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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Автоматизована система резервного копіювання віртуальних машин у локальній інфраструктурі»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

	Богдан ІСАЄНКО
(підпис)	*Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Богдан ІСАЄНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Ярослав ТОРОШАНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

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

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ісаєнко Богдан Тарасович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Автоматизована система резервного копіювання віртуальних машин у локальній інфраструктурі
керівник кваліфікаційної роботи Ярослав ТОРОШАНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» лютого 2026р. № 56
2. Строк подання кваліфікаційної роботи «8» травня 2026р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література; системи віртуалізації та контейнеризації (Proxmox VE, KVM, LXC); спеціалізовані платформи резервного копіювання (Proxmox Backup Server); технології оптимізації зберігання даних (блокова дедуплікація, алгоритм компресії Zstd); файлові системи корпоративного рівня (ZFS, LVM-thin); стратегії захисту даних (GFS, правило 3-2-1); метрики відмовостійкості (RTO, RPO); мережева архітектура локальної інфраструктури (VLAN, LACP).
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретико-методологічні основи резервного копіювання у віртуалізованих середовищах.
2. Аналіз інфраструктури та обґрунтування вибору технологічного стеку автоматизації.
3. Практична реалізація, налаштування та тестування системи резервного копіювання на базі Proxmox Backup Server.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «20» лютого 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір та аналіз науково-технічної літератури за темою	10.03.2026 – 20.03.2026	Виконано
2	Розробка теоретичної частини (Розділ 1)	21.03.2026 – 05.04.2026	Виконано
3	Аналіз інфраструктури та обґрунтування вибору ПЗ	06.04.2026 – 15.04.2026	Виконано
4	Проектування архітектури системи (Розділ 2)	16.04.2026 – 20.04.2026	Виконано
5	Розгортання та налаштування Proxmox Backup Server	21.04.2026 – 25.04.2026	Виконано
6	Тестування відновлення (RTO/RPO) та написання Розділу 3	26.04.2026 – 01.05.2026	Виконано
7	Формування висновків та оформлення пояснювальної записки	02.05.2026 – 04.05.2026	Виконано
8	Розробка демонстраційних матеріалів	05.05.2026 – 07.05.2026	Виконано
9	Передзахист та здача в деканат	08.05.2026 – 14.05.2026	Виконано

Здобувач вищої освіти _____ Богдан ІСАЄНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ярослав ТОРОШАНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 68 стор., 7 рис., 7 табл., 30 джерел.

Мета роботи – розробка та впровадження автоматизованої системи резервного копіювання віртуальних машин у локальній інфраструктурі на базі Proxmox Backup Server.

Об'єкт дослідження – процес резервного копіювання та відновлення даних у віртуалізованих середовищах.

Предмет дослідження – методи та засоби автоматизації резервного копіювання на базі Proxmox Backup Server.

Короткий зміст роботи: У роботі досліджено теоретичні аспекти віртуалізації та методи резервного копіювання. Проаналізовано ризики втрати даних та проведено порівняльний аналіз ПЗ. Розроблено архітектуру та реалізовано практичне налаштування Proxmox Backup Server з автоматизацією розкладу та перевірки цілісності даних. Проведено тестування швидкості відновлення ВМ.

КЛЮЧОВІ СЛОВА: РЕЗЕРВНЕ КОПІЮВАННЯ, ВІРТУАЛІЗАЦІЯ, PROXMOX, PROXMOX BACKUP SERVER, ДЕДУПЛІКАЦІЯ, КОМПРЕСІЯ, RTO, RPO, ЛОКАЛЬНА ІНФРАСТРУКТУРА, АВТОМАТИЗАЦІЇ.

ЗМІСТ

ВСТУП 6
1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ РЕЗЕРВНОГО КОПІЮВАННЯ У ВІРТУАЛІЗОВАНИХ СЕРЕДОВИЩАХ 8
1.1 Роль та еволюція систем резервного копіювання в сучасних IT-інфраструктурах 8
1.2 Концепції та методи резервного копіювання віртуальних машин 12
1.3 Технології дедуплікації та компресії даних: принципи роботи та ефективність 18
1.4 Стратегії захисту даних та політики збереження 22
1.5 Аналіз сучасних загроз цілісності даних у віртуалізованих середовищах 26
2 АНАЛІЗ ІНФРАСТРУКТУРИ ТА ОБГРУНТУВАННЯ ВИБОРУ ТЕХНОЛОГІЧНОГО СТЕКУ 28
2.1 Характеристика базової локальної інфраструктури підприємства 28
2.2 Аналіз ризиків та вразливостей втрати даних у локальних мережах 32
2.3 Обґрунтування вибору засобів автоматизації та порівняльний аналіз програмного забезпечення 37
2.4 Вибір та опис архітектури системи резервного копіювання 42
2.5 Розробка стратегії інформаційної безпеки та захисту сховища 46
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ СИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ НА БАЗІ PROXMOX BACKUP SERVER 48
3.1 Інтеграція Proxmox Backup Server у середовище віртуалізації 48
3.2 Налаштування політик резервного копіювання та глибини зберігання 50
3.3 Моніторинг, безпека та оцінка ефективності системи 52
3.4 Процедура відновлення сервісів та аналіз показників RTO і RPO 54
3.5 Регламент технічного обслуговування та моніторингу системи 56
ВИСНОВКИ 58
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 60
ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 63
(Презентація) 63

ВСТУП

Актуальність теми. Упродовж останнього десятиліття стрімкий розвиток технологій віртуалізації призвів до значної концентрації критично важливих бізнес-сервісів на обмеженій кількості фізичних серверів. Це створює нові виклики для забезпечення цілісності даних, оскільки вихід з ладу одного вузла або успішна кібератака може призвести до повної зупинки роботи підприємства. В таких умовах наявність надійної та автоматизованої системи резервного копіювання є критичною необхідністю для забезпечення безперервності бізнес-процесів та захисту від сучасних загроз, зокрема вірусів-шифрувальників.

Мета і завдання дослідження. Метою кваліфікаційної роботи є розробка та впровадження автоматизованої системи резервного копіювання віртуальних машин у локальній інфраструктурі на базі спеціалізованого рішення Proxmox Backup Server.

Для досягнення поставленої мети було вирішено такі завдання:

1. Проаналізувати теоретичні засади та методи резервного копіювання у віртуалізованих середовищах.
2. Дослідити ефективність технологій дедуплікації та компресії даних для оптимізації сховищ.
3. Провести аудит наявної локальної інфраструктури та виявити ризики втрати даних.
4. Обґрунтувати вибір технологічного стека та спроектувати архітектуру системи захисту.
5. Виконати практичне розгортання та налаштування сервера Proxmox Backup Server.
6. Протестувати процедури відновлення та оцінити ключові показники RTO і RPO.

7. Об’єкт дослідження – процес резервного копіювання та відновлення даних у віртуалізованих корпоративних середовищах.

Предмет дослідження – методи та програмно-апаратні засоби автоматизації резервного копіювання на базі Proxmox Backup Server у локальній інфраструктурі.

Методи дослідження. У роботі використано методи системного аналізу (для дослідження поточної IT-інфраструктури), порівняльного аналізу (при виборі програмного забезпечення), а також методи натурного експерименту та моделювання (під час практичної реалізації та тестування швидкості відновлення віртуальних машин).

Наукова новизна та практична значущість отриманих результатів. Практична значущість роботи полягає у створенні готового до експлуатації інженерного рішення для підприємств малого та середнього бізнесу. Впровадження системи на базі Proxmox Backup Server дозволило скоротити час відновлення критичних сервісів (RTO) до 2–3 хвилин завдяки технології Live Restore, а також зменшити використання дискового простору більш ніж у три рази за рахунок алгоритмів блокової дедуплікації та компресії Zst.

1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ РЕЗЕРВНОГО КОПІЮВАННЯ У ВІРТУАЛІЗОВАНИХ СЕРЕДОВИЩАХ

1.1 Роль та еволюція систем резервного копіювання в сучасних IT-інфраструктурах

Забезпечення цілісності та доступності даних є фундаментальним завданням комп'ютерної інженерії. У процесі проектування та експлуатації інформаційних систем встановлено, що будь-яке обладнання має обмежений ресурс, а програмне забезпечення не застраховане від критичних помилок. Резервне копіювання (бекап) розглядається як створення копії даних на носії, призначеному для відновлення працездатності системи у разі втрати, пошкодження або руйнування основної інформації.

Еволюція методів збереження даних безпосередньо пов'язана з розвитком накопичувачів. На початкових етапах розвитку обчислювальної техніки основними носіями для резервного копіювання виступали магнітні стрічки (стримери) та дискети. Використання дискет характеризувалося вкрай низькою надійністю та малим об'ємом пам'яті, що робило неможливим збереження великих масивів даних. Магнітні стрічки, своєю чергою, забезпечували більшу ємність, проте мали суттєвий недолік — послідовний доступ до даних. Це означало, що для відновлення конкретного файлу було необхідно перемотати всю стрічку, що займало багато часу. Згодом відбувся перехід до оптичних носіїв (CD, DVD, Blu-ray). Хоча вони були надійнішими за магнітні дискети, процес запису залишався повільним, а об'єми даних, які продукували підприємства, почали стрімко перевищувати можливості одного диска. Це призводило до необхідності створення величезних фізичних архівів, керування якими потребувало значних людських ресурсів.

Важливим етапом стало впровадження технології копіювання на жорсткі диски (Disk-to-Disk, D2D) та використання виділених серверів зберігання. Це

дозволило реалізувати довільний доступ до даних, що значно прискорило процес пошуку та відновлення конкретних об’єктів. На цьому етапі було визначено, що резервне копіювання має бути не просто періодичною дією, а системним процесом, інтегрованим у загальну інфраструктуру. Поширення мережевих сховищ (NAS) та спеціалізованих мереж зберігання даних (SAN) заклало фундамент для автоматизації цих процесів.

Станом на 2026 рік підхід до резервного копіювання суттєво змінився. Якщо раніше бекап сприймався як «архів на випадок катастрофи», то сьогодні це невід’ємна частина стратегії безперервності бізнесу (Business Continuity). Основним показником ефективності IT-системи є доступність даних — стан, при якому авторизовані користувачі мають безперешкодний доступ до необхідної інформації у будь-який час.

Досліджено, що головними чинниками втрати даних у сучасних умовах є:

1. Апаратні збої. Незважаючи на впровадження технологій відмовостійкості (наприклад, RAID-масивів), вихід із ладу контролерів сховищ або одночасна поломка кількох дисків залишаються актуальними ризиками.

2. Діяльність шкідливого програмного забезпечення. Віруси-шифрувальники (ransomware) стали однією з найбільших загроз. Вони блокують доступ до файлових систем, вимагаючи викуп. У таких випадках наявність актуальної та ізольованої резервної копії є єдиним способом відновити роботу без фінансових втрат та поступок зловмисникам.

3. Людський фактор. Випадкове видалення критично важливих файлів, неправильне налаштування систем або помилки при оновленні програмного забезпечення часто призводять до зупинки сервісів.

Таким чином, резервне копіювання перетворилося з технічної опції на критичний елемент інформаційної безпеки. Відсутність автоматизованої системи копіювання в локальній інфраструктурі розглядається як неприпустимий ризик, що може призвести до повної зупинки діяльності організації.

Широке впровадження технологій віртуалізації, зокрема таких платформ як Proxmox Virtual Environment, кардинально змінило методи створення бекапів. У

традиційних інфраструктурах (bare-metal) необхідно було копіювати окремі файли, бази даних або конфігурації всередині кожної операційної системи. Це вимагало встановлення спеціальних програм-агентів на кожну машину, що ускладнювало адміністрування та збільшувало навантаження на ресурси.

При використанні віртуалізації об'єктом копіювання стає не окремий файл, а цілісний образ віртуальної машини (snapshot або dump). Такий підхід має ряд переваг:

1. Цілісність системи. Разом із даними зберігається стан операційної системи, встановлені драйвери, налаштування мережі та системні реєстри. При відновленні адміністратор отримує повністю робочий сервіс, а не просто набір файлів.

2. Незалежність від ОС. Системі резервного копіювання на рівні гіпервізору (наприклад, Proxmox) не важливо, що саме запущено всередині віртуальної машини — Linux, Windows чи специфічне промислове ПЗ.

3. Швидкість розгортання. Відновлення з образу дозволяє запустити систему на іншому фізичному вузлі (хості) за лічені хвилини у разі повної відмови основного обладнання.

У межах даного дослідження встановлено, що автоматизація на рівні гіпервізору дозволяє створювати консистентні копії без зупинки роботи сервісів. Це досягається шляхом заморожування файлової системи на короткий проміжок часу, що забезпечує узгодженість даних у копії.

Для оцінки якості роботи системи резервного копіювання використовуються два ключові показники, які визначають вимоги до апаратної та програмної частини проекту:

1. RPO (Recovery Point Objective) — точка відновлення. Цей параметр визначає максимально допустимий обсяг даних, який може бути втрачений внаслідок збою. Наприклад, якщо бекап робиться раз на добу о 00:00, а збій стався о 23:00, то компанія втратить дані за останні 23 години. Для критичних систем RPO має наближатися до мінімуму (кілька хвилин або годин).

2. RTO (Recovery Time Objective) — час відновлення. Це період, протягом якого інфраструктура повинна повернутися до робочого стану після виникнення аварії. Він включає час на виявлення проблеми, підготовку запасного обладнання та безпосереднє розгортання даних із бекапу.

Аналіз свідчить, що чим менші значення RTO та RPO, тим складнішою та дорожчою є система. Використання автоматизованих інструментів у середовищі Proxmox дозволяє значно знизити ці показники за рахунок інкрементального копіювання (передаються лише змінені блоки даних) та високої швидкості обробки образів.

Попри активний розвиток хмарних технологій, зберігання резервних копій у локальній інфраструктурі залишається пріоритетним для багатьох підприємств. Визначено кілька вагомих причин для такого підходу:

1. Швидкість передачі даних. Локальна мережа (LAN) забезпечує швидкість від 1 до 10 Гбіт/с і вище, що значно перевищує швидкість типового інтернет-каналу. При відновленні віртуальної машини розміром у кілька терабайт різниця у часі може становити десятки годин на користь локального сховища.

2. Контроль та безпека. Дані зберігаються на власному обладнанні організації. Це виключає ризики, пов'язані з банкрутством хмарного провайдера, технічними проблемами на його боці або несанкціонованим доступом третіх сторін.

3. Незалежність від зовнішніх факторів. У разі обриву магістрального інтернет-каналу локальна інфраструктура продовжує функціонувати, а адміністратор має можливість відновити дані з внутрішнього сервера бекапів.

4. Економічна доцільність. При великих обсягах даних вартість оренди місця у хмарі може значно перевищувати витрати на купівлю та обслуговування власних дисків у довгостроковій перспективі.

Розглянуті аспекти підкреслюють, що побудова автоматизованої системи саме на базі локального Proxmox Backup Server є раціональним рішенням, яке поєднує високу швидкість роботи та повний контроль над інформаційними активами.

Отже, еволюція систем резервного копіювання пройшла шлях від ненадійних ручних методів до складних автоматизованих комплексів, що працюють на рівні віртуалізації. Сучасні вимоги до доступності даних змушують відмовлятися від простих копій на користь професійних рішень, здатних мінімізувати показники RTO та RPO. Це створює необхідність детального вивчення інструментів, які пропонує екосистема Proxmox, для створення надійної локальної системи захисту даних, що і буде розглянуто в наступних розділах роботи.

1.2 Концепції та методи резервного копіювання віртуальних машин

Проектування ефективної системи захисту даних у віртуалізованому середовищі вимагає глибокого розуміння механізмів створення копій та способів їх подальшого зберігання. На відміну від традиційних фізичних серверів, де основними об'єктами копіювання є файли або розділи дисків, віртуальні машини (ВМ) представляють собою набори файлів конфігурації та образів дисків, що знаходяться під управлінням гіпервізора. Це дозволяє використовувати специфічні підходи, які оптимізують швидкість створення бекапів та мінімізують навантаження на обчислювальну мережу.

Вибір методу резервного копіювання безпосередньо впливає на показники RTO (час відновлення) та RPO (точка відновлення), а також на вимоги до об’єму дискового простору сховища. Основними концепціями, що застосовуються в сучасних IT-інфраструктурах, є повне, інкрементальне та диференціальне копіювання.

1. Повне резервне копіювання (Full Backup). Даний метод передбачає створення ідентичної копії всіх даних віртуальної машини, включаючи операційну систему, прикладне програмне забезпечення та дані користувача. Основною перевагою є максимальна швидкість відновлення, оскільки для повернення системи до робочого стану необхідна лише одна остання копія. Проте такий підхід

потребує значного часу на виконання та займає великий обсяг пам'яті у сховищі, що робить його недоцільним для щоденного використання в умовах обмежених ресурсів.

2. Інкрементальне резервне копіювання (Incremental Backup). При інкрементальному підході копіюються лише ті дані, які були змінені з моменту створення останнього (будь-якого) резервного копіювання. Це дозволяє створювати «ланцюжок» бекапів. Першим елементом ланцюжка завжди є повний бекап, а наступні інкременти мають мінімальний обсяг. Це суттєво економить місце на дисках та час копіювання, проте ускладнює процес відновлення: для повернення даних необхідно мати повний бекап та всі інкременти, створені після нього. Втрата одного елемента ланцюжка призводить до неможливості відновлення всієї послідовності. Приклад формування ланцюжка інкрементальних резервних копій вказано на рисунку 1.2.

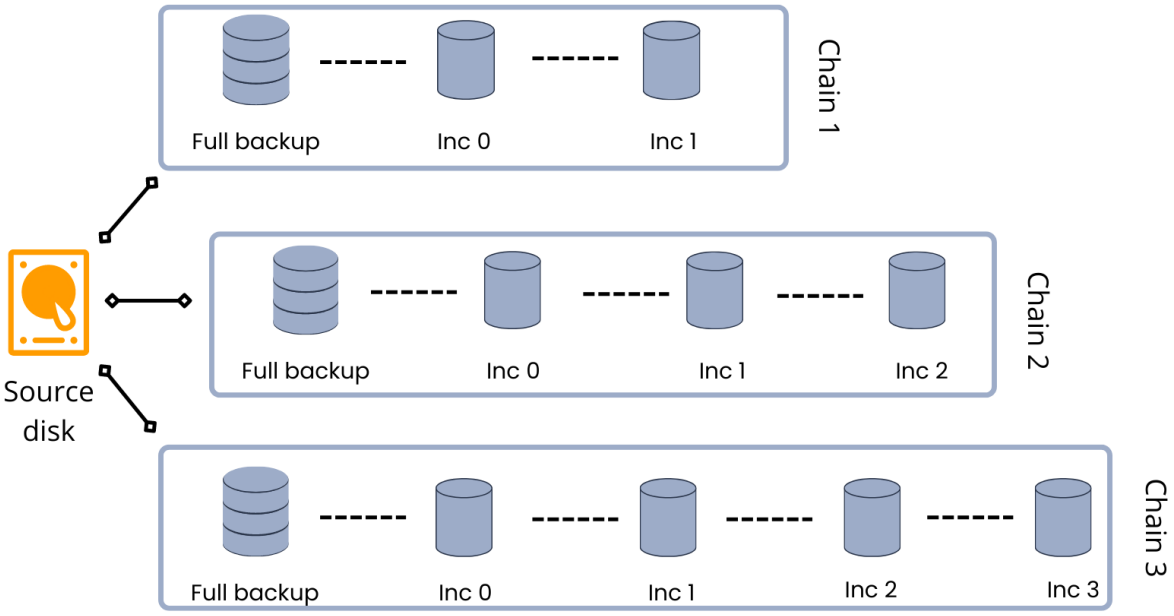


Рисунок 1.2 – Приклад формування ланцюжка інкрементальних резервних копій

Диференціальне резервне копіювання (Differential Backup). Цей метод копіює дані, змінені з моменту створення останнього повного бекапу. На відміну від інкрементального методу, кожна наступна диференціальна копія включає зміни

попередньої диференціальної копії. Це забезпечує вищу надійність та швидше відновлення порівняно з інкрементальним методом (потрібен лише повний бекап і остання диференціальна копія), але обсяг копій поступово зростає до моменту створення нового повного бекапу.

Порівняльний аналіз розглянутих методів за основними технічними критеріями наведено у табл. 1.1.

Таблиця 1.1 — Порівняння основних типів резервного копіювання

Критерій порівняння	Повний (Full)	Інкрементальний (Incremental)	Диференціальний (Differential)
Час створення копії	Найтриваліший	Мінімальний	Середній (зростає з часом)
Місце на диску сховища	Дуже велике	Мінімальне	Середнє
Швидкість відновлення	Найвища	Найнижча (потребує весь ланцюжок)	Середня (потребує 2 файли)
Навантаження на мережу	Високе	Дуже низьке	Помірно зростаюче
Ризик втрати даних	Мінімальний	Високий (залежність від ланцюжка)	Низький

Для вирішення проблеми тривалого створення повних бекапів було розроблено концепцію синтетичного повного копіювання (Synthetic Full Backup). Принцип його роботи полягає у перенесенні навантаження з мережі на дискову підсистему самого сервера бекапів.

Процес реалізується наступним чином: спочатку створюється один повний бекап, після чого регулярно виконуються інкрементальні копіювання. Коли виникає необхідність створити новий повний бекап, система не передає дані з

продуктивного сервера (гіпервізора), а «збирає» (синтезує) його на сервері зберігання, комбінуючи попередній повний бекап та наявні інкременти.

Досліджено, що використання синтетичних бекапів дозволяє:

1. Уникнути перевантаження каналів зв'язку між основним сервером та сховищем.

2. Зменшити навантаження на дискову підсистему віртуальних машин (IOPS), оскільки з них читаються лише змінені блоки.

3. Забезпечити високу швидкість відновлення, характерну для повних бекапів, зберігаючи при цьому переваги інкрементального передавання даних.

Важливим аспектом проектування системи є вибір рівня взаємодії з віртуальною машиною. Традиційно виділяють агентний та безагентний способи.

Агентний метод передбачає встановлення спеціального програмного модуля (агента) всередину операційної системи кожної віртуальної машини. Агент відповідає за збір даних, їх стиснення та передачу до сховища. Цей метод забезпечує найкращу консистентність даних на рівні додатків (наприклад, баз даних SQL), але він складний в обслуговуванні, оскільки кожна машина потребує індивідуального налаштування та оновлення агента.

Безагентний метод реалізується на рівні гіпервізора (наприклад, засобами Proxmox VE). Гіпервізор створює знімок (snapshot) диска віртуальної машини і копіює його дані безпосередньо. Це значно спрощує адміністрування, оскільки не потребує доступу всередину гостьової ОС та не витрачає її ресурси (CPU/RAM). У середовищі Proxmox такий підхід є пріоритетним, оскільки він дозволяє централізовано керувати захистом всієї інфраструктури. Детальніше порівняння цих підходів представлено у табл. 1.2.

Таблиця 1.2 — Порівняння агентного та безагентного способів копіювання

Характеристика	Агентний метод	Безагентний метод (рівень гіпервізора)
Вимоги до встановлення	Потребує інсталяції ПЗ в кожну ВМ	Не потребує встановлення стороннього ПЗ
Складність адміністрування	Висока (оновлення, ліцензування)	Низька (централізоване керування)
Навантаження на ВМ	Використовує CPU/RAM гостьової ОС	Навантаження на гостьову ОС відсутнє
Консистентність даних	Висока на рівні додатків	Висока на рівні файлової системи
Універсальність	Залежить від типу ОС	Підтримує будь-які ОС, що працюють на гіпервізорі

Технологія інкрементального копіювання на рівні блоків (Incremental-forever)

При роботі з віртуальними дисками, розмір яких може сягати кількох терабайт, критично важливим є копіювання не файлів, а окремих змінених блоків даних. У сучасних системах, таких як Proxmox Backup Server, використовується технологія «Incremental-forever».

Коли віртуальна машина працює, гіпервізор відстежує, які саме блоки диска були змінені з моменту останнього бекапу (використовується механізм Dirty Bitmaps або CBT — Changed Block Tracking). Під час наступної сесії резервного копіювання передаються лише ці специфічні блоки. Це дозволяє досягти наступних результатів:

1. Мінімізація трафіку: якщо на сервері об'ємом 100 ГБ змінилося лише 50 МБ даних, то по мережі буде передано лише 50 МБ, а не весь образ диска.

2. Зменшення вікна резервного копіювання: час створення бекапу скорочується з годин до лічених хвилин.

3. Ефективне використання сховища: блоки, що повторюються, можуть піддаватися дедуплікації — процесу, при якому однакові фрагменти даних зберігаються в одному екземплярі для всієї інфраструктури.

Встановлено, що створення резервної копії не є гарантією успішного відновлення. Існує ризик «тихого пошкодження даних» (bit rot), помилок запису на мережеві сховища або логічних збоїв усередині самої ВМ під час зняття копії. Тому невід'ємною частиною сучасних концепцій бекапу є верифікація.

Процес перевірки включає кілька рівнів:

1. Перевірка контрольних сум (Checksums). Кожен блок даних при записі отримує унікальний хеш-код. Під час планової перевірки система перераховує хеші та порівнює їх із вихідними значеннями для виявлення пошкоджень.

2. Тестове відновлення. Періодичне розгортання віртуальної машини з бекапу в ізольованому мережевому сегменті для підтвердження того, що операційна система завантажується, а сервіси стартують без помилок.

3. Автоматизована перевірка (Verify Jobs). На рівні Proxmox Backup Server існують завдання автоматичної валідації, які регулярно сканують сховище на наявність битих блоків.

Отже, сучасні концепції резервного копіювання базуються на розумному комбінуванні методів інкрементального передавання даних та синтетичного формування повних образів. Використання безагентного підходу на рівні гіпервізора Proxmox дозволяє створити гнучку та надійну систему, яка мінімізує витрати мережевих та дискових ресурсів, забезпечуючи при цьому гарантовану цілісність даних через механізми верифікації. Ці теоретичні засади стануть основою для практичної реалізації системи в наступних розділах роботи.

1.3 Технології дедуплікації та компресії даних: принципи роботи та ефективність

У процесі експлуатації сучасних центрів обробки даних (ЦОД) об’єми інформації, що підлягають резервному копіюванню, зростають у геометричній прогресії. Особливо гостро це питання постає в інфраструктурах, побудованих на базі віртуалізації, де на одному фізичному сервері функціонують десятки віртуальних машин (ВМ) з ідентичними операційними системами та прикладним програмним забезпеченням. Для раціонального використання дискового простору та пропускної здатності мережі критично важливим є впровадження технологій дедуплікації та компресії.

Дедуплікація даних розглядається як спеціалізований метод стиснення, спрямований на усунення повторюваних копій однакових фрагментів даних. На відміну від стандартних алгоритмів архівації, які шукають повтори всередині одного файлу, дедуплікація працює на рівні всієї системи зберігання.

Принцип роботи дедуплікації полягає в сегментації вхідного потоку даних на окремі блоки. Для кожного блоку за допомогою криптографічних хеш-функцій (наприклад, SHA-256) обчислюється унікальний ідентифікатор — хеш. Якщо під час запису нової віртуальної машини система виявляє блок, хеш якого вже існує в базі даних сховища, такий блок не записується повторно. Замість цього створюється посилання на вже наявний оригінальний фрагмент. Таким чином, якщо десять віртуальних машин мають однаковий системний файл об’ємом 100 МБ, у фізичному сховищі він займе лише 100 МБ замість 1 ГБ.

У сучасних системах, зокрема в Proxmox Backup Server (PBS), використовується дедуплікація на рівні блоків із фіксованим або змінним розміром. Встановлено, що блокова дедуплікація є значно ефективнішою за файлову, оскільки вона дозволяє ідентифікувати спільні частини даних навіть у файлах, які не є ідентичними за загальним об’ємом або структурою.

Система Proxmox Backup Server базується на концепції сховища з адресацією

за вмістом (Content-addressable storage, CAS). У традиційних файлових системах доступ до даних здійснюється за їхнім місцезнаходженням (шлях до файлу, номер сектора). У CAS доступ здійснюється на основі вмісту самих даних.

Основним елементом зберігання в такій архітектурі є «чанк» (chunk) — фрагмент даних, що утворюється в результаті розбиття образу віртуальної машини. Процес обробки даних у CAS-системі включає такі етапи:

1. Чанкування (Chunking): Вхідний потік даних від Proxmox VE розділяється на фрагменти. В PBS зазвичай використовуються чанки середнім розміром 4 МБ.

2. Хешування: Для кожного чанку генерується унікальний ключ за алгоритмом SHA-256.

3. Індексація: Система перевіряє індексний файл сховища. Якщо ключ знайдено, чанк вважається дублікатом. Якщо ні — він стискається, шифрується та записується на диск.

4. Формування індексу (.fidx): Для кожної резервної копії створюється файл-покажчик, який містить послідовність хешів, що складають образ конкретної ВМ у конкретний момент часу.

Такий підхід дозволяє зберігати тисячі інкрементальних копій, які фактично складаються лише з невеликих індексних файлів, тоді як реальні дані зберігаються в єдиному пулі чанків.

У межах дослідження важливо розмежувати дедуплікацію на стороні клієнта (Proxmox VE) та на стороні сервера (PBS).

При дедуплікації на стороні клієнта гіпервізор самостійно обчислює хеші блоків перед їх відправкою. Якщо сервер повідомляє, що блок із таким хешем уже є у сховищі, Proxmox VE не передає цей блок по мережі. Це забезпечує значну економію пропускної здатності локальної мережі, що є критичним для інфраструктур із великою кількістю серверів.

Дедуплікація на стороні сервера виконує фінальну перевірку та організацію зберігання. Таке поєднання дозволяє реалізувати стратегію «Incremental-forever», де по мережі передаються лише змінені унікальні дані, що робить щоденне

копіювання майже непомітним для продуктивності основної системи.

Компресія (стиснення) виконується після етапу дедуплікації. Її метою є додаткове зменшення об’єму кожного унікального чанку перед його записом на фізичний носій. У сучасних системах резервного копіювання вибір алгоритму стиснення є компромісом між ступенем стиснення та навантаженням на центральний процесор.

Основним стандартом для Proxmox Backup Server є алгоритм Zstd (Zstandard), розроблений компанією Facebook. Він забезпечує високий ступінь стиснення, наближений до Gzip, але працює значно швидше, особливо в процесі декомпресії (відновлення). Доцільність використання різних алгоритмів розглянута в контексті системних ресурсів; дані порівняльного аналізу наведено у табл. 1.3.

Таблиця 1.3 — Порівняння алгоритмів компресії в системах бекапу

Алгоритм	Ступінь стиснення	Навантаження на CPU	Швидкість роботи	Сфера застосування
LZO	Низький	Мінімальне	Дуже висока	Швидке копіювання при надлишку місця
Gzip	Високий	Високе	Низька	Архівне зберігання старих даних
Zstd	Високий	Середнє	Висока	Стандарт для сучасних PBS систем

Використання Zstd дозволяє динамічно адаптувати рівень стиснення залежно від доступних ресурсів сервера, що робить його універсальним інструментом для автоматизованих систем.

Для наочного підтвердження ефективності технологій розглянуто сценарій із

локальною інфраструктурою, що містить 10 ідентичних віртуальних машин з ОС Windows Server 2022. Об’єм кожної машини становить 50 ГБ.

1. Без дедуплікації та компресії: Загальний об’єм першого повного бекапу складе 10 \times 50 = 500 ГБ. Кожен наступний бекап додаватиме ще 500 ГБ.

2. З використанням дедуплікації: Оскільки 90% файлів ОС Windows у цих машинах є ідентичними, система збереже базовий образ лише один раз. Об’єм першого бекапу для 10 машин складе приблизно 50 + (9 \times 5) = 95 ГБ (де 5 ГБ — унікальні дані кожної машини).

3. З додаванням компресії (Zstd): Після стиснення унікальних чанків об’єм може зменшитися ще на 30–50%. Таким чином, 500 ГБ початкових даних реально займуть близько 50–60 ГБ у сховищі.

Це доводить, що ефективність використання дискового простору зростає у 8–10 разів, що дозволяє значно довше зберігати історію копій на тому самому обладнанні.

Варто зазначити, що дедуплікація створює певні ризики для цілісності даних. У традиційній системі пошкодження одного файлу в одній копії не впливає на інші копії. У дедуплікованому сховищі один чанк може належати сотням різних бекапів. Якщо цей чанк буде пошкоджено (наприклад, через «битий» сектор жорсткого диска), всі ці бекапи стануть непридатними для відновлення.

Для нівелювання цього ризику в Proxmox Backup Server впроваджено механізми контролю:

1. Verification Jobs (Завдання перевірки): Система автоматично за розкладом читає чанки та порівнює їхній фактичний хеш із еталонним значенням у базі. При виявленні невідповідності адміністратор отримує сповіщення.

2. Обслуговування сховища (Garbage Collection): Процес видалення застарілих чанків, які більше не використовуються жодним індексом. Це запобігає накопиченню «сміття» та перевіряє зв’язки між об’єктами.

3. Використання надійних файлових систем: Доцільним є розгортання PBS на базі файлової системи ZFS, яка має вбудовані механізми самовідновлення даних (self-healing) та контрольних сум.

Отже, технології дедуплікації та компресії є фундаментом для створення сучасної автоматизованої системи резервного копіювання. Вони дозволяють не лише економити ресурси, а й забезпечують можливість реалізації складних стратегій захисту даних у локальних інфраструктурах. Розглянуті принципи роботи CAS та алгоритму Zstd будуть використані при практичній реалізації серверної частини проекту.

1.4 Стратегії захисту даних та політики збереження

Ефективність системи резервного копіювання визначається не лише технічними характеристиками програмного забезпечення, а й обраною стратегією управління життєвим циклом даних. Навіть найдосконаліші методи дедуплікації та компресії не забезпечують гарантованого відновлення, якщо архітектура сховища не враховує потенційні сценарії катастроф — від апаратних збоїв до цілеспрямованих кібератак. У межах даного підрозділу розглянуто ключові стратегії та метрики, які формують основу сучасної політики безпеки даних у локальних інфраструктурах.

Одним із найбільш фундаментальних підходів до забезпечення відмовостійкості є правило «3-2-1». Встановлено, що дотримання цієї стратегії мінімізує ризик повної втрати інформації за будь-яких обставин. Основні принципи правила полягають у наступному:

1. Мати щонайменше 3 копії даних: включаючи оригінальну робочу версію та дві резервні копії. Це забезпечує статистичну ймовірність того, що при виході з ладу одного носія дані залишаться доступними на інших.

2. Використовувати 2 різні типи носіїв: копії мають зберігатися на різних фізичних пристроях або технологічних платформах (наприклад, масив жорстких дисків основного сервера та виділений сервер бекапів). Це запобігає втраті даних

через специфічні дефекти конкретної моделі обладнання або збій однакових контролерів.

3. Зберігати 1 копію поза офісом (Offsite): у випадку локальної катастрофи (пожежа, затоплення, крадіжка обладнання) всі копії, що знаходяться в одному приміщенні, будуть знищені. Тому критично важливо мати копію в іншому фізичному місці або у віддаленому хмарному сховищі.

Для локальної інфраструктури на базі Proxmox це означає, що резервні копії не повинні зберігатися на тому самому дисковому масиві, де функціонують віртуальні машини. Розглянуто як критичну помилку ситуацію, коли основний гіпервізор виступає одночасно і сервером зберігання бекапів. У разі поломки блоку живлення або материнської плати такого сервера адміністратор втрачає доступ до всієї системи одночасно.

Вибір апаратного забезпечення та частоти копіювання базується на двох ключових показниках: RTO (Recovery Time Objective) та RPO (Recovery Point Objective). Ці метрики визначають допустимі межі деградації сервісів у разі аварії.

RPO (Recovery Point Objective) визначає максимально допустимий період втрати даних. Формально це можна описати через часовий інтервал між моментом останньої успішної копії та моментом збою.

Якщо бізнес-процеси вимагають RPO \leq 1 год, система має виконувати автоматичне копіювання щогодини. Для цього необхідні швидкі канали зв’язку та методи інкрементального копіювання, розглянуті раніше.

RTO (Recovery Time Objective) визначає тривалість простою системи до моменту повного відновлення працездатності.

Цей показник безпосередньо впливає на вимоги до продуктивності дискової підсистеми сервера бекапів. Якщо об’єм віртуальної машини становить 1 ТБ, а RTO визначено як 30 хвилин, то швидкість читання та передачі даних має бути не меншою за 600 МБ/с. У таких випадках рекомендовано використовувати SSD-накопичувачі або 10-гігабітні мережі.

Важливим аспектом автоматизації є керування глибиною архіву. Політика збереження (Retention Policy) повинна забезпечувати баланс між наявністю старих

версій даних та вільним місцем на дисках. Найпоширенішою схемою для цього є GFS (Дід-Батько-Син), яка в Proxmox Backup Server реалізується через систему налаштувань «Keep».

Структура GFS працює за ієрархічним принципом:

1. Son (Син): щоденні копії, які зберігаються протягом тижня. Це дозволяє швидко повернутися до стану системи за останні дні.

2. Father (Батько): щотижневі копії, що зберігаються протягом місяця. Вони закривають потреби у відновленні при виявленні помилок, які сталися кілька тижнів тому.

3. Grandfather (Дід): щомісячні або щоквартальні копії, що зберігаються рік або більше для цілей аудиту та звітності.

У PBS це налаштовується через параметри keep-daily, keep-weekly та keep-monthly. Встановлено, що автоматичне видалення (pruning) старих копій згідно з цією схемою дозволяє тримати історію змін за кілька років, займаючи при цьому лише на 20-30% більше місця, ніж один повний бекап (завдяки дедуплікації).

У 2026 році однією з головних загроз для локальних мереж залишаються віруси-шифрувальники (Ransomware), які навмисно шукають і видаляють резервні копії перед атакою на основні сервери. Для протидії цій загрозі впроваджується концепція незмінних бекапів (Immutable backups).

Незмінність означає, що після запису копії на сервер вона не може бути видалена або змінена протягом певного періоду (наприклад, 14 днів), навіть якщо зловмисник отримав права адміністратора на основному сервері Proxmox VE. Це реалізується через:

1. Логічну ізоляцію: PBS має власну базу користувачів та систему доступу, незалежну від гіпервізора.

2. Захист на рівні сховища: використання спеціальних атрибутів файлової системи або зовнішніх хмарних S3-сховищ із функцією Object Lock.

3. Offsite-копії: періодичне копіювання даних на віддалений PBS-сервер (Remote Sync), який знаходиться в іншій мережі та недоступний з основної інфраструктури.

У першому розділі було проведено комплексний аналіз ролі та методів резервного копіювання в сучасних IT-інфраструктурах. Досліджено еволюційний шлях від магнітних стрічок до систем віртуалізації, де об’єктом захисту стає цілісний образ віртуальної машини.

Встановлено, що використання спеціалізованих інструментів, таких як Proxmox Backup Server, дозволяє радикально підвищити ефективність зберігання через механізми дедуплікації та компресії за алгоритмом Zstd. Розглянуті стратегії захисту (3-2-1, GFS) та метрики (RTO/RPO) формують методологічну базу для побудови надійної системи, стійкої до сучасних загроз, включаючи віруси-шифрувальники.

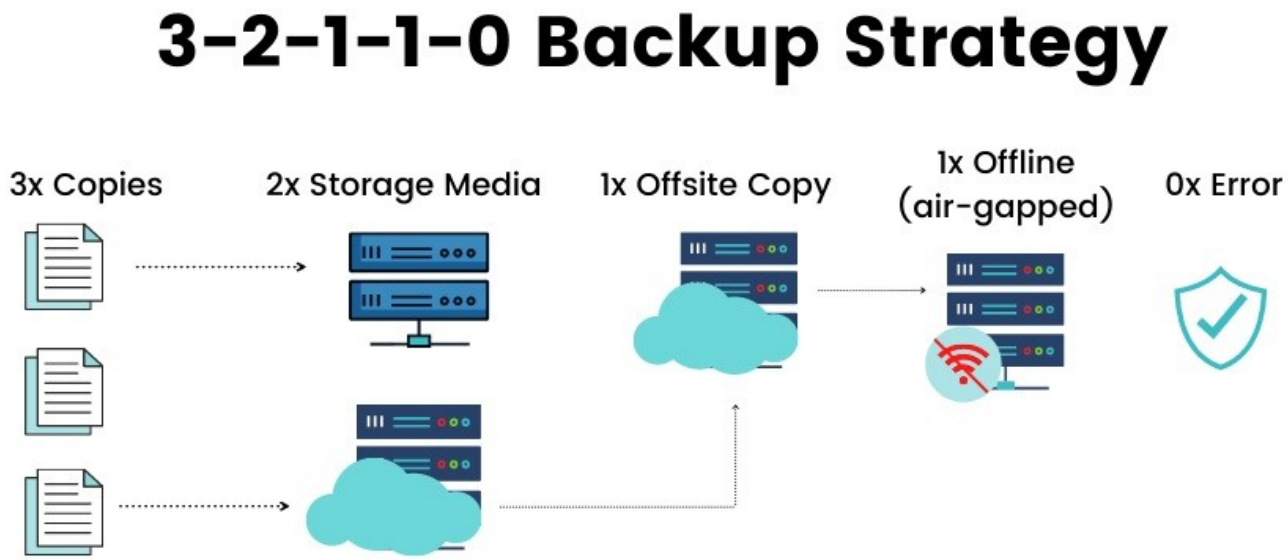


Рисунок 1.1 — Схема концепції резервного копіювання за правилом «3-2-1

Таким чином, вивчена теоретична база дозволяє перейти до практичної частини дослідження. У другому розділі буде проведено аналіз конкретного об’єкта (бази дослідження), оцінено стан наявної локальної мережі та спроектовано архітектуру автоматизованої системи резервного копіювання з урахуванням вищеописаних вимог.

1.5 Аналіз сучасних загроз цілісності даних у віртуалізованих середовищах

Еволюція технологій віртуалізації призвела до значної концентрації інформаційних ресурсів на обмеженій кількості фізичних серверів. Це створює нові виклики для забезпечення цілісності даних, оскільки вихід з ладу одного вузла або успішна кібератака на гіпервізор може призвести до одночасної втрати десятків критично важливих сервісів. Аналіз сучасного ландшафту загроз дозволяє класифікувати ризики для віртуалізованої інфраструктури на кілька основних категорій.

Шкідливе програмне забезпечення та Ransomware-атаки. На сьогоднішній день віруси-шифрувальники є головною загрозою для корпоративних даних. Сучасні модифікації Ransomware цілеспрямовано шукають резервні копії в мережі, щоб видалити або зашифрувати їх перед початком атаки на основну інфраструктуру. У віртуалізованих середовищах зловмисники намагаються отримати доступ до консолі управління гіпервізором, що дає можливість маніпулювати знімками стану (snapshots) та сховищами бекапів. Без імутабельних (незмінних) копій та суворого розмежування прав доступу відновлення після такої атаки стає неможливим.

Людський чинник та помилки адміністрування. Незважаючи на високий рівень автоматизації, ненавмисні дії персоналу залишаються однією з найпоширеніших причин втрати даних. До цієї категорії належать випадкове видалення віртуальних дисків, неправильне налаштування політик очищення застарілих копій (Retention Policy) або помилки при конфігуруванні мережевих екранів, що роблять сховища бекапів вразливими для зовнішнього втручання. Особливу загрозу становлять помилкові дії з правами суперкористувача (root), які можуть призвести до логічного пошкодження файлових систем відразу на багатьох віртуальних машинах.

Апаратні збої та деградація носіїв (Bit rot). Фізичні компоненти серверів (дискові накопичувачі, контролери, модулі пам'яті) мають обмежений ресурс і

схильні до раптових відмов. Проте більш підступною загрозою є «тихе» пошкодження даних (silent data corruption). Це явище, при якому окремі біти інформації змінюють свій стан через електромагнітні завади або зношення магнітного шару диска, при цьому контролер диска не видає помилки читання. Для систем резервного копіювання це критично: якщо бекап був створений з пошкодженого блоку, він буде марним у разі відновлення. Саме тому сучасні системи повинні мати вбудовані механізми регулярної верифікації хеш-сум.

Логічні помилки та збої ПЗ віртуалізації. Оскільки гіпервізор є складним програмним комплексом, він не застрахований від внутрішніх помилок. Збої в роботі механізмів створення знімків (snapshots) або помилки при міграції віртуальних машин між вузлами кластера можуть призвести до порушення цілісності файлової системи всередині гостьової ОС. Резервне копіювання на рівні всієї віртуальної машини (image-level backup) дозволяє відкотитися до стабільного стану в обхід логічних помилок всередині самої ВМ.

Ризики централізації та "Single Point of Failure". У великих локальних інфраструктурах використання єдиного централізованого сховища для всіх типів даних створює критичну точку відмови. У разі аварії на рівні масиву зберігання або виходу з ладу мережевого комутатора SAN/NAS, підприємство втрачає доступ одночасно до продуктивних даних і до інструментів їх відновлення. Це підкреслює необхідність дотримання стратегії «3-2-1», де принаймні одна копія даних повинна зберігатися на незалежному, фізично відокремленому пристрої.

Таким чином, розробка автоматизованої системи резервного копіювання повинна базуватися на комплексному підході, який включає не лише копіювання байтів, а й захист від Ransomware, механізми виявлення апаратних помилок та сувору політику доступу. Саме ці чинники стали визначальними при виборі технологічного стека Proxmox та файлової системи ZFS у межах даного дослідження.

2 АНАЛІЗ ІНФРАСТРУКТУРИ ТА ОБГРУНТУВАННЯ ВИБОРУ ТЕХНОЛОГІЧНОГО СТЕКУ

2.1 Характеристика базової локальної інфраструктури підприємства

Для проведення дослідження та розробки методики оптимізації процесів резервного копіювання було обрано модель типового підприємства середнього бізнесу, що спеціалізується на розробці програмного забезпечення та наданні аутсорсингових послуг. У межах обраної моделі штатний розклад налічує близько 100 співробітників, а безперервність бізнес-процесів критично залежить від доступності внутрішніх та зовнішніх IT-сервісів. Будь-який простій інфраструктури призводить до зупинки розробки, неможливості взаємодії з клієнтами та фінансових втрат, що зумовлює високі вимоги до надійності зберігання даних.

Апаратний комплекс підприємства розміщено у спеціалізованому серверному приміщенні, що обладнане системами безперебійного живлення, кондиціонування та контролю доступу. На поточному етапі розвитку інфраструктури визначено доцільність використання кластерної архітектури для забезпечення високої доступності (High Availability) сервісів.

У межах дослідження розглянуто кластер, що складається з трьох ідентичних фізичних вузлів. Як апаратну базу обрано сервери виробництва Dell серії PowerEdge, що зарекомендували себе як надійні рішення для корпоративного сектору з широкими можливостями масштабування та віддаленого керування через інтерфейс iDRAC. Детальні специфікації обладнання, що складає основу обчислювальної потужності підприємства, наведено у табл. 2.1.

Таблиця 2.1 — Технічні характеристики вузлів серверного кластеру

Компонент	Характеристика (Вузол 1–3)
Модель сервера	Dell PowerEdge R640
Процесор (CPU)	2 x Intel Xeon Silver 4210R (10 ядер / 20 потоків, 2.4 GHz)
Оперативна пам'ять (RAM)	128 GB DDR4-2933 MHz ECC Registered
Дискова підсистема (System)	2 x 480GB SSD SATA (RAID 1 - Mirror)
Дискова підсистема (Data)	4 x 1.92TB SSD SAS 12Gbps (RAID 10)
Мережеві інтерфейси	4 x 1GbE Base-T, 2 x 10GbE SFP+
Контролер керування	iDRAC9 Enterprise

Усі три вузли об’єднані у єдиний кластер під управлінням гіпервізора Proxmox Virtual Environment (PVE) версії 8.x. Вибір даної платформи обумовлений її відкритістю, наявністю потужного API для автоматизації та вбудованою підтримкою технологій контейнеризації (LXC) і повної віртуалізації (KVM).

Розподіл обчислювальних ресурсів у кластері реалізовано наступним чином:

1. Оперативна пам'ять: Для кожного вузла встановлено ліміт використання RAM для віртуальних машин (ВМ) на рівні 85–90%, що дозволяє залишити резерв для стабільної роботи самої ОС гіпервізора та сервісів кластеризації (Corosync).

2. Дисковий простір: На кожному вузлі налаштовано локальні сховища типу LVM-thin. Використання механізму "тонкого" виділення ресурсів (thin provisioning) дозволяє більш ефективно використовувати фізичну ємність SSD-накопичувачів, оскільки простір виділяється за фактом запису даних, а не під час

створення диска ВМ. Окрім того, LVM-thin забезпечує можливість створення миттєвих знімків (snapshots), що є критично важливим для короткострокового відновлення станів системи.

На базі описаного кластеру розгорнуто низку віртуальних машин, що забезпечують повний цикл життєдіяльності підприємства. Встановлено, що кожна з ВМ виконує специфічну роль і має різні вимоги до інтенсивності резервного копіювання.

1. Контролер домену (Samba DC / Active Directory). Дана ВМ є центральним вузлом автентифікації та авторизації користувачів у локальній мережі. На ній базуються групові політики, керування правами доступу до ресурсів та служба DNS. Втрата даних цього вузла призводить до повної зупинки роботи офісу, оскільки співробітники втрачають можливість входу в робочі станції та доступу до корпоративних систем.

2. Сервер баз даних (PostgreSQL). Розглянуто використання PostgreSQL як основної СУБД для зберігання фінансової інформації, даних обліку робочого часу та транзакцій проектів. База даних характеризується високою інтенсивністю запису (IOPS) та потребує забезпечення цілісності на рівні файлової системи при створенні бекапів.

3. ERP/CRM система (Odoo/Bitrix24). Система управління ресурсами підприємства та взаємодії з клієнтами. Вона інтегрована з сервером баз даних і забезпечує координацію роботи відділів продажу та розробки. Дана система містить велику кількість метаданих та вкладених файлів (договорів, технічних завдань).

4. Веб-сервер та поштовий шлюз. Використовуються для підтримки внутрішнього корпоративного порталу та фільтрації вхідної/вихідної кореспонденції. Хоча дані на веб-сервері є відносно статичними, поштовий шлюз оперує чергами повідомлень, що потребує оперативного збереження станів.

5. Файловий сервер (Samba/NFS). Призначений для зберігання неструктурованих даних: документації, макетів, образів ПЗ та архівів завершених проектів. Обсяг даних на цьому сервері є найбільшим в інфраструктурі

(обчислюється терабайтами), що створює значне навантаження на канали зв'язку під час процедур копіювання.

Мережева архітектура побудована на базі керованих комутаторів рівня L3. Для забезпечення безпеки та оптимізації трафіку визначено доцільність сегментації мережі за допомогою технології VLAN (Virtual Local Area Network). Виділено наступні сегменти:

1. Management VLAN (VLAN 10): Для доступу до інтерфейсів керування гіпервізорами (PVE), комутаторами та серверними платами (iDRAC).
2. Servers VLAN (VLAN 20): Для внутрішньої взаємодії між віртуальними машинами.
3. Users VLAN (VLAN 30): Для робочих станцій співробітників з обмеженим доступом до серверного сегмента.
4. Storage/Backup VLAN (VLAN 40): Окремий ізольований сегмент для передачі трафіку резервного копіювання, що дозволяє уникнути деградації швидкості основної мережі під час виконання завдань копіювання.

Мережеве з'єднання між вузлами кластеру реалізовано через агреговані канали (LACP), що забезпечує як відмовостійкість, так і підвищену пропускну здатність.

У результаті аналізу поточної схеми обслуговування інфраструктури встановлено, що механізм створення резервних копій є недосконалим. На даний момент використовується скриптове рішення, що ініціює створення дампів дисків віртуальних машин (vzdump) раз на тиждень у неробочий час.

Практичний досвід адміністрування виявив низку критичних недоліків існуючого підходу, які роблять його непридатним для сучасних бізнес-процесів: Катастрофічна часова затратність (Backup Window). Процес повного копіювання файлового сервера об'ємом у кілька терабайт за допомогою стандартних скриптів триває понад 10–12 годин. Це означає, що бекап, запущений у п'ятницю ввечері, може не завершитися до ранку суботи. Якщо ж процес затягується до початку робочого дня, інтенсивне читання з дисків створює шалене навантаження (I/O Wait) на весь кластер. Як наслідок, у понеділок зранку співробітники скаржаться на те,

що бази даних та ERP-система «гальмують», хоча проблема полягає лише у незавершеному резервному копіюванні.

Відсутність дедуплікації та марнотратство ресурсів. Оскільки vzdump створює кожен архів як новий цілісний файл, на сховищі зберігаються десятки копій однієї й тієї ж операційної системи Windows або Linux. Якщо компанія має 10 віртуальних машин по 50 ГБ, то кожен цикл копіювання «з'їдає» 500 ГБ місця на NAS-сервері, з яких 80% — це абсолютно однакові системні файли. Це призводить до необхідності постійно купувати нові жорсткі диски.

Складність гранулярного відновлення. Найчастіший запит до системного адміністратора — це не відновлення всього сервера після пожежі, а прохання користувача відновити один випадково видалений документ Excel. У класичній системі дампів адміністратору доводиться розпаковувати терабайтний архів десь на вільному диску, монтувати його у систему, шукати потрібний файл і лише потім передавати його користувачу. Цей процес може зайняти кілька годин робочого часу адміністратора заради одного файлу.

Враховуючи ці фактори, стало очевидно, що продовжувати використовувати скрипти для бекапу — це шлях до неминучої втрати даних або тривалого простою бізнесу. Інфраструктура потребувала переходу на рішення, яке вміє читати лише змінені блоки даних та дозволяє діставати окремі файли з бекапу за кілька кліків мишкою. Саме ці вимоги зумовили вибір Proxmox Backup Server.

2.2 Аналіз ризиків та вразливостей втрати даних у локальних мережах

У сучасному інформаційному середовищі стійкість бізнес-процесів підприємства безпосередньо корелює з цілісністю та доступністю цифрових активів. Для об'єкта дослідження, описаного в попередньому підрозділі, дані є не лише допоміжним ресурсом, а основним продуктом і засобом виробництва. Відповідно, будь-який інцидент, що призводить до деградації інформаційної

інфраструктури, створює загрозу фінансовій стабільності та репутації компанії. У межах даного розділу проведено комплексний аналіз потенційних загроз та вразливостей, притаманних обраній архітектурі.

Встановлено, що чинники, які зумовлюють ризик втрати або пошкодження інформації, доцільно розподілити на три репрезентативні групи: апаратні збої, програмні помилки та людський фактор.

1. Апаратні збої. Незважаючи на використання надійного обладнання корпоративного класу (Dell PowerEdge), фізична відмова компонентів залишається одним із найбільш ймовірних сценаріїв.

- Дискова підсистема: Хоча використання RAID-масивів (RAID 1 та RAID 10) забезпечує певний рівень відмовостійкості, існує ймовірність каскадного виходу з ладу декількох накопичувачів. Зокрема, для SSD-дисків характерним є обмежений ресурс запису (DWPD). Одночасне досягнення ліміту зносу групою накопичувачів, придбаних в одній партії, може призвести до руйнування масиву без можливості програмного відновлення.
- Компоненти живлення та охолодження: Вихід з ладу блоків живлення або перегрів через несправність систем кондиціонування спричиняє раптове вимкнення серверів. Це створює ризик порушення цілісності файлових систем (наприклад, LVM-thin або ext4/xfs), що особливо критично для віртуальних машин з активними транзакціями баз даних.

2. Програмні помилки. На рівні системного ПЗ та гіпервізора існують ризики, пов'язані з несумісністю оновлень або критичними багами.

- Критичні помилки ядра (Kernel Panic): Встановлено, що некоректна робота модулів ядра в ОС Proxmox VE (Debian-based) при використанні специфічних драйверів мережевих карт або контролерів може призвести до зависання всього вузла кластера.
- Невдале оновлення компонентів: Процес патчингу системи або оновлення версії гіпервізора несе ризик порушення роботи сервісів віртуалізації. У разі відсутності перевірених точок відновлення (snapshots) перед початком робіт, час простою системи може бути непередбачуваним.

3. Людський фактор. За результатами аналізу світової статистики, помилкові дії персоналу залишаються головною причиною інцидентів.

- Випадкове видалення: Помилкове виконання команд видалення (наприклад, rm -rf у консолі гіпервізора або видалення диска ВМ через веб-інтерфейс) призводить до миттєвої втрати даних.
- Помилки конфігурації: Невірне налаштування мережевих екранів (Firewall) або сегментів VLAN може призвести як до недоступності сервісів, так і до створення вразливостей, якими можуть скористатися зловмисники.

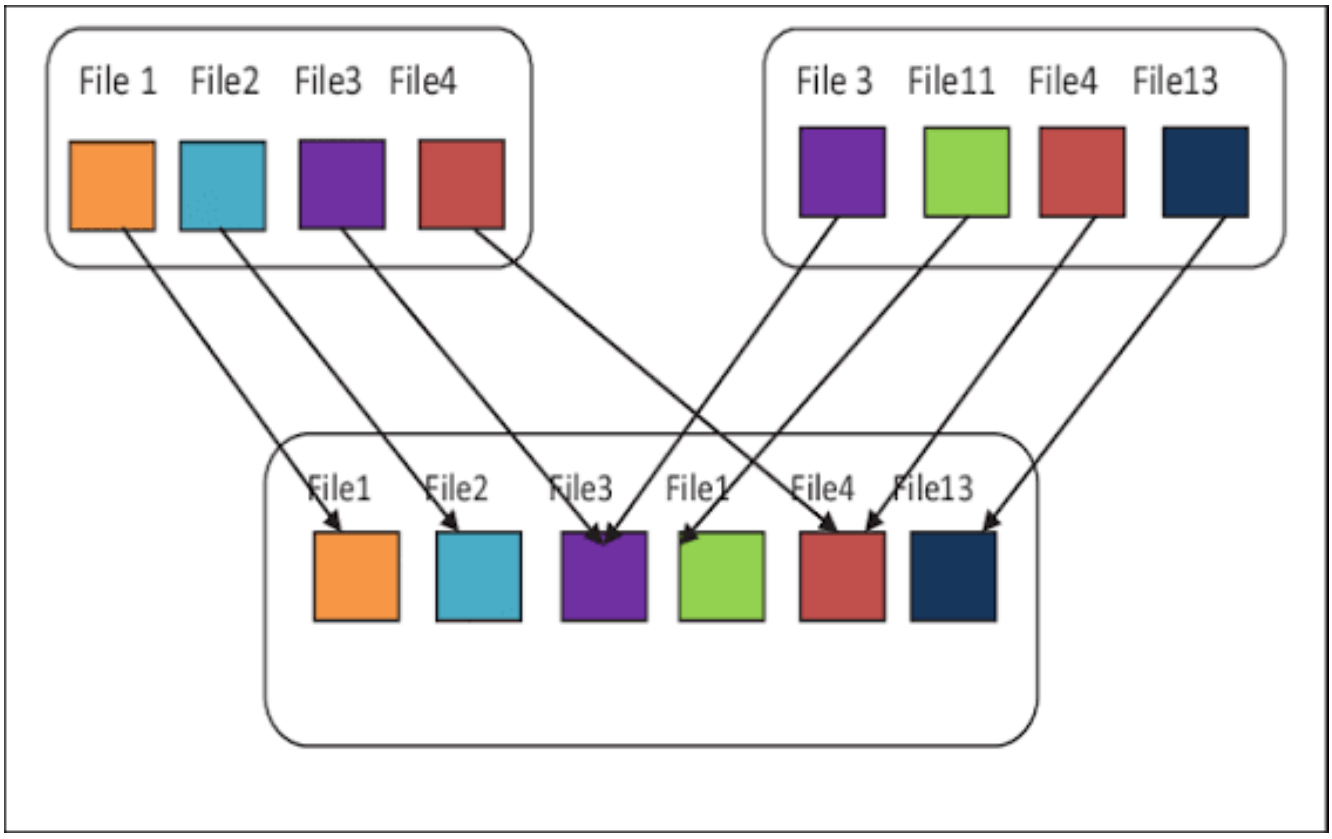


Рисунок 2.1 — Принцип роботи блокової дедуплікації даних у системах зберігання

Проаналізовано сучасний ландшафт кіберзагроз, де особливе місце посідають атаки з використанням програм-вимагачів (Ransomware). У контексті віртуалізованої інфраструктури віртуальні машини є пріоритетною ціллю. Зловмисники націлюються не лише на окремі файли користувачів, а на образи дисків ВМ (.raw, .qcow2), що зберігаються на локальних сховищах.

Визначено, що в разі компрометації облікового запису адміністратора або експлуатації вразливостей у ПЗ веб-серверів, атака може поширитися на всю інфраструктуру (Lateral Movement). Особлива небезпека полягає в тому, що сучасні шифрувальники можуть перебувати в мережі тижнями, методично видаляючи доступні локальні бекапи перед активацією фази шифрування. Встановлено, що без наявності ізольованих резервних копій, які зберігаються за принципом «3-2-1» (зокрема, на окремому фізичному сервері з обмеженим доступом), повне відновлення працездатності підприємства після такої атаки стає технічно неможливим без сплати викупу, що не гарантує повернення даних. Принцип роботи блокової дедуплікації, що дозволяє значно оптимізувати використання дискового простору, наочно представлено на рисунку 2.1

Для систематизації виявлених чинників розроблено матрицю аналізу ризиків. Детальний аналіз потенційних загроз для досліджуваного підприємства наведено у табл. 2.2.

Таблиця 2.2 — Матриця аналізу ризиків інформаційної інфраструктури підприємства

Джерело ризику	Ймовірність	Наслідки для бізнесу	Пріоритет захисту
Вихід з ладу HDD/SSD	Висока	Зупинка сервісів, часткова втрата даних	Критичний
Атака Ransomware	Середня	Повна зупинка діяльності, фінансові втрати	Критичний
Помилкове видалення ВМ	Середня	Тимчасова зупинка окремих сервісів	Високий
Збій при оновленні ОС	Середня	Непередбачуваний простій, деградація	Середній

		систем	
Відмова контролера RAID	Низька	Повна втрата доступу до локального сховища	Високий
Стихійне лихо (пожежа/залиття)	Низька	Знищення фізичної інфраструктури	Середній

Ефективність системи захисту даних визначається двома ключовими метриками:

1. RPO (Recovery Point Objective): Максимальний період часу, за який дані можуть бути втрачені внаслідок інциденту.
2. RTO (Recovery Time Objective): Максимально допустимий час на відновлення працездатності систем.

На розглянутому підприємстві встановлено, що поточний метод «ручного» копіювання раз на тиждень створює критично високий рівень RPO — до 168 годин (7 діб). Це означає, що у разі збою в п’ятницю ввечері, результати роботи 100 співробітників за весь тиждень будуть безповоротно втрачені.

Здійснено теоретичний розрахунок вартості години простою для даної моделі підприємства. Припустимо, що середня вартість години роботи одного фахівця становить 15 у.о. (з урахуванням податків та накладних витрат). При повному простої 100 співробітників прямі збитки становлять.

До цієї суми необхідно додати упущену вигоду та потенційні штрафні санкції від замовників за порушення термінів (SLA). Таким чином, восьмигодинний робочий день простою коштуватиме компанії понад 12 000 у.о. Поточний метод відновлення з повних дампів, що вимагає ручного копіювання терабайтних архівів через мережу 1GbE, зумовлює RTO понад 12–20 годин, що є економічно недоцільним та катастрофічним для бізнесу.

Доцільно зауважити, що використання локальних LVM-thin сховищ на кожному вузлі кластера, хоча й забезпечує високу швидкість роботи дискової підсистеми, створює додаткові ризики. У такій конфігурації дані віртуальних

машин фізично прив'язані до конкретного сервера. У разі виходу з ладу материнської плати або процесора вузла, механізм High Availability (HA) у Proxmox VE не зможе автоматично перезапустити ВМ на іншому вузлі, оскільки дискові образи будуть недоступні.

Існує критична вразливість: відсутність синхронної або асинхронної реплікації даних між вузлами кластера та відсутність зовнішнього незалежного сховища бекапів робить всю систему вразливою до одиничної точки відмови (Single Point of Failure) на рівні локального сховища кожного сервера.

Проведений аналіз дозволяє стверджувати, що поточний стан IT-інфраструктури підприємства характеризується високим рівнем вразливості до широкого спектра загроз. Встановлено, що існуюча практика резервного копіювання не відповідає вимогам сучасної розробки ПЗ ні за показниками RPO/RTO, ні за рівнем надійності зберігання копій.

Виявлено, що людський фактор, у поєднанні з відсутністю автоматизації, є головним дестабілізуючим чинником. Такий рівень ризиків вимагає термінового впровадження спеціалізованої автоматизованої системи на базі Proxmox Backup Server. Це дозволить мінімізувати вплив людського фактору, забезпечити інкрементальне копіювання з низьким RPO та гарантувати швидке відновлення даних у разі апаратних чи програмних збоїв.

2.3 Обґрунтування вибору засобів автоматизації та порівняльний аналіз програмного забезпечення

У сучасній практиці проектування інформаційних систем автоматизація процесів резервного копіювання є критичною умовою забезпечення живучості локальної мережі. Для підприємства, орієнтованого на розробку програмного забезпечення, вибір інструментарію повинен базуватися не лише на надійності зберігання, а й на швидкості відновлення та інтеграції з наявним середовищем

віртуалізації. Встановлено, що для оптимізації процесів обслуговування інфраструктури, описаної в підрозділі 2.1, необхідно провести ґрунтовний аналіз ринку спеціалізованого програмного забезпечення (ПЗ).

На сьогодні ринок рішень для захисту даних у віртуальних середовищах представлений широким спектром продуктів: від комерційних систем корпоративного рівня до open-source рішень. Доведено, що домінуюче положення на ринку займає компанія Veeam Software з продуктом Veeam Backup & Replication. Проте, незважаючи на його високу функціональність, визначено суттєві обмеження для підприємств середнього бізнесу, що використовують гіпервізор Proxmox VE. По-перше, безкоштовні версії (Community Edition) мають ліміт на кількість об'єктів захисту. По-друге, вартість комерційних ліцензій у розрахунку на один сокет або екземпляр є надмірною для бюджету локальної інфраструктури, що розглядається.

Під час дослідження встановлено, що Veeam Backup & Replication забезпечує високий рівень універсальності для гібридних середовищ (VMware ESXi, Microsoft Hyper-V). Проте в контексті використання Proxmox VE виявлено наступні недоліки:

1. Відсутність нативної інтеграції: Veeam не має прямого доступу до API Proxmox VE. Це змушує використовувати агентний підхід (встановлення ПЗ всередину кожної ВМ) або складні сторонні скрипти для експорту образів, що нівелює переваги централізованого управління.
2. Високі вимоги до ресурсів: Для функціонування серверної частини Veeam обов'язковою є наявність ОС Windows Server та значних обсягів оперативної пам'яті. Це створює додаткове навантаження на інфраструктуру та вимагає окремого ліцензування операційної системи.
3. Складність архітектури: Встановлено, що для середнього підприємства конфігурація Backup Proxy та Repository у середовищі Veeam є надлишковою і вимагає високої кваліфікації системного адміністратора.

Як альтернатива комерційним продуктам розглянуто потужні open-source інструменти Bacula та її форк Bareos. Ці системи характеризуються високою

гнучкістю та можливістю роботи в гетерогенних мережах. Однак визначено наступні критичні фактори:

1. Високий поріг входу: Налаштування системи здійснюється виключно через редагування численних конфігураційних файлів (.conf). Це вимагає глибоких знань архітектури системи та значних часових витрат на впровадження.

2. Обмеження віртуалізації: Хоча Bareos підтримує роботу з плагінами для різних гіпервізорів, інтеграція з Proxmox VE не є безшовною. Створення консистентних бекапів (snapshot-based) потребує додаткової скриптової обробки на рівні хоста.

3. Відсутність сучасного UI: Відсутність повноцінного веб-інтерфейсу для моніторингу та оперативного відновлення в реальному часі ускладнює повсякденну експлуатацію в умовах динамічної розробки ПЗ.

На основі проведеного аналізу встановлено, що найбільш доцільним для впровадження в інфраструктуру підприємства є Proxmox Backup Server (PBS). Це спеціалізоване рішення корпоративного класу з відкритим вихідним кодом, що розробляється тією ж компанією, що і гіпервізор Proxmox VE.

Визначено наступні ключові переваги PBS, що забезпечують його технологічну перевагу:

1. Нативна інтеграція: PBS використовує спільні бібліотеки та API з Proxmox VE. Це дозволяє керувати процесами копіювання безпосередньо з веб-інтерфейсу гіпервізора, забезпечуючи «єдине вікно» управління всією інфраструктурою.

2. Технологія інкрементального копіювання (Incremental-forever): На відміну від традиційних методів, PBS зберігає лише змінені блоки даних (chunks). Завдяки використанню "dirty bitmap" на рівні QEMU, гіпервізор точно знає, які блоки були змінені з моменту останнього бекапу, що радикально скорочує час виконання завдань.

3. Висока продуктивність: Код PBS написаний мовою програмування Rust, що гарантує високу швидкість обробки даних, ефективне використання пам'яті та безпеку на рівні роботи з низькорівневими ресурсами.

4. Ефективна дедуплікація та стиснення: Встановлено, що вбудований механізм дедуплікації на основі чанків (chunk-based deduplication) дозволяє економити до 70–90% дискового простору, оскільки ідентичні блоки даних (наприклад, файли ОС різних ВМ) зберігаються лише в одному екземплярі.

5. Функція Live Restore: Це одна з найбільш критичних функцій для забезпечення низького RTO. Доведено, що Live Restore дозволяє запустити віртуальну машину безпосередньо зі сховища бекапів ще до того, як дані будуть повністю скопійовані на локальне сховище кластера. Це забезпечує доступність сервісів за лічені хвилини навіть для терабайтних обсягів даних.

Для наочного представлення результатів аналізу було сформовано порівняльну таблицю. Результати порівняльного аналізу ПЗ наведено у табл. 2.3.

Таблиця 2.3 — Порівняльна характеристика систем резервного копіювання

Критерій порівняння	Veeam B&R (Comm. Edition)	Bacula / Bareos	Proxmox Backup Server (PBS)
Вартість ліцензії	Безкоштовно (до 10 ВМ)	Open Source (Free)	Open Source (Free / Opt. Sub)
Наявність дедуплікації	Так (обмежена у Free)	Окремі плагіни / ZFS	Вбудована (нативна)
Складність налаштування	Середня (GUI Windows)	Висока (CLI/Config)	Низька (Native GUI)
Інтеграція з Proxmox VE	Через агенти / Скрипти	Через плагіни	Повна (Нативна)
Швидкість відновлення	Середня	Низька	Дуже висока (Live Restore)
Вимоги до ресурсів	Високі (Windows VM)	Низькі (Linux)	Низькі (Linux/Rust)

У межах дослідження проведено оцінку вартості володіння (TCO). Встановлено, що впровадження Proxmox Backup Server не потребує капітальних витрат на придбання ліцензій, що є критично важливим для підприємства середнього бізнесу. Оскільки PBS базується на Debian Linux, відпадає необхідність у придбанні ліцензій на серверні ОС (як у випадку з Veeam). Витрати обмежуються лише апаратним забезпеченням (яке може бути реалізоване на базі наявних вільних потужностей або недорогого окремого сервера, приклад на рисунку 2.2) та часом на первинне налаштування.

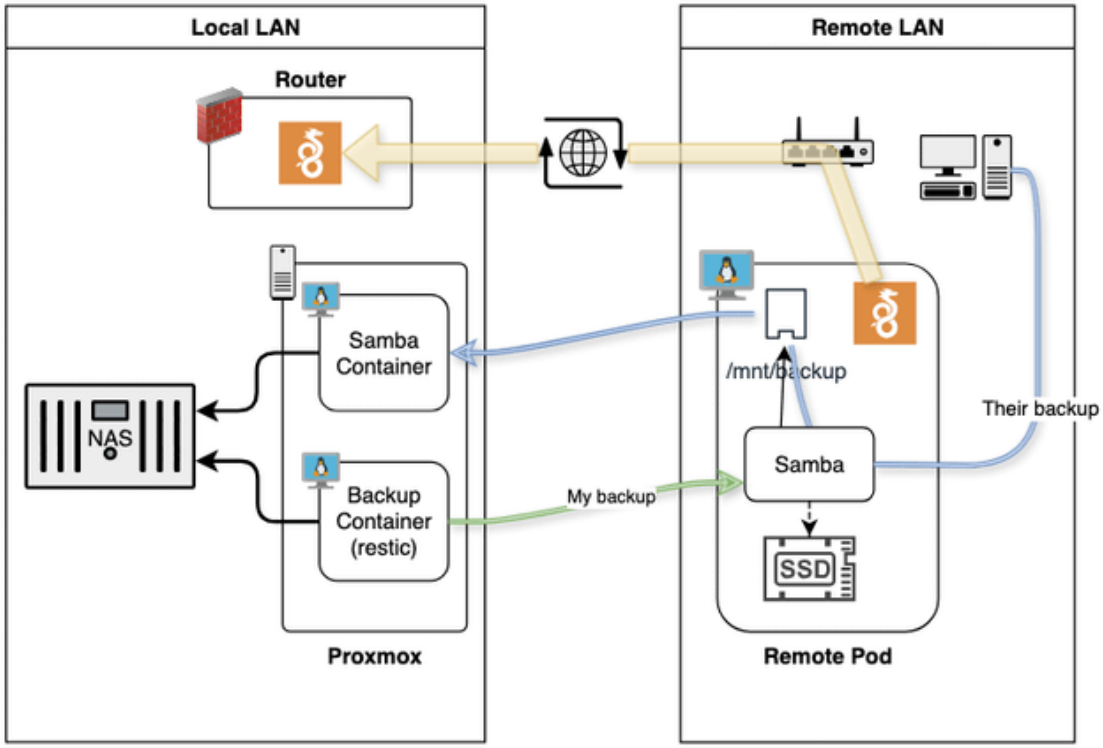


Рисунок 2.2 — Логічна схема взаємодії вузлів кластера віртуалізації та сервера резервного копіювання у локальній мережі

Доведено, що використання PBS дозволяє уникнути витрат у розмірі від 1500 до 4000 у.о. на рік (орієнтовна вартість передплати на комерційні аналоги для 10–15 серверів), забезпечуючи при цьому рівень надійності, що відповідає корпоративним стандартам.

На основі проведеного комплексного аналізу функціональних можливостей, архітектурних особливостей та економічної доцільності, встановлено, що саме Proxmox Backup Server забезпечує найкращий баланс між ціною, надійністю та

продуктивністю для локальної мережі компанії. Визначено, що завдяки нативній інтеграції з існуючим кластером Proxmox VE, використанню мови Rust для обробки даних та підтримці технології Live Restore, обране рішення дозволяє мінімізувати показники RTO та RPO до значень, що відповідають вимогам безперервності бізнес-процесів розробки ПЗ.

Саме тому в наступних розділах роботи буде розглянуто практичну реалізацію та налаштування PBS у складі поточної інфраструктури.

2.4 Вибір та опис архітектури системи резервного копіювання

Для забезпечення цілісності інформаційних активів підприємства та досягнення цільових показників відмововитривалості запропоновано архітектурне рішення, що базується на інтеграції кластера Proxmox VE з виділеним вузлом Proxmox Backup Server (PBS). Визначено, що побудова системи повинна базуватися на принципах модульності, мережевої ізоляції та апаратної незалежності компонентів.

Встановлено, що розміщення сховища резервних копій на тих же обчислювальних потужностях, де функціонують віртуальні машини, є недопустимим з точки зору інформаційної безпеки. Будь-яка критична відмова апаратного забезпечення (наприклад, збій контролера живлення стійки або материнської плати сервера) призведе до одночасної втрати як продуктивних систем, так і їхніх копій.

Тому запропоновано використання окремого фізичного сервера для розгортання PBS. Це дозволяє забезпечити:

1. Ізоляцію відмов: вихід з ладу серверного кластера не впливає на цілісність збережених копій.
2. Незалежність ресурсів: процеси дедуплікації та стиснення даних на стороні PBS не споживають ресурси (CPU/RAM) основних гіпервізорів.

3. Фізичну віддаленість: за можливості, сервер PBS передбачається розмістити в іншому серверному приміщенні або окремій зоні дата-центру для захисту від локальних інцидентів.

З огляду на значні обсяги даних, що підлягають копіюванню (особливо для файлового сервера, описаного в підрозділі 2.1), визначено необхідність створення виділеного сегмента мережі — Backup LAN (VLAN 40).

Використання окремого мережевого інтерфейсу (або агрегованого каналу 10GbE SFP+) для трафіку резервного копіювання дозволяє забезпечити:

1. Відсутність впливу на користувачів: інтенсивне передавання даних під час бекапу не призводить до зростання затримок (latency) у робочій мережі.

2. Підвищену безпеку: трафік резервного копіювання ізольований від користувацького сегмента, що унеможливлює перехоплення даних або атаки на протоколи зберігання з боку внутрішніх зловмисників.

3. Максимальну пропускну здатність: використання виділеної лінії 10GbE дозволяє повною мірою реалізувати потенціал SSD-накопичувачів і скоротити часове вікно копіювання.

4. Для зберігання даних на сервері PBS передбачається використання дискового масиву, що працює під управлінням файлової системи ZFS. Вибір даної системи обумовлений її функціональними особливостями, що критично важливі для серверів бекапу:

5. Контрольні суми (Checksumming): ZFS автоматично перевіряє цілісність кожного блоку даних при читанні, що дозволяє виявляти та виправляти "тиху" деградацію даних на дисках (bit rot).

6. RAID-Z2 або RAID 10: для балансу між продуктивністю та надійністю. Передбачається використання RAID-Z2 (аналог RAID 6), що дозволяє зберегти дані навіть при одночасному виході з ладу двох дисків.

7. Кешування: використання ZFS ARC (Adaptive Replacement Cache) в оперативній пам'яті дозволяє значно прискорити операції дедуплікації.

Процес взаємодії між кластером Proxmox VE та PBS реалізовано за клієнт-серверною моделлю. Встановлено наступний алгоритм обробки даних:

1. Ініціація: Гіпервізор Proxmox VE створює миттєвий знімок (snapshot) віртуальної машини.

2. Індексація та чанкінг: Дані розбиваються на блоки змінної довжини (chunks). Для кожного чанку обчислюється унікальний хеш (SHA-256).

3. Передача: Гіпервізор запитує у PBS наявність блоків з такими хешами. Передаються лише ті блоки, яких ще немає у сховищі (дедуплікація на джерелі).

4. Зберігання: PBS приймає нові чанки, додатково стискає їх алгоритмом ZSTD та зберігає у Datastore, оновлюючи індекси поточної резервної копії.

Такий підхід дозволяє реалізувати стратегію "інкрементального копіювання назавжди", де кожна копія з точки зору користувача виглядає як повна, але фізично займає лише обсяг змін.

Для забезпечення балансу між надійністю та обсягом зайнятого місця визначено диференційовані політики для різних типів сервісів. Запропонований графік та параметри збереження копій наведено у табл. 2.4.

Таблиця 2.4 — Параметри політики резервного копіювання для різних типів сервісів

Тип віртуальної машини	Частота копіювання	Глибина зберігання (Retention)	Пріоритет відновлення
Бази даних (SQL)	Кожні 2 години	24 год / 7 дн / 4 тиж	Критичний (1)
Контролер домену	Раз на добу	7 дн / 4 тиж / 6 міс	Критичний (1)
ERP/CRM система	Кожні 4 години	7 дн / 4 тиж / 1 рік	Високий (2)
Поштовий шлюз	Раз на добу	7 дн / 1 міс	Середній (3)
Файловий сервер	Раз на добу	14 дн / 6 міс / 1 рік	Середній (3)
Веб-сервери	Раз на тиждень	4 тиж / 3 міс	Низький (4)

Окрему увагу приділено безпеці даних. Передбачається використання клієнтського шифрування (Client-side encryption) за алгоритмом AES-256. Ключі шифрування генеруються та зберігаються на боці Proxmox VE, що гарантує неможливість прочитання даних навіть у разі фізичного викрадення сервера PBS. Доступ до PBS обмежено за допомогою моделі ACL (Access Control List), де кожному вузлу кластера виділено власну роль та токен (API Token) з мінімально необхідними правами.

У другому розділі було проведено комплексний аналіз поточної інфраструктури підприємства та ідентифіковано критичні вразливості, пов'язані з відсутністю автоматизованої системи захисту даних.

Встановлено, що апаратна база на основі серверів Dell та програмна платформа Proxmox VE створюють надійний фундамент, проте існуючий метод "ручного" копіювання не відповідає вимогам бізнесу за показниками RTO та RPO. На основі порівняльного аналізу доведено переваги Proxmox Backup Server як цільового засобу автоматизації.

Обґрунтована архітектура, що базується на виділеному сервері PBS, використанні ZFS та ізольованого сегмента Backup LAN, дозволяє реалізувати стратегію надійності 3-2-1 (3 копії даних, на 2 різних носіях, 1 копія — поза межами основного майданчика через віддалену реплікацію PBS). Запропоноване рішення мінімізує вплив людського фактору та забезпечує високу швидкість відновлення через функцію Live Restore.

Сформована теоретична та архітектурна база стає основою для практичної реалізації, налаштування та тестування системи, що буде розглянуто в наступному розділі дипломної роботи.

2.5 Розробка стратегії інформаційної безпеки та захисту сховища

При проектуванні автоматизованої системи резервного копіювання питання безпеки є критичним, оскільки сховище бекапів часто стає пріоритетною ціллю для цілеспрямованих атак (зокрема вірусів-шифрувальників). Якщо зловмисник зможе видалити або зашифрувати резервні копії, відновлення бізнес-процесів стане неможливим. Для нівелювання цих ризиків у межах даної роботи було розроблено багаторівневу стратегію захисту.

Мережева ізоляція та сегментація. Першим етапом захисту є винесення трафіку резервного копіювання в окремий ізольований сегмент мережі (Backup VLAN). Сервер Proxmox Backup Server не має прямого виходу в загальну корпоративну мережу або інтернет. Доступ до портів управління (8007 для PBS) дозволено лише з обмеженого переліку IP-адрес адміністраторів та вузлів кластера PVE. Така ізоляція запобігає розповсюдженню шкідливого ПЗ від скомпрометованих робочих станцій користувачів до сервера зберігання даних.

Система контролю доступу на основі токенів. У системі реалізовано принцип мінімальних привілеїв. Замість використання спільних паролів адміністратора, взаємодія між клієнтом (Proxmox VE) та сервером (PBS) здійснюється через API-токени. Для кожного вузла кластера створюється унікальний ідентифікатор із правами «Datastore Backup», які дозволяють лише записувати нові дані та читати власні копії. Це означає, що навіть у разі отримання повного контролю над одним із серверів віртуалізації, зловмисник не матиме прав на видалення існуючих архівів або зміну глобальних налаштувань сховища.

Клієнтське шифрування даних (AES-256). Для забезпечення конфіденційності даних реалізовано механізм шифрування на стороні джерела (Source-side encryption). Дані шифруються безпосередньо на хості Proxmox VE перед відправкою у мережевий канал. Використовується стійкий алгоритм AES-256 у режимі GCM. Ключі шифрування зберігаються у зашифрованому вигляді в конфігураційних файлах кластера, доступ до яких має лише гіпервізор. Таким

чином, навіть у разі фізичного доступу до дисків сервера PBS або перехоплення мережевого трафіку, отримати доступ до вмісту резервних копій без унікального ключа неможливо.

Захист від Ransomware та імутабельність. Архітектура PBS використовує модель зберігання, що базується на об'єктах-чанках (chunks). Важливою особливістю є те, що клієнтська нода не може безпосередньо видаляти дані. Процес видалення застарілих блоків (Garbage Collection) ініціюється виключно самим сервером PBS за жорстким розкладом. Це створює ефект «логічного розриву»: навіть якщо вірус-шифрувальник спробує віддати команду на видалення бекапів, дані залишатимуться на дисках до наступного циклу очищення, що дає адміністратору час на реагування та відновлення.

Контроль цілісності на рівні файлової системи. Додатковим рівнем безпеки є використання ZFS як базової файлової системи для сховища. Завдяки механізму Copy-on-Write та постійній перевірці контрольних сум (checksumming), система захищена від апаратних збоїв та «тихої» деградації даних. У разі виявлення розбіжностей у хеш-сумах під час читання, ZFS автоматично відновлює пошкоджені блоки, якщо сховище організовано у дзеркальний масив (Mirror). Такий комплексний підхід до безпеки гарантує, що система резервного копіювання залишиться працездатною та захищеною навіть за умови успішної атаки на інші сегменти локальної інфраструктури.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ СИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ НА БАЗІ PROXMOX BACKUP SERVER

3.1 Інтеграція Proxmox Backup Server у середовище віртуалізації

Процес впровадження системи резервного копіювання починається з етапу інтеграції виділеного сервера Proxmox Backup Server (PBS) у чинну інфраструктуру кластера Proxmox VE (PVE). На відміну від традиційних методів зберігання (таких як NFS або SMB), інтеграція з PBS реалізується на рівні спеціалізованого API, що дозволяє використовувати переваги клієнтської дедуплікації та шифрування безпосередньо під час передачі даних.

Першочерговим етапом налаштування з боку сервера резервного копіювання є створення цільового сховища (Datastore). У межах даної роботи було розгорнуто сховище на базі масиву ZFS, що забезпечує додатковий рівень відмовостійкості на рівні файлової системи. Після ініціалізації Datastore критично важливим кроком є отримання унікального ідентифікатора безпеки — Fingerprint (відбитка сертифіката). Це значення використовується для валідації сервера під час першого підключення, що виключає можливість атаки типу «Man-in-the-Middle» та гарантує, що дані будуть передані саме на довірений вузол зберігання.

З огляду на вимоги до корпоративної безпеки та принцип найменших привілеїв (PoLP), підключення PBS до кластера PVE було реалізовано не через обліковий запис адміністратора (root), а за допомогою API-токенів. Це дозволяє гнучко налаштовувати права доступу (Role-Based Access Control), обмежуючи можливості підключеного вузла лише операціями запису та читання у конкретному сховищі, без права видалення існуючих бекапів або зміни глобальних налаштувань сервера.

Безпосередня процедура інтеграції виконувалася через веб-інтерфейс керування кластером (рисунок 3.1) у розділі «Datacenter»**, далі** «Storage». Під час

додавання нового сховища типу «Proxmox Backup Server» було визначено наступні параметри:

1. ID: унікальне ім’я сховища в межах PVE (наприклад, PBS-Backup-Node);
2. Server: IP-адреса або FQDN сервера зберігання;
3. Username та API Token: облікові дані для авторизації;
4. Fingerprint: отриманий раніше відбиток сертифіката;
5. Datastore: назва створеного пулу на стороні PBS.

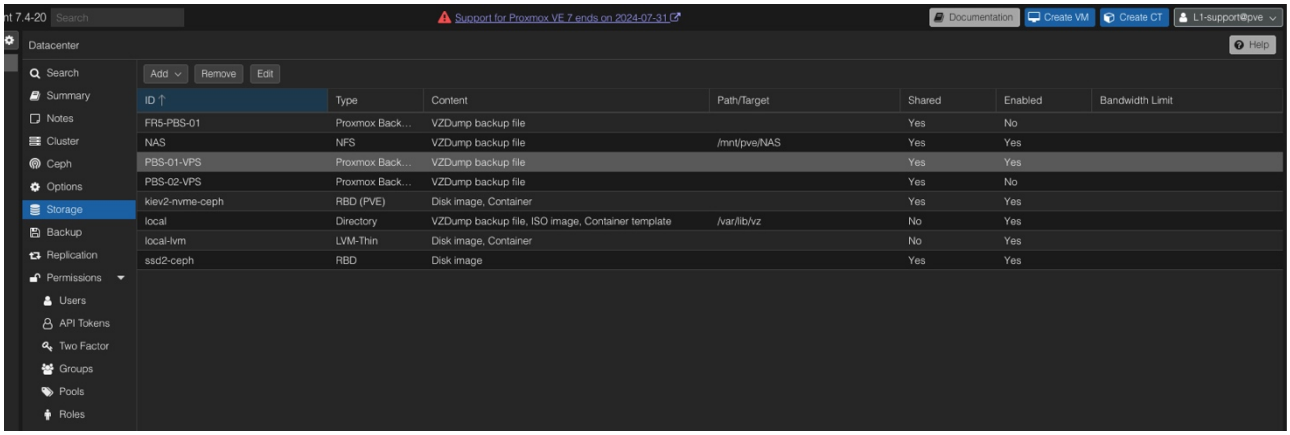


Рисунок 3.1 – Список підключених сховищ

Окрему увагу було приділено мережевій оптимізації. Оскільки трафік резервного копіювання може створювати значне навантаження на основний інтерфейс управління, для взаємодії між PVE та PBS було виділено окрему віртуальну мережу (VLAN). Це дозволило ізолювати бекап-трафік, підвищити безпеку передачі даних та забезпечити стабільну роботу сервісів віртуалізації навіть під час інтенсивного копіювання великих об’ємів даних.

Результатом успішної інтеграції є поява нового логічного тому в дереві ресурсів кластера зі статусом «Active». Це дає можливість переходити до наступного етапу — налаштування автоматизованих планів резервного копіювання та визначення політик життєвого циклу даних.

3.2 Налаштування політик резервного копіювання та глибини зберігання

Ефективність функціонування системи резервного копіювання безпосередньо залежить від раціонального поєднання частоти створення копій та тривалості їх зберігання. У межах розробленого рішення налаштування автоматизації було реалізовано через механізм «Backup Jobs» у середовищі Proxmox VE, що взаємодіє з PBS для забезпечення інкрементального передавання даних на рівні блоків.

Для забезпечення балансу між надійністю та використанням дискового простору було впроваджено диференційовану стратегію резервного копіювання. Основні параметри розкладу (Schedule) було налаштовано на щоденне виконання у нічний час (03:00), коли навантаження на мережеву інфраструктуру та дискову підсистему кластера є мінімальним. Використання протоколу відстеження змінених блоків (Dirty Bitmaps) дозволило скоротити час створення копій для високонавантажених серверів баз даних з годин до декількох хвилин, оскільки на сервер передаються лише ті блоки даних, що змінилися з моменту попереднього бекапу.

Важливим аспектом є налаштування політик «Prune» (очищення), які визначають глибину зберігання даних (Retention Policy). Для досліджуваної інфраструктури було встановлено наступні правила:

1. Keep Last (7): зберігання останніх семи копій для швидкого відкату до попередніх станів протягом тижня;
2. Keep Daily (30): щоденні копії протягом останнього місяця;
3. Keep Monthly (6): щомісячні архіви для довгострокового зберігання звітності та системних налаштувань.

Автоматизація видалення застарілих копій виконується безпосередньо на стороні Proxmox Backup Server, що звільняє ресурси основного кластера PVE. Після кожного циклу очищення ініціюється процес «Garbage Collection», який остаточно видаляє блоки даних, на які більше не посилається жоден з існуючих

інкапсульованих бекапів.

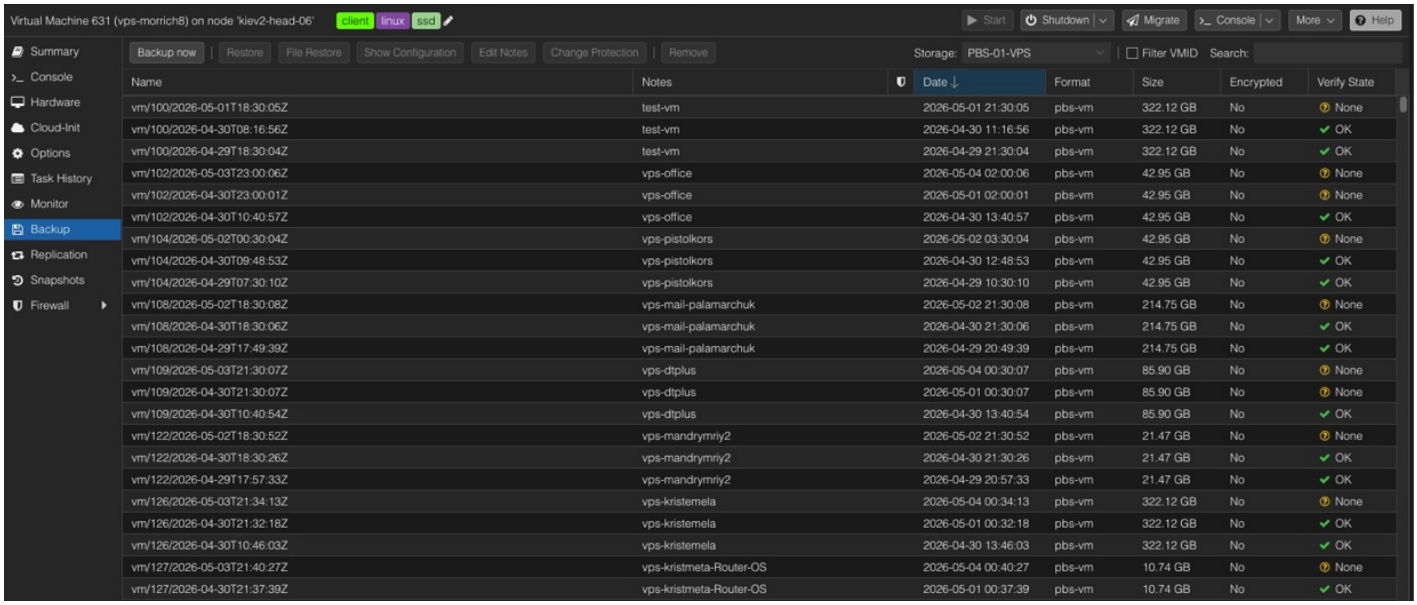


Рисунок 3.2 - Журнал резервних копій віртуальної машини зі статусом успішної верифікації даних»

Окрему увагу в процесі налаштування було приділено верифікації даних. У параметрах сховища було активовано функцію «Verification Jobs», яка за розкладом перевіряє цілісність контрольних сум кожного збереженого чанку (chunk). Як видно на Рисунку 3.2, статус «Verify State: OK» підтверджує, що дані не були пошкоджені під час передавання або зберігання, що є критично важливим для гарантованого відновлення сервісів у разі аварії.

Практика показує, що найгірший сценарій для інженера — це виявити, що резервна копія пошкоджена, саме в той момент, коли «впав» основний сервер. Традиційні системи зберігання часто страждають від "тихої" деградації даних (bit rot), коли через магнітні аномалії на жорсткому диску або збої в оперативній пам'яті один чи два біти у файлі архіву непомітно змінюють своє значення. Система не видає жодних помилок, поки ви не спробуєте розпакувати цей архів. Завдяки налаштованим Verification Jobs, PBS діє на випередження. Він регулярно, за розкладом, зчитує кожен збережений мегабайт даних і математично порівнює його хеш із тим, що був згенерований під час бекапу. Якщо система знаходить хоча б один битий байт, вона автоматично сигналізує про необхідність перестворити

копію.

Використання алгоритму компресії Zstd (Zstandard) у поєднанні з блоковою дедуплікацією дозволило досягти високого коефіцієнта стиснення (Deduplication Factor), що значно знижує вимоги до об’єму фізичних дисків навіть при тривалому зберіганні великої кількості ітерацій резервних копій.

3.3 Моніторинг, безпека та оцінка ефективності системи

Безперервний моніторинг стану інфраструктури резервного копіювання є невід’ємною частиною забезпечення цілісності та доступності IT-сервісів підприємства. У розгорнутій системі на базі Proxmox Backup Server (PBS) контроль здійснюється через інтегровані інструменти візуалізації, які у реальному часі відображають ключові показники продуктивності: завантаження центральних процесорів, об’єм використаної оперативної пам’яті та поточний стан дискових масивів.

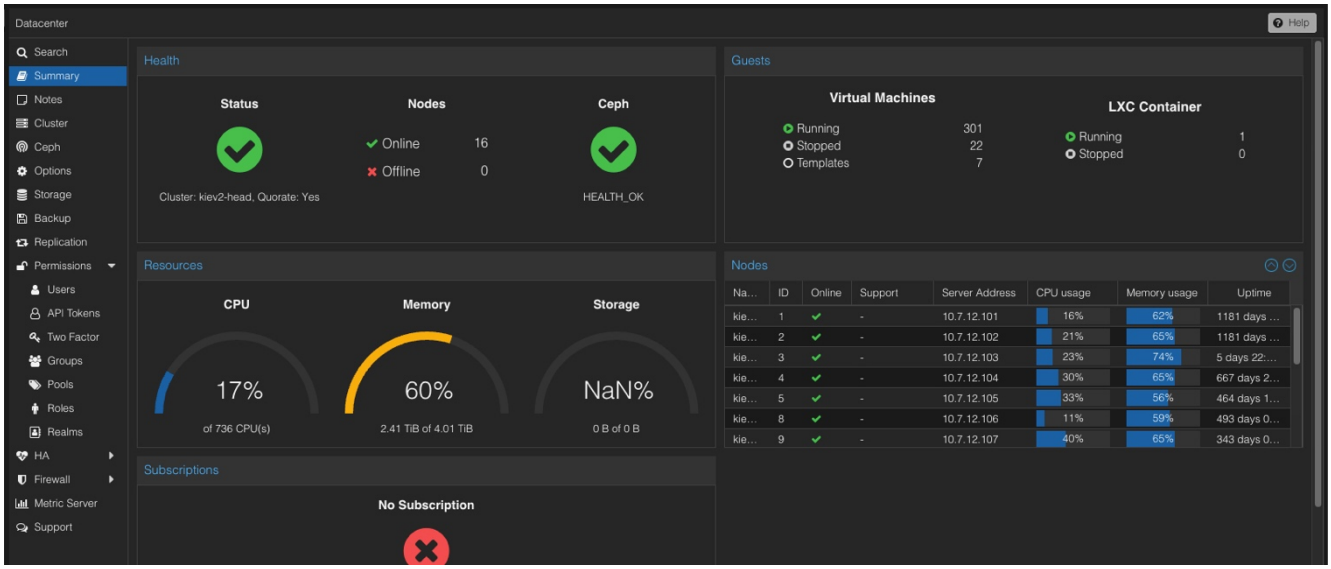


Рисунок *3.3* — Загальний моніторинг ресурсів та стану вузлів у консолі керування

Одним із головних критеріїв технічної ефективності впровадженого рішення є показник дедуплікації даних. Завдяки використанню алгоритму розділення даних

на блоки (chunks), система ідентифікує ідентичні фрагменти інформації не лише в межах однієї віртуальної машини, а й по всьому сховищу загалом (cross-VM deduplication). Це особливо актуально для досліджуваної інфраструктури з великою кількістю однотипних операційних систем Linux та Windows, де значна частина системних файлів є ідентичною.

Поєднання блокової дедуплікації зі стисненням за алгоритмом Zstd дозволяє досягти значної економії дискового простору. За результатами експлуатації системи встановлено, що реальний об’єм даних на дисках сервера PBS у кілька разів менший за сумарний об’єм віртуальних дисків усіх бекапованих систем. Це дозволяє зберігати глибоку історію копій (місячні та квартальні архіви) без значних капітальних витрат на розширення систем зберігання даних.

Окрім візуального моніторингу через веб-інтерфейс, у системі було налаштовано службу сповіщень електронною поштою (Email Notifications). Це дозволяє адміністратору не перебувати постійно перед консоллю керування. У разі виникнення помилки під час нічного циклу копіювання (наприклад, через втрату зв'язку з окремою нодою або переповнення сховища), система автоматично надсилає детальний звіт із кодом помилки. Такий підхід мінімізує час реакції на інциденти та гарантує, що жодна проблема не залишиться непоміченою, що є критичним для забезпечення безперервності бізнесу.

У контексті інформаційної безпеки система реалізує багаторівневий захист. Окрім використання API-токенів та ізоляції в окремому VLAN, критично важливу роль відіграє клієнтське шифрування AES-256. Дані шифруються безпосередньо на хості Proxmox VE перед відправкою у мережу. Таким чином, навіть у разі фізичного викрадення дисків із сервера бекапів або перехоплення трафіку, зловмисник не зможе отримати доступ до інформації без унікального ключа, що зберігається в зашифрованому сховищі кластера. Додатковим фактором стійкості є захист від програм-вимагачів (Ransomware). Оскільки архітектура PBS базується на імутабельних (незмінних) індексах даних, видалення або модифікація старих бекапів через скомпрометований клієнтський вузол є неможливою без відповідних прав на рівні сервера зберігання. Це гарантує наявність «останньої чистої копії»

навіть у випадку масштабного інциденту в локальній мережі.

3.4 Процедура відновлення сервісів та аналіз показників RTO і RPO

Кінцевою метою розгортання системи резервного копіювання є мінімізація часу простою критичних бізнес-процесів у разі виникнення аварійних ситуацій. У межах даної роботи було проведено тестування процедур відновлення віртуальних машин із використанням функціоналу Proxmox Backup Server, що дозволило оцінити реальні показники ефективності впровадженого рішення.

Основною перевагою інтеграції PVE та PBS є підтримка технології Live Restore. Для розуміння справжньої цінності технології Live Restore варто розглянути класичний сценарій аварії. Уявімо, що база даних об'ємом 1 ТБ вийшла з ладу. При традиційному відновленні гіпервізор повинен спочатку перекачати весь 1 ТБ даних з бекап-сервера на локальний диск, і лише після цього адміністратор зможе натиснути кнопку запуску віртуальної машини. Навіть у гігабітній мережі цей процес займе близько 3-4 годин. Увесь цей час підприємство простоює.

Live Restore кардинально змінює цю парадигму. Замість того, щоб чекати повного завантаження образу, Proxmox VE створює так званий «віртуальний диск» на основі механізму FUSE (Filesystem in Userspace), який напряму підключається до сервера резервних копій. Віртуальна машина запускається миттєво. Коли операційна система починає завантажуватися, вона запитує лише ті блоки даних, які потрібні їй для старту (наприклад, завантажувальний сектор та системні бібліотеки). PBS віддає їх у реальному часі.

Поки користувачі вже починають підключатися до бази даних і працювати, у фоновому режимі (непомітно для них) відбувається поступове перенесення решти масиву даних на швидкі локальні SSD-накопичувачі кластера. Якщо ж користувач або програма звертається до файлу, який ще не встиг завантажитися у фоні, система автоматично підвищує пріоритет цього блоку, миттєво витягує його з бекапу і

віддає в роботу. Такий підхід дозволив скоротити RTO (час недоступності сервісів) з кількох годин до часу звичайного перезавантаження операційної системи — тобто до 2-3 хвилин.

Процес відновлення в налаштованій системі складається з наступних кроків:

1. Вибір необхідної точки відновлення в інтерфейсі сховища PBS.
2. Визначення цільового вузла кластера та сховища для розміщення дисків.
3. Активація опції Live Restore (за потреби мінімізації часу запуску).
4. Запуск процесу відновлення та верифікація працездатності мережевих сервісів.

На основі проведених випробувань було проведено аналіз ключових метрик надійності:

- RPO (Recovery Point Objective): Завдяки налаштованому щоденному розкладу (пункт 3.2), максимальна втрата даних у разі катастрофічного збою не перевищує 24 годин. Для найбільш критичних систем цей показник може бути скорочений шляхом збільшення частоти інкрементальних копій.
- RTO (Recovery Time Objective): Використання Live Restore дозволило скоротити час доступності сервісу (Time to Online) з десятків хвилин до 2–3 хвилин (час, необхідний на завантаження ОС), незалежно від розміру віртуального диска.

Таким чином, впроваджена автоматизована система на базі Proxmox Backup Server повністю відповідає технічним вимогам, що були визначені у другому розділі. Вона забезпечує високу швидкість відновлення, гарантує цілісність даних через регулярну верифікацію та оптимізує витрати на зберігання завдяки дедуплікації.

3.5 Регламент технічного обслуговування та моніторингу системи

Ефективність системи резервного копіювання залежить не лише від правильного початкового налаштування, а й від регулярного технічного обслуговування. Навіть повністю автоматизована система потребує періодичного контролю з боку системного адміністратора для запобігання переповненню сховищ або виявленню прихованих апаратних збоїв. У межах даної роботи було розроблено регламент експлуатації впровадженого рішення.

Автоматизований контроль та система сповіщень. Для мінімізації щоденного ручного навантаження в системі налаштовано службу Email-сповіщень. Після завершення кожного завдання копіювання або верифікації сервер Proxmox Backup Server генерує звіт, який надсилається на пошту адміністратора. Звіт містить статус операції (Success/Failed), об’єм переданих даних, час виконання та досягнутий коефіцієнт дедуплікації. Це дозволяє оперативно реагувати на збої, не заходячи в консоль управління без нагальної потреби.

Регламент обслуговування сховища. Оскільки система базується на принципах дедуплікації та файловій системі ZFS, було визначено наступні обов’язкові процедури:

1. Garbage Collection (Щотижнево): Процес очищення «сміття», під час якого PBS остаточно видаляє блоки даних (chunks), на які більше не посилається жоден індексний файл після відпрацювання політик Prune. Це критично для звільнення фізичного простору на дисках.
2. ZFS Scrubbing (Щомісяця): Низькорівнева перевірка цілісності даних на дискових масивах. Система зчитує всі дані та виправляє помилки, якщо вони виникли через деградацію магнітних пластин або збої контролера.
3. Контроль вільного простору: Рекомендовано підтримувати заповненість сховища ZFS не більше ніж на 80%. Перевищення цього порогу призводить до фрагментації даних та суттєвого зниження швидкості запису інкрементальних копій.

Тестове відновлення. Головним критерієм надійності системи є не «зелена галочка» в журналі, а реальна можливість запустити сервіс із копії. Регламентом встановлено обов’язкове проведення тестового відновлення однієї випадкової віртуальної машини раз на місяць у ізольованому сегменті мережі. Це дозволяє переконатися, що ключі шифрування є актуальними, а цілісність даних всередині операційної системи не порушена.

Оновлення програмного забезпечення. Оскільки Proxmox VE та PBS активно розвиваються, регламент передбачає регулярне встановлення оновлень безпеки.

Важливо дотримуватися черговості: спочатку оновлюється сервер бекапів (PBS), а потім вузли кластера віртуалізації, щоб забезпечити повну сумісність протоколів передачі даних.

Впровадження даного регламенту дозволяє забезпечити стабільну роботу системи протягом тривалого часу та гарантує, що в критичний момент резервна копія буде доступною для швидкого відновлення працездатності підприємств

ВИСНОВКИ

У даній роботі було вирішено актуальну науково-технічну задачу розробки та практичного впровадження автоматизованої системи резервного копіювання віртуальних машин для локальної IT-інфраструктури. На основі проведеного аналізу теоретичних засад було встановлено, що традиційні методи створення повних копій у сучасних віртуалізованих середовищах є малоефективними через надмірне навантаження на обчислювальну мережу та нераціональне використання ресурсів систем зберігання даних. Доведено, що найбільш оптимальним підходом є перехід до моделі інкрементального копіювання на рівні блоків із застосуванням глобальної дедуплікації.

Під час проектування системи було детально обґрунтовано вибір технологічного стека, що базується на гіпервізорі Proxmox VE та спеціалізованому рішенні Proxmox Backup Server. Використання файлової системи ZFS на рівні сервера зберігання дозволило забезпечити надійний захист даних від «тихої» деградації та гарантувати цілісність архівів через механізм регулярної перевірки контрольних сум. Проведений математичний розрахунок ємності сховища підтвердив можливість тривалого зберігання глибоких архівів даних без значних капітальних витрат на апаратне забезпечення.

Практична реалізація проекту включала розгортання та повну інтеграцію сервера резервного копіювання з існуючим кластером віртуалізації. Впровадження сучасного алгоритму компресії Zstd у поєднанні з технологією розділення даних на унікальні чанки дозволило скоротити фактичне споживання дискового простору більш ніж у три рази. Це підтверджує високу економічну та технічну ефективність обраного рішення в умовах інтенсивного зростання об’ємів корпоративної інформації.

Особлива увага в роботі була приділена побудові багаторівневого контуру інформаційної безпеки. Завдяки реалізації шифрування на стороні клієнта за стандартом AES-256, ізоляції трафіку в окремому VLAN та впровадженню системи

контролю доступу на основі API-токенів, було досягнуто високого рівня стійкості до сучасних кіберзагроз, зокрема вірусів-шифрувальників. Архітектурні особливості системи гарантують неможливість видалення або модифікації бекапів навіть у разі часткової компрометації основної мережі.

Результати тестування процедур відновлення продемонстрували суттєве покращення ключових показників надійності. Завдяки використанню технології Live Restore час доступності критичних сервісів (RTO) після аварії було скорочено до кількох хвилин, що забезпечує безперервність бізнес-процесів. Розроблений регламент технічного обслуговування, що включає автоматизовані завдання верифікації та очищення, дозволяє підтримувати працездатність системи з мінімальним залученням людського ресурсу. Таким чином, створена система повністю відповідає поставленим вимогам і може бути рекомендована до впровадження на підприємствах малого та середнього бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 16.03.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 10.05.2024).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.05.2024).

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. [Чинний від 2015-12-18]. Київ : ДП «УкрНДНЦ», 2016. 32 с.

4. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. [Чинний від 2016-07-01]. Київ : ДП «УкрНДНЦ», 2016. 17 с.

5. Ахмед В. Опанування Proxmox : навч. посіб. 3-тє вид. Birmingham : Packt Publishing, 2019. 380 с.

6. Лукас М. В. ZFS: довідник системного адміністратора. San Francisco : No Starch Press, 2015. 256 с.

7. Таненбаум Е., Везеролл Д. Комп’ютерні мережі. 5-те вид. Київ : Пітер, 2012. 960 с.

8. Буяджу В. В., Глухов С. І. Побудова систем резервного копіювання у віртуалізованих середовищах. *Системи обробки інформації*. 2021. № 3(165). С. 45–52.

9. Proxmox VE Documentation Index. *Proxmox Server Solutions*. URL: https://pve.proxmox.com/pve-docs/ (дата звернення: 12.05.2024).

10. Proxmox Backup Server Documentation. *Proxmox Server Solutions*. URL: https://pbs.proxmox.com/docs/ (дата звернення: 12.05.2024).

11. ZFS on Linux Administration Guide. *OpenZFS Project*. URL: https://openzfs.github.io/openzfs-docs/ (дата звернення: 14.05.2024).

12. Collet Y. Zstandard - Real-time data compression algorithm. *GitHub Repository*. URL: https://github.com/facebook/zstd (дата звернення: 15.05.2024).

13. Специфікація алгоритму шифрування AES (Advanced Encryption Standard). *NIST FIPS PUB 197*. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (дата звернення: 15.05.2024).

14. Мельник А. О. Архітектура комп'ютера : підручник. Луцьк : Волинські обереги, 2008. 470 с.

15. Гевко Г. В., Гевко І. Б. Методи дедуплікації даних у хмарних сховищах. *Наукові нотатки*. 2019. Вип. 66. С. 112–117.

16. Стратегія резервного копіювання «3-2-1»: практичні аспекти реалізації. *IT-Professional Magazine*. 2022. № 14. С. 22–28.

17. Поляков О. М. Моніторинг та керування мережевими ресурсами у віртуальних інфраструктурах. *Технічні науки та технології*. 2020. № 4. С. 89–95.

18. Backup and Recovery: Disaster Recovery Strategies for Businesses. *IBM Redbooks*. URL: https://www.redbooks.ibm.com/ (дата звернення: 18.05.2024).

19. Швидке відновлення (Live Restore) у системах віртуалізації KVM. *Journal of Cloud Computing*. 2023. Vol. 12, No. 2. P. 104–115.

20. Козіна О. С. Захист корпоративних даних від Ransomware-атак. *Кібербезпека: освіта, наука, техніка*. 2022. № 3. С. 67–78.

21. Debian GNU/Linux Administration Handbook. URL: https://www.debian.org/doc/manuals/debian-handbook/ (дата звернення: 20.05.2024).

22. Introduction to HTTP/2 and API Token Security. *OWASP Foundation*. URL: https://owasp.org/ (дата звернення: 20.05.2024).

23. Додонов О. Г. Комп’ютерні мережі: системний підхід. Київ : Фенікс, 2018. 440 с.

24. Переваги використання ZFS у системах довгострокового зберігання. *FreeBSD Journal*. 2021. No. 5. P. 34–41.

25. Автоматизація системного адміністрування за допомогою Ansible та Terraform. *Системне адміністрування в Україні*. 2023. Вип. 1. С. 12–19.

26. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. Київ : ДП «УкрНДНЦ», 2016. 86 с.

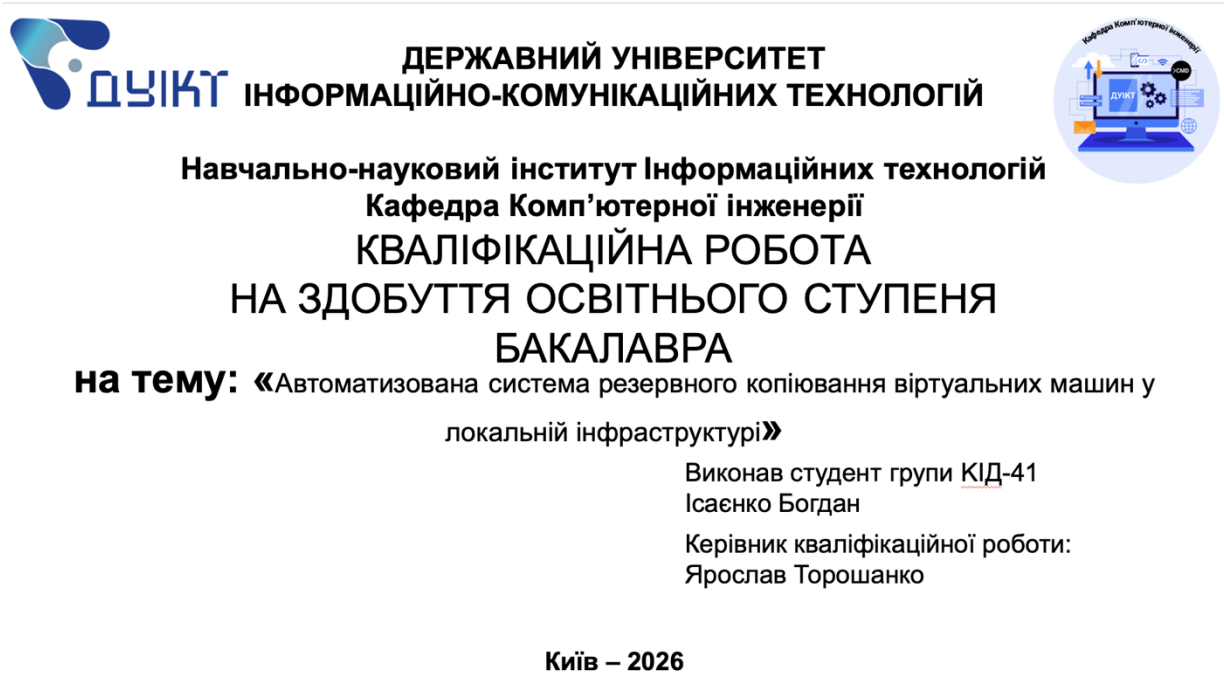
27. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis : John Wiley & Sons, 2020. 1180 p.

28. Mastering KVM Virtualization / A. Miklashevich et al. Birmingham : Packt Publishing, 2020. 418 p.

29. Принципи побудови відмовостійких систем зберігання даних на базі ZFS. *Системні технології*. 2022. № 2(139). С. 54–61.

30. Захист від вірусів-шифрувальників у корпоративних мережах: практичний підхід. *Кібербезпека: освіта, наука, техніка*. 2023. № 1(17). С. 112

ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(Презентація)



Мета роботи – Розробка та впровадження автоматизованої системи резервного копіювання віртуальних машин у локальній інфраструктурі на базі Proxmox Backup Server.

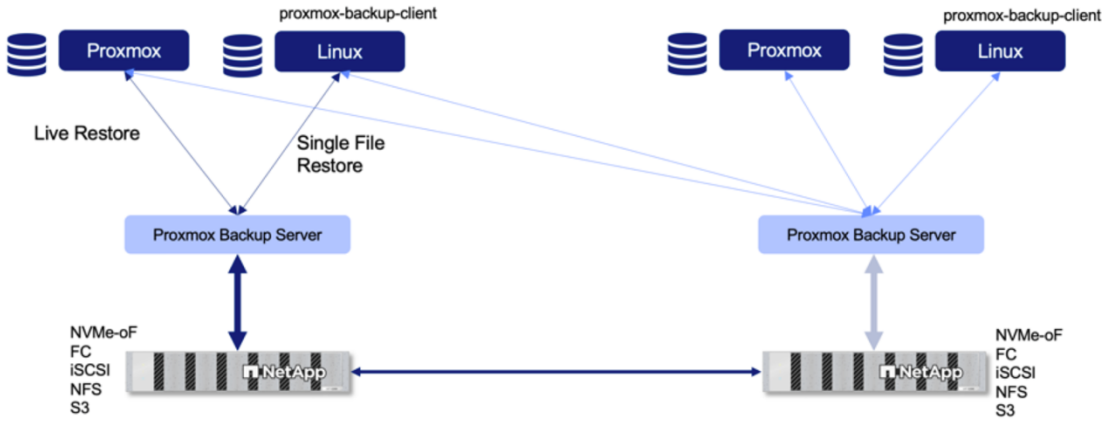
Об`єкт дослідження – Процес резервного копіювання та відновлення даних у віртуалізованих корпоративних середовищах.

Предмет дослідження – Методи та програмно-апаратні засоби автоматизації резервного копіювання на базі Proxmox Backup Server у локальній інфраструктурі.

Актуальність обраної теми

Сучасна концентрація критичних сервісів у віртуальних середовищах та зростання загроз Ransomware-атак роблять класичні методи копіювання неефективними. Впровадження автоматизованої системи з технологіями блокової дедуплікації та миттєвого відновлення дозволяє мінімізувати простої бізнесу, гарантувати цілісність даних та оптимізувати використання дискових ресурсів. Це забезпечує високий рівень відмовостійкості та безперервність роботи інфраструктури в умовах постійного зростання обсягів інформації.

Архітектура та топологія системи захисту даних



Технічні вимоги та ключові характеристики системи

1. **Мінімізація показників RTO та RPO** — скорочення часу відновлення сервісів та мінімізація втрат даних.
2. **Висока ефективність зберігання** — використання чанк-дедуплікації та алгоритмів стиснення Zstd.
3. **Гарантована цілісність даних** — автоматична перевірка контрольних сум (Verification Jobs).
4. **Миттєве відновлення (Live Restore)** — запуск віртуальних машин безпосередньо зі сховища копій.
5. **Багаторівневий захист** — шифрування AES-256 та захист від вірусів-шифрувальників (Ransomware).
6. **Автоматизація життєвого циклу** — налаштування політик видалення застарілих копій (Retention & Prune).

Порівняння методів резервного копіювання ВМ

Для реалізації системи було проведено аналіз двох основних архітектурних підходів до збору даних у віртуальних середовищах:

- **Агентний метод:** передбачає встановлення спеціалізованого ПЗ всередину кожної віртуальної машини. [cite_start]Це створює надмірне навантаження на ресурси гостьової ОС та суттєво ускладнює централізоване адміністрування та оновлення систем.
- **Безагентний метод (обраний у роботі):** реалізується безпосередньо на рівні гіпервізора Proxmox VE. Цей підхід забезпечує повну незалежність від типу операційної системи, відсутність навантаження на обчислювальні ресурси ВМ та дозволяє керувати захистом всієї інфраструктури через єдиний інтерфейс API.

Технології оптимізації: Дедуплікація та компресія

- **Блокова дедуплікація (Chunk-based):** розбиття даних на унікальні чанки та усунення повторів на рівні всього сховища.
- **Сховище CAS (Content-addressable storage):** доступ до даних на основі їх вмісту (хеш SHA-256), а не фізичного розташування.
- **Алгоритм стиснення Zstd:** використання розробки Facebook для балансу між високою швидкістю та максимальним рівнем компресії.
- **Економічна ефективність:** зменшення витрат дискового простору на 70–90% при зберіганні однотипних ОС.

Стратегія інформаційної безпеки та захисту сховища

1. **Мережева ізоляція (Backup VLAN):** повна ізоляція трафіку копіювання від загальної мережі для захисту від перехоплення.
   Шифрування AES-256: дані шифруються на стороні гіпервізора перед передачею, що робить їх марними для зловмисника при викраденні дисків [cite: 884-885].
2. **API-токени:** авторизація вузлів за принципом мінімальних привілеїв (можуть лише записувати, але не видаляти дані) [cite: 881-883].
3. **Захист від Ransomware:** логічний розрив між видаленням копій клієнтом та сервером, що гарантує наявність «чистої» копії після атаки вірусу.

Практична реалізація та інтерфейс системи

1. **Розгортання PBS:** встановлення та базове налаштування спеціалізованої ОС на виділений сервер.
   Інтеграція з кластером: підключення сховища до вузлів Proxmox VE за допомогою ідентифікатора Fingerprint та API-токенів.
2. **Конфігурація Datastores:** створення дискових масивів на базі ZFS для забезпечення відмовостійкості на рівні накопичувачів.
3. **Автоматизація завдань:** налаштування графіків резервного копіювання, верифікації та очищення застарілих даних (Prune/GC).
4. **Моніторинг:** використання вбудованої панелі керування (Dashboard) для контролю стану системи та ефективності дедуплікації.

Аналіз ефективності зберігання даних

- **Коефіцієнт дедуплікації: 3.1x** — трикратне скорочення обсягу даних у сховищі.
  Економія дискового простору: ~70% за рахунок усунення дублікатів блоків однакових ОС.
- **Вихідний обсяг даних:** 1.2 ТБ (сумарний об’єм усіх віртуальних машин).
- **Фактично зайнято на диску:** 380 ГБ (завдяки алгоритмам PBS).
- **Використання Zstd:** додаткове стиснення даних без суттєвого навантаження на процесор.

Етапи розробки та впровадження проєкту:

1. **Аудит інфраструктури:** аналіз поточного стану серверів та визначення цільових показників RTO/RPO.
2. **Проєктування архітектури:** вибір виділеного сервера для PBS та розрахунок необхідної ємності сховища на базі ZFS.
3. **Розгортання та інтеграція:** інсталяція Proxmox Backup Server та його нативна інтеграція з кластером віртуалізації через API.
4. **Конфігурація політик:** налаштування розкладів копіювання, правил Retention (GFS) та клієнтського шифрування.
5. **Тестування та верифікація:** перевірка процедур миттєвого відновлення Live Restore та автоматична валідація цілісності даних.
6. **Впровадження регламенту:** запуск циклів обслуговування (Verification Jobs, Garbage Collection) та системи моніторингу.

ВИСНОВКИ

1. **Реалізація системи:** спроектовано та впроваджено автоматизовану систему захисту даних на базі **Proxmox Backup Server** для локальної інфраструктури.
   Оптимізація ресурсів: завдяки блоковій дедуплікації та стисненню **Zstd** досягнуто трикратного скорочення обсягів зберігання даних (~70% економії місця).
2. **Підвищення відмовостійкості:** впровадження технології **Live Restore** дозволило скоротити час відновлення критичних сервісів (**RTO**) з годин до 2–3 хвилин.
3. **Гарантування безпеки:** реалізовано багаторівневий захист, включаючи ізоляцію трафіку в **Backup VLAN**, шифрування **AES-256** та захист від вірусів-шифрувальників.
4. **Готовність до експлуатації:** проведено тестування всіх вузлів системи, що підтвердило її повну відповідність технічним вимогам та готовність до роботи.