

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми управління доступом до
даних за допомогою Active Directory Rights Management
Services у віртуалізованому середовищі на базі
Proxmox»

Виконав: студент 4-го курсу групи КІ-21-1
спеціальності 123 «Комп'ютерна інженерія»



Даниїл ШЕЙКО

Керівник: доцент кафедри КІ та КБ, к.пед.н., доцент



Олена ГОЛОВНЯ

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



Олексій ШЕЛУХА

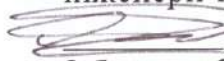
Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Шейко Даниїл Костянтинович

Тема роботи: «Проект підсистеми управління доступом до даних за допомогою
Active Directory Rights Management Services у віртуалізованому середовищі на
базі Proxmox »

затверджена Наказом університету від 3 березня 2025 р. № 97/с

Термін здачі студентом закінченої роботи 9 червня 2025 р.

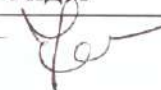
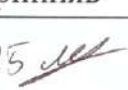
Вихідні дані роботи:

Технології управління доступом до даних у корпоративному середовищі, зокрема засоби впровадження Active Directory Rights Management Services (AD RMS) у віртуальній інфраструктурі на базі Proxmox. Інформаційна система підприємства з централізованим управлінням обліковими записами та правами доступу, побудована з використанням Active Directory, AD RMS, Windows Server 2019 та клієнтських систем Windows 10 у віртуальному середовищі.

Обладнання та програмне забезпечення:

1. Робоча станція HP Z840
2. Windows server 2019
3. Windows 10
4. Proxmox VE

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І.Г.	03.03.25 	06.03.2025 

Студент Даниїл ШЕЙКО

Керівник Олена ГОЛОВНЯ



Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025-13.03.2025	
2	Написання вступної частини кваліфікаційної роботи	01.04.2025-05.04.2025	
3	Аналіз основних теоретичних відомостей.	05.04.2025-30.04.2025	
4	Вибір обладнання на технологій	30.04.2025-07.05.2025	
5	Проектування мережі	07.05.2025-20.05.2025	
6	Налаштування мережі для впровадження обраних технологій	20.05.2025-31.05.2025	
7	Написання висновків	31.05.2025-06.06.2025	
8	Оформлення кваліфікаційної роботи	06.06.2025-19.06.2025	
9	Підготовка презентації до захисту	19.06.2025-20.06.2025	

Студент Даниїл ШЕЙКО

Керівник Олена ГОЛОВНЯ




АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи на тему «Проект підсистеми управління доступом до даних за допомогою Active Directory Rights Management Services у віртуалізованому середовищі на базі Proxmox» складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Пояснювальна записка містить 58 сторінок, з них 2 сторінки додатків. В роботі наведено 16 рисунків та 4 таблиці. Список використаних джерел містить 14 найменувань і займає 2 сторінки.

Метою кваліфікаційної роботи є розробка та впровадження підсистеми управління доступом до даних на основі Active Directory RMS у віртуальному середовищі для забезпечення безпеки корпоративної інформації.

Проаналізовано базові принципи роботи служби Active Directory та технології управління правами доступу AD RMS. Показано розробку повноцінної мережевої інфраструктури із двома серверами (основним і реплікаційним) та кількома клієнтськими машинами. Наведено результати тестування шаблонів політик доступу та перевірки обмежень на документи Microsoft Office.

Ключові слова: AD, RMS, Сервер, Proxmox, Backup, Доступ до даних.

					ККІКБ.КР.Б – 123 – 17 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми управління доступом до даних за допомогою Active Directory Rights Management Services у віртуалізованому середовищі на базі Proxmox	Літ.	Арк.	Аркуші	
Розроб.		Шейко Д. К.		20.06.25					
Керівник		Головня О. С.		20.06.25			4	58	
Реценз.		Шелуха О. О.		10.06.25		ФІКТ, Гр. К1-21-1			
Н. контр.		Головня О. С.		20.06.25					
Затверд.		Сфіменко А. А.		20.06.25					

ANNOTATION

The explanatory note to the qualification thesis on the topic “Data Access Management Using Active Directory Rights Management Services in a Virtualized Environment Based on Proxmox” consists of an introduction, three chapters, conclusions, a list of references, and appendices. The explanatory note comprises 56 pages, including 2 pages of appendices. The work contains 11 figures and 4 tables. The list of references includes 10 sources and occupies 1 page.

The goal of the thesis is the development, implementation, and testing of a data access management system based on Active Directory Rights Management Services (AD RMS) in a Proxmox virtual environment using Active Directory infrastructure and backup functionality.

The thesis analyzes the basic principles of Active Directory services and AD RMS access rights management technology. A complete network infrastructure is presented, including two servers (a primary and a replica) and several client machines. The results of testing access policy templates and enforcing restrictions on Microsoft Office documents are provided.

Keywords: AD, RMS, Server, Proxmox, Backup, Data Access.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 Теоретичні основи управління доступом до даних	9
1.1 Поняття та основні принципи управління доступом до даних.....	9
1.2 Технології захисту інформації у корпоративному середовищі	12
1.3 Теоретичні основи Active Directory та його роль у захисті даних.....	14
1.4 Огляд Active Directory Rights Management Services	18
1.5 Proxmox Backup Server: призначення, архітектура, можливості в інфраструктурі управління доступом до даних.	20
РОЗДІЛ 2 Проєктування інфраструктури AD RMS для корпоративної мережі.	24
2.1 Аналіз вимог для впровадження AD RMS	24
2.2 Обґрунтування вибору Active Directory	26
2.3 Вибір віртуального середовища та програмного забезпечення	28
РОЗДІЛ 3 РОЗРОБКА ТА ТЕСТУВАННЯ МЕРЕЖІ ТА СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ ДО ДАНИХ.....	39
3.1 Розгортання віртуального середовища	39
3.2 Створення домену Active Directory.....	42
3.3 Впровадження служби Active Directory Rights Management Services	45
3.4 Тестування роботи Active Directory Rights Management Services.....	47
3.5 Забезпечення та тестування резервного копіювання та відновлення даних за допомогою Proxmox Backup Server.....	49
ВИСНОВКИ	54
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	56
ДОДАТКИ	58

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

AD – Active Directory

AD RMS – Active Directory Rights Management Services

PBS – Proxmox Backup Server

DHCP – Dynamic Host Configuration Protocol

AD CS – Active Directory Certificate Services

GUI – Graphical User Interface (графічний інтерфейс користувача)

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Управління доступом до даних є однією з ключових задач сучасних інформаційних систем, що забезпечує захист конфіденційної інформації та підтримує контроль над її розповсюдженням. У сучасному світі, цифровізація документів і процесів стрімко зростає, тому питання інформаційної безпеки набуває особливої актуальності. Завдяки впровадженню Active Directory Rights Management Services (AD RMS) відкриваються можливості для залучення ефективних механізмів захисту корпоративних даних від несанкціонованого доступу та витоку.

Метою кваліфікаційної роботи є розробка та впровадження підсистеми управління доступом до даних на основі Active Directory RMS у віртуальному середовищі для забезпечення безпеки корпоративної інформації.

Визначена мета обумовлює наступні завдання:

- проаналізувати існуючі технології управління доступом в корпоративному середовищі;
- дослідити принципи функціонування та структуру AD RMS;
- спроектувати віртуальну інфраструктуру для розгортання служби AD RMS;
- реалізувати та протестувати систему управління доступом до даних.

Об'єктом дослідження є інформаційна інфраструктура підприємства з елементами централізованого управління доступом до даних.

Предметом дослідження є технології та засоби забезпечення захисту даних за допомогою Active Directory RMS у віртуалізованому середовищі.

У процесі виконання кваліфікаційної роботи було розроблено проект інтегрованої підсистеми управління доступом до даних з використанням AD RMS у віртуальному середовищі Proxmox із підтримкою резервного копіювання даних через Proxmox Backup Server.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 Теоретичні основи управління доступом до даних

1.1 Поняття та основні принципи управління доступом до даних

Управління доступом до даних є і надалі завжди буде важливим аспектом сучасних інформаційних систем, основна мета якого спрямована на захист конфіденційної інформації, контроль її використання та розповсюдження. Ефективне та коректне управління доступом може гарантувати цілісність, конфіденційність та доступність даних.

Управління доступом визначає, хто і в який спосіб може взаємодіяти з певною інформацією. У цій галузі є декілька основних понять: ідентифікація, аутентифікація, авторизація, та контроль доступу

Ідентифікація — процес визначення особи, яка намагається отримати доступ до системи або ресурсу.

Аутентифікація — перевірка достовірності ідентифікаційної інформації (наприклад, пароля, сертифіката тощо).

Авторизація — визначення прав та привілеїв, які має користувач або система щодо доступу до конкретного ресурсу.

Контроль доступу — процес забезпечення виконання політик безпеки, які визначають, хто може отримати доступ до ресурсів і як вони можуть їх використовувати.

Для забезпечення надійного управління доступом до даних варто використовувати принцип найменших привілеїв (Least Privilege). Цей принцип наголошує що користувачам надаються лише ті права, які необхідні для виконання їхніх завдань. Це знижує ризик зловживання привілеями. Також варто не забувати про принцип розподілу обов'язків (Separation of Duties), що вимагає розподіляти критичні операції між декількома користувачами, для того щоб зменшувати ризики шахрайства або помилок. Хорошою практикою є дотримання принципу контролю на основі ролей (Role-Based Access Control, RBAC). Цей принцип передбачає надання доступу залежно від ролі користувача в організації, а не індивідуально для кожного. Ну і,

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

звісно, варто згадати про аудит і моніторинг: постійний контроль та логування доступу до даних дозволяє виявляти спроби порушення політик безпеки, та виявити помилки.

Залежно від способу реалізації, можна виокремити наступні моделі контролю доступу: дискреційний контроль доступу, мандатний контроль, контроль доступу на основі атрибутів.

Дискреційний контроль доступу (Discretionary Access Control, DAC). Заснований на тому, що власник ресурсу повинен мати у повний контроль над тим, хто і як отримує доступ до ресурсу, та які права матиме. Реалізується шляхом створення списків доступу (Access Control Lists, ACL), де вказані права кожного користувача. Може використовуватись у невеликих системах, де контроль над доступом здійснюється вручну. Основним недоліком є послаблення безпеки, оскільки користувачі можуть навмисно або помилково надавати доступ небажаним особам. Застосовується переважно в операційних системах Windows та Unix. Прикладом використання є файли або папки у Windows, для яких власник може сам визначати, хто має права на читання, запис, виконання та інші дії, через властивості об'єкта.

Мандатний контроль доступу (Mandatory Access Control, MAC). Ця модель передбачає централізований контроль над доступом до ресурсів, за якого політики доступу встановлюються адміністраторами системи.

Усі політики доступу базуються на раніше встановлених рівнях конфіденційності (наприклад, “Секретно”, “Конфіденційно”, “Тільки для керівництва” і т.п.). Користувачі мають певні рівні дозволів, а доступ до ресурсів визначається шляхом порівняння користувача з рівнем ресурсу. Цей спосіб вважається більш безпечним, оскільки користувачі не можуть самотійно змінювати права доступу, що викорінює можливість користувачів навмисно або випадково надавати доступ небажаним користувачам. Недоліком можна вважати складності впровадження та адміністрування. Частіше використовується в системах з високими вимогами до безпеки, таких як військові або урядові системи. Приклад використання - MAC у операційній системі SELinux де права доступу строго контролюються заздалегідь заданими політиками.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC).Ця модель вважається сучасною та гнучкою, у ній доступ до ресурсів надається на основі набору атрибутів. Вони можуть стосуватися користувача (роль, посада, відділ), ресурсу (тип, власник), дій (читання, запис) або середовища (час, місце, пристрій). Рішення про доступи до файлів ухвалюється динамічно на основі логічних умов, які заздалегіть визначені адміністраторами. Цей підхід вважається підходящим для складних систем із великою кількістю змінних і вимог до безпеки. Основним недоліком є — висока складність налаштування і висока потреба операційної потужності.Приклад використання: хмарні платформи (AWS, Microsoft Azure), де доступи до ресурсів надаються залежно від різних атрибутів, наприклад таких як географічне розташування користувача або час доби.

Контроль доступу на основі ролей (Role-Based Access Control, RBAC). У цій моделі права доступу призначаються не окремим користувачам, а заздалегіть визначеним ролям (адміністратор, бухгалтер, аналітик тощо). Кожна роль містить перелік дозволених операцій із ресурсами, а користувач одержує доступ до об'єктів автоматично після призначення йому відповідної ролі. Такий підхід спрощує адміністрування у середовищах із великою кількістю співробітників: змінюючи набір дозволів у ролі, адміністратор одразу коригує доступ сотням користувачів, не редагуючи кожен обліковий запис окремо. Перевагами RBAC є прозорість і простота налаштування, а також зменшення ризику випадкового надання зайвих прав. Недоліком вважають обмежену гнучкість порівняно з ABAC: для нетипових сценаріїв часто доводиться створювати додаткові ролі, що ускладнює структуру. Приклад використання: Active Directory в організаціях, де ролі «Domain Admins», «HR Managers» чи «Developers» визначають, які файли, сервери або програми можуть використовувати працівники. [3]

Надану інформацію можна структурувати у невеличку таблицьку (таблиця 1.1)

Таблиця 1.1

Порівняння моделей контролів доступу

Характеристика	DAC	MAC	ABAC	RBAC
----------------	-----	-----	------	------

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Гнучкість	Висока	Низька	Дуже висока	Середня
Рівень безпеки	Середній	Високий	Високий	Високий
Адміністрування	Просте	Складне	Складне	Просте
Централізований контроль	Немає	Є	Є	Є
Сфери застосування	Малі організації	Високосекретні системи	Хмарні платформи, корпоративні мережі	Бізнес, корпоративні ІТ-системи, Active Directory

1.2 Технології захисту інформації у корпоративному середовищі

Технології захисту інформації в корпоративному середовищі охоплюють широкий спектр засобів, методів та інструментів, що спрямовані на захист конфіденційності, цілісності та доступності даних користувачів та організації. Virізняється декілька основних категорій таких технологій – криптографія, засоби управління доступом, захист кінцевих пристроїв, захист втрати даних, резервне копіювання, політики безпеки та навчання співробітників.

Криптографія включає – шифрування інформації на дисках і в переданих повідомленнях, цифрові підписи для автентифікації користувачів та перевірки цілісності даних, а також такі протоколи як SSL (Secure Sockets Layer) та TLS (Transport Layer Security). Це криптографічні протоколи, що забезпечують захищене спілкування для клієнтських та серверних додатків через інтернет. Вони забезпечують конфіденційність, цілісність та автентичність даних що проходять між веб-браузером та сервером.

Принцип роботи SSL/TLS є наступним. Спершу відбувається автентифікація. При встановленні з'єднання між клієнтом і сервером провокується перевірка автентичності сервера. Сервер надає свій сертифікат SSL/TLS, який містить у собі публічний ключ та інформацію про його довіру (за допомогою сертифікаційних центрів, що підписують цей сертифікат). Це дозволяє клієнту переконатися, що підключення до серверу є не підробленим.(для захисту від атаки "man-in-the-middle"). Далі

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

здійснюється шифрування. Одразу після аутентифікації клієнт і сервер домовляються про спільний ключ, що використовуватиметься для шифрування даних що будуть передані. Таке шифрування дозволяє гарантувати, що зломисник не зможе прочитати повідомлення навіть, якщо перехопить його. Шифрування за допомогою симетричних ключів значно швидше за асиметричне (яке використовує пари публічних і приватних ключів), тому саме симетричне шифрування використовується для з'єднання, на томість асиметричне — лише для початкового обміну ключами. SSL/TLS також забезпечують цілісність даних. Протокол використовує хеш-функції, завдяки яким проходить перевірка, що дані не були змінені під час передачі. Це означає, що передані дані не можуть бути непомітно змінені.

Засоби управління доступом – це технології що контролюють, хто може отримати доступ до яких ресурсів. До основних засобів, які працюючи в комплексі, забезпечують управління доступом у Windows-системах, належать: Active Directory, RBAC (Role-Based Access Control), MFA (Multi-Factor Authentication), Active Directory RMS. *Active Directory* використовується для централізованого управління обліковими записами та правами доступу. *Role-Based Access Control* — це модель управління доступом, в котрій права доступу користувачів визначаються на основі їхніх ролей в організації. Ця модель доступу дозволяє централізовано управляти правами доступу, зменшуючи складність адміністрування та підвищуючи безпеку. *Multi-Factor Authentication* (багатофакторна автентифікація) вимагає кілька методів підтвердження особи, наприклад, таких як пароль, одноразові коди або біометричні дані, для підвищення безпеки доступу. *Rights Management Services* є системою, що забезпечує захист інформації, дозволяючи організаціям контролювати, хто може отримувати доступ до документів і електронних листів, а також які операції можна виконувати з цими даними (наприклад, перегляд, редагування, копіювання або пересилання). Це дозволяє зберігати конфіденційність інформації, навіть якщо вона залишає організацію. До технологій захисту кінцевих пристроїв належать: антивірусні програми (для захисту від шкідливих програм і вірусів); фаєрволи на кінцевих пристроях(дозволяють контролювати вхідний та вихідний трафік); системи уп-

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

равління мобільними пристроями (для захисту мобільних пристроїв на кшталт смартфонів, планшетів і ноутбуків, підключених до корпоративної мережі); системи виявлення і запобігання вторгненням (виявляють аномальні активності на кінцевих пристроях), а також комплекси рішень, такі як EDR та XDR- *Захист від втрати даних* (Data Loss Prevention) це технології, які виявляють та запобігають витоку конфіденційної інформації за допомогою моніторингу (передавання даних у мережі, виявлення несанкціонованих спроб передавання інформації); шифрування даних (для захисту їх на носіях або під час пересилання), політик безпеки (для заборони копіювання, передачі або доступу до чутливої інформації без дозволу). *Резервне копіювання та відновлення* - це технології, що гарантують відновлення даних у випадку їх втрати що здійснюються на основі систем резервного копіювання для збереження копій даних. Це використовується для відновлення даних після збоїв або кібератак, для аварійного відновлення (Disaster Recovery) для відновлення функціонування критичних бізнес-процесів після інцидентів. *Політики безпеки та навчання співробітників* перелбчають інструкції та політики безпеки для визначення правил доступу до даних і технологій. Навчання користувачів з безпеки для зниження ризику людських помилок, що можуть призвести до витоку або втрати даних. [10]

Комплексне впровадження цих технологій дозволяє підвищити рівень безпеки корпоративних систем, а також забезпечити конфіденційність даних і запобігти втратам інформації.

1.3 Теоретичні основи Active Directory та його роль у захисті даних

Active Directory (AD) — це централізована служба каталогів, розроблена компанією Microsoft, яка використовується для управління користувачами, комп'ютерами та ресурсами в корпоративних мережах. Ця технологія дозволяє адміністраторам налаштовувати права доступу, організовувати об'єкти в логічні структури та забезпечувати аутентифікацію й авторизацію в межах організації. Головною особливістю AD є її ієрархічна будова, що дає змогу ефективно організовувати мережеве середовище та централізовано керувати ресурсами.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Структуру Active Directory можна представити як декілька ключових компонентів. Домен є основною адміністративною одиницею, що об'єднує користувачів, комп'ютери та інші об'єкти під єдиним простором імен. Контролер домену (Domain Controller, DC) є сервером, який зберігає базу даних AD, обробляє запити на аутентифікацію та авторизацію, а також забезпечує реплікацію змін між іншими контролерами домену. Вищий рівень структури AD представлений лісом (forest), який може містити один домен або кілька взаємопов'язаних доменів. Усередині лісу домени можуть утворювати дерево (tree), якщо вони поділяють спільний простір імен. Для логічної організації ресурсів використовується організаційна одиниця (Organizational Unit, OU), яка дозволяє групувати користувачів, комп'ютери й групи в межах домену, що спрощує керування правами та політиками безпеки.

Active Directory відіграє важливу роль у централізованому управлінні корпоративною мережею. Вона дозволяє автоматизувати процеси створення та налаштування облікових записів, реалізовувати групові політики для контролю параметрів операційної системи та забезпечувати єдиний механізм аутентифікації користувачів у межах усієї інфраструктури. Завдяки AD адміністратори можуть швидко змінювати політики доступу, забезпечуючи баланс між безпекою та зручністю користування ресурсами. Крім того, AD тісно інтегрується з іншими службами, такими як DNS, DHCP та AD RMS, що дозволяє створювати комплексні рішення для захисту даних і управління інформаційною безпекою в організації.

Однією з основних функцій Active Directory є аутентифікація та авторизація користувачів. Кожен користувач, який хоче отримати доступ до корпоративної мережі, проходить перевірку облікових даних через контролер домену, що підтверджує його особу. Після успішної аутентифікації система визначає рівень доступу, який надано користувачу, відповідно до його членства в певних групах та налаштованих політик безпеки. Цей механізм дозволяє централізовано керувати правами доступу та забезпечувати високий рівень безпеки.

Active Directory також містить потужний інструмент для адміністраторів – групові політики (Group Policy Objects, GPO). Вони дозволяють автоматизовано налаштовувати параметри операційних систем та програмного забезпечення на всіх

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

пристроях, що входять до домену. За допомогою GPO можна встановлювати правила використання паролів, обмежувати доступ до певних функцій, налаштовувати мережеві параметри та навіть встановлювати додатки. Це забезпечує єдині стандарти безпеки в межах компанії та значно спрощує адміністрування великої кількості пристроїв.[8]

Важливою перевагою Active Directory є її інтеграція з іншими службами Microsoft, такими як DNS, DHCP, Exchange та AD RMS. Взаємодія з DNS дозволяє автоматично реєструвати й знаходити мережеві ресурси, що спрощує управління інфраструктурою. DHCP, у свою чергу, забезпечує автоматичну видачу IP-адрес пристроям у мережі, що полегшує керування адресним простором. Exchange використовує дані з AD для організації електронної пошти та контактних записів користувачів, а AD RMS (Active Directory Rights Management Services) допомагає захищати конфіденційну інформацію за допомогою механізмів шифрування та контролю доступу.

Завдяки цим функціональним можливостям Active Directory є ключовим компонентом корпоративних мереж, що забезпечує зручне та безпечне управління користувачами, пристроями та ресурсами організації.

Active Directory відіграє ключову роль у забезпеченні інформаційної безпеки корпоративної мережі, оскільки надає потужні механізми контролю доступу, та є фундаментом для впровадження служби автентифікації, авторизації, централізованого управління політиками безпеки, а також базою для інтеграції з іншими сервісами захисту даних.

Адміністратори можуть створювати групи користувачів, кожній з яких надаються певні рівні дозволів для доступу до ресурсів мережі. Наприклад, розробники можуть мати права на зміну вихідного коду, у той час як HR-департамент отримує доступ до конфіденційних даних співробітників. Використання груп дозволяє мінімізувати ризики несанкціонованого доступу та значно спрощує управління правами користувачів.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Ще одним важливим аспектом безпеки є аудит подій і журналювання для виявлення потенційних загроз. Active Directory дозволяє збирати та аналізувати інформацію про всі дії користувачів і адміністраторів у мережі. Це включає вхід у систему, зміну прав доступу, спроби доступу до ресурсів та інші критичні події. Використовуючи централізовані журнали подій, адміністратори можуть швидко виявляти підозрілі дії, такі як багаторазові невдалі спроби входу або несанкціоновані зміни в політиках безпеки. Такі механізми дозволяють реагувати на загрози та запобігати кібератакам.

Завдяки гнучким інструментам контролю доступу, технологіям шифрування та розширеним можливостям моніторингу, Active Directory є фундаментальним компонентом інформаційної безпеки сучасних Windows-мереж, що дозволяє ефективно управляти ризиками та забезпечувати захист корпоративних даних.

Active Directory (AD) є основою для впровадження Active Directory Rights Management Services (AD RMS), оскільки забезпечує централізоване управління користувачами, групами, пристроями та політиками доступу. Без AD неможливо належним чином реалізувати механізми контролю прав на документи та ресурси, оскільки саме AD відповідає за автентифікацію та авторизацію користувачів у корпоративному середовищі.[1]

Однією з ключових причин, чому AD є критично важливим для AD RMS, є можливість використання централізованого управління ідентифікацією та доступом. AD дозволяє визначати, які користувачі та групи можуть отримувати певні дозволи на документи, які захищає AD RMS. Завдяки інтеграції з доменними групами адміністратори можуть легко налаштовувати права доступу на основі вже існуючих політик безпеки в організації. Це спрощує адміністрування та зменшує ризики помилок при наданні прав доступу.

Крім того, AD забезпечує механізм автентифікації користувачів перед тим, як AD RMS застосує політики управління правами доступу до документів. Якщо користувач не входить до домену або не має відповідних облікових даних, він не

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

зможеть отримати доступ до захищеного контенту. Це дозволяє ефективно обмежувати можливості несанкціонованого доступу, навіть якщо документ потрапить за межі корпоративної мережі.

Ще одним важливим аспектом є використання групових політик (GPO) в Active Directory для централізованого управління налаштуваннями AD RMS на клієнтських пристроях. Адміністратори можуть автоматично розгортати необхідні конфігурації, забезпечуючи належний рівень безпеки та контроль над процесом шифрування й розподілу прав.

Завдяки інтеграції AD RMS з AD також можливе ведення детального аудиту дій користувачів. Усі спроби доступу до захищених документів можуть бути відстежені та проаналізовані, що є важливим елементом забезпечення інформаційної безпеки.

1.4 Огляд Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) — це серверна технологія, що може забезпечити захист інформації, дозволяючи організаціям гнучко контролювати доступ до конфіденційних даних і документів. AD RMS може не тільки регулювати, хто може отримати доступ до інформації, але й встановлює умови її використання, та розповсюдження. До цих умов можуть входити, заборона копіювання, друк або пересилання. Цей сервіс є важливою частиною загальної екосистеми Active Directory і відповідає сучасним вимогам до захисту корпоративних даних.

Основне завдання AD RMS — надати організаціям можливість захищати дані не тільки в середині, а й навіть за межами корпоративного середовища. Доприкладу, якщо конфіденційний документ був переданий зовнішньому партнеру, права на доступ і використання цього документа залишаються під контролем компанії-власника.

Архітектура AD RMS складається з декількох ключових компонентів, які забезпечують правильну роботу, та функціональність. AD RMS Cluster— це набір

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

серверів AD RMS, які працюють разом для забезпечення високої доступності. Кожен сервер відповідає за видачу ліцензій та ключів шифрування, і має однакові налаштування. В основі роботи AD RMS лежать сертифікати та. Сертифікати та ключі використовуються для захисту даних, видачі прав доступу та підтвердження ідентичності користувачів. AD RMS тісно інтегрується з Active Directory, використовуючи її як базу для автентифікації користувачів і груп, а також для призначення прав доступу. На клієнтських пристроях встановлюється спеціальне програмне забезпечення, яке дозволяє працювати з файлами, захищеними AD RMS. Цей компонент відповідає за перевірку прав користувача та виконання політик безпеки. Політики доступу до даних зберігаються в централізованій базі, і кожен запит до захищеного документа перевіряється відповідно до цих політик.

AD RMS пропонує широкий набір функцій для захисту інформації. Документи, що захищаються AD RMS, шифруються, і доступ до них можуть отримати лише ті користувачі, які мають відповідні ключі та права. Адміністратори можуть точно визначати, які користувачі і що саме можуть робити з документами: читати, редагувати, друкувати, копіювати або пересилати. Наприклад, можна надати доступ лише для перегляду без можливості друку або збереження копії, для окремих груп користувачів. AD RMS інтегрується з Microsoft Exchange, що дозволяє захищати електронну пошту. Це особливо важливо для конфіденційного листування для користувачів. Адміністратори можуть встановлювати термін дії доступу до даних. Після закінчення цього терміну файл стає недоступним. AD RMS дозволяє вести журнали використання документів. Це допомагає виявляти порушення політик безпеки завдяки інформації, з'ясовуючи, хто, коли і з якою метою отримував доступ до документів. Завдяки AD RMS користувачі можуть безпечно співпрацювати над документами, знаючи, що їх вміст захищений навіть після передачі зовнішнім партнерам. Ця технологія також може працювати у зв'язці з іншими продуктами Microsoft, такими як Office, SharePoint і Exchange, що забезпечує безшовну інтеграцію та легкість використання.

Варто підсумувати переваги використання AD RMS.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- *Захист даних незалежно від їхнього розташування.* Інформація залишається захищеною навіть після виходу за межі корпоративної мережі.
- *Гнучке управління доступом.* Адміністратори можуть визначати правила доступу на основі ролей, ідентифікацій користувачів або груп.
- *Спрощення процесів відповідності стандартам.* Цей інструмент допомагає організаціям відповідати вимогам щодо конфіденційності та безпеки, таким як GDPR, HIPAA, ISO 27001.
- *Інтеграція з іншими службами.* Платформа забезпечує зручну роботу в екосистемі Microsoft, дозволяючи безшовно впроваджувати політики захисту.
- *Підтримка різних типів контенту.* RMS забезпечує захист текстових документів, електронних таблиць, презентацій, електронної пошти та інших типів файлів.

Отже, використання AD RMS дозволяє компаніям створити надійне середовище для роботи з даними, що сприяє підвищенню ефективності роботи, зменшенню ризиків і забезпеченню дотримання стандартів безпеки.

1.5 Proxmox Backup Server: призначення, архітектура, можливості в інфраструктурі управління доступом до даних.

У сучасному корпоративному середовищі забезпечення надійного резервного копіювання та відновлення критично важливої інформації є невід'ємною частиною побудови системи управління доступом до даних. Одним із ефективних інструментів для цього завдання є Proxmox Backup Server (PBS) — спеціалізоване рішення з відкритим кодом, яке забезпечує повноцінне резервне копіювання віртуальних машин, контейнерів, а також фізичних серверів, використовуючи сучасні технології стиснення, дедуплікації та шифрування даних.

Proxmox Backup Server розроблено як централізований сервер резервного копіювання, тісно інтегрований з Proxmox Virtual Environment (Proxmox VE, PVE), але також придатний для використання в будь-якій ІТ-інфраструктурі, яка потребує зберігання великих обсягів резервних копій. Основна мета PBS — захист від втрати

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

даних у випадку збою обладнання, зловмисних атак, людських факторів або інших критичних подій.[13]

У системах, де впроваджено Active Directory та Active Directory Rights Management Services (AD RMS), резервне копіювання має особливе значення, адже порушення цілісності чи втрата даних на контролерах домену або серверах політик доступу може повністю зупинити роботу організації.

PBS використовує архітектуру типу клієнт-сервер. Серверна частина приймає резервні копії по захищеному протоколу (HTTPS), які надсилаються з клієнтів, що можуть бути як окремими машинами, так і вузлами PVE. Зберігання даних реалізовано через сховище типу Datastore, яке може знаходитись на локальному або мережевому носії.

Ключові компоненти PBS є наступними.

Datastore — логічне сховище для резервних копій, яке підтримує дедуплікацію.

Backup client (pve-client або proxmox-backup-client) — програма, яка здійснює копіювання даних.

Pruning — механізм очищення старих або непотрібних резервних копій за заданим розкладом.

Verification — регулярна перевірка цілісності резервних даних.

Access control (ACL) — система керування доступом до репозиторіїв, що дозволяє обмежити права користувачів.

Proxmox Backup Server підтримує низку опцій для оптимізації процесів резервного копіювання, підвищення їх надійності та захищеності, зокрема наступні.

- Інкрементне резервне копіювання на рівні блоків — зменшує обсяг збережених даних та пришвидшує процес копіювання.
- Дедуплікація — унікальні блоки зберігаються один раз, що суттєво економить місце.
- Стиснення — підтримка алгоритмів Zstandard (zstd), LZ4 тощо для оптимізації розміру копій.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- Шифрування — резервні копії можуть шифруватися за допомогою AES-256, зберігаючи безпеку навіть при фізичному доступі до сховища.
- Автоматичне очищення та верифікація — планувальник дозволяє автоматизувати ці процеси.
- Інтеграція з Proxmox VE — через інтерфейс Proxmox можна створювати завдання резервного копіювання, відновлення, моніторити статуси.

У межах побудови інфраструктури з AD RMS, Proxmox Backup Server виконує стратегічну роль за наступними напрямками.

1) Створення регулярних резервних копій серверів Active Directory гарантує відновлення структури користувачів, політик GPO та OU.

2) Резервне копіювання сервера AD RMS дозволяє зберегти всі налаштування кластеру, сертифікати, SCP-записи, політики прав доступу.

3) У випадку порушення системи (наприклад, втрата реплікаційного RMS-сервера), PBS дозволяє швидко відновити повноцінну працездатність без втрати політик або доступу до документів.

4) Автоматизоване збереження копій дозволяє тестувати нові шаблони AD RMS або впроваджувати зміни з можливістю швидкого “відкату”.

Таким чином, PBS — це не просто інструмент резервного копіювання, а ключовий елемент безпеки та надійності системи захисту корпоративних даних у середовищі Windows Server та Active Directory.

Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи управління доступом до даних, а також актуальні технології, що забезпечують захист інформації в корпоративному середовищі.

Проаналізовано ключові поняття управління доступом, серед яких найважливішими є принципи мінімальних привілеїв, розмежування доступу та централізоване адміністрування. Було встановлено, що забезпечення інформаційної безпеки неможливе без впровадження політик контролю доступу до ресурсів.

Розглянуто основні технології захисту даних, які застосовуються в корпоративних мережах, включаючи шифрування, автентифікацію, багаторівневий захист

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

та систему контролю доступу на основі ролей. Особливу увагу приділено інфраструктурі Microsoft, зокрема — Active Directory як фундаменту для впровадження централізованої моделі управління ресурсами.

Вивчено теоретичний функціонал Active Directory Rights Management Services, що дозволяє створювати політики захисту документів на основі прав доступу, а також обмеження на перегляд, зміну, копіювання чи друк документів. Показано, що AD RMS є ефективним рішенням для контролю над розповсюдженням конфіденційної інформації.

Окремо було проаналізовано Proxmox Backup Server як сучасне рішення для резервного копіювання у віртуалізованому середовищі. Визначено його переваги — простота інтеграції, підтримка дедуплікації, зручна система збереження та відновлення даних, а також можливість централізованого адміністрування. У порівнянні з іншими аналогами (наприклад, Veeam, Acronis), PBS вирізняється відкритістю, відсутністю ліцензійних обмежень та гарною підтримкою середовища Proxmox.

Таким чином, у розділі сформовано теоретичне підґрунтя для практичної реалізації проекту побудови інфраструктури захисту доступу до даних на базі Active Directory, AD RMS та засобів резервного копіювання.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

РОЗДІЛ 2 Проєктування інфраструктури AD RMS для корпоративної мережі.

2.1 Аналіз вимог для впровадження AD RMS

Для того щоб ефективно використовувати AR RMS варто провести детальний аналіз потреб компанії, та вимог до системи. Після такого аналізу можна визначити вимоги до політик безпеки, масштаб і навантаження на систему, архітектуру мережі.

Проєктування інфраструктури AD RMS починається з аналізу бізнес-потреб організації, які безпосередньо впливають на вимоги до впровадження цієї технології. Організації, що працюють з конфіденційними даними, особливо потребують надійних механізмів захисту інформації. AD RMS дозволяє впроваджувати такі правила, що критично важливо для організацій, які прагнуть забезпечити дотримання нормативних актів та внутрішніх політик безпеки.

Вимоги до безпеки даних та управління доступом є одними з найважливіших аспектів. Організація повинна визначити рівні конфіденційності даних і політики доступу до них, потрібно враховувати потенційні загрози, включаючи внутрішніх та зовнішніх зловмисників. Це передбачає аналіз існуючої інфраструктури безпеки, рівня довіри до користувачів та партнерів, а також наявних інструментів для моніторингу й аудиту доступу до даних.

Розрахунок навантаження та масштабованості є наступним кроком у процесі аналізу. Для ефективного впровадження AD RMS необхідно оцінити кількість користувачів, які активно взаємодіятимуть із захищеними документами. Важливо врахувати не лише поточний стан справ, але й можливе зростання організації, яке може призвести до збільшення обсягу даних та кількості запитів до служби. Недооцінювання цих факторів може призвести до перевантаження серверів і, як наслідок, зниження продуктивності системи.

У процесі аналізу розраховуються рекомендовані ресурси для серверів AD RMS. Це включає потреби у процесорній потужності, обсязі оперативної пам'яті та місця на дисках для забезпечення стабільної роботи служби. Зокрема, необхідно

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

враховувати мінімальні вимоги, зазначені в технічній документації Microsoft, а також додатковий резерв ресурсів для пікових навантажень.

Окремо розглядається обґрунтування використання фізичних або віртуальних серверів. У невеликих організаціях може бути доцільним використання віртуальних середовищ, таких як Proxmox, оскільки це дозволяє зекономити кошти та забезпечити гнучкість у керуванні інфраструктурою. Однак, у випадках, коли високий рівень продуктивності та доступності є критично важливими, фізичні сервери можуть забезпечити кращі результати, оскільки вони не піддаються впливу обмежень віртуалізації.

Окрім технічних аспектів, необхідно врахувати відповідність AD RMS політикам безпеки організації та регуляторним вимогам, таким як GDPR або внутрішні корпоративні стандарти. Неправильне налаштування доступу або слабке управління політиками може призвести до порушень у безпеці та юридичних ризиків.

Нарешті, визначаються потреби в апаратному забезпеченні, включаючи обсяг пам'яті, кількість процесорних ядер та дисковий простір. Ці параметри залежать від масштабів організації, кількості активних користувачів та обсягу даних, що підлягають захисту. Важливо враховувати також резерв для майбутніх оновлень та розширення інфраструктури. Таким чином, якісний аналіз вимог до впровадження AD RMS є фундаментом для побудови ефективної, масштабованої та безпечної системи управління доступом до даних.

На основі проведеного аналізу було визначено оптимальну конфігурацію віртуальних машин для реалізації та тестування моделі підсистеми управління доступом. За потреби цю конфігурацію можна масштабувати для більшої мережі. Для забезпечення відмовостійкості та балансування навантаження використовуються два сервери Active Directory, кожен з яких має 8 віртуальних процесорів, 8 ГБ оперативної пам'яті та 100 ГБ дискового простору. Така конфігурація дозволяє стабільно обробляти запити на аутентифікацію, авторизацію та застосування політик безпеки.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Робочі станції користувачів, яких у системі передбачається 10 і більше, отримали розподілені ресурси у вигляді 12 віртуальних ядер процесора, 16 ГБ оперативної пам'яті та 60 ГБ дискового простору на кожную машину. Це забезпечує ефективну роботу користувачів з документами, що захищені AD RMS, і гарантує швидку обробку запитів на доступ до зашифрованих даних.

Окрему увагу приділено резервному копіюванню. Для цього було виділено окремий сервер Proxmox Backup Server, який має 4 процесорних ядра, 2 ГБ оперативної пам'яті та 500 ГБ дискового простору. Це дозволить регулярно створювати резервні копії та гарантувати швидке відновлення даних у разі збою. З урахуванням обсягу даних і частоти створення резервних копій, поточна конфігурація вважається достатньою, хоча у майбутньому може знадобитися збільшення оперативної пам'яті.

Таким чином, запропонована архітектура оптимально відповідає потребам цієї кваліфікаційної роботи, забезпечуючи належний рівень продуктивності та відмовостійкості системи AD RMS у віртуальному середовищі.

2.2 Обґрунтування вибору Active Directory

У сучасному корпоративному середовищі для управління доступом і каталогами використовуються різні технології. Active Directory (AD) — одна з найпоширеніших, але також існує багато альтернатив, такі як OpenLDAP, FreeIPA, Okta, JumpCloud, а також інші рішення. Розглянемо детальніше ці технології, їх особливості, переваги та недоліки.

Active Directory — це рішення від Microsoft для реалізації служби каталогів, яке є основою для централізованого управління ідентифікацією, доступом і ресурсами у корпоративних мережах. AD є універсальним для різних завдань управління доступом. AD пропонує багатий функціонал, включаючи управління груповими політиками, централізовану автентифікацію та управління ресурсами. Цей продукт є комерційним, що означає що він вимагає ліцензування, але це компенсується такими факторами як: високий рівень підтримки від Microsoft, часті оновлення, ши-

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

рокий набір інструментів для адміністрування. Його популярність у корпоративному середовищі можна пояснити багатим функціоналом, та можливістю масштабування для організацій різного розміру. Основна перевага AD — це інтеграція з продуктами Microsoft, такими як Exchange Server, SharePoint, Teams та Azure. Це дозволяє створити єдину екосистему для бізнесу. [14]

OpenLDAP є відкритим рішенням для реалізації служби каталогів, заснованим на одноіменному протоколі LDAP. Воно може підходити компаніям що шукають недорогі й масштабовані рішення, адже використання цього рішення може знизити витрати на підставі відсутності платних ліцензій. OpenLDAP забезпечує гнучкість у налаштуванні та підтримує інтеграцію з різними операційними системами, включаючи Linux, macOS і Windows. Цей інструмент підтримує його спільнота, що забезпечує розвиток і надає ресурси для вирішення проблем. Однак через складність налаштування та управління, його частіше використовують організації з високим рівнем технічної експертизи. Також OpenLDAP не має багатьох вбудованих функцій, таких як GPO, які є стандартними для Active Directory.

FreeIPA — це рішення, що може поєднувати служби каталогів, Kerberos, управління сертифікатами та контроль доступу в одному пакеті. Воно призначене для середовищ Linux і забезпечує просту інтеграцію в них. FreeIPA є безкоштовним, завдяки відкритому коду, що робить його привабливим для організацій із обмеженим бюджетом. Інструмент також підтримує централізоване управління доступом, політиками й аутентифікацією, що є важливим для забезпечення безпеки. Однак, через свою вузьку спрямованість, FreeIPA має складнощі з інтеграцією у інші середовища, які включають Windows. Крім того, функціонал FreeIPA є малим, що може бути недостатнім для великих організацій з високими вимогами до масштабованості.

Okta є хмарною платформою для управління ідентифікацією та доступом. Так як вона повністю базується на хмарі, це забезпечує простоту налаштування та використання що є основною перевагою, і в той же час усуває потребу в локальній інфраструктурі. Okta надає інструменти для інтеграції з SaaS-додатками, підтримує багатофакторну аутентифікацію та забезпечує централізоване управління доступом

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

до хмарних ресурсів. Це рішення підходить для організацій, які орієнтуються на хмарні технології. Водночас, Окта залежить від стабільного Інтернет-з'єднання, і її вартість може бути високою для великих організацій. Крім того, у локальних середовищах її використання може бути обмеженим.

JumpCloud — це також хмарна служба каталогів, яка дозволяє централізовано керувати користувачами, пристроями та доступом у гетерогенних середовищах. Вона підтримує Windows, macOS і Linux, що робить її непоганим вибором для компаній із різномірними інфраструктурами. JumpCloud також пропонує багатфакторну аутентифікацію. Завдяки хмарній архітектурі усувається потреба у локальних серверах. Однак, як і інші хмарні рішення, JumpCloud залежить від надійного Інтернет-з'єднання. Її інтеграція з локальними Windows-середовищами може потребувати додаткових налаштувань, а вартість може бути значною для великих організацій.

Google Workspace Identity надає інструменти для управління доступом до Google Workspace і сторонніх додатків. Це хмарне рішення забезпечує багатфакторну аутентифікацію, також управління доступом і політиками для хмарних середовищ. Завдяки інтеграції з екосистемою Google, цей інструмент підходить для організацій, які вже використовують Google Workspace. Простота налаштування та використання робить його привабливим для малого і середнього бізнесу. Проте, Google Workspace Identity має обмежені можливості для інтеграції з локальними ресурсами. Це рішення також підходить переважно для організацій, які не залежать від екосистеми Microsoft або інших локальних рішень.

2.3 Вибір віртуального середовища та програмного забезпечення

Наступним розглянемо вибір гіпервізора та платформу віртуалізації, які допоможуть створити локальну мережу для роботи усіх пристроїв та технологій, пов'язаних з AD RMS.

Гіпервізор — це спеціалізоване програмне забезпечення, що забезпечує створення, управління та ізоляцію віртуальних машин на фізичному носії. Головною

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

функцією гіпервізора є розподіл апаратних ресурсів між віртуальними машинами та гарантування їх ефективного використання та безпеки.

Таким чином, основні функції гіпервізора є наступними.

- розподіл ресурсів(динамічне управління CPU, RAM, дисковою пам'яттю та мережею між віртуальними машинами);
- ізоляція середовищ(кожна VM працює незалежно від інших, що підвищує безпеку та стабільність);
- підтримка живої міграції (можливість перенесення віртуальної машини між фізичними серверами без зупинки роботи) ;
- моніторинг і управління(контроль продуктивності та використання ресурсів у віртуалізованому середовищі) ;

Також гіпервізори бувають двох основних типів.

Гіпервізор типу 1 (bare-metal). Це програмне забезпечення, яке працює безпосередньо на апаратному рівні сервера, без проміжної операційної системи. Завдяки цьому забезпечується висока продуктивність і мінімальна затримка при розподілі ресурсів. Прикладами таких гіпервізорів є Proxmox VE, VMware ESXi, Microsoft Hyper-V (у серверній версії), Xen та KVM.

Гіпервізор типу 2 (hosted). Даний тип встановлюється як додаток на вже існуючу операційну систему. Це зменшує продуктивність порівняно з bare-metal рішеннями, оскільки віртуальні машини працюють поверх ОС хоста. Прикладами є VMware Workstation, Oracle VirtualBox, Microsoft Hyper-V (у клієнтських версіях Windows).

Було здійснено порівняльний аналіз гіпервізорів KVM, VMware ESXi, Hyper-V та VirtualBox на основі ключових характеристик, таких як продуктивність, вартість, ліцензія, підтримка гостьових операційних систем, масштабованість та безпека. Результати аналізу відображено у таблиці 2.1, дозволяє наочно оцінити сильні та слабкі сторони кожного рішення, і визначити, який гіпервізор найбільш підходить для конкретних завдань та інфраструктури.

Таблиця 2.1

Порівняння гіпервізорів

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Критерій	KVM	VMware ESXI	Hyper-V	VirtualBox
Тип гіпервізора	1-ий тип	1-ий тип	1-ий тип	2-ий тип
Ліцензція	Open-source	Пропрієтарна	Пропрієтарна (є безкоштовна версія)	Open-source
Вартість	Безкоштовний	Платний, частково безкоштовний	Безкоштовний у Windows Server	Безкоштовний
Продуктивність	Висока, завдяки інтеграції в ядро Linux	Висока, оптимізована під сервер	Висока, зокрема у Windows Server	Не висока, працює поверх хостової ОС
Масштабованість	Висока	Висока	Висока	Низька
Безпека	Висока	Висока	Висока	Середня

У процесі вибору гіпервізора для віртуалізації ми зупинилися на KVM, оскільки він пропонує оптимальне поєднання продуктивності, безпеки та гнучкості. Це рішення є частиною ядра Linux, що забезпечує високу швидкодію та ефективну підтримку апаратної віртуалізації без додаткових витрат. KVM дозволяє створювати повноцінні віртуальні машини, ізольовані одна від одної, із можливістю гнучкого налаштування ресурсів, що робить його ідеальним для широкого спектра завдань – від тестових середовищ до розгортання корпоративної інфраструктури.

Однією з головних переваг KVM є його відкритий код і відсутність ліцензійних обмежень. Це дозволяє використовувати його без додаткових фінансових витрат, на відміну від комерційних гіпервізорів, таких як VMware ESXi, які вимагають значних вкладень для отримання повного функціоналу. Крім того, KVM має широкі можливості інтеграції з іншими open-source рішеннями, такими як Proxmox

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

VE, Serp для розподіленого сховища даних та ZFS для ефективного управління файловими системами. Це забезпечує гнучке управління віртуалізованим середовищем без прив'язки до конкретного постачальника програмного забезпечення.

З точки зору продуктивності, KVM забезпечує мінімальні затримки завдяки безпосередній інтеграції в ядро операційної системи. Він підтримує всі сучасні технології віртуалізації, включаючи апаратне прискорення, live migration та масштабованість, що дозволяє створювати потужні кластери з високим рівнем відмовостійкості. Завдяки підтримці Windows і Linux у ролі гостей ОС, він є універсальним рішенням для будь-якого середовища. Враховуючи всі ці фактори, KVM стає найбільш логічним вибором для побудови ефективної, безпечної та масштабованої віртуалізованої інфраструктури.

Віртуальне середовище – це програмно-апаратний комплекс, що дозволяє створювати, керувати та ізолювати віртуальні машини і / або контейнери всередині фізичної інфраструктури. В основі такого середовища лежить концепція віртуалізації, яка дозволяє запускати кілька операційних систем на одному фізичному сервері, ефективно використовуючи його апаратні ресурси. Завдяки віртуалізації можливе динамічне управління обчислювальними ресурсами, гнучке масштабування, підвищена безпека та спрощене адміністрування ІТ-інфраструктури.

Ключовим компонентом віртуального середовища є гіпервізор – програмний або апаратний рівень, що забезпечує абстракцію апаратних ресурсів і дозволяє одночасно працювати кільком віртуальним машинам на одному фізичному хості. Гіпервізор розподіляє обчислювальну потужність, оперативну пам'ять, дисковий простір і мережеві ресурси між ВМ, контролюючи їхню взаємодію з фізичним обладнанням. Саме гіпервізор є тим компонентом, який створює ізольовані середовища для віртуальних машин, що дозволяє уникнути конфліктів між ними та підвищує безпеку даних.

Віртуальне середовище може складатися не тільки з ВМ, а й з контейнерів - легких ізольованих процесів, які працюють у межах однієї операційної системи. Наприклад, у Proxmox VE є підтримка контейнерів LXC, що дозволяє запускати

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

оптимізовані середовища для додатків без необхідності емулювати повноцінну операційну систему для кожного екземпляра. Завдяки цьому ресурси використовуються ще ефективніше, а продуктивність значно вища, ніж у класичних віртуальних машин.

Вибір відповідного віртуального середовища напряму залежить від потреб організації: Proxmox VE підходить для тих, хто шукає гнучке, безкоштовне та масштабоване рішення з відкритим кодом, VMware vSphere – для корпоративного рівня з високим рівнем підтримки, а Microsoft Hyper-V – для тісної інтеграції з екосистемою Windows. Таким чином, розуміння роботи віртуального середовища та його зв'язку з гіпервізором дозволяє ефективно використовувати ресурси ІТ-інфраструктури та створювати стабільні й безпечні системи для розгортання сервісів і додатків.[2]

Після ретельного дослідження різних віртуальних середовищ, з урахуванням таких аспектів, як вартість, продуктивність, підтримка операційних систем та масштабованість, було сформовано порівняльну таблицю табл. 2.2. Вона містить ключові критерії, які дозволяють оцінити переваги та недоліки кожного з рішень, таких як Proxmox VE, VMware, Hyper-V та інших, і допомогти вибрати найбільш підходящий варіант для конкретних потреб і задач віртуалізації

Таблиця 2.2

Порівняння віртуальних середовищ

Критерій	Proxmox VE	VMware vSphere	Microsoft Hyper-V	VirtualBox
Гіпервізор	KVM 1-ий тип	ESXI 1-ий тип	Hyper-V 1-ий тип	2-ий тип
Ліцензія	Open-source	Пропрієтарна	Пропрієтарна (є безкоштовна версія)	Open-source
Продуктивність	Висока	Висока	Висока у середовищі Windows	Середня

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Масштабованість	Висока, добре підходить для серверних рішень	Висока, використовується у великих дата-центрах	Висока'	Низька
Зручність управління	Веб-інтерфейс, консоль	Веб-інтерфейс vCenter	Windows GUI	Графічний інтерфейс
Захист та резервне копіювання	Вбудоване рішення Proxmox Backup Server	VMware vSphere Data Protection	Windows Backup	Відсутнє

Після аналізу різних віртуальних середовищ було прийнято рішення обрати Proxmox VE. Він поєднує в собі найкращі можливості для роботи як з віртуальними машинами, так і з контейнерами. Це відкритий програмний продукт, який не вимагає великих фінансових вкладень на відміну від багатьох інших рішень на ринку, таких як VMware. Завдяки його гнучкості та масштабованості, Proxmox став популярним вибором для тих, хто прагне отримати потужну платформу без необхідності витрачати значні кошти на ліцензії.

Однією з головних переваг Proxmox є підтримка різних типів віртуалізації. Він працює на основі KVM-гіпервізора для віртуальних машин, а також надає можливість використовувати LXC контейнери для легких і швидких середовищ. Це дозволяє максимально ефективно використовувати апаратні ресурси, даючи змогу запустити безліч середовищ на одному фізичному сервері. Крім того, Proxmox VE має вбудоване рішення для кластеризації, що дозволяє зручним чином об'єднувати кілька серверів в єдину інфраструктуру для досягнення високої доступності та балансу навантаження. Ця функціональність є важливою для бізнесів, де необхідно забезпечити безперервну роботу і відмовостійкість систем.

Ще одним важливим аспектом є підтримка резервного копіювання даних через вбудоване рішення Proxmox Backup Server. Це дозволяє створювати автомати-

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

зовані бекапи віртуальних машин і контейнерів, що є критично важливим для забезпечення безпеки даних та швидкого відновлення в разі непередбачених ситуацій. Рішення з резервного копіювання від Proxmox забезпечує високий рівень надійності та є гнучким, що дозволяє налаштувати регулярне збереження та відновлення важливої інформації з мінімальними затратами часу та ресурсів.

Proxmox також вирізняється простотою в управлінні завдяки веб-інтерфейсу, який надає зручний доступ до всіх налаштувань і дозволяє здійснювати моніторинг, налаштування та масштабування середовищ без необхідності зайвого втручання в консоль чи сервер. Це робить його дуже привабливим рішенням для адміністраторів, які шукають потужну, але водночас доступну і зручну платформу для віртуалізації. Завдяки цьому Proxmox VE став оптимальним вибором для ефективної організації віртуальних інфраструктур без великих витрат.

Для налаштування мережевих ресурсів у Proxmox необхідно ретельно спланувати, які IP-адреси будуть використовувати віртуальні машини та як вони будуть взаємодіяти з іншими пристроями в мережі. Перш за все, важливо зрозуміти, що для серверів, які працюють віртуально, ми можемо обрати статичні або динамічні IP-адреси в залежності від вимог до доступу та управління.

У нашому випадку ми плануємо призначити статичні IP-адреси для серверів. Це забезпечить стабільність з'єднання та спрощене управління ресурсами, оскільки статичні адреси не змінюватимуться після перезавантаження машин. Для серверів у мережі ми можемо вибрати діапазон адрес з підмережі 192.168.88.0/24, де, наприклад, для головного сервера AD ми призначимо IP-адресу 192.168.88.100, а для резервного сервера AD — 192.168.88.101. Це дозволить чітко визначити місце для кожного сервера в мережі та забезпечити стабільний доступ до них.[6]

Для решти пристроїв у мережі, таких як звичайні комп'ютери або інші робочі станції, можна налаштувати динамічне призначення IP-адрес через DHCP-сервер. Це дозволяє автоматично отримувати адреси з заданого діапазону, що значно спрощує налаштування нових пристроїв без необхідності вручну вводити кожен адресу. В рамках цього налаштування ми можемо визначити, що діапазон DHCP буде

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

розташовуватися між адресами 192.168.88.200 і 192.168.88.254, що дозволить без проблем підключати нові пристрої до мережі.

Для забезпечення коректної маршрутизації трафіку, на кожній віртуальній машині в Proxmox ми будемо налаштовувати шлюз за замовчуванням. В нашій мережі шлюзом за замовчуванням виступатиме роутер MikroTik з адресою 192.168.88.1. Вказівка шлюзу за замовчуванням дозволить забезпечити правильне перенаправлення всього зовнішнього трафіку через роутер до інших мереж, таких як Інтернет. Це є важливим аспектом налаштування для збереження стабільного та безперебійного з'єднання з глобальними ресурсами.

У Proxmox також є можливість вибору типу мережевого інтерфейсу для кожної віртуальної машини, що дозволяє налаштувати взаємодію з іншими пристроями в мережі. Ми обираємо віртуальні мережеві адаптери типу "virtio", які забезпечують високу продуктивність, або "e1000", якщо потрібна більш універсальна сумісність, хоча з меншими можливостями в плані швидкості передачі даних. Для кожної віртуальної машини ми будемо вручну вводити параметри мережі, включаючи статичну IP-адресу, маску підмережі, шлюз та DNS-сервери, щоб гарантувати правильну маршрутизацію і доступ до зовнішніх ресурсів.

Загалом, вибір параметрів мережі для віртуальних машин у Proxmox — це важливий крок у забезпеченні належної роботи інфраструктури. Підключення до фізичної мережі, налаштування IP-адрес і правильне визначення типів мережевих адаптерів впливають на стабільність і ефективність роботи віртуальних машин, а також на їхню взаємодію з іншими пристроями та сервісами в мережі. Крім того, правильне налаштування шлюзу за замовчуванням, вказуючи адресу роутера, гарантує правильне маршрутування зовнішнього трафіку та підключення до Інтернету. Усі призначені IP-адреси показані у табл. 2.3.

Таблиця 2.3

Схема адресації

Пристрій	Ip-адреса	Маска	Префікс
Маршрутизатор (Mikrotik)	192.168.88.1	255.255.255.0	24

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Server-main(AD)	192.168.88.100	255.255.255.0	24
Server-replica(AD)	192.168.88.101	255.255.255.0	24
Proxmox Backup Server	192.168.88.102	255.255.255.0	24
Робочі станції	DHCP	255.255.255.0	24

Важливі технології AD Для налаштування і ефективної роботи з Active Directory Rights Management Services (AD RMS) у нашій інфраструктурі, ми будемо використовувати декілька основних технологій, що забезпечать належну безпеку та управління доступом до даних у середовищі Windows Server.

По-перше, ми будемо використовувати Active Directory (AD) для централізованого управління обліковими записами користувачів і комп'ютерів у нашій мережі. AD забезпечує основну структуру, яка необхідна для функціонування AD RMS, оскільки дані про користувачів, групи та їхні права зберігаються в базі даних Active Directory. Це дозволяє здійснювати централізований контроль за доступом до захищених документів та інших ресурсів у межах організації. Використання Active Directory для інтеграції з AD RMS дозволяє максимально ефективно керувати правами доступу та застосовувати політики безпеки до документів.

По-друге, для роботи з AD RMS необхідно налаштувати сертифікаційні служби, такі як Active Directory Certificate Services (AD CS). Вони використовуються для видачі сертифікатів, які забезпечують захист і автентифікацію користувачів та комп'ютерів у мережі. Сертифікати служать основним механізмом для захисту даних і підтвердження автентичності користувачів, які мають доступ до захищених ресурсів. У нашій інфраструктурі ми будемо використовувати AD CS для створення і управління сертифікатами, які необхідні для налаштування AD RMS і створення умов для безпечного доступу до документів.

Важливим аспектом налаштування AD RMS є правильна конфігурація серверів. Перш за все, потрібно налаштувати сервер AD RMS, який буде відповідати за захист даних і застосування політик доступу до інформації. Цей сервер буде

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

взаємодіяти з іншими серверами в інфраструктурі, зокрема з сервером сертифікаційних служб (AD CS), для забезпечення механізмів захисту даних на рівні операційної системи.

Також для налаштування AD RMS необхідно інтегрувати відповідні політики захисту документів у межах всіх сервісів, які підтримують RMS. Вони визначатимуть, хто має доступ до документів, які дозволи на редагування, копіювання або друк документів доступні користувачам, і які саме дані повинні бути захищені. Для цього ми будемо використовувати групові політики і політики управління правами доступу до документів, які забезпечують застосування обмежень на файли в залежності від ролі користувача та його прав.

Нарешті, необхідно налаштувати додаткові технології для моніторингу і аудиту, що дозволить забезпечити прозорість операцій з документами, які підлягають захисту. Це включає в себе ведення журналів доступу та змін до файлів, що допомагає у разі необхідності провести аудит і виявити порушення політик доступу.

Таким чином, для успішного впровадження AD RMS в нашій мережі, ми будемо використовувати технології, які не тільки забезпечують централізоване управління і захист ресурсів, але й надають механізми для гнучкого налаштування політик доступу і надійного моніторингу всіх операцій з даними. Всі ці технології необхідні для того, щоб AD RMS міг ефективно виконувати свою роль в захисті корпоративних даних і підтримці вимог до безпеки інформації в організації.

Висновки до розділу 2

У другому розділі було здійснено проектування інфраструктури для впровадження служби Active Directory Rights Management Services у корпоративному середовищі. Розділ охоплює ключові етапи підготовки до впровадження системи управління доступом до даних, включаючи аналіз вимог, вибір технологій та побудову мережевої архітектури.

На етапі аналізу вимог визначено, що для ефективної роботи AD RMS необхідно мати налагоджену інфраструктуру Active Directory, стабільне мережеве се-

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

редовище, сертифікаційні служби (AD CS) та належним чином організовані групові політики. Також окреслено вимоги до захисту конфіденційних документів, сценарії доступу та обмеження для користувачів.

У підрозділі порівняння Active Directory з конкурентами розглянуто альтернативні рішення (OpenLDAP, FreeIPA, Samba), проте зроблено обґрунтований висновок на користь AD як найкращого вибору для реалізації системи контролю доступу завдяки її глибокій інтеграції з інфраструктурою Windows, підтримці RMS і широким адміністративним можливостям.

Вибір віртуального середовища базувався на аналізі доступних платформ. В результаті обрано Proxmox як просте у налаштуванні, безкоштовне та ефективне рішення для побудови тестової мережі. Зазначено, що це середовище дозволяє створити повноцінну модель корпоративної інфраструктури, включаючи сервери AD, AD RMS, клієнтські машини та окремий Proxmox Backup Server для резервного копіювання.

У підрозділі архітектури мережі розроблено топологію, яка передбачає наявність головного та реплікованого серверів Active Directory, кількох підмереж для відокремлення ролей, а також систему резервного копіювання. Визначено фіксовані IP-адреси, налаштування шлюзів і DNS, що забезпечує стабільність і керуваність мережі. Показано, як ця архітектура дозволяє централізовано контролювати доступ до документів і забезпечити надійність зберігання даних.

Загалом, у другому розділі створено концептуальну та технічну основу для практичної реалізації системи управління доступом на базі AD RMS. Обґрунтовано вибір платформ, технологій і схеми розгортання, які відповідають завданням безпеки корпоративного рівня.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

РОЗДІЛ 3 РОЗРОБКА ТА ТЕСТУВАННЯ МЕРЕЖІ ТА СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ ДО ДАНИХ

3.1 Розгортання віртуального середовища

Процес інсталяції Proxmox VE на фізичний сервер є важливим етапом, оскільки він забезпечує основну платформу для віртуалізації. Після завантаження ISO-образ Proxmox VE з офіційного сайту, було підготовлено фізичний носій для інсталяції ISO-образу на сервер. Система автоматично визначила відповідні налаштування для процесора, пам'яті та диска. Проте важливим було правильно вибрати диск для інсталяції та конфігурації, оскільки Proxmox VE має підтримку як локальних, так і мережевих сховищ для зберігання віртуальних машин.

Після завантаження образу на сервер і початку інсталяції, було пройдено кілька етапів налаштування. На першому етапі інсталяції система запропонувала вибір диска, на який буде встановлений Proxmox VE. Важливо врахувати, що для оптимальної роботи системи бажано використовувати SSD-диски або диски з великою пропускнуою здатністю. Під час налаштування також було вказано базові параметри, такі як мережеві налаштування — IP-адресу, маску підмережі та шлюз.

Одним із важливих кроків під час інсталяції було налаштування обчислювальних ресурсів, зокрема пам'яті та CPU. Proxmox VE дозволяє гнучко розподіляти ресурси між віртуальними машинами.

По завершенню інсталяції, сервер перезавантажився, після чого у нас є змога підключитися до веб-інтерфейсу Proxmox. Успішне перезавантаження показано на рисунку 3.1.

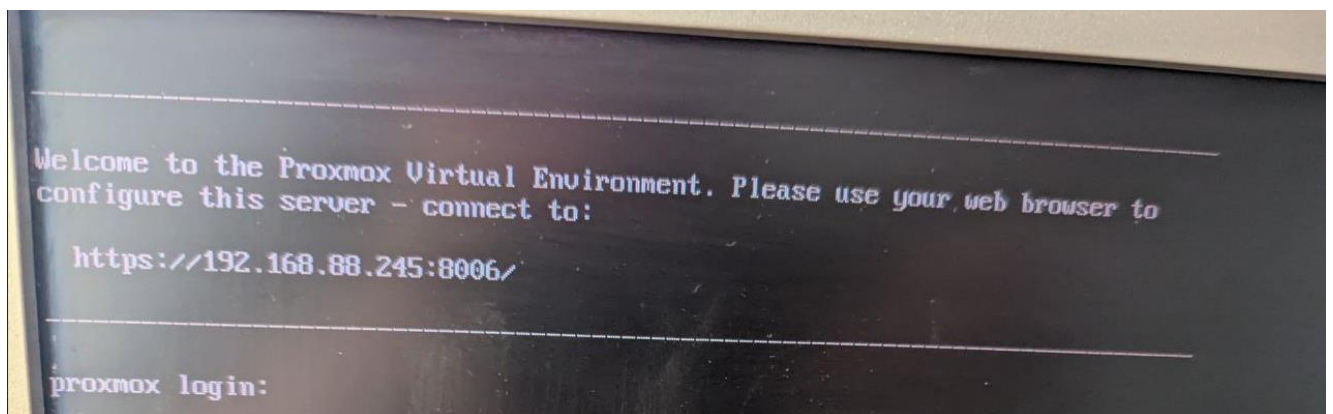


Рисунок 3.1. Успішний запуск Proxmox VE

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Для підключення потрібно ввести IP-адресу сервера в браузері, що відкриє веб-інтерфейс, де ми продовжимо здійснювати подальше налаштування системи. Веб-інтерфейс Proxmox VE є зручним і інтуїтивно зрозумілим, що дозволило швидко налаштувати систему без необхідності глибоких технічних знань. Зазначені кроки дозволили не тільки налаштувати базову конфігурацію сервера, але й підготувати інфраструктуру для подальшого використання віртуалізації.

Далі було обрано ISO образи для встановлення віртуальних операційних систем. Було завантажено офіційні ISO-образи Windows 10 та Windows Server 2019 із сайту Microsoft. Для реалізації клієнтської частини інфраструктури використовувалась версія Windows 10 Pro x64, що забезпечила необхідний функціонал для участі в доменній структурі, а також підтримку групових політик та служб AD RMS. Для серверної частини інфраструктури було обрано Windows Server 2019 Standard x64, яка встановлювалась на дві віртуальні машини: основний контролер домену та реплікаційний сервер. Ця версія серверної ОС дозволила налаштувати Active Directory, DNS-сервер, AD RMS, а також створити надійне середовище для керування політиками безпеки й доступом до даних. Під час підготовки віртуальних машин було враховано архітектуру x64 для забезпечення повної сумісності та стабільності роботи в середовищі Proxmox. Інсталяція операційних систем проводилась із попередньо підготовлених ISO-файлів, що були прикріплені до віртуальних машин через інтерфейс Proxmox VE.

Було створено дві віртуальні машини для контролерів домену, декілька клієнтських машин для представлення працівників з різних департаментів, а також окрема машина для резервного копіювання, яка відповідає за збереження важливих даних і образів систем. Під час встановлення кожної з них, потрібно було обрати ID, ім'я, та ISO-образ, це продемонстровано на рисунках 3.2 та 3.3.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

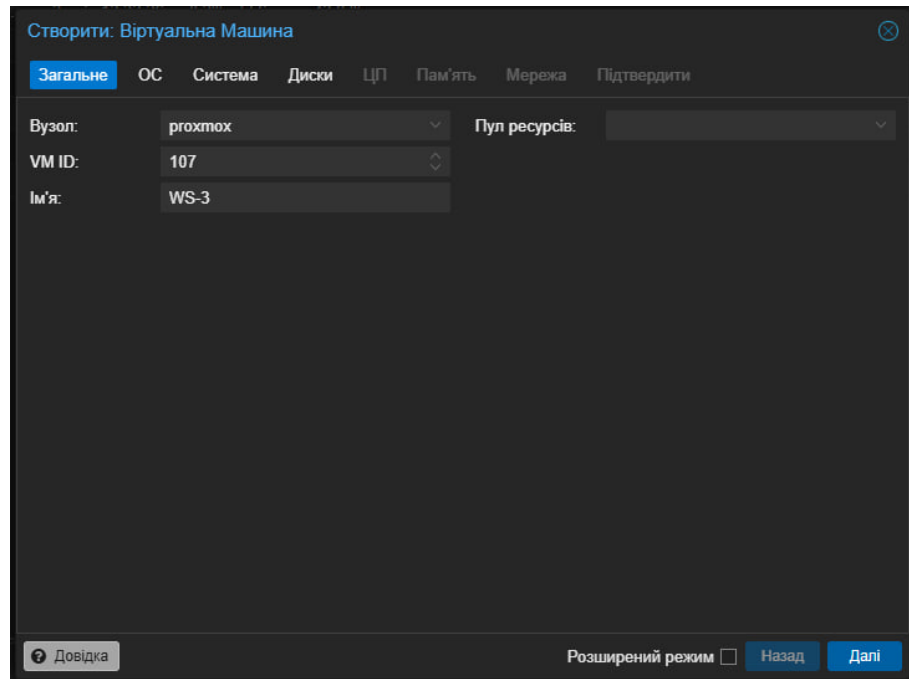


Рис. 3.2. Загальний етап встановлення віртуальної машини

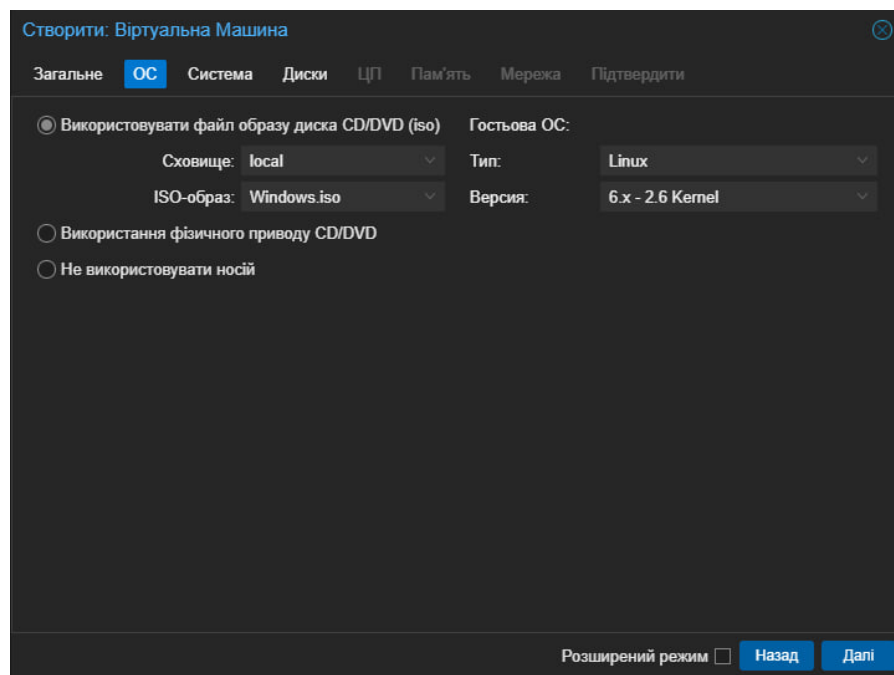


Рис. 3.3. Другий етап встановлення віртуальної машини

Під час конфігурації ресурсів враховувалися реальні потреби для стабільної роботи системи. Кожному з контролерів домену було виділено по 8 процесорних ядер, 8 ГБ оперативної пам'яті та 100 ГБ дискового простору. Клієнтське середовище було змодельоване за допомогою кількох машин, які в сукупності використовували 12 ядер процесора, 16 ГБ оперативної пам'яті та 60 ГБ місця на диску.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Окремо для машини з резервним середовищем було виділено 4 ядра, 2 ГБ оперативної пам'яті та 500 ГБ пам'яті, необхідної для збереження резервних копій. Приклад налаштування однієї з віртуальних машин показано на рисунку 3.4.

Пам'ять	8.00 GiB
Процесори	8 (1 sockets, 8 cores) [x86-64-v2-AES]
BIOS	OVMF (UEFI)
Дисплей	За замовчуванням
Комп'ютер	pc-q35-9.0
Контролер SCSI	VirtIO SCSI single
Жорсткий диск (ide0)	local-lvm:vm-101-disk-1,size=100G
Привід CD/DVD (ide2)	local.iso/Win-Server-19.iso,media=cdrom,size=5519618K
Пристрій мережі (net0)	e1000=BC:24:11:B2:2C:55,bridge=vbr0,firewall=1
EFI Диск	local-lvm:vm-101-disk-0,efitype=4m,pre-enrolled-keys=1,size=4M
TPM-Пристрій	local-lvm:vm-101-disk-2,size=4M,version=v2.0

Рис. 3.4. Підсумування налаштувань для створення віртуальної машини

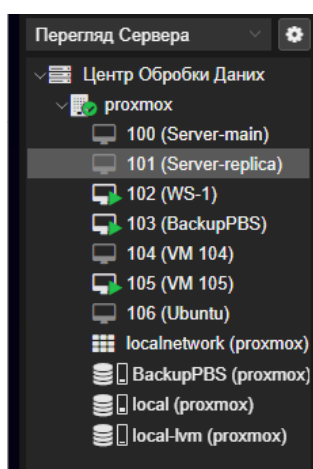


Рис. 3.5. Розгорнуті віртуальні машини в середовищі Proxmox для імітації корпоративної мережі.

3.2 Створення домену Active Directory

У віртуальному середовищі було розгорнуто два сервери під управлінням Windows Server 2019:

server-main.sheiko.net - головний контролер домену.

server-replica.sheiko.net - додатковий контролер домену для забезпечення реплікації та підвищення відмовостійкості системи.

Для створення домену було використано стандартну процедуру встановлення полі Active Directory Domain Services (AD DS) через Server Manager. Після встановлення головного сервера контролером домену, другий сервер було додано як додатковий контролер із реплікацією усіх контейнерів та об'єктів.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

На цьому етапі було здійснено налаштування структури домену, що базується на логіці централізованого управління ресурсами. Основною метою було створення чіткої організаційної моделі, яка дозволяє ефективно адмініструвати користувачів, комп'ютери та застосовувати політики безпеки залежно від функціональних обов'язків. У межах домену було створено головну організаційну одиницю Department, яка включає чотири ключові підрозділи (OU): Development, HR, Management, Marketing. У кожному з цих підрозділів були сформовані окремі OU для Users та PCs, що дозволило розділити облікові записи користувачів і комп'ютерів, пов'язаних із конкретними департаментами. Такий підхід забезпечив зручність у налаштуванні групових політик (GPO), делегуванні прав, а також дозволив легко керувати правами доступу. Кожному співробітнику призначалось місце в структурі відповідно до його відділу, що дало змогу централізовано застосовувати політики доступу, обмеження, а також розмежувати повноваження. Окремо було створено організаційну одиницю Admins, де були зібрані облікові записи адміністраторів, що мають розширені повноваження в межах домену. Це дозволило сконцентрувати керування критичними компонентами системи в одному місці та спростило контроль за адміністративними діями. Таким чином, розгорнута структура домену забезпечила гнучке управління ресурсами, спростила адміністрування й підвищила рівень безпеки мережевої інфраструктури. Створена модель залишається масштабованою та готовою до подальшого розширення підприємства без потреби в кардинальних змінах.

Такий підхід дозволяє легко застосовувати групові політики (GPO) окремо до користувачів і пристроїв кожного підрозділу, що забезпечує гнучкість і безпеку адміністрування. Для зручності розуміння була створена Структурна діаграма домену. (рисунок 3.2)

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

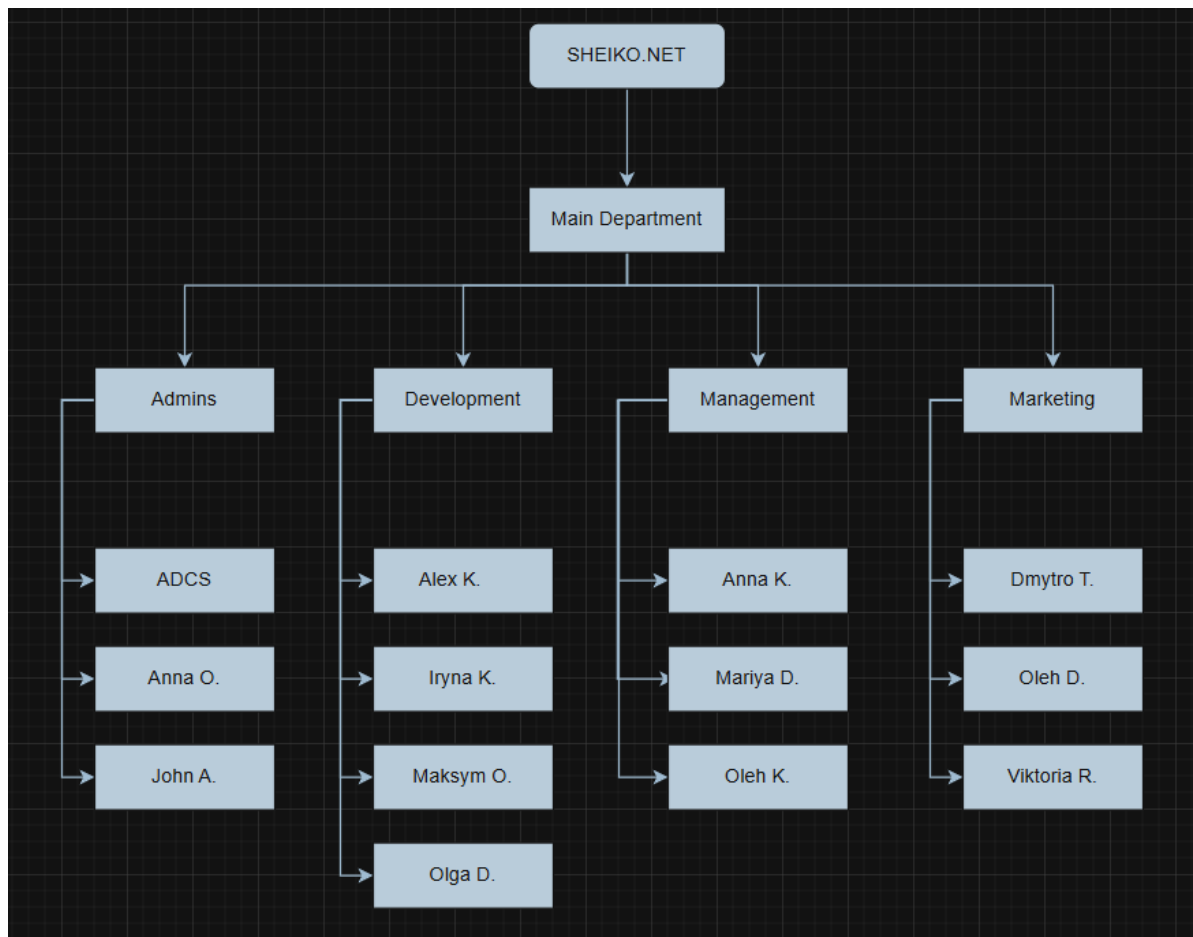


Рис. 3.2. Структурна діаграма домену

Окрім створення OU, було організовано облікові записи адміністраторів для кожного з підрозділів:

adm-admins

adm-dev

adm-mgmt

adm-mktg

Кожному адміністратору було делеговано обмежені права управління об'єктами в межах відповідної організаційної одиниці, що підвищує безпеку системи та запобігає помилкам при адмініструванні інших частин домену.

Також було налаштовано службову роль DNS для забезпечення коректного іменування ресурсів мережі та безперебійної роботи механізмів автентифікації та реплікації між контролерами домену. Було перевірено стабільність реплікації за допомогою інструментів реплікаційного моніторингу, що підтвердило успішну синхронізацію всіх об'єктів домену (рисунок 3.3, а також більш детально у додатку Б).

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

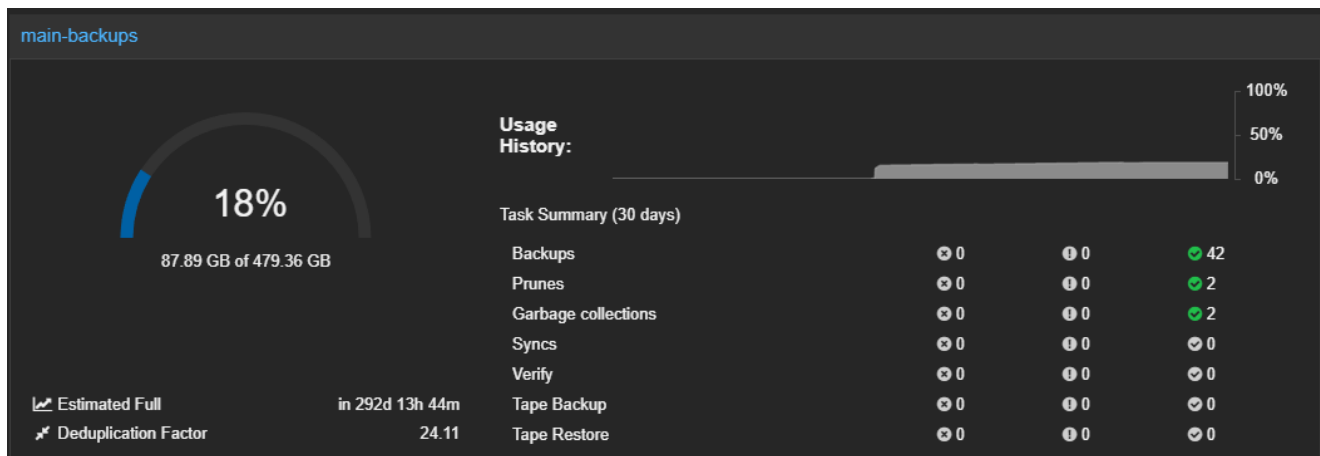


Рис. 3.3. Інструменти реплікаційного моніторингу

3.3 Впровадження служби Active Directory Rights Management Services

Перед початком розгортання служби AD RMS було виконано підготовчі дії, що включали створення спеціального облікового запису служби, підготовку серверного середовища та налаштування сертифікатної інфраструктури. У межах OU Admins було створено обліковий запис `adrms_service`, який надалі використовувався як службовий для запуску компонентів AD RMS. Обліковому запису було надано лише мінімально необхідні права, що відповідає принципам найменших привілеїв та підвищує безпеку системи. (рисунок 3.4)

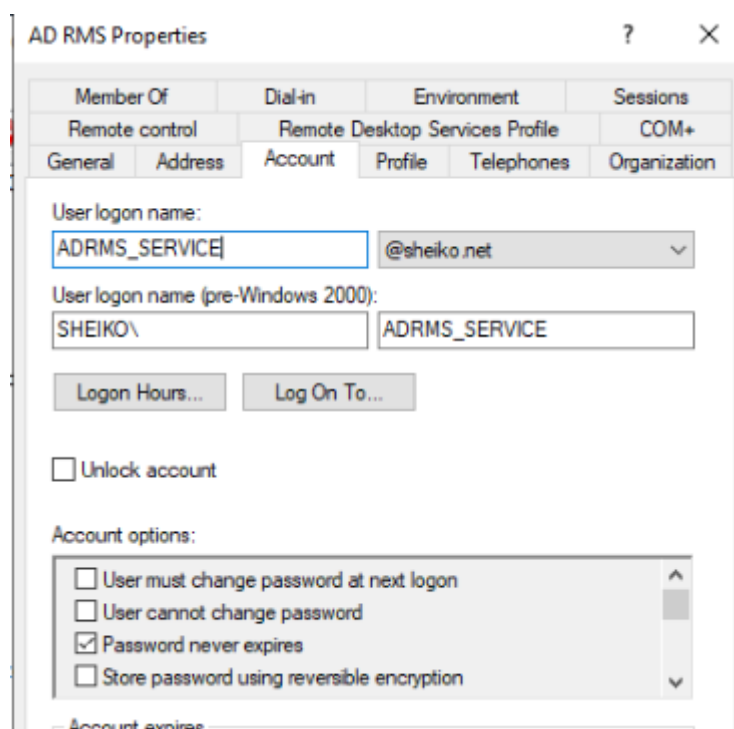


Рис. 3.4. Обліковий запис `adrms_service`

Через обмеження і складнощі, пов'язані з використанням внутрішнього центру сертифікації, було прийнято рішення створити самопідписаний сертифікат для AD RMS. Він був згенерований через інструмент IIS Manager (Create Self-Signed Certificate), збережений у сховищі Personal, а згодом вручну імпортований до Trusted Root Certification Authorities на тому ж сервері. Цей сертифікат було обрано під час встановлення AD RMS як серверний сертифікат для шифрування трафіку. Такий підхід значно спрощує розгортання RMS у тестовому середовищі, оскільки не вимагає налаштування повноцінної PKI.

Перед початком інсталяції було також перевірено налаштування IIS, зокрема наявність Default Web Site, коректну роботу Windows Authentication та доступність службових портів.

Встановлення служби AD RMS відбувалося на другому сервері (server-replica.sheiko.net). У майстрі конфігурації було обрано створення нового кластеру, використання внутрішньої бази даних та централізоване зберігання ключів. Сертифікат, створений раніше, було обрано зі сховища Personal, а кластерна адреса вказана у вигляді повного доменного імені: <https://server-replica.sheiko.net>.

Після завершення налаштування автоматично створився SCP-запис у службі Active Directory.

Після завершення встановлення служби AD RMS було створено шаблони політик прав доступу. Через консоль керування AD RMS було створено декілька distributed rights policy templates, кожен з яких описує конкретну політику доступу до документів:

- Development Confidential — дозволяє лише групі Development перегляд і редагування документів, усім іншим — заборонено.
- Marketing Confidential — доступ надано лише групі Marketing із заборonoю копіювання і друку.
- Top Secret (Admins only) — тільки Admins має доступ до читання, інші групи виключені.
- Read-Only Documents — дозволяє лише перегляд документів без можливості редагування або друку.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

У шаблонах було також реалізовано обмеження на функції друку, зняття скріншотів та копіювання тексту, що є ключовими у системах захисту даних. (Рисунок 3.5)

Після створення шаблонів публічна частина сертифіката була експортована у форматі .cer та імпортована до сховища довірених сертифікатів на клієнтських комп'ютерах. Це дозволило уникнути помилок автентифікації та забезпечити успішну комунікацію між клієнтськими програмами (Word, Excel) і сервером RMS. Також на клієнтах було виконано оновлення політик.

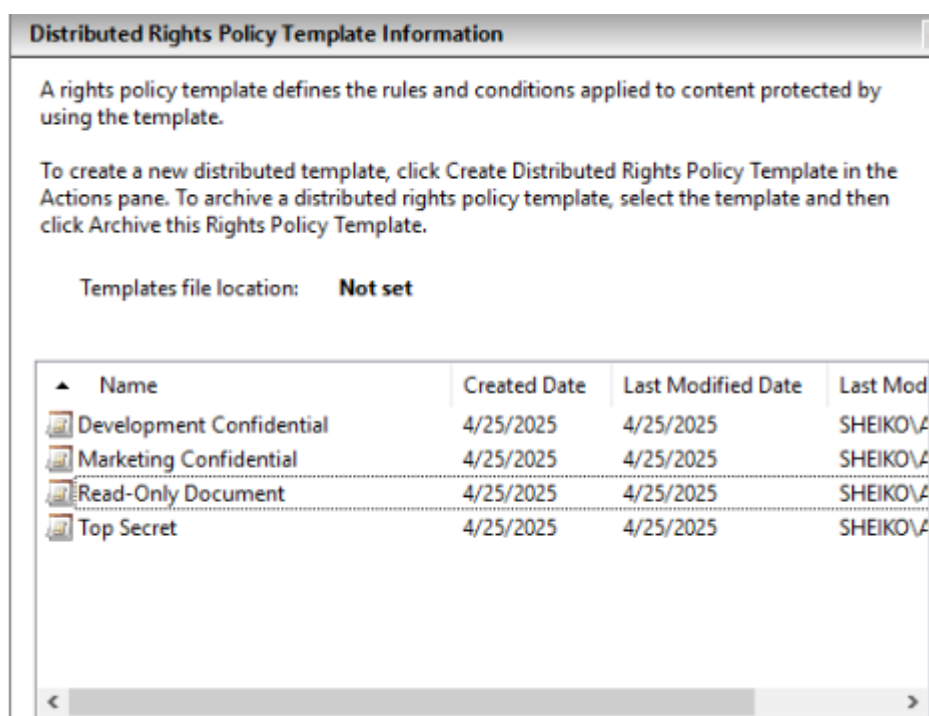


Рис. 3.5. Створені шаблони

Таким чином, служба AD RMS була успішно налаштована з використанням самопідписаного сертифіката, що є оптимальним рішенням для тестового середовища. Шаблони були створені з урахуванням логіки доступу до документів у межах різних департаментів, що дозволяє ефективно контролювати розповсюдження та використання конфіденційної інформації в організації.

3.4 Тестування роботи Active Directory Rights Management Services

Після завершення розгортання та початкового налаштування служби AD RMS було проведено тестування її функціональності для перевірки коректності захисту документів відповідно до створених політик доступу.

На клієнтських комп'ютерах, що входять до домену, було попередньо виконано оновлення групових політик та очищення кешу Kerberos. Це дозволило оновити інформацію про доступні SCP-записи та політики доступу RMS.

Оскільки сервер AD RMS використовує самопідписаний сертифікат, було імпортовано публічну частину сертифіката у сховище Trusted Root Certification Authorities на кожному клієнтському ПК. Це забезпечило довіру клієнтів до сервера RMS та дозволило уникнути помилок TLS-підключення.

Для перевірки роботи служби на клієнтських комп'ютерах було використано програму Microsoft Word. У тестовому документі було виконано такі дії:

1. Створено новий документ Word.
2. У меню Файл → Відомості → Захистити документ → Обмежити доступ було перевірено наявність доступних RMS-шаблонів.
3. Було обрано один із створених шаблонів, наприклад, Development Confidential.

Після застосування шаблону документ набував захищеного статусу. При спробі відкрити цей документ під обліковим записом користувача, який не входить до відповідної групи безпеки, доступ до файлу було заборонено відповідно до налаштувань політики. Користувачі, які мали права лише на перегляд документа, не могли його редагувати, друкувати або копіювати вміст, що підтвердило правильність реалізації обмежень у шаблонах.

Додатково тестування включало перевірку застосування різних рівнів обмежень:

- Шаблон Read-Only Documents дозволяв переглядати документ без можливості внесення змін чи друку, як було передбачено політикою.

Таким чином, проведене тестування показало (рисунки 3.6, 3.7 та 3.8), що служба AD RMS працює коректно, а створені шаблони політик ефективно обмежують доступ до документів залежно від прав користувачів. Це підтверджує правильність побудови всієї системи управління доступом до даних у корпоративній мережі організації.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

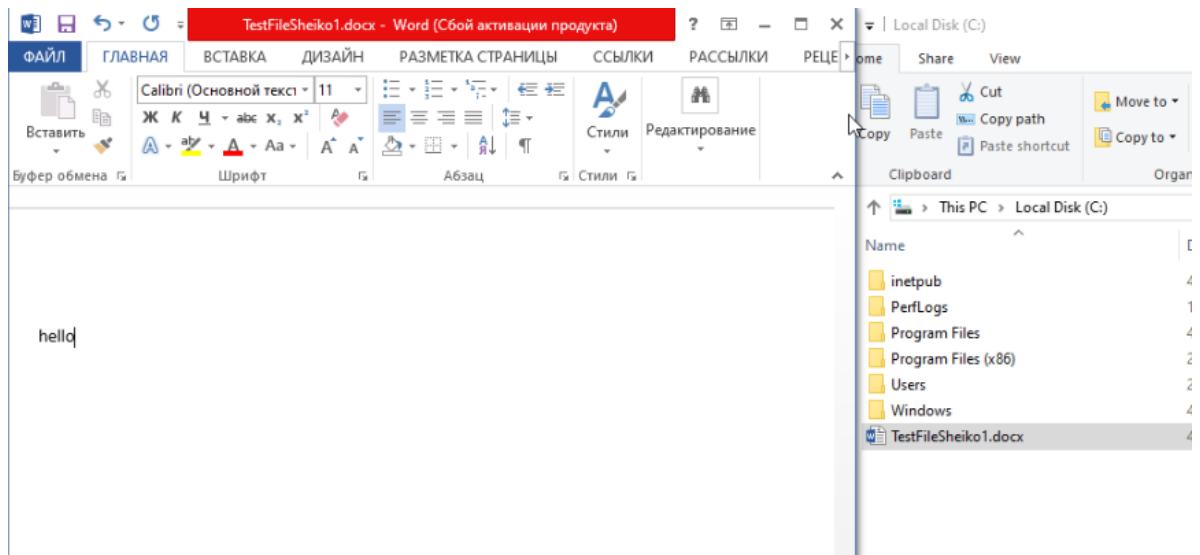


Рис. 3.6 Створений тестовий файл, захищений шаблоном Read-Only Documents



Рис. 3.7 Доступ до документу від імені власника Aretrov@sheiko.net

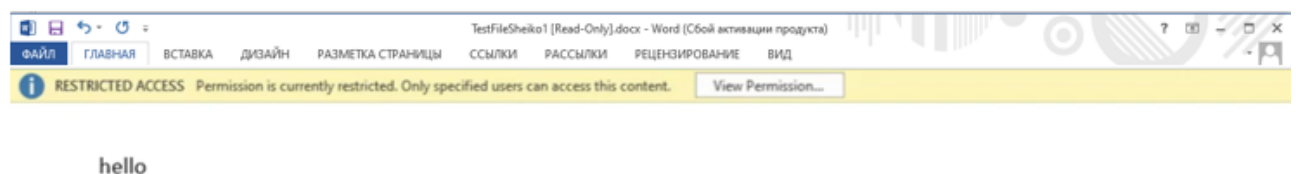


Рис. 3.8 Доступ до документу від імені іншогокористувача Atkachuk@sheiko.net

3.5 Забезпечення та тестування резервного копіювання та відновлення даних за допомогою Proxmox Backup Server

Як вже і було зазначено до цього, основна мета Proxmox Backup Server (надалі - PBS) забезпечити безперервність роботи та можливість швидкого відновлення у випадку збоїв або пошкодження даних.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Для початку було створено окрему віртуальну машину PBS, а саме консольну версію для зниження споживання ресурсів. Встановлено статичну IP-адресу з підмережі 192.168.88.0/24, шлюз за замовчуванням, та хостнейм. Мережеве налаштування продемонстровано на рисунку 3.9.

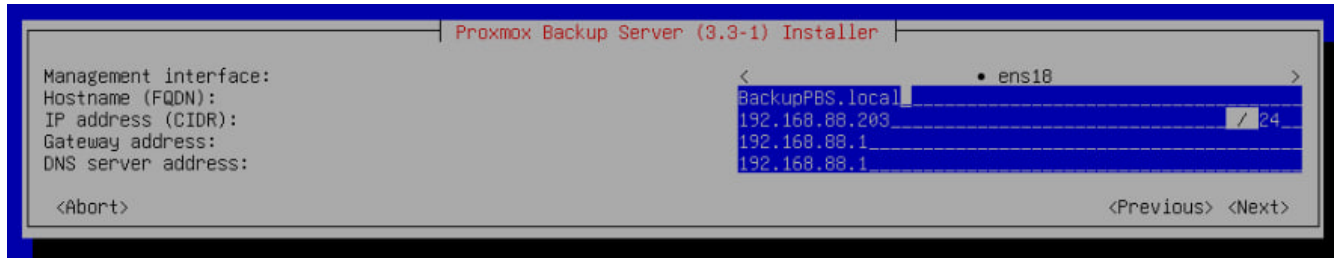


Рис. 3.9. Мережеве налаштування PBS

Подальші дії були виконані у веб-інтерфейсі PBS за адресою 192.168.88.203:8007. На цьому етапі було створено сховище для зберігання резервних копій, та налаштовано розклад видалення старих резервних копій, продемонстровано на рисунках 3.10.

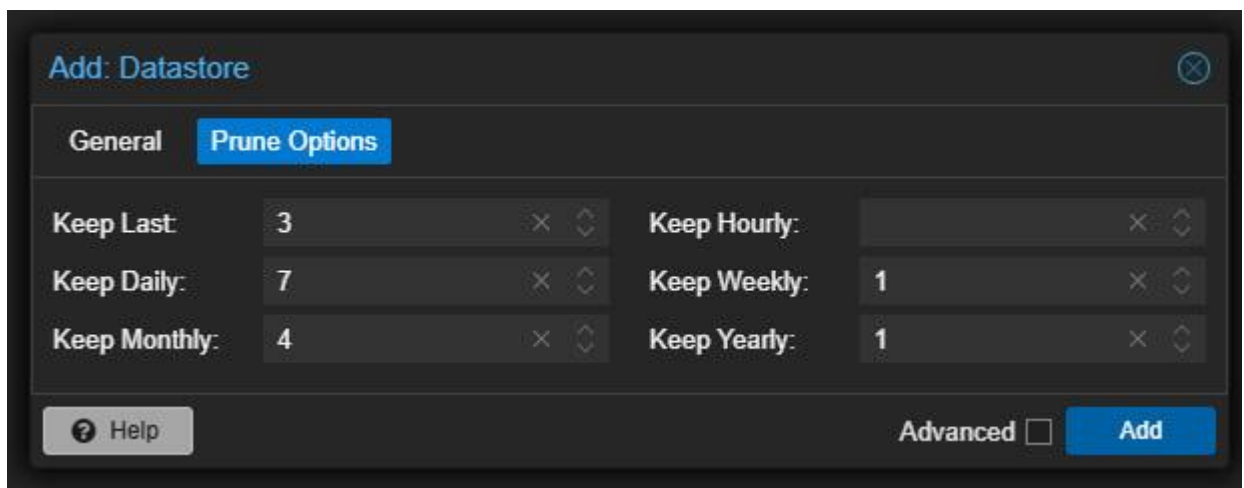


Рис. 3.10. Налаштування видалення старих резервних копій

Для організації безпечного доступу до PBS, було створено окремого користувача, який має право лише на резервне копіювання та відновлення. Це дозволило уникати використання облікового запису root. Аби відповідний користувач мав усі необхідні права, потрібно налаштувати дозволи. Було створено permission з шляхом до datastore, логіном користувача, та роллю DatastoreBackup. Продemonстровано на рисунку 3.11.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

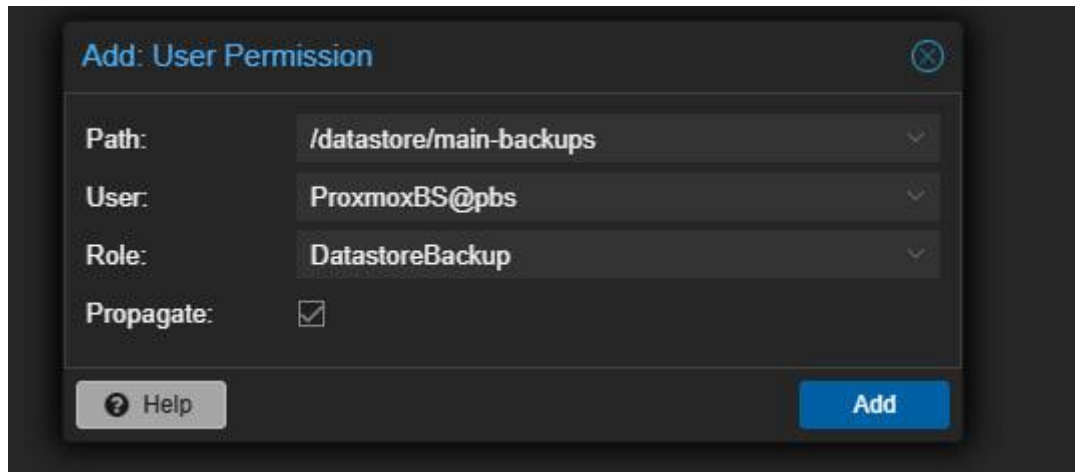


Рис. 3.11. Налаштування дозволів для юзера ProxmoxBS@pbs

Останнім кроком в налаштуванні є створення API токена для підключення Proxmox VE до PBS, токен прив'язаний до юзера.

Аби Proxmox VE мав доступ до PBS потрібно додати його у вкладці Сховище. Було вказано його ID, Ір-адреса серверу, ім'я користувача, datastore та відбиток, який було витягнуто з консолі командою `openssl x509 -in /etc/proxmox-backup/proxy.pem -noout -fingerprint -sha256`.

Для завершення усіх налаштування, потрібно забезпечити резервне копіювання певних машин за певним графіком. Для цього було обрано віртуальні машини, а саме server-main, server-replica та WS-1. Встановлено розклад та обрано сховище, налаштування зображено на рисунку 3.12.

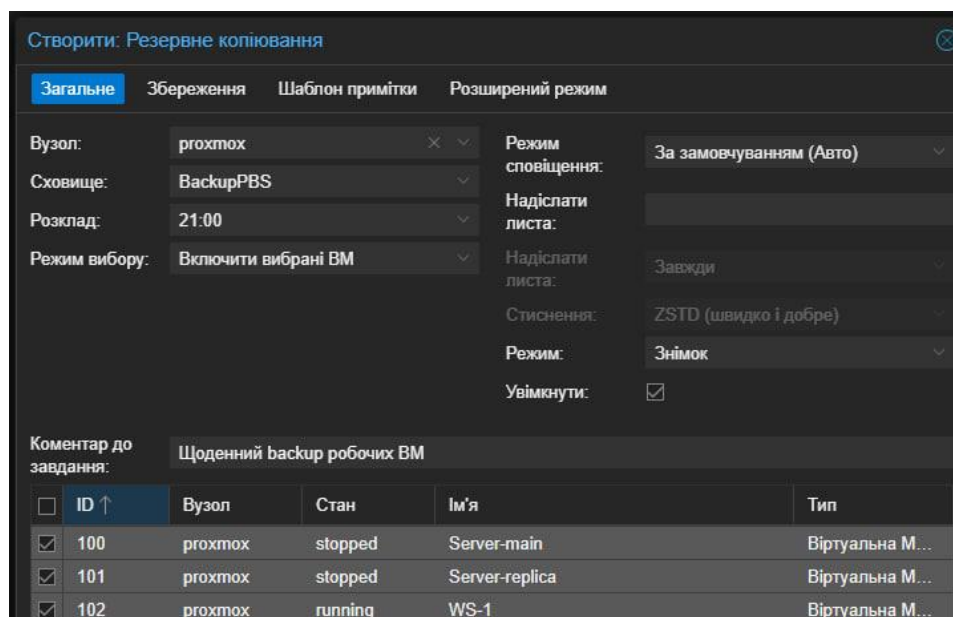


Рис. 3.12. Налаштування резервного копіювання.

Для тестування було запущено примусове збереження, успішне виконання можна переглянути у вкладці “Завдання” (Додаток А).

Висновки з розділу 3

У третьому розділі було реалізовано практичну частину роботи — побудову віртуального середовища, створення домену, впровадження служби Active Directory Rights Management Services (AD RMS) та налаштування резервного копіювання за допомогою Proxmox Backup Server (PBS).

На етапі розгортання віртуального середовища було налаштовано інфраструктуру на базі Proxmox, яка включає в себе основні сервери: контролери домену, RMS-сервер, клієнтські машини, а також окремий сервер для резервного копіювання. Проведено налаштування мережі, визначено IP-адресацію та базову взаємодію між машинами. Це забезпечило повноцінну модель корпоративної мережі для подальшого тестування.

У підрозділі створення домену Active Directory показано процес налаштування контролера домену, створення організаційної структури, груп безпеки, користувачів та об'єктів політик груп. Побудована структура дозволяє гнучко керувати доступом та налаштовувати права в межах різних підрозділів організації.

На етапі впровадження AD RMS було здійснено встановлення та налаштування RMS-сервера. Обрано кластер з самопідписаним сертифікатом, налаштовано інтеграцію з Active Directory, створено шаблони прав доступу (наприклад, "Лише для читання", "Заборонено пересилання"), протестовано їх застосування в середовищі Microsoft Office. Продемонстровано можливість обмеження дій користувачів над документами — редагування, копіювання, друку тощо.

У підрозділі тестування AD RMS показано, як працює контроль доступу: один користувач створює документ, інший — не має змоги його редагувати або надсилати. Зафіксовано приклади повідомлень про обмежений доступ та відсутність прав. Це підтверджує ефективність налаштованих політик безпеки та реальне обмеження дій відповідно до встановлених шаблонів.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Було проведено налаштування резервного копіювання за допомогою Proxmox Backup Server. Встановлено PBS як окрему віртуальну машину, налаштовано сховище, політики резервного копіювання (включно з `prune`-опціями для автоматичного очищення старих бекапів), додано цільову віртуальну машину до резервування. Проведено тестове створення резервної копії та її успішне відновлення. Також створено API-токен та роль з обмеженими правами доступу для кращої безпеки.

Таким чином, розділ демонструє повний цикл розгортання, налаштування та перевірки роботи інтегрованої системи управління доступом до даних. Впроваджене рішення забезпечує як захист інформації на рівні політик доступу, так і її збереження за допомогою регулярного резервного копіювання, що в комплексі підвищує надійність та безпеку корпоративного середовища.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розглянуто питання побудови та захисту інформаційної інфраструктури організації за допомогою технологій Active Directory та Active Directory Rights Management Services (AD RMS). Було проведено аналіз вимог до впровадження системи управління доступом до даних, здійснено проектування мережі, створено віртуальне середовище з двома контролерами домену, клієнтськими комп'ютерами та резервною інфраструктурою.

Під час побудови домену Active Directory було розроблено логічну структуру організаційних одиниць, яка відображає реальні потреби корпоративного середовища та забезпечує ефективне розмежування доступу й делегування прав. Налаштування DNS і реплікації дозволило гарантувати стабільну роботу доменної інфраструктури.

Особливу увагу було приділено впровадженню служби AD RMS, що забезпечує захист конфіденційних даних за допомогою механізмів шифрування та політик обмеження доступу. Для цілей тестового середовища було використано самопідписаний сертифікат, що спростило розгортання служби у змодельованому середовищі.

Створення шаблонів політик доступу дозволило моделювати типові сценарії використання захищених документів у рамках окремих департаментів організації, що довело можливість реалізації гнучкого управління доступом залежно від ролі користувача.

Тестування роботи служби AD RMS показало ефективність впроваджених механізмів захисту: доступ до документів був успішно обмежений відповідно до встановлених політик, що підтвердило правильність налаштувань і готовність системи до реального використання.

Окрему роль у побудові надійної інфраструктури відіграв Proxmox Backup Server, який було розгорнуто як окрему віртуальну машину. Було налаштовано сховище резервних копій, політику очищення (prune), створено користувача з обмеженими правами та згенеровано API-токен для безпечного доступу. Проведено резервне копіювання ключових віртуальних машин та здійснено успішне тестове

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

‘
відновлення, що підтвердило працездатність системи захисту даних від втрати. Це забезпечує додатковий рівень надійності для всієї інфраструктури.

Таким чином, поставлені завдання кваліфікаційної роботи були повністю виконані, а отримані результати демонструють високий рівень ефективності побудованої системи управління доступом до даних на базі технологій Microsoft.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Active directory domain services overview. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> (date of access: 05.05.2025).
2. Ahmed W. Mastering proxmox. Packt Publishing, Limited, 2014.
3. Benantar M. Access control systems: security, identity management and trust models. Springer, 2010.
4. Cisco networking academy program. / ed. by C. S. Inc, C. N. A. Program. 2nd ed. Indianapolis, Ind : Cisco Press, 2004. 229 c.
5. Ferraiolo D. F., Kuhn D. R., Chandramouli R. Role-Based access control. Artech House Publishers, 2003. 338 c.
6. Lammle T. CCNA Cisco certified network associate study guide. 6th ed. Indianapolis, Ind : Wiley Pub., 2007. 965 c.
7. Mauerer W. Professional linux kernel architecture. New York : John Wiley & Sons, Ltd., 2008.
8. Moskowitz J. Group policy: fundamentals, security, and the managed desktop. Wiley & Sons, Incorporated, John, 2010.
9. Preston W. C. Backup and recovery: inexpensive backup solutions for open systems. O'Reilly Media, Incorporated, 2007.
10. SSL and TLS: theory and practice / ed. by E. Inc. Boston : Artech House, 2009. 273 c.
11. Test lab guide: deploying an AD RMS cluster. Microsoft Learn: Build skills that open doors in your career. URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj134037\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj134037(v=ws.11)) (date of access: 11.05.2025).
12. Thomas O. Windows server 2019 inside out. Microsoft Press, 2021.
13. Welcome to the Proxmox Backup documentation! – Proxmox Backup 3.4.1-1 documentation. Proxmox Backup Server. URL: <https://pbs.proxmox.com/docs/> (date of access: 05.05.2025).

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

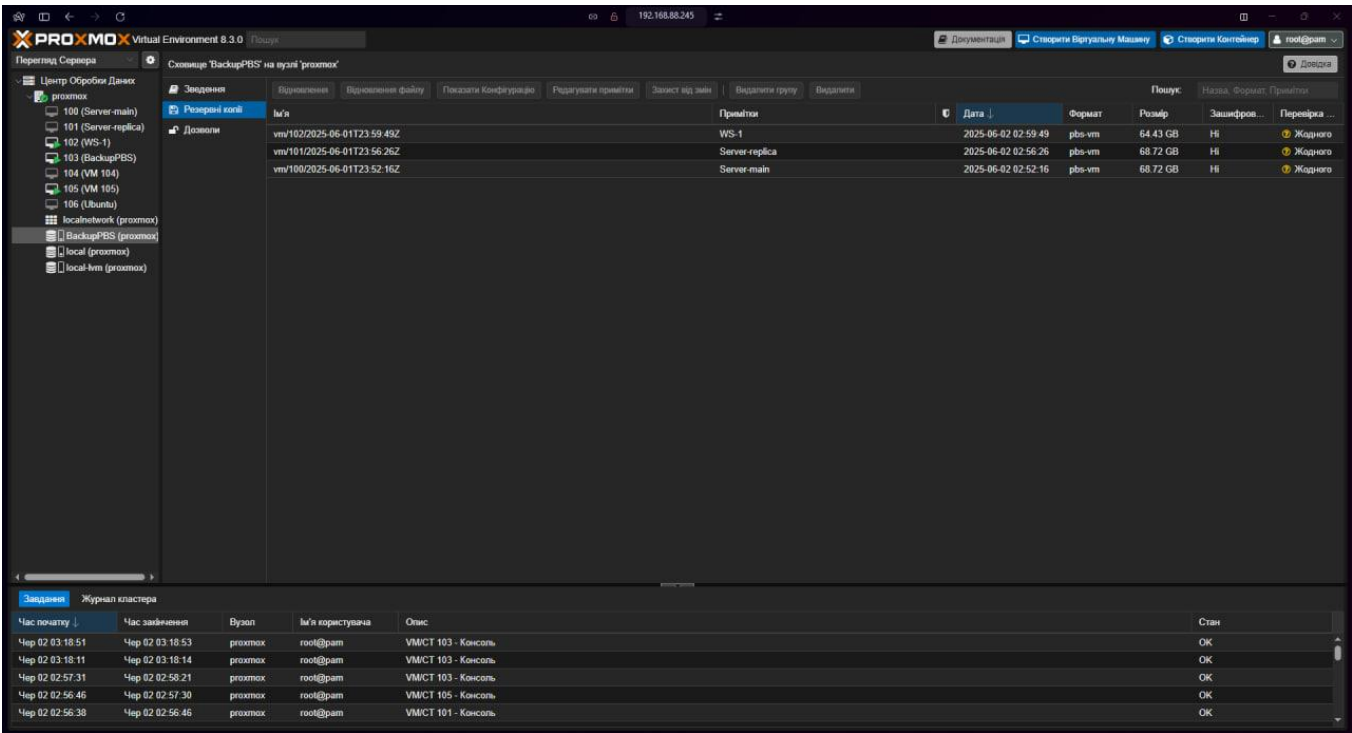
14. Westbrook C. Active directory in windows server 2012 R2. Certpro Limited, 2016.

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Шейко Д. К.			ККІКБ.КР.Б – 123 – 17 – ПЗ	Арк.
		Головня О. С.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Результати примусового збереження.



Огляд інструментів реплікаційного моніторингу.

