, що є критично важливим для сучасного бізнесу.

Позитивні сторони:
1. Робота відзначається глибоким аналізом теоретичної бази: детально розглянуто складові IT-інфраструктури, моделі хмарних обчислень та широкий спектр мережевих загроз.
2. У роботі детально опрацьовано практичну частину: від розрахунку апаратних ресурсів до створення специфічних шаблонів політик прав. Реалізація технічних обмежень, таких як блокування PrintScreen та буфера обміну, свідчить про глибоке розуміння можливостей технології.
3. Важливим елементом роботи є інтеграція системи резервного копіювання Proxmox Backup Server, що забезпечує цілісність та доступність інфраструктури управління правами, роблячи систему стійкою до збоїв.

Недоліки:
1. У практичній реалізації для захисту каналів зв'язку було використано самопідписаний сертифікат, що є прийнятним для тестового середовища, але в реальних виробничих умовах великого підприємства вимагало б розгортання повноцінної інфраструктури відкритих ключів з довіреним кореневим центром, про що варто було б зазначити детальніше.
2. Робота зосереджена переважно на клієнтах ОС Windows. Було б доцільно розглянути можливості розширення доступу до захищеного контенту для мобільних пристроїв за допомогою додаткових розширень, враховуючи сучасні тенденції BYOD.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку "відмінно", а здобувач Школьний І. М. заслуговує присвоєння кваліфікації: магістр з комп'ютерної інженерії.*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП.....10
1 БАЗОВІ ТЕОРЕТИЧНІ АСПЕКТИ РЕГУЛЮВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ.....12
1.1 Ключові концепції та засади розмежування доступу до даних.....12
1.2 Інструментарій та методики забезпечення інформаційної безпеки в корпоративному секторі.....16
1.3 Архітектурні принципи функціонування Active Directory як базової складової екосистеми інформаційної безпеки.....18
1.4 Функціональні можливості та архітектура системи управління правами AD RMS.....22
1.5 Архітектурні особливості та функціональне призначення платформи Proxmox Backup Server у системі забезпечення доступності даних.....24
2 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АРХІТЕКТУРНЕ ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ AD RMS У КОРПОРАТИВНОМУ СЕГМЕНТІ МЕРЕЖІ..28
2.1 Дослідження передумов та формування технічного завдання на розгортання системи захисту.....28
2.2 Порівняльний аналіз платформ управління ідентифікацією та аргументація вибору технологічного стеку.....31
2.3 Обґрунтування вибору платформи віртуалізації та системного програмного забезпечення.....34
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ПРОЄКТУ ТА ВЕРИФІКАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.....48
3.1 Інсталяція платформи віртуалізації та базове налаштування хост-системи 48
3.2 Реалізація доменної структури та конфігурація служби каталогів.....53
3.3 Підготовчі заходи та конфігурація службових компонентів для розгортання AD RMS.....57

ВИСНОВКИ.....63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....65
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....68

ВСТУП

У сучасному цифровому просторі інформація є одним із найцінніших активів будь-якої організації, а її захист стає критично важливим завданням. Зростання обсягів корпоративних даних, розширення периметра мереж та необхідність віддаленої роботи створюють нові виклики для систем безпеки. Традиційні методи захисту, такі як міжмережеві екрани, вже не можуть гарантувати безпеку даних після того, як вони залишають захищений периметр компанії. Втрата контролю над конфіденційною інформацією може призвести до значних фінансових та репутаційних збитків.

Це зумовлює необхідність переходу до більш досконалих моделей управління доступом, які забезпечують захист безпосередньо самого контенту, незалежно від місця його зберігання. Впровадження технологій управління цифровими правами (Rights Management Services) дозволяє реалізувати персистентний захист, де політики доступу невіддільні від файлів. Використання таких систем у поєднанні з сучасними платформами віртуалізації дозволяє створити гнучку, масштабовану та відмовостійку інфраструктуру безпеки.

Мета і завдання дослідження. Метою роботи є підвищення рівня захищеності корпоративних інформаційних ресурсів шляхом розробки та впровадження системи управління правами доступу AD RMS у віртуалізованому середовищі.

Для досягнення мети поставлені наступні завдання:

1. Проаналізувати базові теоретичні аспекти та моделі розмежування доступу до інформаційних ресурсів.
2. Дослідити архітектурні принципи функціонування Active Directory та технології AD RMS як інструментів забезпечення безпеки.
3. Обґрунтувати вибір платформи віртуалізації (Proxmox VE) та спроєктувати архітектуру мережі з урахуванням вимог до відмовостійкості.

4. Виконати розгортання доменної інфраструктури та базових сервісів.

5. Реалізувати систему захисту AD RMS, налаштувати шаблони політик прав для різних департаментів та забезпечити обмеження функціоналу.

6. Провести верифікацію системи захисту та перевірити ефективність застосованих політик на клієнтських робочих станціях.

Об’єкт дослідження – процеси управління доступом та захисту інформації в корпоративних комп'ютерних системах.

Предмет дослідження – методи та засоби реалізації системи управління цифровими правами (AD RMS) на базі технологій віртуалізації.

Методи дослідження. У роботі використано методи системного аналізу, порівняльного аналізу програмно-апаратних засобів, методи віртуалізації та експериментального моделювання мережевих процесів.

Практичне значення. Розроблена система дозволяє гарантувати конфіденційність даних навіть за межами корпоративної мережі, мінімізувати ризики інсайдерських загроз та забезпечити автоматизоване управління доступом на основі рольової моделі.

1 БАЗОВІ ТЕОРЕТИЧНІ АСПЕКТИ РЕГУЛЮВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Ключові концепції та засади розмежування доступу до даних

Питання управління доступом до інформаційних активів залишається і в майбутньому залишатиметься наріжним каменем функціонування сучасних інформаційних систем. Головна мета цього процесу полягає у забезпеченні надійного захисту конфіденційних відомостей, а також у здійсненні суворого контролю за їх використанням та поширенням. Лише коректно побудована система розмежування доступу здатна виступати гарантом дотримання тріади інформаційної безпеки, забезпечуючи цілісність, конфіденційність та доступність даних для легітимних користувачів.

Саме поняття управління доступом окреслює коло суб'єктів та методи їхньої взаємодії з конкретними масивами інформації. У цій предметній області ключову роль відіграють кілька фундаментальних процесів. Першим із них є ідентифікація, під якою слід розуміти процедуру розпізнавання особи або суб'єкта, що ініціює запит на доступ до системи чи ресурсу. Наступним кроком виступає аутентифікація, яка полягає у перевірці справжності наданих ідентифікаційних даних, таких як паролі, цифрові сертифікати або біометричні показники. Після успішного проходження цих етапів відбувається авторизація, що визначає обсяг прав та привілеїв, наданих користувачеві або системі для роботи з конкретним об'єктом. Завершує цей ланцюжок безпосередньо контроль доступу — процес, що забезпечує неухильне дотримання політик безпеки, які регламентують, хто саме і яким чином може використовувати наявні ресурси.

Для побудови надійної архітектури доступу фахівці рекомендують спиратися на принцип найменших привілеїв (Least Privilege). Суть цього

підходу полягає у наданні користувачам мінімально необхідного обсягу прав, достатнього виключно для виконання їхніх безпосередніх службових обов'язків, що суттєво знижує ймовірність зловживань. Не менш важливим є принцип розподілу обов’язків (Separation of Duties), який вимагає, щоб критично важливі операції не зосереджувалися в руках однієї особи, а розподілялися між кількома співробітниками задля мінімізації ризиків шахрайства чи людських помилок. Загальновизнаною ефективною практикою є також застосування контролю на основі ролей, коли права доступу надаються не персонально, а відповідно до функціональної ролі працівника в організації. Окрім того, невід'ємною складовою системи безпеки є постійний аудит та моніторинг, що передбачає безперервне логування дій користувачів для своєчасного виявлення аномалій, помилок або спроб порушення встановлених правил.

Враховуючи особливості технічної реалізації, у теорії та практиці виокремлюють кілька базових моделей розмежування доступу, серед яких основними є дискреційна, мандатна та рольова моделі, а також контроль на основі атрибутів.

Дискреційний контроль доступу (Discretionary Access Control, DAC) базується на концепції, згідно з якою власник ресурсу має повноваження самостійно визначати, хто і з якими правами отримує доступ до об'єкта. Технічно це часто реалізується через списки контролю доступу (ACL), де прописані дозволи для кожного користувача. Хоча такий підхід є прийнятним для невеликих систем або персонального використання, його суттєвим недоліком є знижений рівень безпеки, оскільки користувачі через недбалість або помилку можуть надати доступ стороннім особам. Ця модель широко застосовується в операційних системах сімейства Windows та Unix, де власник файлу може самостійно встановити атрибути читання, запису чи виконання.

На противагу попередній моделі, мандатний контроль доступу (Mandatory Access Control, MAC) передбачає жорстку централізацію управління правами, де політики безпеки формуються виключно

адміністраторами системи. В основі цього підходу лежить використання міток конфіденційності (наприклад, грифи «Таємно» чи «Конфіденційно»). Система автоматично порівнює рівень допуску користувача з рівнем секретності ресурсу, приймаючи рішення про надання доступу. Це значно підвищує захищеність даних, оскільки звичайні користувачі позбавлені можливості змінювати налаштування безпеки, проте впровадження та адміністрування такої системи є складним процесом. Сферою застосування MAC зазвичай є військові та урядові структури, а яскравим прикладом реалізації є система SELinux.

Більш сучасною та адаптивною вважається модель контролю доступу на основі атрибутів (Attribute-Based Access Control, ABAC). У цьому випадку рішення про допуск приймається динамічно, базуючись на аналізі сукупності атрибутів суб'єкта (посада, відділ), об'єкта (тип файлу, власник), дії (читання, модифікація) та середовища (час доби, геолокація, тип пристрою). Логічні правила, встановлені адміністраторами, дозволяють гнучко керувати доступом у складних розподілених системах, таких як хмарні платформи AWS чи Microsoft Azure. Попри високу гнучкість, недоліком ABAC є складність первинного налаштування та підвищені вимоги до обчислювальних потужностей.

Широкого розповсюдження в корпоративному секторі набув контроль доступу на основі ролей (Role-Based Access Control, RBAC). Ця модель оперує не окремими обліковими записами, а рольовими групами (наприклад, «Бухгалтер», «Адміністратор», «Аналітик»). Кожній ролі присвоюється набір дозволених операцій, і користувач автоматично отримує відповідні права при призначенні йому певної ролі. Це значно спрощує адміністрування у великих колективах: зміна прав для однієї ролі миттєво оновлює дозволи для сотень співробітників, що зменшує ризик помилок. Хоча RBAC може поступатися гнучкістю атрибутивній моделі при виникненні нетипових сценаріїв, його прозорість робить його стандартом для таких систем, як Active Directory.

Для наочного відображення характеристик розглянутих моделей та їх порівняння, узагальнену інформацію доцільно систематизувати у вигляді таблиці, табл.1.1. [3]

Таблиця 1.1. Порівняльний аналіз ключових моделей розмежування доступу до інформаційних ресурсів

Критерій оцінки	DAC (Дискреційна)	MAC (Мандатна)	ABAC (На основі атрибутів)	RBAC (Рольова)
Гнучкість налаштування	Високий рівень	Обмежена (низька)	Максимальна (дуже висока)	Помірна (середня)
Рівень захищеності	Базовий (середній)	Максимальний (високий)	Високий	Високий
Складність адміністрування	Низька (спрощене управління)	Висока (потребує значних ресурсів)	Висока (складне налаштування політик)	Низька (спрощене завдяки ролям)
Наявність централізації	Відсутня (децентралізована модель)	Присутня (повний контроль)	Присутня	Присутня
Типові сфери впровадження	Невеликі локальні мережі, персональне використання	Режимні об'єкти, військові та урядові системи з високим рівнем секретності	Хмарні інфраструктури, складні розподілені корпоративні мережі	Комерційні структури, бізнес-системи, середовища Active Directory

1.2 Інструментарій та методики забезпечення інформаційної безпеки в корпоративному секторі

Система захисту інформаційних активів у межах корпоративного середовища являє собою складний комплекс різнопланових засобів, методик та програмно-апаратних інструментів. Їхня спільна мета полягає у забезпеченні фундаментальної тріади інформаційної безпеки: конфіденційності, цілісності та доступності даних, якими оперує організація та її користувачі. У сучасній практиці виокремлюють низку ключових напрямів реалізації захисту, серед яких центральне місце посідають криптографічні методи, системи управління доступом, механізми захисту кінцевих точок, технології запобігання витокам даних, а також стратегії резервного копіювання, нормативне регулювання через політики безпеки та підвищення кваліфікації персоналу.

Криптографія виступає фундаментом безпеки, охоплюючи процеси шифрування даних як у стані спокою на фізичних носіях, так і під час їх передачі каналами зв'язку. Важливим елементом є використання цифрових підписів, які дозволяють не лише аутентифікувати користувачів, але й гарантувати незмінність даних. Яскравим прикладом практичного застосування криптографії є використання протоколів транспортного рівня, таких як SSL (Secure Sockets Layer) та його більш сучасної версії TLS (Transport Layer Security). Ці протоколи створюють захищений тунель для обміну інформацією між клієнтськими додатками, наприклад веб-браузерами, та серверами, гарантуючи при цьому, що дані залишаться конфіденційними, цілісними та автентичними.

Алгоритм роботи протоколів SSL/TLS базується на послідовності чітко визначених етапів. Процес розпочинається з аутентифікації, під час якої сервер підтверджує свою справжність, надаючи клієнту цифровий сертифікат. Цей документ містить публічний ключ і засвідчений підписом довіреного центру

сертифікації, що дозволяє клієнту переконатися у легітимності сервера та уникнути атак типу «людина посередині» (man-in-the-middle). Після успішної перевірки сторони переходять до етапу узгодження шифрування. Клієнт і сервер генерують спільний сеансовий ключ, який надалі використовується для симетричного шифрування потоку даних. Вибір саме симетричного алгоритму для передачі інформації зумовлений його вищою швидкодією порівняно з асиметричними методами, які використовуються переважно на етапі встановлення з'єднання. Окрім конфіденційності, SSL/TLS гарантують цілісність повідомлень шляхом застосування хеш-функцій, які дозволяють виявити будь-які несанкціоновані зміни в пакеті даних під час його транзиту мережею.

Наступним критично важливим ешелоном оборони є засоби управління доступом, які регламентують права користувачів щодо використання ресурсів мережі. У середовищі Windows ці функції реалізуються через інтегрований комплекс технологій. Основою виступає служба каталогів Active Directory, що забезпечує централізоване адміністрування облікових записів. Для спрощення керування правами застосовується модель рольового доступу (RBAC), де дозволи прив'язуються до функціональних обов'язків працівника, а не до його особистості, що суттєво знижує навантаження на адміністраторів. Додатковий рівень захисту створює багатофакторна аутентифікація (MFA), яка вимагає від користувача підтвердження особи кількома незалежними способами, наприклад, паролем та біометрією. Окремої уваги заслуговує технологія Active Directory Rights Management Services (AD RMS), яка дозволяє захищати самі документи та електронні листи, визначаючи права на їх перегляд, редагування чи пересилання навіть за межами корпоративної мережі.

Захист кінцевих пристроїв передбачає використання спеціалізованого програмного забезпечення. Сюди входять класичні антивірусні сканери для боротьби зі шкідливим кодом, персональні брандмауери для фільтрації трафіку, а також системи управління мобільними пристроями (MDM), що дозволяють контролювати безпеку смартфонів і планшетів співробітників. Для

виявлення складних загроз застосовуються системи виявлення вторгнень, а також комплексні рішення класу EDR та XDR, які забезпечують розширений моніторинг та реагування на інциденти. Паралельно з цим впроваджуються технології запобігання втраті даних (DLP), які аналізують інформаційні потоки та блокують спроби несанкціонованої передачі конфіденційної інформації за межі організації.

Невід'ємною складовою стратегії безпеки є забезпечення неперервності бізнесу через механізми резервного копіювання та відновлення. Системи бекапування створюють копії критично важливих даних, що дозволяє відновити роботу після технічних збоїв або кібератак у рамках планів аварійного відновлення (Disaster Recovery). Нарешті, організаційні заходи, такі як розробка політик безпеки та регулярне навчання персоналу, спрямовані на мінімізацію людського фактору, який часто стає причиною інцидентів. Лише комплексне поєднання технічних засобів та адміністративних заходів дозволяє досягти належного рівня захищеності корпоративної інфраструктури. [10]

1.3 Архітектурні принципи функціонування Active Directory як базової складової екосистеми інформаційної безпеки

Служба каталогів Active Directory (AD), розроблена корпорацією Microsoft, є фундаментальним елементом сучасної IT-інфраструктури, що забезпечує централізоване управління мережевими об'єктами, такими як облікові записи користувачів, робочі станції та периферійне обладнання. Ця технологічна платформа виступає ключовим інструментом для системних адміністраторів, надаючи їм можливість гнучко налаштовувати права доступу, структурувати ресурси в логічні ієрархії, а також реалізовувати надійні механізми автентифікації та авторизації в межах усього підприємства. Визначальною характеристикою Active Directory є її масштабована ієрархічна

архітектура, яка дозволяє адаптувати мережеве середовище до потреб організації будь-якого розміру та забезпечувати повний контроль над використанням корпоративних ресурсів.

Архітектурна будова Active Directory базується на взаємодії кількох критично важливих компонентів, що утворюють єдину логічну структуру. Базовою адміністративною одиницею виступає домен, який консолідує користувачів, комп'ютери та інші об'єкти в єдиному просторі імен та підпорядковує їх спільним політикам безпеки. Функціонування домену забезпечується контролером домену (Domain Controller, DC) — спеціалізованим сервером, що зберігає копію бази даних каталогу, обробляє всі запити на вхід у систему та відповідає за реплікацію, тобто синхронізацію змін між іншими контролерами для забезпечення відмовостійкості. На вищому рівні ієрархії знаходиться ліс (forest), який може об'єднувати один або кілька доменів, що мають спільну схему та глобальний каталог. У межах лісу домени можуть групуватися в дерева (trees), якщо вони використовують суміжний простір імен. Для більш детальної та гранульованої організації об'єктів усередині домену застосовуються організаційні одиниці (Organizational Unit, OU). Ці контейнери дозволяють адміністраторам групувати об'єкти за функціональними або географічними ознаками, що значно спрощує делегування повноважень та застосування групових політик.

Впровадження Active Directory відіграє вирішальну роль у процесах автоматизації та централізації управління корпоративною мережею. Система дозволяє значно пришвидшити процедури створення нових облікових записів, налаштування робочих місць та керування доступом, забезпечуючи при цьому необхідний баланс між суворими вимогами безпеки та зручністю роботи для кінцевих користувачів. Завдяки тісній інтеграції з базовими мережевими службами, такими як система доменних імен (DNS) та протокол динамічної конфігурації хоста (DHCP), а також із засобами захисту контенту, зокрема AD RMS, Active Directory стає ядром комплексної системи захисту інформації.

Однією з пріоритетних функцій служби є забезпечення процедур ідентифікації та перевірки повноважень. Кожен суб'єкт, що прагне отримати доступ до мережевих ресурсів, проходить обов'язкову процедуру аутентифікації через контролер домену, який звіряє надані облікові дані зі збереженими в захищеній базі. Після успішного підтвердження особи ініціюється процес авторизації, під час якого система на основі членства користувача в групах та чинних політик безпеки визначає обсяг дозволених дій. Такий підхід гарантує, що доступ до критично важливих даних отримають лише легітимні користувачі.

Потужним інструментом у руках адміністраторів є механізм групових політик (Group Policy Objects, GPO), який дозволяє централізовано керувати конфігураціями операційних систем та прикладного програмного забезпечення на всіх комп'ютерах домену. Використання GPO надає можливість автоматично встановлювати вимоги до складності паролів, блокувати доступ до певних системних налаштувань, конфігурувати параметри брандмауерів та навіть дистанційно розгортати програмне забезпечення. Це забезпечує уніфікацію стандартів безпеки в усій організації та звільняє IT-персонал від необхідності налаштовувати кожен пристрій вручну. [8]

Інтеграційні можливості Active Directory з екосистемою продуктів Microsoft суттєво розширюють функціонал мережі. Взаємодія з DNS є критичною для коректної роботи самої служби каталогів, оскільки дозволяє комп'ютерам знаходити контролери домену та інші служби. Служба DHCP автоматизує керування IP-адресацією, спрощуючи адміністрування мережевого рівня. Поштові сервери, такі як Microsoft Exchange, використовують базу даних AD для зберігання глобального списку адрес та налаштувань поштових скриньок. Особливе місце займає інтеграція зі службою управління правами Active Directory (AD RMS), яка використовує інфраструктуру AD для криптографічного захисту документів та електронних

листів, контролюючи їх використання навіть за межами периметра корпоративної мережі.

Таким чином, Active Directory виступає не просто як довідник користувачів, а як фундамент інформаційної безпеки підприємства. Адміністратори мають можливість створювати рольові групи безпеки, розмежовуючи доступ до даних відповідно до посадових обов'язків. Наприклад, співробітники відділу кадрів отримують доступ до персональних даних працівників, тоді як інженери мають права на технічну документацію, і ці права не перетинаються. Така сегментація мінімізує ризики внутрішніх загроз та витоку конфіденційної інформації. Крім того, AD надає розширені можливості аудиту та журналювання подій. Система фіксує всі спроби входу, зміни прав доступу та модифікації політик, що дозволяє службі безпеки оперативно виявляти аномальну активність, розслідувати інциденти та запобігати потенційним кібератакам.

Окремо варто наголосити на нерозривному зв'язку між Active Directory та системою Active Directory Rights Management Services (AD RMS). Служба каталогів є необхідною передумовою для розгортання та функціонування RMS, оскільки саме вона забезпечує ідентифікацію користувачів, необхідну для видачі ліцензій на використання захищеного контенту. Без надійної аутентифікації, яку надає AD, неможливо гарантувати, що зашифрований документ відкриє саме та особа, якій це дозволено автором. Інтеграція дозволяє використовувати існуючі групи безпеки та списки розсилки для призначення прав на документи, що значно спрощує процеси адміністрування. Якщо користувач не має активного облікового запису в домені або його обліковий запис заблоковано, він автоматично втрачає можливість доступу до захищеної інформації, що є критично важливим аспектом захисту інтелектуальної власності компанії. Крім того, завдяки централізованому управлінню через групові політики, адміністратори можуть автоматично налаштовувати клієнтські компоненти AD RMS, забезпечуючи безперебійну роботу системи захисту інформації в масштабах усієї організації. [1]

1.4 Функціональні можливості та архітектура системи управління правами AD RMS

Технологія Active Directory Rights Management Services (AD RMS) посідає важливе місце в екосистемі рішень компанії Microsoft, виступаючи потужним серверним інструментом для забезпечення інформаційної безпеки. Ця система надає організаціям можливість реалізувати гнучкий та надійний контроль над доступом до конфіденційних документів та даних. Ключовою відмінністю AD RMS від традиційних засобів захисту є те, що вона не просто обмежує доступ до файлу, а регламентує умови його подальшого використання та розповсюдження. Адміністратори або автори документів можуть встановлювати специфічні обмеження, такі як заборона на копіювання вмісту в буфер обміну, блокування функції друку, заборона редагування або пересилання повідомлень електронної пошти. Будучи невід'ємною складовою інфраструктури Active Directory, цей сервіс дозволяє компаніям відповідати найсуворішим сучасним вимогам щодо захисту корпоративної інтелектуальної власності.

Стратегічне завдання AD RMS полягає у забезпеченні так званого «персистентного» захисту, який залишається з даними незалежно від місця їх зберігання. Це означає, що захист діє не лише всередині захищеного периметра корпоративної мережі, але й за її межами. Наприклад, у ситуації, коли конфіденційний звіт передається зовнішньому контрагенту або копіюється на флеш-накопичувач, права доступу та політики використання залишаються незмінними. Власник інформації продовжує контролювати документ, і неавторизована особа не зможе відкрити його навіть маючи фізичний доступ до файлу.

Архітектурна побудова AD RMS базується на взаємодії низки критично важливих компонентів, що гарантують стабільність та функціональність системи. Центральним елементом є кластер AD RMS — група серверів, що

функціонують як єдине ціле для забезпечення відмовостійкості та високої доступності сервісу. Ці сервери відповідають за генерацію та видачу ліцензій на використання контенту, а також керують криптографічними ключами. Фундаментом безпеки в AD RMS виступає інфраструктура відкритих ключів та цифрових сертифікатів, які використовуються для шифрування даних, підтвердження легітимності користувачів та валідації прав доступу. Система тісно інтегрована зі службою каталогів Active Directory, яка виступає джерелом істини для аутентифікації користувачів та визначення їхньої приналежності до груп безпеки. На боці кінцевого користувача функціонує спеціалізоване клієнтське програмне забезпечення або вбудовані компоненти операційної системи, які звертаються до серверів RMS для отримання дозволів і технічно забезпечують виконання політик (наприклад, роблять кнопку «Друк» неактивною). Усі шаблони політик прав зберігаються в централізованій базі даних, до якої система звертається при кожній спробі доступу до захищеного об'єкта.

Функціональний спектр AD RMS надає широкі можливості для гранулярного захисту інформації. Будь-який документ, оброблений цією службою, піддається шифруванню, і дешифрувати його можуть виключно користувачі з валідними ключами та ліцензіями. Система дозволяє налаштовувати права з високою точністю: адміністратори можуть дозволити одній групі користувачів лише переглядати документ, іншій — вносити правки, при цьому для обох груп може бути заблокована можливість створення копій або друку. Особливої уваги заслуговує інтеграція з поштовим сервером Microsoft Exchange, що дозволяє захищати електронне листування, унеможливлюючи пересилання конфіденційних листів третім особам. Також доступна функція встановлення часових обмежень, коли після настання певної дати файл автоматично стає недоступним для відкриття, що є критично важливим для документів з обмеженим терміном актуальності. Важливим елементом безпеки є ведення детальних журналів аудиту, які дозволяють

відстежувати, хто, коли та з якою метою звертався до захищених файлів, що спрощує розслідування інцидентів безпеки.

Підсумовуючи переваги впровадження AD RMS, необхідно виділити кілька ключових аспектів. По-перше, система забезпечує захист даних незалежно від їхньої локації, гарантуючи безпеку інформації навіть після її виходу за межі корпоративної мережі. По-друге, реалізовано механізм гнучкого управління доступом, що базується на ролях, ідентифікаторах користувачів або групах AD. По-третє, використання даного інструментарію суттєво спрощує дотримання регуляторних вимог та міжнародних стандартів, таких як GDPR, HIPAA чи ISO 27001, оскільки дозволяє технічно підтвердити контроль над чутливою інформацією. По-четверте, глибока інтеграція з екосистемою Microsoft (Office, SharePoint, Exchange) дозволяє впроваджувати політики захисту безшовно, не порушуючи звичні робочі процеси користувачів. І, нарешті, технологія підтримує широкий спектр типів контенту, включаючи текстові документи, таблиці, презентації та електронну пошту. Таким чином, AD RMS створює надійний фундамент для безпечної співпраці та обміну даними, підвищуючи загальну ефективність бізнес-процесів при одночасному зниженні кіберризиків.

1.5 Архітектурні особливості та функціональне призначення платформи Proxmox Backup Server у системі забезпечення доступності даних

У контексті функціонування сучасного корпоративного сектору гарантування безперервності бізнес-процесів неможливе без надійної стратегії резервного копіювання та аварійного відновлення інформації. Цей аспект є критичним елементом у загальній схемі управління доступом, адже втрата облікових даних або політик безпеки може паралізувати роботу організації.

Одним із найбільш ефективних та технологічно досконалих рішень для вирішення цих завдань є Proxmox Backup Server (PBS). Це спеціалізоване програмне забезпечення з відкритим вихідним кодом, яке спроєктоване для створення резервних копій віртуальних машин, контейнерів та фізичних хостів. Його функціональність базується на передових алгоритмах стиснення інформації, механізмах дедуплікації та криптографічного захисту.

Платформа Proxmox Backup Server розроблялася як централізований вузол для зберігання бекапів, що має глибоку нативну інтеграцію з середовищем віртуалізації Proxmox Virtual Environment (PVE). Водночас, архітектура рішення дозволяє його використання в будь-яких IT-ландшафтах, де існує потреба в надійному збереженні великих масивів даних. Стратегічною метою впровадження PBS є мінімізація ризиків незворотної втрати інформації внаслідок апаратних збоїв, кібернетичних атак, помилкових дій персоналу або інших форс-мажорних обставин. [13]

Особливої ваги застосування засобів резервного копіювання набуває в інфраструктурах, побудованих на базі Active Directory та Active Directory Rights Management Services (AD RMS). Це зумовлено тим, що будь-яке порушення цілісності бази даних контролерів домену або втрата конфігурації серверів управління правами може призвести до повної зупинки доступу користувачів до корпоративних ресурсів.

Архітектурно Proxmox Backup Server побудований за класичною клієнт-серверною моделлю. Серверна частина відповідає за прийом, обробку та зберігання даних, які передаються захищеним каналом HTTPS від клієнтських систем. Клієнтами можуть виступати як окремі фізичні сервери, так і вузли віртуалізації. Безпосереднє зберігання інформації організовано через логічні сутності, що називаються Datastore. Ці сховища можуть розміщуватися як на локальних дискових масивах сервера, так і на підключених мережевих ресурсах.

Система складається з низки взаємопов'язаних компонентів, що забезпечують її ефективну роботу. Основою зберігання є Datastore — логічний

простір, що підтримує технологію дедуплікації для оптимізації використання дискового простору. Процес передачі даних ініціюється клієнтським програмним забезпеченням (pve-client або proxmox-backup-client). Важливою складовою життєвого циклу резервних копій є механізм Pruning, який автоматизує процес видалення застарілих копій відповідно до налаштованого розкладу, залишаючи лише актуальні дані. Для гарантії того, що збережені дані придатні до відновлення, використовується механізм верифікації (Verification), який регулярно перевіряє цілісність архівів. Керування правами доступу до репозиторіїв здійснюється через систему списків контролю доступу (ACL), що дозволяє гнучко налаштовувати дозволи для різних користувачів та сервісів.

Функціональний набір Proxmox Backup Server включає низку опцій, спрямованих на підвищення продуктивності та безпеки. Зокрема, реалізовано інкрементне резервне копіювання на блоковому рівні, що дозволяє передавати мережею лише змінені частини файлів, суттєво зменшуючи час виконання завдання. Технологія дедуплікації забезпечує зберігання лише унікальних блоків даних, що дозволяє досягти значної економії місця на носіях. Для додаткового зменшення обсягу архівів застосовуються сучасні алгоритми стиснення, такі як Zstandard (zstd) та LZ4. Критично важливим аспектом є безпека, яка забезпечується шифруванням резервних копій алгоритмом AES-256 на стороні клієнта. Це гарантує конфіденційність інформації навіть у випадку фізичного викрадення дисків зі сховища. Крім того, вбудований планувальник дозволяє повністю автоматизувати процеси очищення старих копій та їх перевірку, а тісна інтеграція з інтерфейсом Proxmox VE надає адміністраторам єдину консоль для керування всіма аспектами резервного копіювання та моніторингу.

При розгортанні інфраструктури з використанням AD RMS, роль Proxmox Backup Server стає стратегічною. По-перше, регулярне створення образів контролерів домену гарантує можливість швидкого відновлення ієрархії користувачів, групових політик та організаційних одиниць. По-друге, резервування серверів AD RMS дозволяє зберегти критично важливі

компоненти: конфігурацію кластера, криптографічні сертифікати, записи точок підключення служб (SCP) та шаблони прав доступу. По-третє, у кризових ситуаціях, наприклад, при виході з ладу сервера реплікації, наявність актуальної копії в PBS дозволяє відновити працездатність сервісу в найкоротші терміни без втрати доступу до захищених документів. Також автоматизоване створення контрольних точок відновлення створює безпечне середовище для експериментів, дозволяючи тестувати нові політики безпеки з можливістю миттєвого повернення до попереднього стани. Таким чином, Proxmox Backup Server виступає фундаментом надійності в екосистемі захисту корпоративних даних на базі рішень Microsoft.

2 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АРХІТЕКТУРНЕ ПРОЄКТУВАННЯ ІНФРАСТРУКТУРИ AD RMS У КОРПОРАТИВНОМУ СЕГМЕНТІ МЕРЕЖІ

2.1 Дослідження передумов та формування технічного завдання на розгортання системи захисту

Ефективна інтеграція служби Active Directory Rights Management Services (AD RMS) у корпоративне середовище неможлива без попереднього глибокого аудиту потреб організації та детального аналізу вимог до майбутньої системи. Цей етап є критичним, оскільки саме на його основі формуються вимоги до політик інформаційної безпеки, розраховуються масштаби розгортання, прогнозується навантаження на сервери та визначається оптимальна мережева топологія.

Процес проєктування інфраструктури AD RMS бере свій початок із всебічного вивчення бізнес-процесів компанії. Специфіка діяльності організації, особливо якщо вона пов'язана з обробкою конфіденційних даних, диктує необхідність впровадження жорстких механізмів контролю. AD RMS виступає інструментом, що дозволяє перенести абстрактні правила безпеки у площину технічної реалізації, що є життєво необхідним для компаній, які прагнуть гарантувати відповідність як внутрішнім корпоративним стандартам, так і зовнішнім нормативно-правовим актам.

Ключовим аспектом на етапі планування є формування чітких вимог до безпеки даних та управління доступом. Організація повинна розробити класифікацію інформації за рівнями конфіденційності та затвердити матрицю доступу для різних категорій користувачів. При цьому вкрай важливо враховувати вектори потенційних загроз, які можуть походити як від зовнішніх зловмисників, так і від інсайдерів. Це передбачає ревізію існуючого периметра

безпеки, оцінку рівня довіри до співробітників та партнерів, а також перевірку наявності ефективних засобів моніторингу та аудиту подій доступу.

Наступним логічним кроком є математичний розрахунок прогнозованого навантаження та оцінка можливостей масштабування системи. Для забезпечення безперебійної роботи сервісу необхідно проаналізувати кількість користувачів, які будуть активно створювати або споживати захищений контент. Стратегічне планування вимагає врахування не лише поточних показників, а й динаміки росту компанії, що неминуче призведе до збільшення обсягів даних та інтенсивності запитів до кластера AD RMS. Помилки на цьому етапі можуть спричинити дефіцит ресурсів, що призведе до затримок у роботі або відмови в обслуговуванні.

На основі отриманих даних про навантаження здійснюється калькуляція апаратних ресурсів, необхідних для серверної групи AD RMS. Це включає визначення вимог до обчислювальної потужності центральних процесорів, обсягу оперативної пам’яті та місткості дискової підсистеми. Розрахунки повинні базуватися на офіційних рекомендаціях Microsoft, але з обов'язковим додаванням резервного запасу потужності для обробки пікових навантажень.

Окремим питанням під час проєктування є вибір платформи розгортання: фізичне обладнання чи віртуалізація. Для представників малого та середнього бізнесу економічно обґрунтованим є використання середовищ віртуалізації, наприклад Proxmox VE, що забезпечує гнучкість управління та зниження капітальних витрат. Водночас для критично важливих систем з екстремальними вимогами до продуктивності та доступності доцільнішим може бути використання виділених фізичних серверів, що дозволяє уникнути накладних витрат гіпервізора.

Окрім суто технічних параметрів, проєкт повинен враховувати юридичні та нормативні аспекти, зокрема відповідність вимогам GDPR або галузевим стандартам безпеки. Некоректна конфігурація політик доступу може призвести не лише до витоку даних, але й до серйозних правових наслідків для організації. Фіналізація вимог до апаратного забезпечення (ядра CPU, RAM,

HDD/SSD) відбувається з урахуванням усіх вищезазначених факторів, а також закладається потенціал для майбутніх оновлень системи, що створює фундамент для надійної та довгострокової експлуатації сервісу.

Базуючись на проведеному теоретичному аналізі, для реалізації даного проєкту було розроблено та затверджено оптимальну конфігурацію віртуального середовища, яка дозволяє розгорнути та протестувати підсистему управління доступом. Ця модель є масштабованою і за необхідності може бути адаптована для великих корпоративних мереж. Для забезпечення високої доступності та балансування навантаження архітектура включає два сервери Active Directory. Кожен із контролерів домену має виділені ресурси у вигляді восьми віртуальних процесорів, восьми гігабайтів оперативної пам’яті та ста гігабайтів дискового простору. Такі параметри гарантують стабільну та швидку обробку всіх запитів на аутентифікацію, авторизацію та реплікацію даних.

Інфраструктура клієнтських місць, яка у рамках проєкту налічує десять і більше одиниць, спроєктована з урахуванням високих вимог до швидкодії. Кожна робоча станція отримала потужну конфігурацію: дванадцять віртуальних процесорних ядер, шістнадцять гігабайтів оперативної пам’яті та шістдесят гігабайтів дискового простору. Такий розподіл ресурсів забезпечує комфортну роботу користувачів із додатками, що підтримують AD RMS, та мінімізує затримки при дешифруванні контенту.

Критично важливим елементом запропонованої архітектури є підсистема резервного копіювання. Для її реалізації виділено окремий вузол під управлінням Proxmox Backup Server. Його технічні характеристики включають чотири процесорні ядра, два гігабайти оперативної пам’яті та сховище обсягом п'ятсот гігабайтів. Цього ресурсу достатньо для налаштування регулярного створення бекапів та забезпечення оперативного відновлення працездатності інфраструктури у випадку аварій. Поточна конфігурація сервера резервного копіювання повністю відповідає завданням кваліфікаційної роботи, проте передбачає можливість розширення оперативної

пам'яті у майбутньому при зростанні навантаження. Таким чином, спроєктована архітектура є збалансованою, відмовостійкою та повністю готовою до впровадження технологій захисту інформації.

2.2 Порівняльний аналіз платформ управління ідентифікацією та аргументація вибору технологічного стеку

В умовах динамічного розвитку корпоративних інформаційних систем питання вибору оптимального засобу для управління каталогами та контролю доступу набуває критичного значення. Хоча технологія Active Directory (AD) від корпорації Microsoft роками утримує лідерські позиції на ринку, сучасний IT-ландшафт пропонує широкий спектр альтернативних рішень, серед яких варто виділити OpenLDAP, FreeIPA, а також хмарні платформи Okta, JumpCloud та Google Workspace Identity. Кожен із цих продуктів має унікальну архітектуру, набір функціональних можливостей та специфіку впровадження, що вимагає детального аналізу їхніх переваг та недоліків для прийняття зваженого рішення.

Active Directory позиціонується як комплексне рішення для реалізації служби каталогів, що виступає фундаментом для побудови централізованої системи аутентифікації, авторизації та управління ресурсами в корпоративних мережах. Ця платформа є де-факто стандартом для Windows-орієнтованих інфраструктур завдяки своїй універсальності та глибокій інтеграції з екосистемою продуктів Microsoft, таких як Exchange Server, SharePoint, Teams та хмарним середовищем Azure. Така синергія дозволяє бізнесу створити єдиний, безшовний простір для роботи. Попри те, що AD є комерційним продуктом і потребує витрат на ліцензування, ці інвестиції виправдовуються наявністю потужних інструментів адміністрування, зокрема групових політик (GPO), які дозволяють автоматизувати налаштування тисяч робочих станцій.

Крім того, комерційна модель гарантує регулярні оновлення безпеки та професійну технічну підтримку, що є критично важливим для великих організацій.

Як альтернатива пропрієтарним рішенням, на ринку присутній OpenLDAP — система з відкритим вихідним кодом, що базується на полегшеному протоколі доступу до каталогів (LDAP). Основною перевагою цього рішення є економічна ефективність, оскільки воно не потребує придбання ліцензій, що робить його привабливим для компаній з обмеженим бюджетом. OpenLDAP характеризується високою гнучкістю та кросплатформністю, підтримуючи роботу в середовищах Linux, macOS та Windows. Проте, впровадження цієї системи вимагає високої кваліфікації технічного персоналу, оскільки налаштування та адміністрування є складнішими порівняно з комерційними аналогами. Крім того, OpenLDAP у базовій комплектації позбавлений багатьох зручних функцій, таких як вбудовані механізми групових політик, що може ускладнити управління великим парком комп'ютерів.

Для інфраструктур, побудованих переважно на базі Linux, часто розглядається рішення FreeIPA. Цей інтегрований продукт об'єднує в собі службу каталогів, систему аутентифікації Kerberos, центр сертифікації та засоби контролю доступу. Завдяки відкритому коду FreeIPA є безкоштовним інструментом, що забезпечує централізоване управління політиками безпеки та ідентифікацією користувачів. Однак вузька спеціалізація системи стає її недоліком у гетерогенних мережах: інтеграція з Windows-середовищем є складною та часто обмеженою у функціоналі. Це робить FreeIPA менш придатним варіантом для організацій, які використовують змішаний парк обладнання або планують масштабування з використанням пропрієтарного програмного забезпечення.

З розвитком хмарних технологій набувають популярності платформи класу Identity-as-a-Service (IDaaS), яскравим представником яких є Okta. Це повністю хмарне рішення усуває потребу в утриманні локальних серверів та

забезпечує просте й швидке налаштування доступу. Okta ідеально підходить для компаній, що активно використовують SaaS-додатки, надаючи зручні інструменти для багатофакторної аутентифікації та єдиного входу (SSO). Проте, повна залежність від стабільності інтернет-з'єднання та висока вартість передплати можуть стати перешкодою для впровадження у великих корпораціях. Крім того, можливості Okta щодо управління локальними ресурсами та пристроями є обмеженими порівняно з традиційними службами каталогів.

Ще одним хмарним гравцем є JumpCloud, який позиціонує себе як універсальна служба каталогів для гетерогенних середовищ, що охоплюють Windows, macOS та Linux. Платформа дозволяє відмовитися від локальних контролерів домену, пропонуючи централізоване управління користувачами та пристроями через хмару. Це рішення забезпечує гнучкість та сучасні методи захисту, такі як MFA, проте, як і інші хмарні сервіси, залежить від доступності мережі Інтернет. Інтеграція JumpCloud з існуючими локальними системами може вимагати додаткових зусиль, а вартість володіння для великих організацій може перевищувати витрати на локальну інфраструктуру.

Окремо варто згадати Google Workspace Identity, що пропонує інструменти управління доступом у межах екосистеми Google. Це рішення є оптимальним вибором для малого та середнього бізнесу, який вже використовує сервіси Google для своєї діяльності. Воно відзначається простотою налаштування та зручністю використання, забезпечуючи базові функції безпеки. Однак, функціонал Google Workspace Identity є недостатнім для складних корпоративних сценаріїв, що вимагають глибокої інтеграції з локальними ресурсами, мережевим обладнанням або специфічним програмним забезпеченням, яке не входить до екосистеми Google.

Підсумовуючи порівняльний аналіз, можна стверджувати, що для побудови надійної, масштабованої та функціональної системи управління доступом у корпоративному середовищі, де переважають технології Windows, Active Directory залишається безальтернативним лідером. Його можливості

щодо детального контролю політик, сумісність з широким спектром програмного забезпечення та надійність роблять його оптимальним вибором для реалізації поставлених у роботі завдань. [14]

2.3 Обґрунтування вибору платформи віртуалізації та системного програмного забезпечення

Наступним критично важливим етапом проєктування є підбір оптимального гіпервізора та платформи віртуалізації, які стануть фундаментом для розгортання локальної мережі та забезпечать безперебійне функціонування всіх компонентів інфраструктури AD RMS. Гіпервізор являє собою спеціалізований клас програмного забезпечення, що створює шар абстракції між фізичним обладнанням та операційними системами, дозволяючи створювати, ізолювати та керувати віртуальними машинами на базі одного фізичного хоста. Його головна місія полягає у забезпеченні раціонального розподілу апаратних потужностей та гарантуванні безпеки виконання кожної окремої віртуальної інстанції.

Функціональний спектр сучасних гіпервізорів є досить широким і охоплює кілька ключових напрямків. Першочерговим завданням є динамічний розподіл обчислювальних ресурсів, таких як процесорний час, оперативна пам’ять, дисковий простір та пропускна здатність мережі, між запущеними віртуальними машинами відповідно до їхніх потреб та пріоритетів. Не менш важливою функцією є забезпечення суворої ізоляції середовищ, завдяки чому кожна віртуальна машина функціонує в абсолютно автономному режимі. Це означає, що програмний збій або компрометація безпеки в одній системі не вплине на стабільність роботи інших машин чи самого гіпервізора. Крім того, професійні рішення підтримують технологію «живої» міграції, що надає адміністраторам можливість переміщувати працюючі віртуальні машини між

різними фізичними серверами без переривання сервісу, що є критичним для забезпечення високої доступності. Також невід'ємною частиною функціоналу є інструменти моніторингу та управління, які дозволяють у реальному часі відстежувати продуктивність інфраструктури та оптимізувати використання наявних ресурсів.

З точки зору архітектури та способу взаємодії з апаратним забезпеченням, гіпервізори класифікують на два основні типи. Перший тип, відомий як «bare-metal» або гіпервізор першого типу, інсталюється безпосередньо на «голе» залізо сервера, фактично виконуючи роль мінімалістичної операційної системи. Така архітектура виключає необхідність використання проміжної ОС, що мінімізує накладні витрати ресурсів та забезпечує максимальну продуктивність і низькі затримки при обробці даних. До найвідоміших представників цього класу належать такі рішення, як Proxmox VE, VMware ESXi, серверна редакція Microsoft Hyper-V, а також системи Xen та KVM. Саме цей тип гіпервізорів є стандартом для побудови корпоративних центрів обробки даних.

Другий тип, або «hosted» гіпервізор, встановлюється як звичайний програмний додаток поверх вже існуючої базової операційної системи. У такій конфігурації запити віртуальних машин проходять через додатковий шар основної ОС, що неминуче призводить до певного зниження продуктивності порівняно з рішеннями першого типу. Проте такі гіпервізори відрізняються простотою використання та ідеально підходять для тестування, розробки або персонального використання. Типовими прикладами є VMware Workstation, Oracle VirtualBox та клієнтські версії Microsoft Hyper-V.

Для прийняття обґрунтованого рішення щодо вибору платформи було проведено детальний порівняльний аналіз найпопулярніших гіпервізорів, зокрема KVM, VMware ESXi, Hyper-V та VirtualBox. Порівняння здійснювалося за комплексом критеріїв, що включали показники продуктивності, вартість володіння, ліцензійні умови, спектр підтримуваних гостьових операційних систем, можливості масштабування та рівень безпеки.

Узагальнені результати цього дослідження наведено у відповідній таблиці, табл. 2.1, що дозволяє наочно зіставити характеристики розглянутих систем та обрати рішення, яке найкраще відповідає специфічним вимогам проєкту.

Таблиця 2.1. Порівняльна характеристика провідних платформ віртуалізації за ключовими техніко-економічними показниками

Критерій порівняння	KVM (Kernel-based Virtual Machine)	VMware ESXi	Microsoft Hyper-V	Oracle VirtualBox
Архітектурний тип	Гіпервізор 1-го типу (інтегрований у ядро Linux)	Гіпервізор 1-го типу (Bare-metal архітектура)	Гіпервізор 1-го типу (мікроядерна архітектура)	Гіпервізор 2-го типу (працює поверх хостової ОС)
Модель ліцензування	Вільна ліцензія (Open-source, GPL)	Закрита пропрієтарна ліцензія	Комерційна ліцензія (частина екосистеми Microsoft)	Відкритий вихідний код (Open-source, GPL v2)
Фінансова політика	Повністю безкоштовне використання без прихованих платежів	Платний продукт (існує обмежена безкоштовна версія)	Входить у вартість ліцензії Windows Server (або безкоштовний Hyper-V Server)	Безкоштовне розповсюдження для особистого використання
Рівень продуктивності	Максимальний, завдяки прямій роботі	Дуже високий, система	Високий, особливо в середовищі	Помірний, наявні затримки

	з апаратним забезпеченням через ядро Linux	глибоко оптимізована для серверних навантажень	Windows Server та Azure	через роботу поверх основної ОС
Можливості масштабування	Високі (підтримка кластеризації та великих обчислювальних потужностей)	Високі (стандарт для великих дата-центрів та Enterprise-сектору)	Високі (ефективна робота у великих корпоративних мережах)	Низькі (рішення орієнтоване на локальні завдання та тестування)
Рівень безпеки	Високий (підтримка sVirt, SELinux та ізоляції процесів)	Високий (спеціалізована безпечна ОС з мінімальною площею атаки)	Високий (інтеграція з засобами безпеки Windows та Active Directory)	Середній (залежність від вразливостей хостової операційної системи)
Критерій порівняння	KVM (Kernel-based Virtual Machine)	VMware ESXi	Microsoft Hyper-V	Oracle VirtualBox

За результатами проведеного порівняльного аналізу технологій віртуалізації для реалізації поставлених завдань було обрано гіпервізор KVM (Kernel-based Virtual Machine). Це рішення вирізняється оптимальним балансом між високою продуктивністю, гнучкістю налаштувань та рівнем інформаційної безпеки. Ключовою архітектурною особливістю KVM є його повна інтеграція в ядро операційної системи Linux, що дозволяє перетворити ядро на гіпервізор без необхідності встановлення стороннього прошарку

програмного забезпечення. Такий підхід гарантує максимально ефективну підтримку технологій апаратної віртуалізації на рівні процесора та мінімізує накладні витрати системних ресурсів. Завдяки цьому KVM надає можливість розгортати повноцінні ізольовані віртуальні машини, кожна з яких має власне віртуалізоване апаратне забезпечення, що робить його ідеальним інструментом для широкого спектра сценаріїв — від створення локальних тестових лабораторій до побудови складних корпоративних інфраструктур.

Вагомим аргументом на користь KVM стала його ліцензійна політика, що базується на принципах відкритого вихідного коду (Open Source). На відміну від пропрієтарних комерційних платформ, таких як VMware ESXi, використання KVM не вимагає придбання дорогих ліцензій або підписок, що суттєво знижує капітальні витрати на етапі впровадження та операційні витрати під час експлуатації. Відкритість архітектури також сприяє безшовній інтеграції з іншими передовими open-source технологіями. Зокрема, KVM є базовим компонентом платформи управління віртуалізацією Proxmox VE, яка нативно підтримує роботу з розподіленими файловими системами Ceph та прогресивною файловою системою ZFS. Таке поєднання дозволяє створити надійне, відмовостійке середовище зберігання даних без прив'язки до апаратних або програмних рішень конкретного вендора.

У контексті продуктивності KVM демонструє мінімальні затримки при обробці операцій введення-виведення завдяки прямому доступу до функцій ядра Linux. Гіпервізор підтримує повний спектр сучасних технологій, включаючи апаратне прискорення, динамічне управління пам'яттю та живу міграцію (live migration), яка дозволяє переміщувати працюючі віртуальні машини між фізичними вузлами кластера без переривання сервісу. Універсальність рішення підтверджується здатністю ефективно працювати як з Windows, так і з Linux у якості гостьових операційних систем. Сукупність цих факторів робить KVM безальтернативним вибором для побудови масштабованої та безпечної інфраструктури в рамках даного проєкту. [2]

Для глибшого розуміння принципів побудови системи необхідно визначити поняття віртуального середовища. Це складний програмно-апаратний комплекс, призначений для створення, адміністрування та логічної ізоляції обчислювальних одиниць — віртуальних машин або контейнерів — у межах наявної фізичної інфраструктури. Фундаментом такого середовища є концепція віртуалізації, яка уможливлює одночасне виконання кількох незалежних операційних систем на єдиному фізичному сервері. Ця технологія дозволяє досягти високої ефективності використання апаратних потужностей, забезпечити динамічний перерозподіл ресурсів відповідно до навантаження та спростити процеси адміністрування IT-ландшафту.

Центральним елементом будь-якого віртуального середовища виступає гіпервізор — шар абстракції, що відокремлює програмне забезпечення від фізичного обладнання. Саме гіпервізор виконує роль арбітра, який розподіляє процесорний час, оперативну пам'ять, дисковий простір та мережеві інтерфейси між запущеними віртуальними машинами. Окрім розподілу ресурсів, критично важливою функцією гіпервізора є забезпечення суворої ізоляції. Це гарантує, що процеси, які відбуваються в одній віртуальній машині, жодним чином не впливають на стабільність та безпеку сусідніх машин або хост-системи, запобігаючи виникненню програмних конфліктів та поширенню загроз.

Сучасні віртуальні середовища, такі як Proxmox VE, не обмежуються лише повною віртуалізацією, а й активно використовують технологію контейнеризації. Контейнери, зокрема LXC (Linux Containers), являють собою легковагові ізольовані простори, які функціонують на базі спільного ядра операційної системи хоста. На відміну від класичних віртуальних машин, контейнери не потребують емуляції повного набору апаратного забезпечення та запуску окремої копії ОС, що робить їх значно продуктивнішими та менш вимогливими до ресурсів. Використання контейнерів є оптимальним рішенням для розгортання мікросервісів та окремих додатків, де критичною є швидкість запуску та щільність розміщення сервісів.

Вибір конкретної платформи віртуалізації завжди базується на специфічних потребах організації. Якщо пріоритетом є гнучкість, відкритість коду та відсутність ліцензійних платежів, оптимальним вибором стає Proxmox VE. Для корпорацій, що потребують гарантованої технічної підтримки та стандартизованих рішень, часто обирають екосистему VMware vSphere, тоді як для середовищ, повністю побудованих на технологіях Microsoft, найкраще підходить Hyper-V. Глибоке розуміння архітектури віртуального середовища та взаємодії його компонентів дозволяє проєктувати стабільні системи, здатні ефективно вирішувати завдання бізнесу.

Для наочного зіставлення характеристик розглянутих платформ та обґрунтування фінального вибору, було проведено детальне дослідження ринку програмного забезпечення, результати якого, включаючи аналіз вартості, функціональних можливостей та підтримки операційних систем, систематизовано у відповідній таблиці, табл.2.2.

Таблиця 2.2. Порівняльна характеристика основних середовищ віртуалізації за технічними та експлуатаційними параметрами

Критерій оцінювання	Proxmox VE	VMware vSphere	Microsoft Hyper-V	Oracle VirtualBox
Архітектура гіпервізора	Гіпервізор 1-го типу (на базі KVM), інтегрований у Debian Linux	Гіпервізор 1-го типу (ESXi), спеціалізована ОС	Гіпервізор 1-го типу (мікроядерна архітектура)	Гіпервізор 2-го типу (працює як додаток поверх основної ОС)
Ліцензійна політика	Відкритий вихідний код (Open-	Пропрієтарна комерційна ліцензія	Пропрієтарна (входить до ліцензії Windows,	Відкритий вихідний код (GPL v2) для базової версії

	source, AGPL v3)	(платна підписка)	існує безкоштовна версія Hyper-V Server)	
Рівень продуктивності	Високий (максимальна ефективність завдяки KVM)	Високий (еталон продуктивності для корпоративного сектору)	Високий (особливо оптимізовано для гостьових ОС Windows)	Середній (наявні накладні витрати хостової операційної системи)
Потенціал масштабування	Високий (підтримка кластеризації, ідеально для серверних рішень)	Дуже високий (стандарт для великих дата-центрів та хмарних провайдерів)	Високий (ефективне масштабування у корпоративних мережах)	Низький (орієнтована на локальне використання)
Інструменти управління	Зручний веб-інтерфейс, командний рядок (CLI)	Веб-консоль vCenter Server, CLI	Графічний інтерфейс Windows GUI, PowerShell	Локальний графічний інтерфейс користувача
Резервне копіювання та захист	Тісна інтеграція з власним рішенням Proxmox Backup Server (PBS)	Використання vSphere Data Protection або сторонніх рішень	Windows Server Backup або стороннє ПЗ	Відсутні вбудовані централізовані засоби

На основі проведеного комплексного аналізу наявних на ринку рішень для віртуалізації, в якості базової платформи для реалізації проєкту було обрано Proxmox Virtual Environment (Proxmox VE). Це рішення є оптимальним, оскільки гармонійно поєднує в собі інструменти для роботи як з повноцінними віртуальними машинами, так і з легковими контейнерами. Вагомим аргументом на користь даного продукту є його ліцензійна політика: будучи програмним забезпеченням з відкритим вихідним кодом, Proxmox VE не потребує значних капітальних інвестицій, що вигідно відрізняє його від комерційних конкурентів, зокрема екосистеми VMware. Завдяки високій гнучкості конфігурації та можливостям масштабування, ця платформа здобула визнання серед фахівців, які прагнуть побудувати продуктивну інфраструктуру, уникаючи надмірних витрат на придбання пропрієтарних ліцензій.

Ключовою технічною перевагою Proxmox VE є гібридна архітектура, що підтримує різні типи віртуалізації. Для розгортання операційних систем, які потребують повної ізоляції та емуляції апаратного забезпечення, використовується потужний гіпервізор KVM. Водночас для запуску мікросервісів та додатків, критичних до швидкодії, платформа пропонує технологію контейнеризації LXC, яка забезпечує мінімальні накладні витрати ресурсів. Такий підхід дозволяє досягти максимальної щільності розміщення сервісів на одному фізичному сервері. Окрім того, система має вбудовані механізми кластеризації, що дозволяє об'єднувати декілька фізичних вузлів у єдиний логічний ресурс. Це є необхідною умовою для забезпечення високої доступності сервісів та автоматичного балансування навантаження, що критично важливо для забезпечення безперервності бізнес-процесів та відмовостійкості корпоративних систем.

Невід'ємною складовою обраної екосистеми є інтегрована підсистема резервного копіювання Proxmox Backup Server (PBS). Вона надає можливість автоматизувати процеси створення бекапів як для віртуальних машин, так і для контейнерів, що виступає гарантом збереження даних та можливості

оперативного відновлення після збоїв. Функціонал PBS забезпечує високу надійність зберігання архівів завдяки механізмам дедуплікації та верифікації, дозволяючи налаштувати гнучкі розклади резервування з мінімальним впливом на продуктивність основної системи.

З точки зору адміністрування, Proxmox VE вирізняється зручним та інтуїтивно зрозумілим веб-інтерфейсом. Це середовище управління надає повний доступ до налаштувань кластера, сховищ та мережі, дозволяючи здійснювати моніторинг ресурсів та масштабування інфраструктури без необхідності глибокого занурення в роботу з командним рядком. Така ергономічність робить платформу привабливою для адміністраторів, які цінують баланс між потужним функціоналом та зручністю експлуатації.

Окремим етапом проєктування є планування мережевої топології, яке вимагає чіткого розподілу адресного простору та визначення правил взаємодії між віртуальними та фізичними компонентами мережі. Критично важливим рішенням є вибір типу адресації для різних класів пристроїв. Для серверної інфраструктури, де стабільність та незмінність доступу є пріоритетом, доцільно використовувати статичні IP-адреси.

У межах даного проєкту для організації локальної мережі обрано діапазон адрес підмережі 192.168.50.0/24. Згідно з розробленим планом, ключові сервери отримають фіксовані адреси, що спростить адміністрування та налаштування політик безпеки. Зокрема, головний контролер домену (Primary AD DC) буде налаштовано на IP-адресу 192.168.50.10, а резервний контролер домену (Secondary AD DC) отримає адресу 192.168.50.11. Такий підхід дозволяє чітко ідентифікувати критичні вузли в мережі та гарантувати стабільний доступ до них для всіх клієнтів. [6]

Для обслуговування клієнтських робочих станцій та інших пристроїв, що не виконують серверних функцій, передбачено використання протоколу динамічної конфігурації хоста (DHCP). Це дозволить автоматизувати процес підключення нових пристроїв, усуваючи необхідність ручного введення параметрів. Для пулу DHCP-адрес виділено діапазон від 192.168.50.100 до

192.168.50.200, що забезпечує достатній запас адрес для масштабування кількості клієнтів.

Забезпечення коректної маршрутизації трафіку за межі локальної мережі, зокрема до мережі Інтернет, покладається на шлюз за замовчуванням. У нашій конфігурації роль шлюзу виконуватиме маршрутизатор (наприклад, MikroTik), якому присвоєно адресу 192.168.50.1. Ця адреса має бути прописана у мережевих налаштуваннях кожної віртуальної машини, що дозволить організувати правильний обмін пакетами із зовнішніми мережами.

При конфігуруванні віртуальних машин у середовищі Proxmox важливо також правильно обрати тип емульованого мережевого адаптера. Для досягнення максимальної пропускної здатності та зниження навантаження на центральний процесор рекомендовано використовувати пара-віртуалізований драйвер типу «virtio». У випадках, коли операційна система не підтримує цей драйвер, можна використовувати емуляцію «e1000», яка забезпечує вищу сумісність, але меншу продуктивність. Для кожного сервера параметри мережі, такі як IP-адреса, маска підмережі, шлюз та адреси DNS-серверів, вводяться вручну для забезпечення повного контролю над з'єднанням.

Підсумовуючи, можна стверджувати, що ретельне планування мережевих параметрів у середовищі Proxmox є фундаментом стабільної роботи всієї IT-інфраструктури. Коректний розподіл статичних та динамічних адрес, правильне налаштування шлюзів та вибір оптимальних драйверів безпосередньо впливають на швидкість, надійність та безпеку обміну даними. Усі затверджені IP-адреси та параметри мережі систематизовано та наведено у табл. 2.3.

Таблиця 2.3. Зведена відомість розподілу адресного простору мережевої інфраструктури

Назва мережевого вузла	Присвоєна IP-адреса	Маска підмережі	Префікс мережі (CIDR)

Маршрутизатор шлюзу	192.168.50.1	255.255.255.0	/24
Primary Domain Controller (AD Main)	192.168.50.10	255.255.255.0	/24
Secondary Domain Controller (AD Replica)	192.168.50.11	255.255.255.0	/24
Proxmox Backup Server (PBS)	192.168.50.12	255.255.255.0	/24
Клієнтські робочі станції	Динамічна (DHCP Range .100-.200)	255.255.255.0	/24

Побудова ефективної та захищеної системи управління цифровими правами вимагає комплексного підходу до вибору та налаштування супутніх технологій. Для коректної роботи Active Directory Rights Management Services (AD RMS) у спроєктованій інфраструктурі необхідно залучити низку фундаментальних сервісів середовища Windows Server, які утворюють єдиний екосистемний ландшафт безпеки. Ці компоненти забезпечують не лише технічну можливість шифрування, але й гарантують надійну ідентифікацію користувачів та керованість процесів доступу.

Фундаментом усієї системи виступає служба каталогів Active Directory (AD). Вона виконує роль центрального репозиторію для зберігання облікових записів користувачів, груп безпеки та об'єктів комп'ютерів. Саме AD забезпечує базову структуру ідентичності, без якої функціонування AD RMS є неможливим, оскільки система повинна чітко розуміти, кому саме надаються права на розшифрування контенту. Інтеграція з AD дозволяє автоматизувати процеси авторизації: коли автор документа призначає права доступу певному відділу, RMS-сервер звертається до каталогу для перевірки членства

користувача у відповідній групі безпеки. Такий підхід забезпечує централізований контроль та значно спрощує адміністрування, оскільки будь-які зміни в кадровій структурі компанії автоматично відображаються на правах доступу до захищених матеріалів.

Невід'ємною складовою інфраструктури є інфраструктура відкритого ключа (PKI), реалізована через служби сертифікації Active Directory Certificate Services (AD CS). Ці служби відповідають за емісію цифрових сертифікатів, які є критично важливими для процесів аутентифікації серверів та клієнтів, а також для побудови довірених каналів зв'язку (наприклад, через протокол HTTPS). У контексті AD RMS сертифікати використовуються для підписання ліцензій на використання контенту та підтвердження легітимності серверів ліцензування. У рамках реалізації проєкту AD CS буде налаштовано для генерації та управління життєвим циклом сертифікатів, що дозволить створити надійне криптографічне середовище, де кожен учасник обміну даними проходить сувору перевірку автентичності перед отриманням доступу до захищених ресурсів.

Наступним кроком є безпосереднє розгортання та конфігурація серверної ролі AD RMS. Цей сервер виступає ключовим елементом архітектури, відповідальним за видачу ліцензій на публікацію та використання захищеного контенту. Його налаштування передбачає тісну взаємодію з іншими компонентами мережі, зокрема з контролерами домену для аутентифікації та з SQL-сервером (або внутрішньою базою даних) для зберігання конфігурації та політик. Правильна конфігурація цього вузла гарантує, що механізми захисту будуть застосовуватися на рівні операційної системи та додатків прозоро для користувача, забезпечуючи при цьому високий рівень стійкості до спроб несанкціонованого доступу.

Для управління поведінкою клієнтських додатків та визначення правил поводження з інформацією застосовуються механізми групових політик (Group Policy) та шаблонів політик прав RMS. Групові політики дозволяють автоматично розповсюджувати налаштування клієнта AD RMS на всі робочі

станції в домені, а також примусово вмикати інтеграцію з офісними пакетами. Шаблони політик прав, у свою чергу, дають можливість адміністраторам заздалегідь визначити типові сценарії доступу, наприклад, «Тільки для читання» або «Конфіденційно: заборонено пересилання». Це дозволяє гранулярно налаштовувати дозволи, обмежуючи такі дії як друк, копіювання в буфер обміну або редагування вмісту залежно від ролі співробітника в організації.

Завершальним, але не менш важливим елементом технологічного стеку є система моніторингу та аудиту. Для забезпечення відповідності вимогам безпеки та можливості розслідування інцидентів необхідно налаштувати детальне логування всіх транзакцій, пов'язаних із видачею ліцензій та доступом до файлів. Служба AD RMS надає можливості ведення журналів, які фіксують, хто, коли та до якого саме документа намагався отримати доступ, і чи був цей доступ успішним. Аналіз цих даних дозволяє адміністраторам безпеки виявляти аномальну активність, потенційні витоки інформації або спроби зловживання наданими правами.

Таким чином, успішна імплементація системи захисту даних базується на синергії описаних технологій. Використання Active Directory, AD CS, механізмів групових політик та засобів аудиту дозволяє створити надійний, керований та масштабований захисний периметр, що відповідає сучасним стандартам корпоративної безпеки.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ПРОЄКТУ ТА ВЕРИФІКАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Інсталяція платформи віртуалізації та базове налаштування хост-системи

Початковим етапом практичної частини роботи є підготовка апаратної платформи та розгортання середовища віртуалізації, яке слугуватиме фундаментом для всієї проєктованої інфраструктури. Процес інсталяції гіпервізора Proxmox Virtual Environment на фізичний сервер є критично важливим, оскільки саме від коректності цього етапу залежить стабільність та швидкодія майбутніх віртуальних машин. Робота розпочалася із завантаження актуального ISO-образу Proxmox VE з офіційного репозиторію розробника та підготовки завантажувального фізичного носія. Хоча інсталятор системи має алгоритми автоматичного визначення апаратної конфігурації, включаючи тип процесора та обсяг оперативної пам'яті, втручання адміністратора є необхідним для прийняття ключових архітектурних рішень. Зокрема, особливу увагу було приділено вибору цільового дискового накопичувача для встановлення системи, адже Proxmox VE підтримує роботу як з локальними дисками, так і зі складними мережевими сховищами, що впливає на стратегію зберігання даних.

Процедура інсталяції складалася з послідовності налаштувань, які визначають параметри функціонування сервера. На першому кроці майстер встановлення запропонував обрати фізичний диск, на який буде розгорнуто операційну систему гіпервізора. Для забезпечення максимальної продуктивності дискової підсистеми та мінімізації часу відгуку віртуальних машин було надано перевагу використанню твердотільних накопичувачів (SSD) з високою пропускною здатністю. Наступним важливим етапом стало

конфігурування мережевих параметрів. Оскільки сервер віртуалізації є критичним вузлом інфраструктури, для нього було встановлено статичну IP-адресу, визначено маску підмережі та шлюз за замовчуванням, що гарантує його постійну доступність для адміністраторів у локальній мережі. Також під час інсталяції було визначено параметри розподілу обчислювальних потужностей, що дозволить у майбутньому гнучко квотувати ресурси центрального процесора та оперативної пам'яті між різними віртуальними середовищами.

Після завершення процесу копіювання файлів та налаштування конфігурації сервер автоматично перезавантажився, що ознаменувало готовність гіпервізора до роботи. Подальше керування системою здійснюється через захищений веб-інтерфейс, доступ до якого відкривається шляхом введення IP-адреси сервера та спеціального порту у адресному рядку браузера. Веб-консоль Proxmox VE вирізняється ергономічністю та інтуїтивно зрозумілою навігацією, що дозволило оперативно провести фінальне налаштування параметрів сховища та мережевих мостів без необхідності використання складних команд терміналу. Виконання цих дій дозволило отримати повністю функціональну платформу, готову до розгортання гостьових операційних систем.

Наступним логічним кроком стала підготовка програмного забезпечення для віртуальних машин. До бібліотеки образів Proxmox було завантажено офіційні дистрибутиви операційних систем від компанії Microsoft. Для емуляції робочих станцій користувачів було обрано операційну систему Windows 10 Pro архітектури x64. Вибір саме редакції Pro обумовлений необхідністю приєднання комп'ютерів до домену Active Directory та підтримкою централізованого управління через групові політики, що є недоступним у домашніх версіях. Для розгортання серверної інфраструктури було використано образ Windows Server 2019 Standard x64. Ця операційна система стала базою для двох ключових віртуальних машин: основного контролера домену та додаткового сервера реплікації. Функціонал Windows

Server 2019 повністю забезпечує роботу необхідних служб, таких як Active Directory, DNS та AD RMS, створюючи надійне середовище для реалізації політик інформаційної безпеки. Використання 64-бітних версій усіх операційних систем гарантує повну сумісність із сучасним обладнанням та стабільну роботу в середовищі віртуалізації.

Безпосереднє створення віртуальної інфраструктури включало генерацію кількох типів машин згідно з розробленою топологією. Було ініціалізовано дві серверні машини для підтримки відмовостійкості служби каталогів, групу клієнтських машин, що імітують робочі місця співробітників різних департаментів, а також окремий вузол для системи резервного копіювання, покликаний забезпечити збереження критичних даних. У процесі створення кожної віртуальної машини в інтерфейсі гіпервізора задавалися унікальні ідентифікатори (VM ID), зрозумілі імена хостів та асоціювалися відповідні ISO-образи для завантаження. Візуалізація процесу конфігурування параметрів нової віртуальної машини та вибору джерела інсталяції представлена на рис.3.1 та рис.3.2 відповідно.

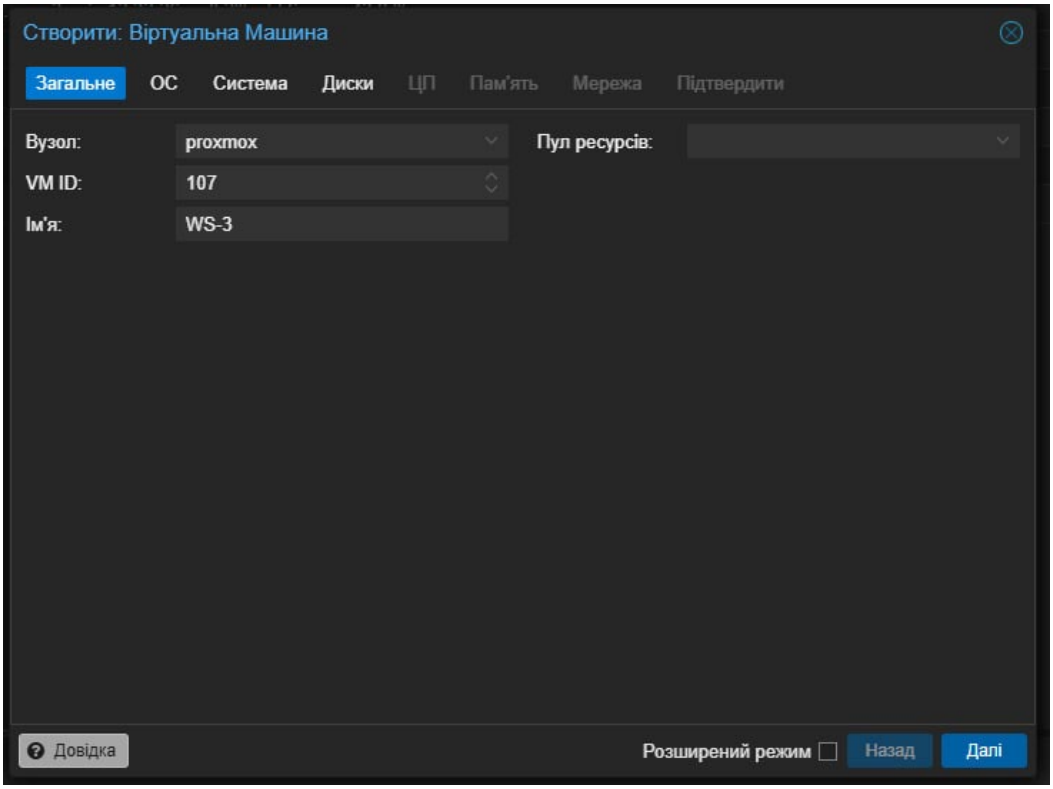


Рисунок 3.1 – Інтерфейс налаштування параметрів нової віртуальної машини

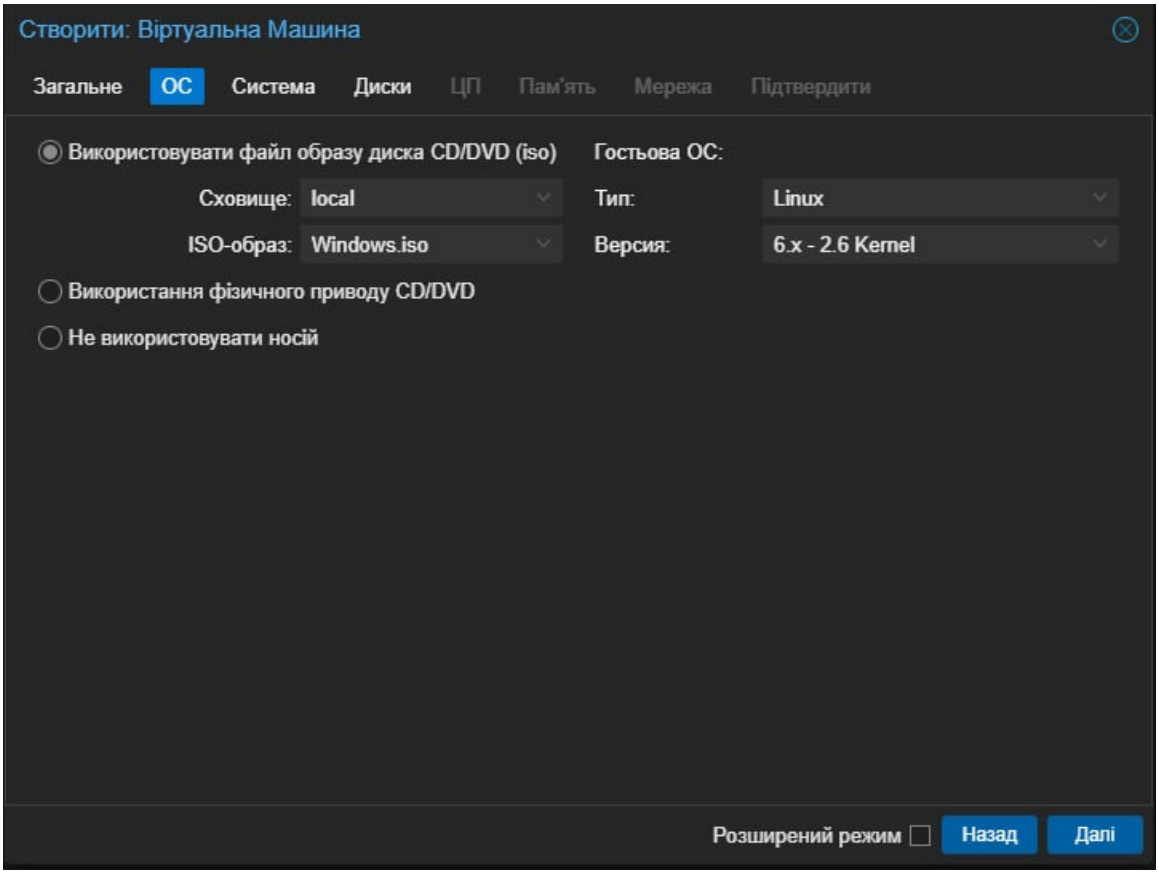


Рисунок 3.2 – Меню вибору інсталяційного образу операційної системи

Процес визначення та розподілу обчислювальних потужностей для кожної віртуальної одиниці базувався на ретельному аналізі прогнозованого навантаження, що є необхідною умовою для гарантування стабільності та відмовостійкості всієї інформаційної системи. Критично важливі вузли інфраструктури, якими виступають контролери домену, потребують значного запасу продуктивності для оперативної обробки запитів аутентифікації, реплікації даних та операцій ліцензування RMS. Виходячи з цих вимог, для кожного з розгорнутих серверів Active Directory було виділено по вісім віртуальних процесорних ядер та вісім гігабайтів оперативної пам’яті. Дискова підсистема цих серверних машин була сконфігурована обсягом у сто гігабайтів, що забезпечує достатній простір для розміщення бази даних каталогу, системних файлів операційної системи та зростаючих журналів аудиту безпеки.

Моделювання клієнтського сегмента мережі, який призначений для імітації реальних робочих місць співробітників компанії, також вимагало виділення відповідного пулу ресурсів. У сукупності для забезпечення належного функціонування групи клієнтських віртуальних машин було задіяно дванадцять ядер центрального процесора та шістнадцять гігабайтів оперативної пам’яті. Дисковий простір для цього сегмента було обмежено шістдесятьма гігабайтами, що відповідає типовим потребам для виконання стандартних офісних завдань та роботи з документами.

Окрему увагу в процесі розподілу ресурсів було приділено конфігурації спеціалізованого вузла, призначеного для резервного копіювання. Оскільки пріоритетним завданням цього сервера є надійне акумулювання та зберігання значних масивів архівних даних, ключовим параметром стала ємність сховища, для якого було виділено дисковий накопичувач обсягом п'ятсот гігабайтів. Водночас вимоги до обчислювальних ресурсів для цього вузла є більш помірними, тому його конфігурацію було оптимізовано до чотирьох процесорних ядер та двох гігабайтів оперативної пам’яті, чого цілком достатньо для ефективної роботи програмного забезпечення Proxmox Backup Server. Деталізований процес налаштування апаратних параметрів та розподілу ресурсів на прикладі однієї з віртуальних машин наочно продемонстровано на рис.3.3 та рис.3.4.

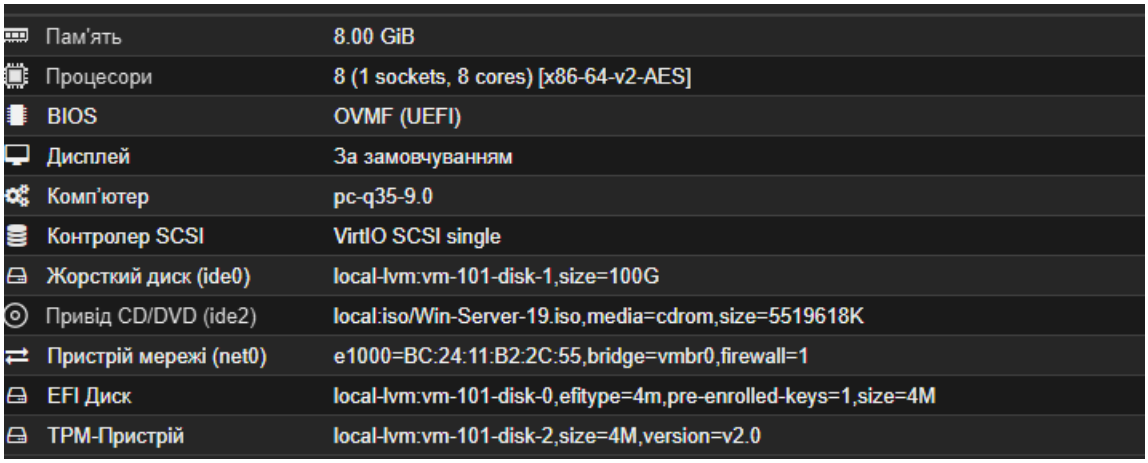


Рисунок 3.3 – Конфігурація процесора та оперативної пам'яті віртуальної машини

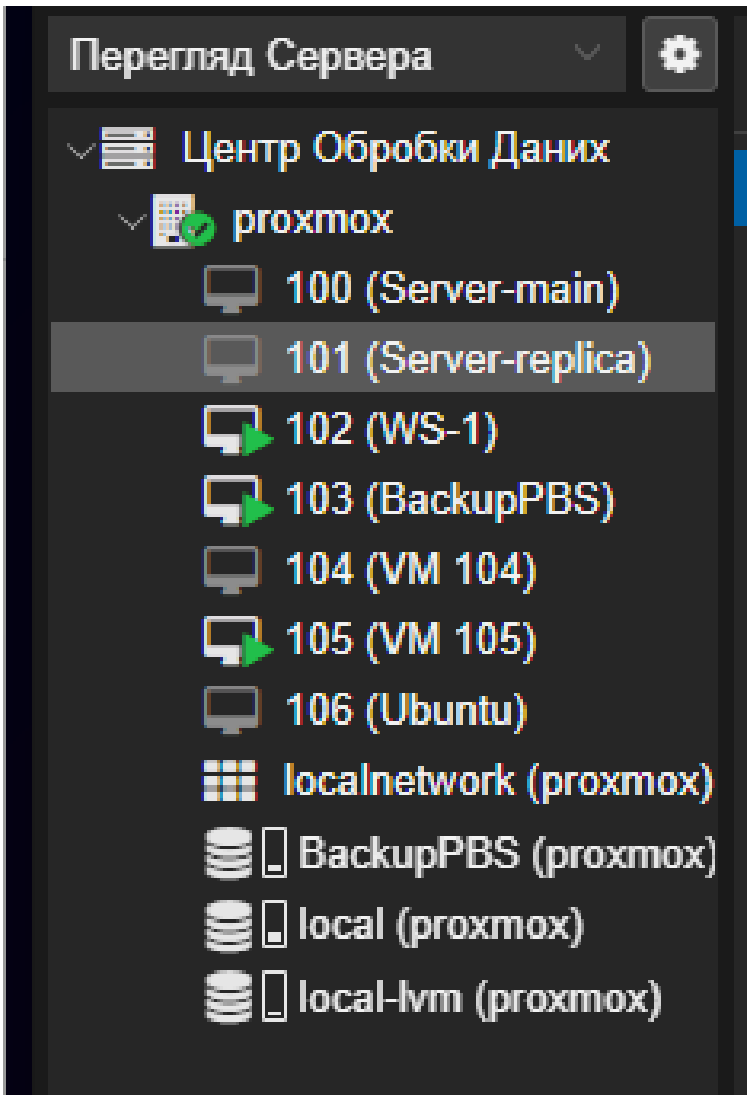


Рисунок 3.4 – Налаштування параметрів віртуального дискового накопичувача

3.2 Реалізація доменної структури та конфігурація служби каталогів

У межах підготовленого віртуального ландшафту було здійснено розгортання та налаштування двох серверних платформ під керуванням операційної системи Windows Server 2019, які стали фундаментом логічної структури мережі. Перший вузол, якому присвоєно повне доменне ім'я server-main.test.net, виконує функцію первинного контролера домену та утримує критично важливі ролі майстрів операцій. Другий сервер, іменований server-

replica.test.net, було сконфігуровано як додатковий контролер домену. Його основне призначення полягає у забезпеченні безперервної реплікації даних каталогу, що гарантує збереження інформації та підвищує загальну відмовостійкість системи у випадку технічних збоїв на основному вузлі.

Технічний процес створення домену розпочався з інсталяції ролі Active Directory Domain Services (AD DS) за допомогою стандартних засобів диспетчера серверів (Server Manager). Після успішного підвищення статусу головного сервера до рівня контролера домену та створення нового лісу, було виконано процедуру приєднання другого сервера. Цей крок дозволив автоматично синхронізувати всі об'єкти, схеми та контейнери каталогу між обома вузлами, створюючи єдиний простір імен та спільну базу даних автентифікації.

Наступним етапом стало проєктування та впровадження ієрархічної структури організаційних одиниць (Organizational Units, OU), яка базується на принципах централізованого та гранулярного управління корпоративними ресурсами. Головною метою було створення такої організаційної моделі, яка б дозволяла ефективно адмініструвати облікові записи та застосовувати диференційовані політики безпеки відповідно до функціональних обов'язків співробітників. Архітектура домену починається з кореневої організаційної одиниці «Department», яка логічно об'єднує чотири ключові департаменти компанії: відділ розробки («Development»), відділ кадрів («HR»), управлінський апарат («Management») та відділ маркетингу («Marketing»).

Для забезпечення максимальної гнучкості адміністрування, всередині кожного з перелічених департаментів було створено вкладені контейнери «Users» та «PCs». Такий підхід дозволив чітко розмежувати об'єкти користувачів та комп'ютерів, що є критично важливим для коректного застосування об'єктів групових політик (Group Policy Objects, GPO). Завдяки такій структурі адміністратори мають змогу застосовувати специфічні налаштування безпеки та програмного забезпечення окремо для робочих станцій та облікових записів персоналу в межах одного відділу. Кожен

співробітник був розміщений у відповідній гілці ієрархії, що автоматизувало надання необхідних прав доступу та обмежень.

Окремою ланкою в структурі стала створена організаційна одиниця «Admins». Цей контейнер призначений виключно для зберігання облікових записів технічного персоналу, наділеного привілейованими правами доступу. Ізоляція адміністративних акаунтів дозволила сконцентрувати керування критичними компонентами інфраструктури в захищеному сегменті та спростити аудит дій привілейованих користувачів. Таким чином, реалізована структура Active Directory забезпечує не лише зручність поточного адміністрування, але й високий рівень безпеки мережевої інфраструктури, залишаючись при цьому повністю масштабованою та готовою до потенційного розширення штату компанії без необхідності докорінної перебудови архітектури.

Окрім побудови ієрархічної структури організаційних одиниць, критично важливим етапом проєктування системи безпеки стала реалізація стратегії розділеного адміністрування. З цією метою було створено спеціалізовані облікові записи для адміністративного персоналу, закріпленого за конкретними департаментами. Зокрема, для загального управління інфраструктурою було згенеровано обліковий запис adm-admins, тоді як для забезпечення технічної підтримки відділів розробки, менеджменту та маркетингу було впроваджено відповідні ідентифікатори: adm-dev, adm-mgmt та adm-mktg. Така диференціація дозволила відмовитися від використання єдиного облікового запису адміністратора домену для рутинних завдань.

Впровадження цих облікових записів супроводжувалося процедурою делегування повноважень. Кожному з локальних адміністраторів було надано чітко окреслений набір прав, що дозволяє їм здійснювати управління об'єктами (скидання паролів, створення користувачів, переміщення комп'ютерів) виключно в межах закріпленої за ними організаційної одиниці. Такий підхід, що базується на принципі найменших привілеїв, суттєво підвищує загальний рівень захищеності системи, оскільки компрометація або помилка

адміністратора одного підрозділу не вплине на функціонування інших сегментів домену та не порушить цілісність глобальної інфраструктури.

Паралельно з налаштуванням політик доступу було проведено детальну конфігурацію служби доменних імен (DNS). Цей сервіс є фундаментом для коректної роботи Active Directory, оскільки відповідає не лише за перетворення доменних імен на IP-адреси, але й за локалізацію контролерів домену клієнтськими машинами через SRV-записи. Налаштування DNS гарантувало правильну реєстрацію ресурсів у мережі та забезпечило безперебійне функціонування механізмів аутентифікації Kerberos. Окрему увагу було приділено перевірці стабільності процесів реплікації між основним та додатковим контролерами домену. Використання спеціалізованих інструментів моніторингу дозволило підтвердити успішну синхронізацію бази даних каталогів, схем та конфігурацій. Результати діагностики, що демонструють відсутність помилок та актуальність реплік на всіх вузлах мережі, візуалізовано на рис.3.5.

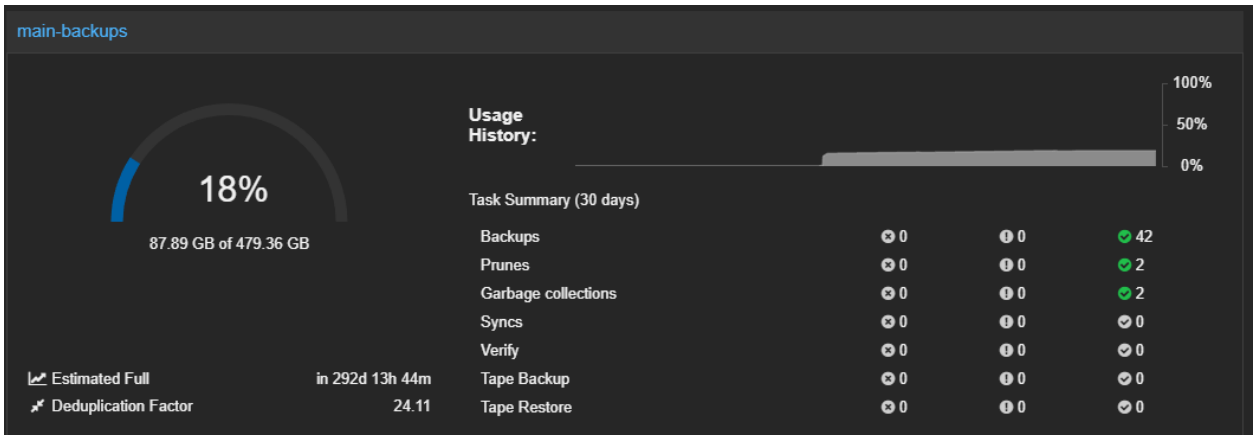


Рисунок 3.5 – Результати діагностики

3.3 Підготовчі заходи та конфігурація службових компонентів для розгортання AD RMS

Практична фаза впровадження системи захисту інформації на базі Active Directory Rights Management Services розпочалася з реалізації комплексу обов'язкових підготовчих процедур. Цей етап є критично важливим, оскільки коректна робота служби управління правами вимагає попередньої адаптації серверного ландшафту та налаштування інфраструктури відкритих ключів. Першочерговим завданням стало створення спеціалізованого ідентифікатора безпеки, який необхідний для функціонування системних процесів кластера RMS. У межах раніше створеної адміністративної організаційної одиниці «Admins» було згенеровано новий службовий обліковий запис із логіном adrms_service.

Основне функціональне призначення цього об'єкта полягає у забезпеченні контексту безпеки, від імені якого будуть запускатися та виконуватися служби компонентів AD RMS, а також здійснюватися взаємодія з базою даних конфігурації. При налаштуванні параметрів цього облікового запису було суворо дотримано фундаментального принципу інформаційної безпеки — принципу найменших привілеїв. Обліковому запису adrms_service було делеговано виключно той мінімальний набір прав та дозволів, який є технічно необхідним для старту служб та доступу до ресурсів, уникаючи надання надлишкових адміністративних повноважень у домені. Такий підхід дозволяє суттєво мінімізувати ризики та підвищити загальну захищеність системи, оскільки навіть у випадку гіпотетичної компрометації служби зловмисник не отримає повного контролю над інфраструктурою. Візуалізацію властивостей створеного службового облікового запису наведено на рис.3.6.

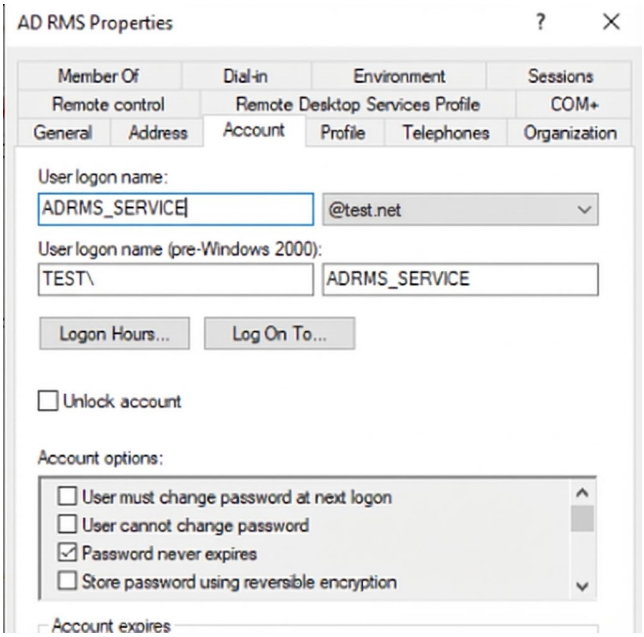


Рисунок 3.6 – Конфігурація службового облікового запису adrms_service

Враховуючи високу архітектурну складність та ресурсоємність розгортання повноцінного внутрішнього центру сертифікації (Enterprise CA) для потреб тестового середовища, було прийнято стратегічне рішення щодо використання самопідписаного сертифіката для забезпечення захищеного з'єднання з сервером AD RMS. Процедура генерації цього сертифіката здійснювалася засобами консолі управління веб-сервером IIS Manager, де було обрано функцію створення самопідписаного сертифіката. Первинно згенерований об'єкт безпеки було автоматично розміщено у сховищі «Personal», проте для коректного розпізнавання сервером його довіреності виникла необхідність виконати ручну операцію експорту та подальшого імпорту до сховища «Trusted Root Certification Authorities» на локальному вузлі. Саме цей криптографічний об'єкт було визначено як основний серверний сертифікат для шифрування HTTPS-трафіку під час подальшої інсталяції служби. Такий підхід дозволив значно оптимізувати процес розгортання RMS у межах лабораторного стенду, усунувши необхідність налаштування багаторівневої ієрархії PKI, при цьому зберігаючи можливість роботи через захищений протокол.

Перед початком безпосередньої інсталяції ролі AD RMS було проведено ретельний аудит налаштувань веб-сервера IIS. Зокрема, було верифіковано наявність та активний статус сайту за замовчуванням («Default Web Site»), перевірено доступність необхідних службових портів, а також активовано та налаштовано модуль «Windows Authentication». Останній аспект є критично важливим, оскільки служба управління правами базується на інтегрованій доменній автентифікації для ідентифікації користувачів, що звертаються за ліцензіями.

Процес інсталяції служби Active Directory Rights Management Services виконувався на потужностях другого сервера з мережевим іменем server-replica.test.net. У ході роботи майстра конфігурації було обрано сценарій створення нового кореневого кластера сертифікації та ліцензування. Для зберігання конфігураційних даних та політик було вирішено використовувати вбудовану базу даних Windows (Windows Internal Database), що є оптимальним варіантом для даного масштабу розгортання. Також було активовано функцію централізованого зберігання ключів кластера. На етапі налаштування захищеного з'єднання було обрано раніше підготовлений сертифікат зі сховища «Personal», а адресу кластера для підключення клієнтів було зафіксовано у форматі повного доменного імені захищеного протоколу: https://server-replica.test.net. Фінальним етапом інсталяції стала автоматична реєстрація точки підключення служби (Service Connection Point, SCP) у лісі Active Directory, що дозволяє клієнтським додаткам автоматично знаходити сервер RMS у мережі.

Після успішної ініціалізації служби та перевірки працездатності кластера, наступним кроком стало налаштування логіки розмежування доступу. За допомогою консолі адміністрування AD RMS було розроблено та впроваджено серію шаблонів політик розподілених прав (Distributed Rights Policy Templates), які стандартизують правила поводження з документами для різних бізнес-сценаріїв. Кожен шаблон містить чітко визначений набір

дозволів та обмежень, що автоматизує процес захисту інформації для кінцевих користувачів.

Перший розроблений шаблон отримав назву «Development Confidential». Його логіка передбачає надання виключних прав на перегляд та редагування технічної документації лише членам групи розробників («Development»), тоді як будь-які інші користувачі домену, включаючи менеджмент, повністю позбавлені доступу до вмісту файлів, захищених цією політикою.

Для потреб відділу маркетингу було створено політику «Marketing Confidential», яка реалізує інший підхід до безпеки. Згідно з цим шаблоном, співробітники департаменту маркетингу отримують доступ до матеріалів, проте на них накладаються суворі обмеження щодо розповсюдження інформації: програмно блокуються функції копіювання вмісту в буфер обміну та виведення документів на друк, що мінімізує ризики витоку промо-матеріалів до їх офіційного релізу.

Для захисту найбільш критичної інформації було впроваджено шаблон «Top Secret (Admins only)». Ця політика забезпечує максимальний рівень ізоляції, надаючи права доступу виключно адміністративному персоналу з групи «Admins». Усі інші облікові записи, незалежно від їхнього статусу в ієрархії компанії, отримують відмову при спробі відкрити такі документи.

Окрім спеціалізованих шаблонів, було створено універсальну політику «Read-Only Documents», призначену для широкого кола користувачів. Цей шаблон дозволяє відкривати та переглядати документи всім авторизованим співробітникам, проте жорстко забороняє будь-які модифікації вмісту, збереження копій або друк, гарантуючи таким чином цілісність та незмінність оприлюдненої інформації.

Окрім розмежування прав доступу, у конфігурації шаблонів було детально опрацьовано та імплементовано механізми контролю за використанням контенту. Зокрема, було активовано технічні заборони на виконання таких операцій, як виведення документів на друкувальні пристрої, створення знімків екрана (включаючи блокування роботи інструмента

«Ножиці») та копіювання текстових або графічних елементів у буфер обміну. Впровадження цих обмежень є критично важливим аспектом у загальній стратегії запобігання витоку даних, оскільки воно закриває найбільш поширені канали несанкціонованого розповсюдження інформації. Наочний приклад налаштування цих параметрів у консолі адміністрування наведено на рис.3.7.

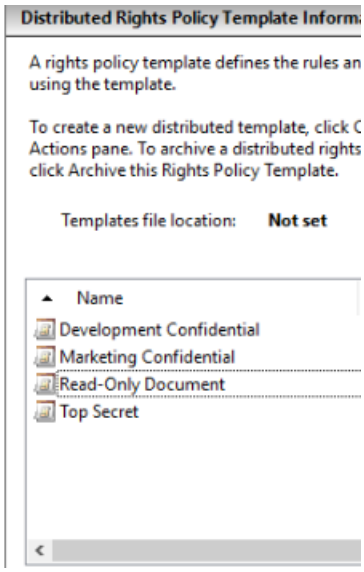


Рисунок 3.7 – Конфігурація обмежень функціональності у шаблонах прав

Для забезпечення коректного функціонування криптографічного захисту в умовах використання самопідписаного сертифіката було виконано процедуру встановлення довіри на стороні клієнтських машин. Публічну частину сертифіката кластера AD RMS було експортовано у файл стандарту X.509 із розширенням .cer. Цей файл було дистрибуйовано та імпортовано до сховища «Довірені кореневі центри сертифікації» (Trusted Root Certification Authorities) на кожній робочій станції домену. Ця операція дозволила уникнути критичних помилок валідації SSL/TLS з'єднання, гарантуючи, що офісні додатки, такі як Microsoft Word та Excel, зможуть безперешкодно комунікувати із сервером ліцензування. Фінальним етапом налаштування клієнтського середовища стала примусова актуалізація конфігурації комп'ютерів через оновлення групових політик, що забезпечило миттєве застосування нових параметрів безпеки.

Підсумовуючи етап впровадження системи захисту, можна констатувати, що процес розгортання та базової конфігурації служби Active Directory Rights Management Services було успішно завершено. Обрана стратегія, що базується на використанні самопідписаного цифрового сертифіката, довела свою ефективність та доцільність в умовах лабораторного або тестового середовища, дозволивши реалізувати повноцінний криптографічний захист каналів зв'язку без залучення ресурсів на розгортання складної ієрархії корпоративного центру сертифікації. Розроблені та імплементовані шаблони політик прав були спроєктовані з урахуванням специфіки функціональних обов'язків та інформаційних потреб кожного департаменту. Такий диференційований підхід забезпечує створення надійного механізму управління цифровими правами, який дозволяє організації здійснювати гранулярний контроль над обігом, тиражуванням та використанням конфіденційних даних, мінімізуючи ризики внутрішніх загроз та несанкціонованого витоку інформації.

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальне завдання щодо побудови надійної системи розмежування доступу та захисту корпоративних даних від несанкціонованого розповсюдження.

Основні результати роботи полягають у наступному:

1. Проведено порівняльний аналіз моделей контролю доступу. Визначено, що для корпоративного сектору найбільш ефективним є поєднання рольової моделі з механізмами управління правами на контент, що реалізується технологією AD RMS.

2. Обґрунтовано вибір платформи віртуалізації Proxmox VE на базі гіпервізора KVM. Це рішення забезпечило високу продуктивність, економічну ефективність та можливості масштабування, що підтверджено порівняльним аналізом з VMware ESXi та Hyper-V.

3. Спроєктовано та реалізовано відмовостійку архітектуру мережі. Розгорнуто два контролери домену на базі Windows Server 2019, що забезпечує безперервність процесів аутентифікації та реплікації даних.

4. Впроваджено систему резервного копіювання на базі Proxmox Backup Server. Налаштовано регулярне створення інкрементних бекапів та механізми дедуплікації, що гарантує можливість швидкого аварійного відновлення критичних вузлів інфраструктури.

5. Виконано розгортання служби Active Directory Rights Management Services. В умовах тестового середовища успішно реалізовано схему захисту з використанням самопідписаних сертифікатів, що дозволило уникнути витрат на розгортання складного CA, зберігаючи при цьому шифрування каналів зв'язку.

6. Розроблено та впроваджено диференційовані шаблони політик прав. Створено політики які реалізують гранулярний контроль доступу.

Експериментально підтверджено блокування функцій друку, копіювання в буфер обміну та створення скріншотів для неавторизованих користувачів.

7. Проведено верифікацію роботи системи на клієнтських робочих станціях. Підтверджено, що захист залишається активним для документів незалежно від їх локації, а централізоване управління через групові політики забезпечує автоматичне застосування налаштувань безпеки.

Розроблена інфраструктура створює практичну основу для впровадження сучасних стандартів інформаційної безпеки та захисту інтелектуальної власності підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. W. Stallings. "Cryptography and Network Security: Principles and Practice." Pearson, 8th Edition (2020): 50-120. https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000003254.

2. B. Desmond et al. "Active Directory." O'Reilly Media, 5th Edition (2013): 15-200. https://www.oreilly.com/library/view/active-directory-5th/9781449361213/.

3. W. Ahmed. "Mastering Proxmox." Packt Publishing, 3rd Edition (2017): 45-112. https://www.packtpub.com/product/mastering-proxmox-third-edition/9781788397605.

4. J. Krause. "Mastering Windows Server 2019." Packt Publishing, 2nd Edition (2019): 210-265. https://www.packtpub.com/product/mastering-windows-server-2019-second-edition/9781789804539.

5. M. E. Whitman et al. "Principles of Information Security." Cengage Learning, 6th Edition (2018): 180-230. https://www.cengage.com/c/principles-of-information-security-6e-whitman/9781337102063/.

6. S. S. Nelson. "Proxmox High Availability." Packt Publishing (2015): 20-55. https://www.packtpub.com/product/proxmox-high-availability/9781785287862.

7. D. F. Ferraiolo et al. "Role-Based Access Control." Artech House, 2nd Edition (2007): 15-85. https://us.artechhouse.com/Role-Based-Access-Control-P108.aspx.

8. B. Komar. "Windows Server 2008 PKI and Certificate Security." Microsoft Press (2008): 300-350. https://www.microsoftpressstore.com/store/windows-server-2008-pki-and-certificate-security-9780735625174.

9. J. Moskowitz. "Group Policy: Fundamentals, Security, and the Managed Desktop." Sybex, 3rd Edition (2015): 80-145. https://www.wiley.com/en-us/Group+Policy%3A+Fundamentals%2C+Security%2C+and+the+Managed+Desktop%2C+3rd+Edition-p-9781119035574.

10. V. Hu et al. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." National Institute of Standards and Technology, Special Publication 800-162 (2014): 1-25. https://doi.org/10.6028/NIST.SP.800-162.

11. R. Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 3rd Edition (2020): 115-160. https://www.wiley.com/en-us/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787.

12. S. Harris et al. "CISSP All-in-One Exam Guide." McGraw-Hill Education, 9th Edition (2021): 650-710. https://www.mhprofessional.com/cissp-all-in-one-exam-guide-ninth-edition-harris-maymi/9781260467376.

13. C. C. Palmer. "Ethical Hacking and Network Defense." Cengage Learning, 4th Edition (2022): 150-195. https://www.cengage.com/c/ethical-hacking-and-network-defense-4e-simpson/9780357508411.

14. J. P. Savill. "Mastering Microsoft Azure Infrastructure Services." Sybex (2015): 90-120. https://www.wiley.com/en-us/Mastering+Microsoft+Azure+Infrastructure+Services-p-9781119003290.

15. Joint Task Force. "Security and Privacy Controls for Information Systems and Organizations." National Institute of Standards and Technology, Special Publication 800-53 Rev. 5 (2020): 45-80. https://doi.org/10.6028/NIST.SP.800-53r5.

16. M. Bishop. "Computer Security: Art and Science." Addison-Wesley Professional, 2nd Edition (2018): 30-75. https://www.informit.com/store/computer-security-art-and-science-9780321712332.

17. D. S. H. Rosenthal. "Digital Preservation." MIT Press (2015): 10-40. https://mitpress.mit.edu/9780262536837/digital-preservation/.

18. International Organization for Standardization. "Information technology — Security techniques — Information security management systems — Requirements." ISO/IEC 27001:2013 (2013): 5-15. https://www.iso.org/standard/54534.html.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)