

ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та
інформаційних технологій
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти бакалавр

на тему: **«Проектування файлового сервера та системи резервного
копіювання даних для підприємства»**

Виконав: здобувач вищої освіти
за освітньою програмою
Інформаційні управляючі системи
спеціальності 126 Інформаційні
системи та технології
ступеня вищої освіти бакалавр
групи 126ІСТ_бз_2021
Буцький Євгеній Андрійович
Керівник: Протас Надія Михайлівна
Рецензент: Муравльов Володимир
Вячеславович

Полтава – 2025 року

ВСТУП

Актуальність. На сьогодні інформаційні технології відіграють ключову роль у забезпеченні ефективності бізнес-процесів підприємств. Централізоване зберігання даних і надійний захист інформації є критично важливими для компаній середнього та малого бізнесу, наприклад таких, що спеціалізується на технічному обслуговуванні та ремонті обладнання. За даними Gartner, у 2024 р. 75% компаній середнього бізнесу інвестували в модернізацію інформаційної інфраструктури для підвищення продуктивності та безпеки [1]. Файлові сервери забезпечують централізоване управління даними, спрощуючи доступ до інформації, підвищуючи безпеку та оптимізуючи робочі процеси. Водночас, за оцінками Cybersecurity Ventures, у 2024 р. 60% компаній, які зазнали втрати даних через відсутність ефективних систем резервного копіювання, припинили діяльність протягом шести місяців [2]. Це підкреслює необхідність впровадження автоматизованих систем резервного копіювання для захисту критичних даних від апаратних збоїв, кібератак чи людських помилок.

Проблема забезпечення швидкого доступу до даних і їхньої безпеки особливо актуальна для підприємств, де обсяг інформації зростає приблизно на 20% щороку. У 2024 р., за даними TechRepublic, 70% компаній середнього бізнесу в Україні модернізували свої системи зберігання даних, надаючи перевагу гібридним рішенням, що поєднують локальні та хмарні сховища [3]. Однак багато компаній стикаються з обмеженим бюджетом, що вимагає вибору економічно ефективних рішень, таких як безкоштовне програмне забезпечення (Cobian Reflector) або недорогі хмарні сервіси (Microsoft Azure Backup). Ця робота спрямована на створення файлового сервера та системи резервного копіювання, які забезпечують централізоване зберігання даних, швидкий доступ для 50 користувачів, захист інформації та автоматизацію резервного копіювання з урахуванням бюджетних обмежень підприємства.

Мета кваліфікаційної роботи полягає в розробці та впровадженні файлового сервера на базі Windows Server 2022 і системи резервного копіювання

з використанням Cobian Reflector та Microsoft Azure Backup для підприємства, що спеціалізується на технічному обслуговуванні та ремонті обладнання.

Відповідно до мети роботи необхідно вирішити наступні завдання:

1) провести аналіз предметної галузі та інформаційної інфраструктури підприємства, визначивши вимоги до файлового сервера та системи резервного копіювання;

2) розробити та налаштувати файловий сервер і систему резервного копіювання, обґрунтувавши вибір операційної системи та програмного забезпечення;

3) оцінити техніко-економічну ефективність запропонованих рішень і розробити рекомендації щодо їхнього впровадження.

Об'єкт дослідження – процеси проектування та впровадження файлових серверів і систем резервного копіювання в інформаційній інфраструктурі підприємств.

Предмет дослідження – проектування та розробка файлового сервера на базі Windows Server 2022 і системи резервного копіювання з використанням Cobian Reflector та Microsoft Azure Backup.

Методи досліджень – дослідження базуються на методах системного аналізу, порівняльного аналізу програмного забезпечення, техніко-економічного обґрунтування, а також методах проектування інформаційних систем і забезпечення їх надійності.

Інформаційна база – інтернет-ресурси, наукові статті та технічна документація, що містять інформацію про файлові сервери, серверні операційні системи, системи резервного копіювання, а також стандарти безпеки та зберігання даних.

Практична значущість – запропоновані рішення, включаючи схему налаштування файлового сервера, систему резервного копіювання, техніко-економічне обґрунтування та рекомендації, спрощують впровадження ефективної інформаційної системи підприємства. Система забезпечує

централізоване зберігання даних, захист інформації та економічну ефективність, що може бути використано іншими підприємствами середнього бізнесу.

Результати роботи апробовані в рамках наукової конференції здобувачів вищої освіти за результатами науково-дослідної роботи у 2024-2025 рр.

Структура кваліфікаційної роботи логічно пов'язана з задачами досліджень і містить вступ, три розділи основної частини, висновки, список використаних джерел. Загальний обсяг текстової частини кваліфікаційної роботи складає 50 сторінок формату А4. Вона містить 13 рисунків і 10 таблиць.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ПРОЄКТУВАННЯ ФАЙЛОВИХ СЕРВЕРІВ ТА СИСТЕМ РЕЗЕРВНОГО КОПЮВАННЯ

1.1 Поняття файлового сервера та його роль в інформаційній інфраструктурі підприємства

Файловий сервер є ключовим елементом інформаційної інфраструктури сучасного підприємства, забезпечуючи централізоване зберігання, обмін та управління даними. Термін «сервер» походить від англійського слова «serve» (обслуговувати), що відображає його основну функцію – надання ресурсів та виконання завдань для клієнтських пристроїв у мережі. Файловий сервер, зокрема, призначений для зберігання файлів, забезпечення їх доступності для користувачів та управління правами доступу до даних. Він дозволяє організувати ефективний обмін інформацією, підвищує безпеку даних і сприяє оптимізації робочих процесів. Основна роль файлового сервера полягає в централізації зберігання даних, що усуває проблеми, пов'язані з використанням локальних накопичувачів чи зовнішніх носіїв, таких як флеш-накопичувачі. Наприклад, за даними дослідження Gartner, у 2023 р. 65% компаній середнього та малого бізнесу перейшли на централізовані системи зберігання даних для підвищення ефективності управління інформацією [1]. Це дозволяє уникнути дублювання файлів, спрощує резервне копіювання та забезпечує контроль доступу до даних. Файловий сервер також підтримує одночасну роботу кількох користувачів із файлами, що є критично важливим для командної роботи в організаціях.

З технічного погляду, файловий сервер – це комп'ютер або спеціалізоване обладнання з встановленою серверною операційною системою (наприклад, Microsoft Windows Server, Linux Ubuntu Server), яке налаштоване для виконання специфічних завдань. Апаратне забезпечення файлового сервера зазвичай включає потужні процесори, великий обсяг оперативної пам'яті та накопичувачі з підтримкою RAID-масивів для забезпечення надійності зберігання даних.

Програмне забезпечення, у свою чергу, може бути як спеціалізованим (наприклад, Samba для Linux), так і універсальним, що підтримує локальні та мережеві задачі обміну повідомленнями (рис. 1.1).

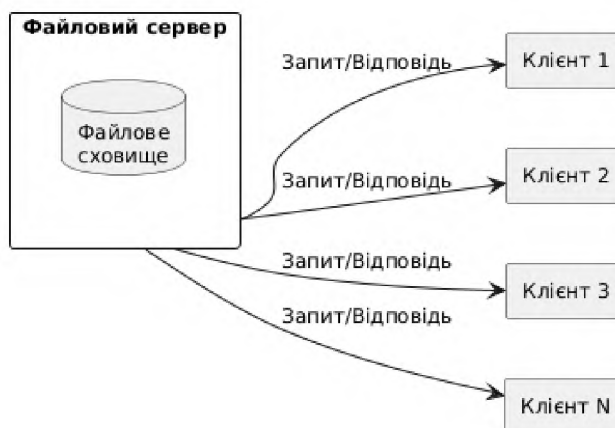


Рисунок 1.1 – Схема роботи файлового сервера в локальній мережі

Функціональність файлового сервера виходить за межі простого зберігання даних. Він забезпечує такі функції як:

1. Розмежування доступу: користувачі отримують доступ до файлів відповідно до їхніх ролей і прав, що підвищує безпеку даних.
2. Підтримка мережевих протоколів, наприклад, SMB (Server Message Block) або NFS (Network File System) для обміну файлами в різних операційних системах.
3. Інтеграція з іншими системами: файловий сервер може бути частиною доменної структури, наприклад, Microsoft Active Directory, для централізованого управління користувачами.

У контексті інформаційної інфраструктури підприємства файловий сервер відіграє стратегічну роль, оскільки забезпечує безперервність бізнес-процесів. Наприклад, у 2024 р., за даними IDC, 78% компаній, які впровадили централізовані файлові сервери, повідомили про зниження часу простою через втрату даних на 40% [2]. Це особливо актуально для організацій, де обмін інформацією між співробітниками є щоденною потребою, а втрата даних може призвести до значних фінансових або репутаційних збитків.

Файловий сервер також є основою для впровадження систем резервного копіювання, оскільки централізоване зберігання даних спрощує створення резервних копій. Наприклад, використання файлового сервера разом із програмним забезпеченням, таким як Cobian Backup, дозволяє автоматизувати процес резервного копіювання, мінімізуючи ризик втрати інформації через апаратні збої чи людські помилки.

Таблиця 1.1 – Переваги та недоліки використання файлового сервера

Переваги	Недоліки
Централізоване управління даними	Висока початкова вартість обладнання
Підвищення безпеки даних	Необхідність регулярного обслуговування
Спрощення резервного копіювання	Залежність від стабільності мережі
Підтримка командної роботи	Потреба в кваліфікованому персоналі

Незважаючи на певні недоліки, зазначені у табл. 1.1, переваги файлового сервера роблять його незамінним компонентом інформаційної інфраструктури. У 2023 р., за оцінками TechRepublic, 85% підприємств, які використовують файлові сервери, відзначили підвищення продуктивності роботи завдяки швидкому доступу до даних і спрощенню управління інформаційними ресурсами [3].

Таким чином, файловий сервер є не лише технічним рішенням, але й стратегічним інструментом, що сприяє підвищенню ефективності, безпеки та стабільності роботи підприємства. Його впровадження дозволяє оптимізувати інформаційні процеси, забезпечити захист даних і створити основу для подальшого розвитку інформаційної інфраструктури.

1.2 Види серверних операційних систем та їх порівняльний аналіз

Серверні операційні системи (ОС) є основою для забезпечення функціонування серверів, які виконують завдання зберігання, обробки та передачі даних у локальних і глобальних мережах. Вони призначені для

управління апаратними ресурсами, забезпечення безпеки, підтримки мережесих протоколів і взаємодії з клієнтськими пристроями. Серверні ОС відрізняються від клієнтських високою стабільністю, підтримкою великої кількості одночасних підключень і можливістю роботи в режимі 24/7. У 2024 р., за даними Gartner, 82% компаній використовують серверні ОС для централізованого управління даними, що підкреслює їхню ключову роль у сучасній інформаційній інфраструктурі [1].

Серверна ОС – це спеціалізоване програмне забезпечення, яке забезпечує роботу серверів, підтримуючи взаємодію між апаратним забезпеченням, мережевими ресурсами та клієнтськими пристроями. Вона виконує такі функції, як управління користувачами, розмежування доступу, підтримка мережесих протоколів (наприклад, SMB, NFS) і забезпечення безпеки даних. На відміну від клієнтських ОС, серверні системи оптимізовані для обробки великої кількості запитів, роботи з великими обсягами даних і забезпечення високої відмовостійкості. Основні вимоги до серверних ОС включають:

- стабільність і надійність: здатність працювати без збоїв у режимі безперервної експлуатації;
- масштабованість: підтримка великої кількості користувачів і пристроїв;
- безпека: захист даних від несанкціонованого доступу та кібератак;
- сумісність: інтеграція з різними апаратними платформами та програмним забезпеченням.

Серверні ОС поділяються на кілька категорій залежно від їхньої архітектури та ліцензування: пропрієтарні (наприклад, Microsoft Windows Server) і з відкритим кодом (наприклад, Linux-дистрибутиви). У 2023 р., за оцінками IDC, Linux-дистрибутиви займали 54% ринку серверних ОС, тоді як Windows Server утримував 35%, що свідчить про зростання популярності відкритих рішень через їхню гнучкість і економічність [2]. Розглянемо особливості найпоширеніших серверних ОС у 2023-2025 рр., логотипи яких представлені на рис. 1.2.



Рисунок 1.2 – Логотипи основних серверних операційних систем Windows Server, Ubuntu Server, RHEL, Debian і CentOS Stream

Microsoft Windows Server є пропрієтарною ОС, яка широко використовується в корпоративному середовищі завдяки простоті адміністрування та інтеграції з іншими продуктами Microsoft, такими як Active Directory. Найновіша версія, Windows Server 2025, підтримує до 128 фізичних процесорів і 48 ТБ оперативної пам'яті, що робить її придатною для великих організацій [6]. Основні переваги включають зручний графічний інтерфейс, підтримку PowerShell для автоматизації та інтеграцію з хмарними сервісами Azure. Проте висока вартість ліцензій і вразливість до кібератак залишаються ключовими недоліками. За даними TechRepublic, у 2024 р. 68% компаній, які використовують Windows Server, відзначали простоту адміністрування як головну перевагу [3].

Ubuntu Server – це Linux-дистрибутив із відкритим кодом, який набув популярності завдяки стабільності, широкій підтримці спільноти та безкоштовному ліцензуванню. Версія Ubuntu Server 24.04 LTS (Long Term Support), випущена у 2024 р., підтримує сучасні апаратні платформи та пропонує інструменти для контейнеризації (Docker, Kubernetes). За оцінками Canonical, у 2024 р. Ubuntu Server використовувався на 40% серверів у хмарних середовищах, що свідчить про його популярність у гібридних інфраструктурах [7].

Red Hat Enterprise Linux (RHEL) – це комерційний Linux-дистрибутив, який цінується за надійність і підтримку від компанії Red Hat. Версія RHEL 9, оновлена у 2024 р., пропонує розширені функції безпеки, такі як SELinux, і підтримку гібридних хмарних середовищ. RHEL є платним продуктом, але його

стабільність робить його вибором для великих організацій. У 2023 р., за даними Forrester, 25% Fortune 500 компаній використовували RHEL для критичних бізнес-додатків [8].

Debian – це безкоштовний Linux-дистрибутив, відомий своєю стабільністю та універсальністю. Debian 12, випущений у 2023 р., включає оновлені пакети програмного забезпечення та підтримку сучасних апаратних платформ. Його перевагою є великий набір попередньо встановлених пакетів, таких як LibreOffice і мультимедійні кодеки. Однак складність початкового налаштування може бути бар’єром для новачків.

CentOS Stream є безкоштовним дистрибутивом, який позиціонується як тестова платформа для RHEL. У 2024 р. CentOS Stream 10 отримав оновлення, що включають підтримку новітніх процесорів і розширені можливості для контейнеризації. Проте, його використання обмежується через меншу стабільність порівняно з RHEL.

Для оцінки серверних ОС використаємо такі критерії: продуктивність, безпека, простота адміністрування, масштабованість, вартість і сумісність із програмним забезпеченням. Порівняльний аналіз представлено в таблиці 1.2.

Таблиця 1.2 – Порівняння серверних операційних систем

ОС	Продуктивність	Безпека	Простота адміністрування	Масштабованість	Вартість	Сумісність з ПЗ
Windows Server 2025	Висока	Середня	Висока	Висока	Висока	Висока
Ubuntu Server 24.04	Висока	Висока	Середня	Висока	Безкоштовна	Висока
RHEL 9	Висока	Дуже висока	Середня	Висока	Висока	Висока
Debian 12	Середня	Висока	Низька	Середня	Безкоштовна	Висока
CentOS Stream 10	Середня	Середня	Середня	Середня	Безкоштовна	Середня

Windows Server і RHEL демонструють високу продуктивність завдяки оптимізації для багатопроцесорних систем. Ubuntu Server також ефективний,

особливо в хмарних середовищах. Debian і CentOS Stream мають дещо нижчу продуктивність через меншу оптимізацію для великих навантажень.

RHEL вирізняється завдяки SELinux і регулярним оновленням безпеки. Ubuntu Server і Debian також мають високий рівень безпеки через активну підтримку спільноти. Windows Server, попри вдосконалення, залишається вразливим до атак через широку популярність. За даними Cybersecurity Ventures, у 2024 р. 30% кібератак на сервери припадали на Windows Server [9].

Windows Server є найзручнішим для адміністраторів із базовими знаннями завдяки графічному інтерфейсу та PowerShell. Linux-дистрибутиви, такі як Ubuntu і RHEL, вимагають знання командного рядка, що може ускладнити адміністрування для новачків.

Усі розглянуті ОС підтримують масштабованість, але Windows Server і RHEL краще підходять для великих організацій завдяки підтримці великої кількості процесорів і пам'яті. Ubuntu Server також ефективний у хмарних і кластерних середовищах.

Ubuntu Server, Debian і CentOS Stream є безкоштовними, що робить їх привабливими для малого та середнього бізнесу. Windows Server і RHEL мають високу вартість ліцензій, що може бути обмеженням для організацій із обмеженим бюджетом.

Windows Server має високу сумісність із корпоративним ПЗ, таким як Microsoft Exchange і SQL Server. Linux-дистрибутиви підтримують широкий спектр відкритих і комерційних програм, але можуть вимагати додаткових налаштувань для специфічного ПЗ.

Кожна ОС має свої сильні та слабкі сторони, які впливають на вибір для конкретного підприємства:

1. Windows Server: переваги включають простоту адміністрування, інтеграцію з Microsoft-екосистемою та підтримку широкого спектра ПЗ. Недоліки – висока вартість і вразливість до кібератак.

2. Ubuntu Server: безкоштовність, висока безпека та підтримка спільноти є ключовими перевагами. Недоліком є потреба в технічних знаннях для налаштування.

3. RHEL: висока надійність і безпека роблять його ідеальним для великих організацій, але висока вартість ліцензій обмежує використання.

4. Debian: стабільність і універсальність є перевагами, але складність налаштування може бути проблемою.

5. CentOS Stream: безкоштовність і сумісність із RHEL є плюсами, але менша стабільність робить його менш придатним для критичних систем.

У 2024 р., за оцінками NetworkWorld, 54% компаній, які впроваджували файлові сервери, обирали Linux-дистрибутиви через їхню економічність і гнучкість (рис. 1.3) [5]. Для файлового сервера вибір ОС залежить від потреб підприємства. Windows Server є оптимальним для організацій, які використовують Microsoft-екосистему та потребують простого адміністрування. Ubuntu Server і Debian підходять для компаній із обмеженим бюджетом і кваліфікованим персоналом. RHEL рекомендується для великих організацій із високими вимогами до безпеки.

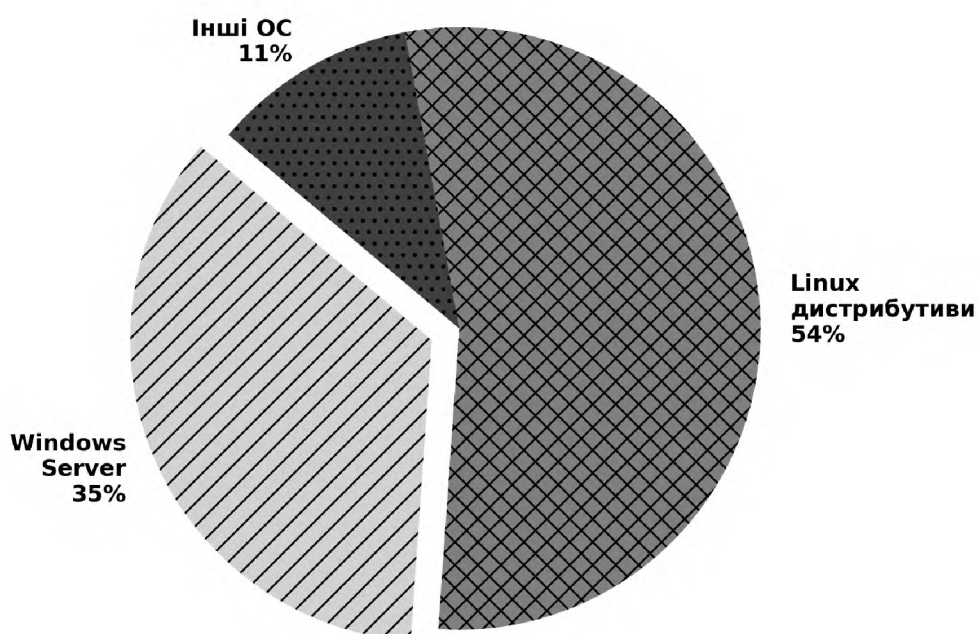


Рисунок 1.3 – Порівняння частки ринку серверних ОС у 2024 р.

Серверні ОС відіграють ключову роль у забезпеченні роботи інформаційних систем підприємства. Windows Server, Ubuntu Server, RHEL, Debian і CentOS Stream є найпоширенішими рішеннями у 2023-2025 рр., кожне з яких має унікальні переваги та недоліки. Вибір ОС залежить від бюджету, вимог до безпеки, масштабу інфраструктури та кваліфікації персоналу. Порівняльний аналіз показав, що Linux-дистрибутиви, такі як Ubuntu Server, є економічно вигідними та гнучкими, тоді як Windows Server залишається лідером у корпоративному сегменті завдяки простоті адміністрування.

1.3 Системи резервного копіювання: принципи та програмні засоби

Системи резервного копіювання є критично важливим компонентом інформаційної інфраструктури підприємства, забезпечуючи захист даних від втрати через апаратні збої, людські помилки, кібератаки чи стихійні лиха. Резервне копіювання передбачає створення копій даних, які зберігаються окремо від основного носія, що дозволяє відновити інформацію у разі її пошкодження чи втрати. У 2024 р., за даними Cybersecurity Ventures, 60% компаній, які зазнали втрати даних через відсутність резервного копіювання, припинили діяльність протягом шести місяців [9]. Резервне копіювання базується на створенні копій даних, які зберігаються на окремому носії або в хмарному середовищі. Основні принципи включають:

- регулярність: резервні копії створюються за визначеним графіком (щоденно, щотижня тощо), щоб мінімізувати втрату даних між копіюваннями;
- надійність: використання стабільних носіїв і перевірка цілісності копій для забезпечення можливості відновлення;
- автоматизація: автоматизовані процеси зменшують ризик людських помилок і забезпечують безперервність копіювання;
- шифрування: захист резервних копій від несанкціонованого доступу за допомогою шифрування;

– різноманітність типів копіювання: повне, інкрементне та диференціальне копіювання для оптимізації обсягу даних і часу виконання.

Різновиди резервного копіювання включають:

1. Повне копіювання: створює копію всіх даних, що забезпечує максимальну надійність, але потребує значного обсягу пам'яті та часу.
2. Інкрементне копіювання: копіюються лише зміни з моменту останнього копіювання (будь-якого типу), що економить місце, але ускладнює відновлення.
3. Диференціальне копіювання: копіюються зміни з моменту останнього повного копіювання, що є компромісом між повним та інкрементним методами.

У 2023 р., за даними Gartner, 70% компаній використовували комбінацію повного та інкрементного копіювання для оптимізації витрат на зберігання даних [1]. Це дозволяє ефективно управляти зростаючими обсягами інформації, особливо в умовах цифровізації бізнес-процесів. На рис. 1.4 представлені особливості етапів різних способів організації резервного копіювання даних підприємств.

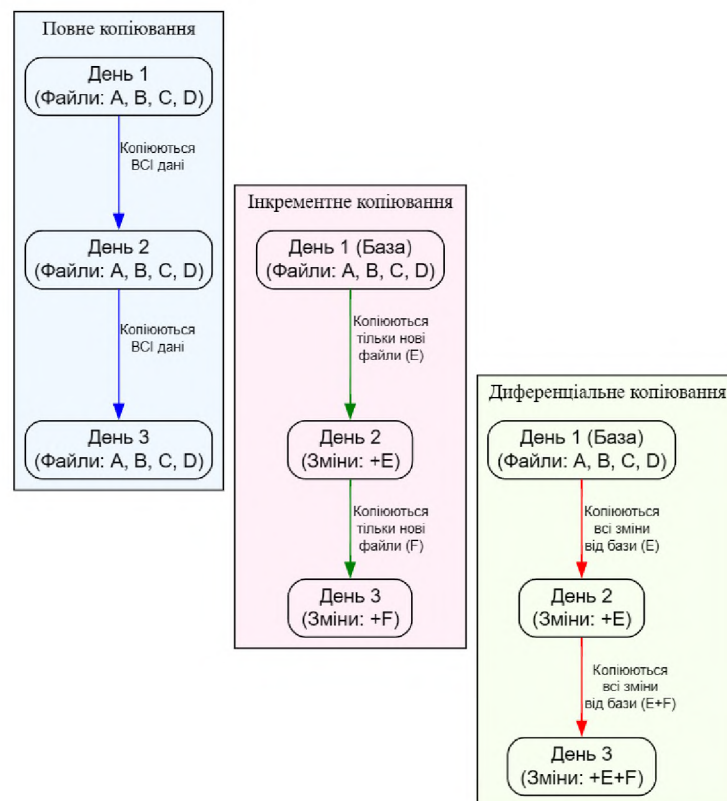


Рисунок 1.4 – Схема типів резервного копіювання

Апаратні засоби резервного копіювання включають носії для зберігання даних, які забезпечують надійність і доступність копій. Переваги та недоліки основних типів апаратних засобів для резервного копіювання зведені до табл. 1.3. Це наступні засоби:

- 1. Жорсткі диски (HDD і SSD): найпоширеніший засіб завдяки доступній ціні та великому обсягу. SSD пропонують вищу швидкість, але дорожчі. Наприклад, у 2024 р. Western Digital випустила HDD ємністю 26 ТБ, що стало популярним рішенням для резервного копіювання [10].
- 2. RAID-масиви: використовуються для підвищення надійності шляхом дублювання даних на кількох дисках. RAID 5 і RAID 6 є популярними для серверів завдяки балансу між надійністю та ефективністю використання пам'яті.
- 3. Стрічкові накопичувачі: застосовуються для довгострокового архівування через низьку вартість зберігання. Наприклад, LTO-9 касети, представлені у 2023 р., мають ємність до 45 ТБ зі стисненням [11].
- 4. Хмарні сховища: хмарні сервіси, такі як AWS S3 або Microsoft Azure Blob Storage, набирають популярності через гнучкість і масштабованість. У 2024 р., за оцінками TechRepublic, 55% компаній використовували хмарні сховища для резервного копіювання [3].

Таблиця 1.3 – Порівняння апаратних засобів резервного копіювання

Засіб	Переваги	Недоліки
Жорсткі диски	Доступна ціна, великий обсяг	Обмежена швидкість (HDD), знос
SSD	Висока швидкість, надійність	Висока вартість
RAID-масиви	Надійність, гаряча заміна дисків	Складність налаштування, висока ціна
Стрічкові накопичувачі	Низька вартість довгострокового зберігання	Низька швидкість доступу
Хмарні сховища	Масштабованість, доступність	Залежність від інтернету, витрати на підписку

Апаратні засоби часто комбінуються для створення гібридних систем, наприклад, локальні RAID-масиви для швидкого відновлення та хмарні сховища для довгострокового зберігання.

Програмні засоби резервного копіювання автоматизують процес створення, управління та відновлення копій. У 2023-2025 рр. ринок програмного забезпечення для резервного копіювання активно розвивається, пропонуючи як комерційні, так і безкоштовні рішення. За даними IDC, у 2024 р. 62% компаній використовували автоматизовані інструменти резервного копіювання для зменшення людських помилок [12].

Veeam Backup & Replication є лідером на ринку комерційних рішень для резервного копіювання, підтримуючи фізичні, віртуальні та хмарні середовища. Версія Veeam Backup & Replication v12, випущена у 2023 р., пропонує розширені функції шифрування та інтеграцію з Kubernetes (рис. 1.5). Основні переваги включають високу швидкість відновлення та підтримку гібридних інфраструктур. Недоліком є висока вартість ліцензії, що може бути бар'єром для малого бізнесу.

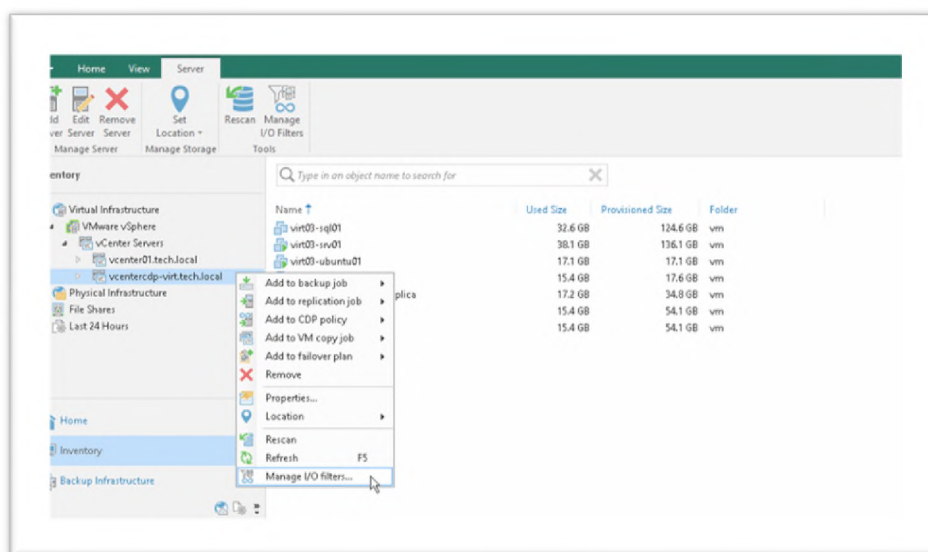


Рисунок 1.5 – Інтерфейс програми Veeam Backup & Replication

Acronis Cyber Backup пропонує комплексне рішення для резервного копіювання з підтримкою блокчейн-шифрування для захисту даних. Версія 2024 р. включає захист від програм-вимагачів і інтеграцію з хмарними сервісами. Продукт є комерційним, але пропонує гнучкі плани для малого та середнього

бізнесу. У 2024 р., за оцінками NetworkWorld, Acronis використовувався 25% компаній для захисту критичних даних [5].

Duplicati – це безкоштовне рішення з відкритим кодом, яке підтримує шифрування, стиснення та хмарне зберігання (Google Drive, OneDrive). Оновлення 2023 р. додало підтримку інкрементного копіювання з покращеною продуктивністю. Duplicati є ідеальним для невеликих організацій, але потребує технічних знань для налаштування.

Cobian Reflector, наступник Cobian Backup, є безкоштовним інструментом, який підтримує повне, інкрементне та диференціальне копіювання. Оновлення 2024 р. додало підтримку сучасних файлових систем і віддалене керування. Продукт простий у використанні, але не підтримує складні сценарії, такі як віртуалізація.

Restic – це сучасне безкоштовне рішення з відкритим кодом, яке підтримує дедуплікацію та шифрування. Версія 2024 р. покращила сумісність із хмарними сховищами, такими як AWS S3. Restic популярний серед технічних адміністраторів завдяки гнучкості, але має складний інтерфейс командного рядка.

Для оцінки програмних засобів використаємо критерії: функціональність, простота використання, безпека, сумісність і вартість. Результати представлено в таблиці 1.4.

Таблиця 1.4 – Порівняння програмних засобів резервного копіювання

Програма	Функціональність	Простота використання	Безпека	Сумісність	Вартість
Veeam Backup	Висока	Висока	Дуже висока	Висока	Висока
Acronis Cyber Backup	Висока	Висока	Висока	Висока	Середня
Duplicati	Середня	Середня	Висока	Середня	Безкоштовна
Cobian Reflector	Середня	Висока	Середня	Середня	Безкоштовна
Restic	Висока	Низька	Висока	Висока	Безкоштовна

Veeam і Acronis пропонують широкий набір функцій, включаючи підтримку віртуалізації та хмарних середовищ. Restic вирізняється дедуплікацією, тоді як Duplicati і Cobian Reflector обмежені базовими сценаріями. Veeam і Acronis мають зручні графічні інтерфейси, тоді як Restic потребує роботи через командний рядок. Cobian Reflector є найпростішим для початківців. Veeam і Acronis забезпечують високий рівень шифрування, включаючи захист від програм-вимагачів. Duplicati і Restic також пропонують надійне шифрування, але Cobian Reflector має обмежені функції безпеки. Veeam і Acronis підтримують широкий спектр платформ, тоді як Duplicati і Cobian Reflector обмежені у підтримці віртуалізації. Restic є універсальним завдяки хмарній інтеграції. Duplicati, Cobian Reflector і Restic є безкоштовними, що робить їх привабливими для малого бізнесу. Veeam і Acronis потребують значних інвестицій.

Вибір програмного засобу залежить від потреб підприємства. Для великих організацій із гібридними інфраструктурами Veeam або Acronis є оптимальними завдяки функціональності та підтримці. Для малого бізнесу з обмеженим бюджетом Duplicati або Cobian Reflector пропонують достатній рівень захисту. Restic підходить для технічних адміністраторів, які працюють із хмарними сховищами. У 2024 р., за оцінками TechTarget, 40% компаній обирали безкоштовні рішення для резервного копіювання через економічні обмеження [4].

Системи резервного копіювання є невід'ємною частиною захисту даних підприємства. Принципи регулярності, автоматизації та шифрування забезпечують ефективність цих систем. Апаратні засоби, такі як жорсткі диски, RAID-масиви та хмарні сховища, комбінуються для створення надійних рішень. Програмні продукти, такі як Veeam, Acronis, Duplicati, Cobian Reflector і Restic, пропонують різноманітні можливості для реалізації резервного копіювання. Вибір залежить від бюджету, технічних вимог і кваліфікації персоналу. У сучасних умовах гібридні системи, що поєднують локальне та хмарне зберігання, стають стандартом для забезпечення безпеки даних.

РОЗДІЛ 2

ДОСЛІДЖЕННЯ ІНФРАСТРУКТУРИ ТА ОБҐРУНТУВАННЯ ТЕХНІЧНИХ РІШЕНЬ ДЛЯ СТВОРЕННЯ СИСТЕМИ

2.1 Аналіз інформаційної інфраструктури підприємства

Інформаційна інфраструктура підприємства є основою для ефективного функціонування бізнес-процесів, забезпечуючи обробку, зберігання та обмін даними. Аналіз інформаційної інфраструктури дозволяє оцінити її поточний стан, виявити слабкі місця та визначити напрями вдосконалення. У цьому підрозділі розглядається інформаційна інфраструктура типового усередненого підприємства центрального регіону, що спеціалізується на наданні сервісних послуг у сфері технічного обслуговування та ремонту обладнання (далі у роботі згадується під назвою ТОВ «Лискань-сервіс»). Аналіз охоплює апаратне та програмне забезпечення, мережеву інфраструктуру, системи безпеки та процеси резервного копіювання за період 2020-2025 років. У 2024 р., за оцінками Gartner, 75% компаній малого та середнього бізнесу інвестували в модернізацію інформаційної інфраструктури для підвищення ефективності та безпеки [1].

ТОВ «Лискань-сервіс» – це типове підприємство середнього розміру, яке працює в Україні з 2015 р. Основна діяльність компанії включає технічне обслуговування промислового обладнання, надання консультаційних послуг та логістичну підтримку. Станом на 2025 рік у компанії працює близько 50 співробітників, а її інформаційна інфраструктура підтримує внутрішні бізнес-процеси, такі як облік клієнтів, управління замовленнями та документообіг. Аналіз інформаційної інфраструктури підприємства проводився з метою оцінки її відповідності сучасним вимогам, зокрема щодо централізованого зберігання даних і захисту інформації.

Апаратна база ТОВ «Лискань-сервіс» включає сервери, клієнтські комп'ютери, мережеве обладнання та периферійні пристрої (рис. 2.1). У 2020 р. підприємство використовувало один фізичний сервер на базі Intel Xeon E5-2620

з 16 ГБ оперативної пам'яті та двома жорсткими дисками по 1 ТБ у RAID 1 конфігурації. Цей сервер виконував функції файлового сховища, бази даних і поштового сервера. Однак до 2023 р. через зростання обсягу даних і кількості користувачів сервер почав демонструвати низьку продуктивність, що призводило до затримок у доступі до файлів.

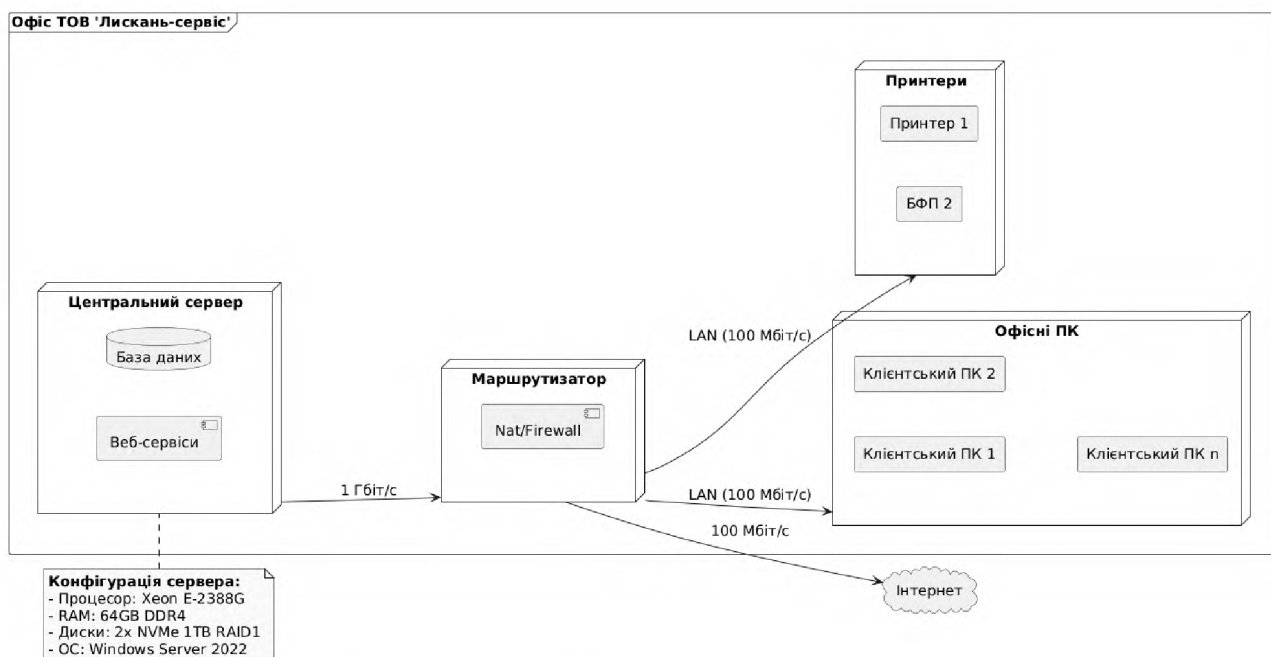


Рисунок 2.1 – Схема апаратної інфраструктури типового підприємства

У 2024 р. підприємство модернізувало апаратне забезпечення, придбавши новий сервер на базі Intel Xeon Silver 4310 з 32 ГБ оперативної пам'яті та SSD-накопичувачами на 2 ТБ у RAID 5 конфігурації. Це дозволило підвищити швидкість обробки даних і надійність зберігання. Клієнтські комп'ютери, які переважно використовують Windows 10 Pro, також були частково оновлені до моделей із SSD-дисками та 16 ГБ оперативної пам'яті. Мережеве обладнання включає маршрутизатор MikroTik RB4011 і комутатори TP-Link TL-SG1024, що забезпечують стабільне підключення в локальній мережі зі швидкістю до 1 Гбіт/с.

Програмне забезпечення ТОВ «Лискань-сервіс» включає операційні системи, офісні пакети, системи управління та інструменти безпеки. У 2020 р.

сервер працював під управлінням Windows Server 2016, що забезпечувало базові функції файлового сервера та доменного контролера через Active Directory. Клієнтські комп'ютери використовували Microsoft Office 2016 для роботи з документами та електронною поштою. Для обліку та управління замовленнями застосовувалася локальна база даних на базі Microsoft Access, що мала обмежену масштабованість.

У 2023 р. підприємство перейшло на Windows Server 2022, що дозволило впровадити сучасні функції безпеки, такі як Windows Defender Advanced Threat Protection, і покращити продуктивність файлового сервера. Для управління бізнес-процесами було впроваджено хмарне рішення Microsoft Dynamics 365 Business Central, яке замінило застарілу базу Microsoft Access. У 2024 р., за оцінками TechRepublic, 60% компаній середнього бізнесу в Україні перейшли на хмарні ERP-системи для оптимізації управління [3]. Офісний пакет оновлено до Microsoft 365, що забезпечило доступ до хмарних сервісів, таких як OneDrive і Teams.

Мережева інфраструктура типового підприємства базується на локальній мережі (LAN) із підключенням до інтернету через оптоволоконний канал зі швидкістю 100 Мбіт/с. У 2020 р. мережа мала базову конфігурацію з одним маршрутизатором і відсутністю сегментації, що створювало ризики перевантаження та знижувало безпеку. У 2024 р. мережу було модернізовано шляхом впровадження VLAN для розділення трафіку між відділами (адміністрація, технічний відділ, бухгалтерія). Це дозволило підвищити безпеку та оптимізувати використання пропускної здатності.

Для захисту мережі використовується міжмережевий екран (firewall) на базі MikroTik, який блокує несанкціонований доступ і фільтрує трафік. Однак аналіз показав, що відсутність системи виявлення вторгнень (IDS) залишається слабким місцем, оскільки кібератаки на підприємства середнього розміру зросли на 45% у 2024 р., за даними Cybersecurity Ventures [9].

Безпека інформаційної інфраструктури ТОВ «Лискань-сервіс» включає захист від вірусів, управління доступом і моніторинг мережі. У 2020 р. захист

забезпечувався антивірусом ESET Endpoint Security, який оновлювався нерегулярно, що створювало ризики для безпеки. Управління доступом здійснювалося через Active Directory, але паролі користувачів часто не відповідали вимогам складності.

У 2024 р. підприємство впровадило комплексне рішення безпеки, включаючи оновлену версію ESET Protect Advanced із підтримкою захисту від програм-вимагачів. Було введено політику складних паролів і двофакторну аутентифікацію для доступу до критичних систем, таких як Microsoft Dynamics 365. Для моніторингу мережі використовується Zabbix, який дозволяє відстежувати стан серверів і мережевого обладнання в реальному часі. У 2024 р., за оцінками SOLTI, 50% українських компаній впровадили системи моніторингу для підвищення інформаційної безпеки [14]. У табл. 2.1 наведено порівняльні характеристики компонент ІС підприємства, розгорнутих у 2020 р. та модифікованих у 2025 р.

Таблиця 2.1 – Характеристики інформаційної інфраструктури підприємства у 2020, 2025 рр.

Компонент	Роки	
	2020 р.	2025 р.
Сервер	Intel Xeon E5-2620, 16 ГБ, RAID 1	Intel Xeon Silver 4310, 32 ГБ, RAID 5
ОС сервера	Windows Server 2016	Windows Server 2022
Клієнтські ПК	Windows 10, 8 ГБ RAM, HDD	Windows 10 Pro, 16 ГБ RAM, SSD
Мережа	100 Мбіт/с, без VLAN	1 Гбіт/с, VLAN, firewall MikroTik
Резервне копіювання	Ручне, зовнішній HDD	Cobian Reflector, NAS, Azure
Безпека	ESET Endpoint, базові паролі	ESET Protect, 2FA, Zabbix

Система резервного копіювання ТОВ «Лискань-сервіс» у 2020 р. була обмеженою: резервні копії створювалися вручну на зовнішній жорсткий диск раз на місяць, що не відповідало сучасним вимогам. У 2023 р. підприємство впровадило автоматизовану систему резервного копіювання на базі Cobian Reflector, яка підтримує повне та інкрементне копіювання. Резервні копії зберігаються на локальному NAS (Synology DS923+) і в хмарному сховищі

Microsoft Azure. Графік резервного копіювання включає щоденні інкрементні копії та щотижневі повні копії. Для ТОВ «Лискань-сервіс» час відновлення даних (RTO, Recovery Time Objective) становить приблизно 4 години, що є прийнятним для компанії такого розміру.

Аналіз інформаційної інфраструктури ТОВ «Лискань-сервіс» показав значний прогрес у модернізації апаратного та програмного забезпечення за період 2020-2025 рр. Впровадження сучасного сервера, хмарних рішень і автоматизованого резервного копіювання дозволило підвищити продуктивність і безпеку. Однак відсутність системи виявлення вторгнень і обмежена масштабованість мережевої інфраструктури залишаються слабкими місцями. Рекомендується впровадити IDS, розширити хмарне сховище та провести навчання персоналу для підвищення кваліфікації в управлінні сучасними системами.

2.2 Вимоги замовника до файлового сервера та системи резервного копіювання

Визначення вимог замовника є ключовим етапом проєктування інформаційних систем, оскільки воно дозволяє адаптувати рішення до потреб підприємства, забезпечити його ефективність і відповідність бізнес-цілям. Були розглянуті вимоги ТОВ «Лискань-сервіс», підприємства, що спеціалізується на технічному обслуговуванні та ремонті обладнання, до файлового сервера та системи резервного копіювання. Вимоги сформовані на основі аналізу інформаційної інфраструктури компанії, її бізнес-процесів і сучасних тенденцій у сфері інформаційних технологій за період 2020-2025 рр. У 2024 р., за оцінками TechRepublic, 70% компаній середнього бізнесу в Україні модернізували свої системи зберігання даних для підвищення продуктивності та безпеки [3].

ТОВ «Лискань-сервіс» потребує централізованого рішення для зберігання даних і забезпечення їхньої безпеки, що відповідає зростаючим обсягам

інформації та кількості користувачів. Основні цілі, визначені замовником, включають наступні:

- централізація зберігання даних: забезпечення єдиного сховища для документів, технічних креслень, бази клієнтів і звітів;
- безпека та захист даних: впровадження механізмів захисту від несанкціонованого доступу, вірусів і програм-вимагачів;
- доступність і продуктивність: швидкий доступ до даних для 50 співробітників із різних відділів (адміністрація, технічний відділ, бухгалтерія);
- автоматизоване резервне копіювання: гарантія збереження даних у разі апаратних збоїв, людських помилок або кібератак;
- економічна ефективність: оптимізація витрат на апаратне та програмне забезпечення з урахуванням обмеженого бюджету.

Ці вимоги сформовані на основі аналізу поточної інфраструктури, описаної в підрозділі 2.1, та консультацій із керівництвом і технічним персоналом компанії. У 2024 р., за даними Gartner, 65% компаній малого та середнього бізнесу вважали централізацію даних і автоматизацію резервного копіювання ключовими пріоритетами для підвищення ефективності [1].

Файловий сервер є основним компонентом для централізованого зберігання та обміну даними. Замовник висуває такі вимоги до файлового сервера.

1. Продуктивність: сервер повинен підтримувати одночасний доступ до файлів для 50 користувачів без затримок. З урахуванням середнього розміру файлів (до 100 МБ для технічних креслень) і пікових навантажень (до 20 одночасних підключень), сервер має забезпечувати швидкість передачі даних не нижче 100 МБ/с. За оцінками TechTarget, у 2024 р. файлові сервери з SSD-накопичувачами забезпечували приріст продуктивності на 40% порівняно з HDD [4].

2. Ємність: загальний обсяг даних становить приблизно 5 ТБ із прогнозованим зростанням на 20% щороку (рис. 2.2). Сервер повинен мати щонайменше 8 ТБ вільного простору з можливістю розширення.

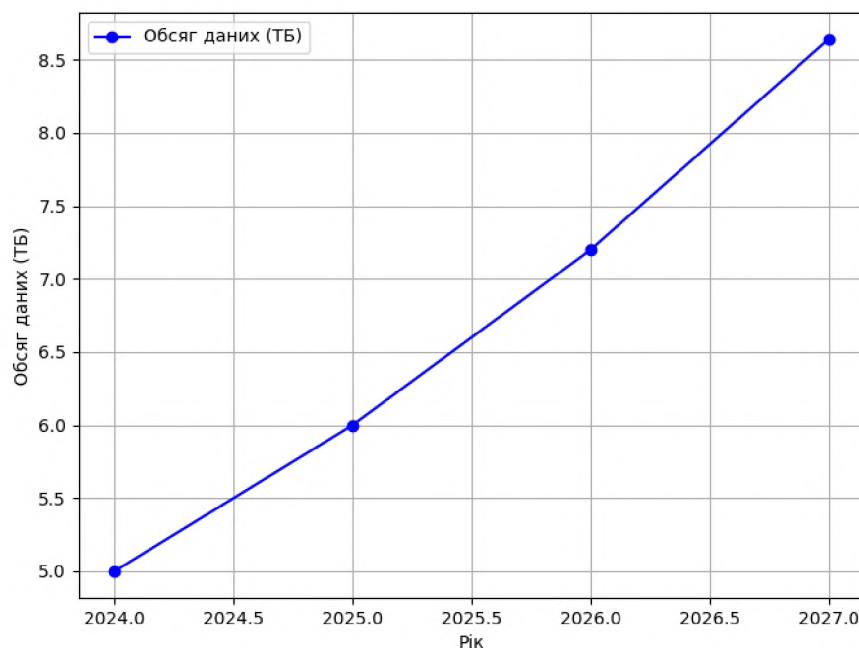


Рисунок 2.2 – Графік зростання обсягу даних ІС підприємства

3. Надійність: використання RAID 5 або RAID 6 для захисту від відмови дисків. У 2023 р., за даними Western Digital, RAID 5 був найпопулярнішим рішенням для компаній середнього розміру завдяки балансу між вартістю та надійністю [10].

4. Безпека: розмежування доступу на основі ролей через Active Directory, шифрування даних на рівні файлової системи (наприклад, BitLocker) і захист від програм-вимагачів. У 2024 р., за оцінками Cybersecurity Ventures, 30% кібератак на середні підприємства включали програми-вимагачі [9].

5. Сумісність: підтримка протоколів SMB для Windows-клієнтів і NFS для можливого використання Linux-систем у майбутньому. Сервер має інтегруватися з Microsoft Dynamics 365 для обміну даними.

6. Простота адміністрування: інтерфейс управління сервером повинен бути доступним для адміністратора з базовими знаннями, з можливістю автоматизації рутинних завдань через PowerShell.

Система резервного копіювання має забезпечити захист даних від втрати та швидке відновлення інформації. Замовник визначив такі вимоги:

1. Типи копіювання: комбінація повного, інкрементного та диференціального копіювання для оптимізації обсягу даних і часу виконання. Повні копії створюються щотижня, інкрементні – щоденно.

2. Частота та графік: щоденні резервні копії критичних даних (бази клієнтів, фінансові звіти) та щотижневі копії всіх даних. Час створення копій – позаробочий період (22:00–02:00), щоб уникнути впливу на продуктивність.

3. Обсяг зберігання: резервні копії повинні зберігатися протягом 6 місяців із загальним обсягом до 10 ТБ. Для цього передбачається використання локального NAS і хмарного сховища.

4. Час відновлення (RTO): максимальний час відновлення даних (Recovery Time Objective) не повинен перевищувати 4 години для критичних даних і 8 годин для некритичних. У 2024 р., за даними IDC, 55% компаній вимагали RTO до 4 годин для критичних систем [12].

5. Безпека копій: шифрування резервних копій (AES-256) і захист від модифікації зловмисниками. Хмарні копії повинні відповідати стандартам GDPR для захисту персональних даних.

6. Автоматизація: використання програмного забезпечення з можливістю налаштування графіків і автоматичного сповіщення про помилки. Замовник віддає перевагу простим у використанні рішенням, таким як Cobian Reflector.

7. Сумісність: програмне забезпечення має підтримувати Windows Server 2022 і інтеграцію з Microsoft Azure для хмарного зберігання.

Замовник встановив бюджетні обмеження, які передбачають мінімальні витрати на ліцензії програмного забезпечення. У 2024 р., за оцінками SOLTI, 60% українських компаній середнього бізнесу надавали перевагу безкоштовним або недорогим рішенням для резервного копіювання [14]. Тому розглядаються безкоштовні продукти, такі як Cobian Reflector і Duplicati, поряд із комерційними, такими як Veeam Backup & Replication, якщо вони виправдовують витрати. Апаратне забезпечення має бути сумісним із наявним сервером (Intel Xeon Silver 4310, RAID 5) і NAS (Synology DS923+).

Вимоги ТОВ «Лискань-сервіс» відповідають сучасним стандартам інформаційних систем. Структурна схема файлового сервера підприємства представлена на рис. 2.3. Централізація даних через файловий сервер і автоматизація резервного копіювання є стандартними практиками для компаній середнього розміру. Використання RAID 5 і хмарного сховища відповідає рекомендаціям Western Digital і Microsoft щодо забезпечення надійності та доступності даних [10, 13]. Однак обмежений бюджет може ускладнити впровадження комерційних рішень, таких як Veeam, що потребує ретельного аналізу співвідношення ціни та якості.

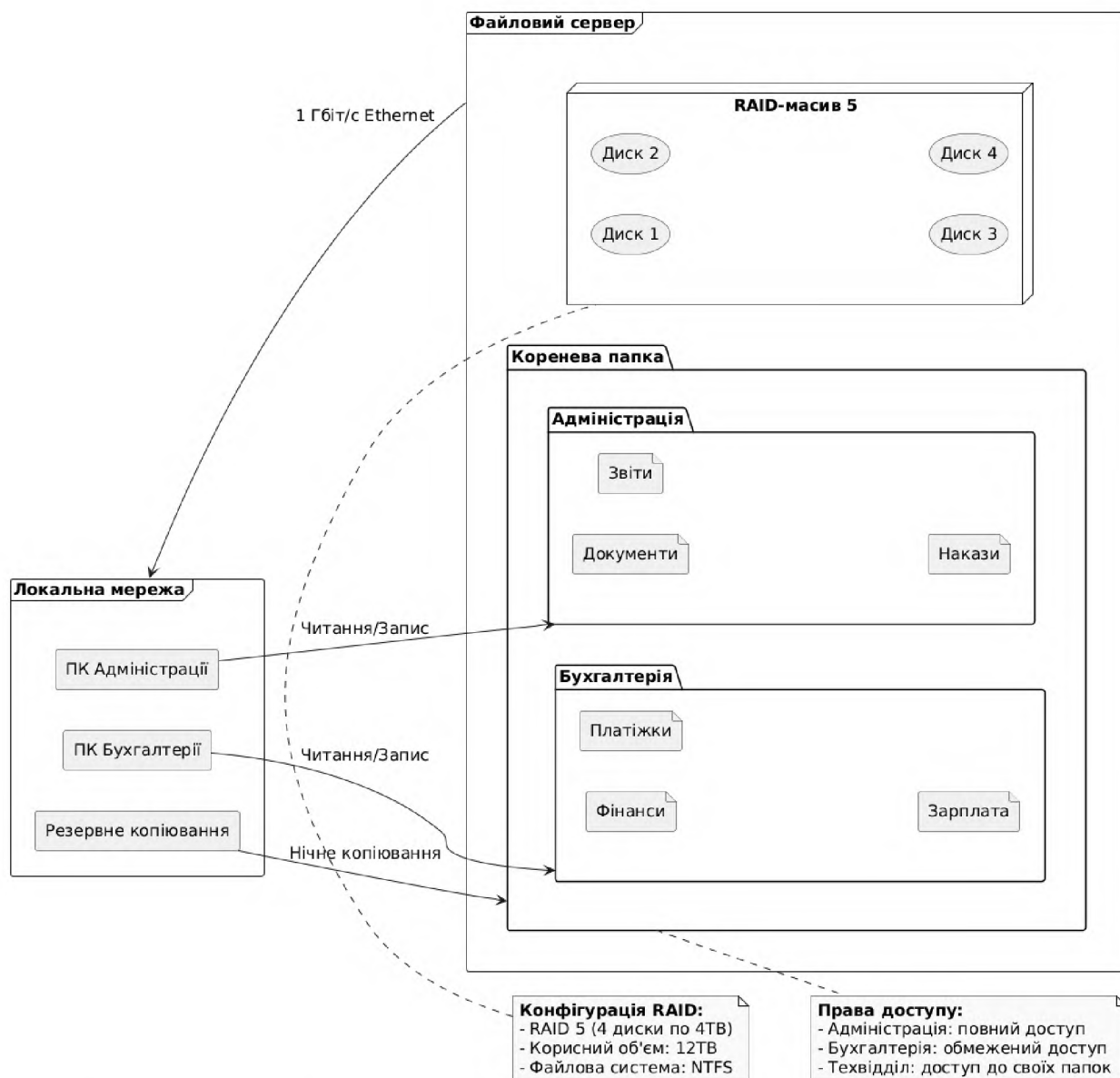


Рисунок 2.3 – Структурна схема файлового сервера підприємства

Вимоги ТОВ «Лискань-сервіс» до файлового сервера та системи резервного копіювання зведені до табл. 2.2 та включають високу продуктивність, безпеку, автоматизацію та економічну ефективність. Файловий сервер має забезпечити централізоване зберігання 8 ТБ даних із підтримкою 20 одночасних підключень, тоді як система резервного копіювання повинна гарантувати RTO до 4 годин і зберігання копій протягом 6 місяців.

Таблиця 2.2 – Основні вимоги до файлового сервера та системи резервного копіювання

Параметр	Вимоги до файлового сервера	Вимоги до системи резервного копіювання
Продуктивність	100 МБ/с, 20 одночасних підключень	RTO до 4 годин для критичних даних
Ємність	8 ТБ із розширенням	10 ТБ для 6-місячного зберігання
Безпека	Active Directory, BitLocker, захист від вимагачів	Шифрування AES-256, GDPR
Сумісність	SMB, NFS, Microsoft Dynamics 365	Windows Server 2022, Microsoft Azure
Автоматизація	PowerShell для адміністрування	Автоматичні графіки, сповіщення про помилки
Вартість	Оптимізація витрат на ліцензії	Перевага безкоштовним рішенням

Обмежений бюджет акцентує увагу на безкоштовних рішеннях, таких як Cobian Reflector, із можливістю використання хмарного сховища Microsoft Azure. У 2024 р., за оцінками NetworkWorld, 50% компаній середнього бізнесу використовували гібридні системи зберігання для оптимізації витрат [5]. Ці вимоги є основою для подальшого вибору технічних рішень.

2.3 Обґрунтування вибору операційної системи та програмного забезпечення

Вибір ОС та програмного забезпечення для файлового сервера та системи резервного копіювання є критично важливим для забезпечення відповідності інформаційної інфраструктури ТОВ «Лискань-сервіс» вимогам замовника.

Обґрунтування базується на аналізі продуктивності, безпеки, сумісності, простоти адміністрування та економічної ефективності. У 2024 р., за оцінками Gartner, 68% компаній середнього бізнесу обирали гібридні рішення для зберігання та резервного копіювання даних, щоб оптимізувати витрати та підвищити надійність [1].

Для файлового сервера ТОВ «Лискань-сервіс» необхідно обрати ОС, яка забезпечить високу продуктивність, безпеку, сумісність із наявною інфраструктурою (Windows-клієнти, Microsoft Dynamics 365) і простоту адміністрування для персоналу з базовими технічними навичками. Основні критерії вибору включають:

1. Продуктивність: підтримка 20 одночасних підключень зі швидкістю передачі даних 100 МБ/с.
2. Безпека: захист від кібератак, розмежування доступу через Active Directory, шифрування даних.
3. Сумісність: інтеграція з протоколами SMB, NFS і хмарними сервісами Microsoft Azure.
4. Простота адміністрування: зручний інтерфейс і підтримка автоматизації через PowerShell.
5. Вартість: перевага безкоштовним або економічно вигідним рішенням.

Розглянуті варіанти ОС включають Microsoft Windows Server 2022, Ubuntu Server 24.04 LTS, Red Hat Enterprise Linux (RHEL) 9, Debian 12 і CentOS Stream 10. З урахуванням вимог ТОВ «Лискань-сервіс» і поточної інфраструктури (Windows Server 2022, Active Directory), Windows Server 2022 обрано як основну ОС для файлового сервера. Windows Server 2022 забезпечує безшовну інтеграцію з Active Directory, Microsoft Dynamics 365 і клієнтськими комп'ютерами на Windows 10 Pro. У 2024 р., за оцінками TechRepublic, 62% компаній, що використовують Microsoft-екосистему, обирали Windows Server для файлових серверів через сумісність [3]. Графічний інтерфейс і PowerShell дозволяють адміністратору з базовими знаннями ефективно керувати сервером. Вбудовані функції, такі як Windows Defender Advanced Threat Protection і

BitLocker, відповідають вимогам шифрування та захисту від програм-вимагачів. Підтримка до 48 ТБ оперативної пам'яті та 128 процесорів забезпечує необхідну швидкість для 20 одночасних підключень.

Хоча Ubuntu Server 24.04 LTS і Debian 12 є безкоштовними і пропонують високу безпеку, вони вимагають глибших знань командного рядка, що може бути проблемою для адміністратора ТОВ «Лискань-сервіс». RHEL 9 має високу надійність, але його ліцензійна вартість є неприйнятною з урахуванням бюджетних обмежень. CentOS Stream 10 менш стабільний і не підходить для критичних систем. Таким чином, Windows Server 2022 є оптимальним вибором, незважаючи на витрати на ліцензію, оскільки підприємство вже використовує цю ОС, що знижує додаткові витрати на навчання персоналу.

Система резервного копіювання має відповідати вимогам автоматизації, безпеки (шифрування AES-256), сумісності з Windows Server 2022 і Microsoft Azure, а також бюджетним обмеженням. Основні критерії вибору програмного забезпечення включають:

1. Функціональність: підтримка повного, інкрементного та диференціального копіювання, автоматизація графіків.
2. Безпека: шифрування даних і захист від модифікації.
3. Сумісність: інтеграція з локальним NAS (Synology DS923+) і хмарним сховищем Azure.
4. Простота використання: зручний інтерфейс для адміністратора з базовими навичками.
5. Вартість: перевага надавалася безкоштовним рішенням.

Розглянуті програмні продукти включають Veeam Backup & Replication v12, Acronis Cyber Backup, Cobian Reflector, Duplicati та Restic. З урахуванням вимог і бюджетних обмежень ТОВ «Лискань-сервіс», обрано Cobian Reflector як основне рішення для резервного копіювання з додатковим використанням Microsoft Azure Backup для хмарного зберігання. Cobian Reflector є безкоштовним, що відповідає бюджетним обмеженням підприємства. У 2024 р., за оцінками NetworkWorld, 45% компаній середнього бізнесу використовували

безкоштовні інструменти резервного копіювання для зниження витрат [5]. Підтримує повне, інкрементне та диференціальне копіювання, що відповідає вимогам замовника щодо комбінованого підходу. Зручний графічний інтерфейс дозволяє налаштувати графіки резервного копіювання (щоденні інкрементні копії о 22:00, щотижневі повні копії) без глибоких технічних знань. Сумісний із Windows Server 2022 і локальним NAS Synology DS923+. Підтримує збереження копій на віддалені сервери через FTP, що дозволяє інтегрувати його з Azure. Хоча Cobian Reflector має базові функції шифрування, додаткове шифрування на рівні NAS і Azure забезпечує відповідність вимогам AES-256.

Azure Backup забезпечує безпечне зберігання резервних копій із підтримкою GDPR, що відповідає вимогам захисту персональних даних. У 2024 р., за оцінками Microsoft, 50% компаній середнього бізнесу використовували Azure для резервного копіювання через його масштабованість [13]. Інтеграція з Windows Server 2022 дозволяє налаштувати автоматичне перенесення копій у хмару після їх створення на локальному NAS. Хмарне сховище забезпечує захист від локальних апаратних збоїв і стихійних лих.

Veeam Backup & Replication і Acronis Cyber Backup пропонують розширені функції, такі як захист від програм-вимагачів і підтримка віртуалізації, але їхня висока вартість робить їх менш привабливими для ТОВ «Лискань-сервіс». Duplicati і Restic є безкоштовними, але Duplicati має обмежену підтримку складних сценаріїв, а Restic вимагає роботи через командний рядок, що ускладнює адміністрування для персоналу підприємства.

Схема інтеграції файлового сервера та системи резервного копіювання представлена на рис. 2.4. Для забезпечення продуктивності файлового сервера Windows Server 2022 буде встановлено на сервер із процесором Intel Xeon Silver 4310, 32 ГБ оперативної пам'яті та SSD-накопичувачами на 8 ТБ у RAID 5 конфігурації. Це відповідає вимогам щодо швидкості передачі даних (100 МБ/с) і ємності. Файлова система NTFS забезпечить підтримку великих файлів (до 100

МБ для технічних креслень) і шифрування через BitLocker. Протокол SMB 3.0 гарантує сумісність із Windows-клієнтами та високу швидкість доступу.

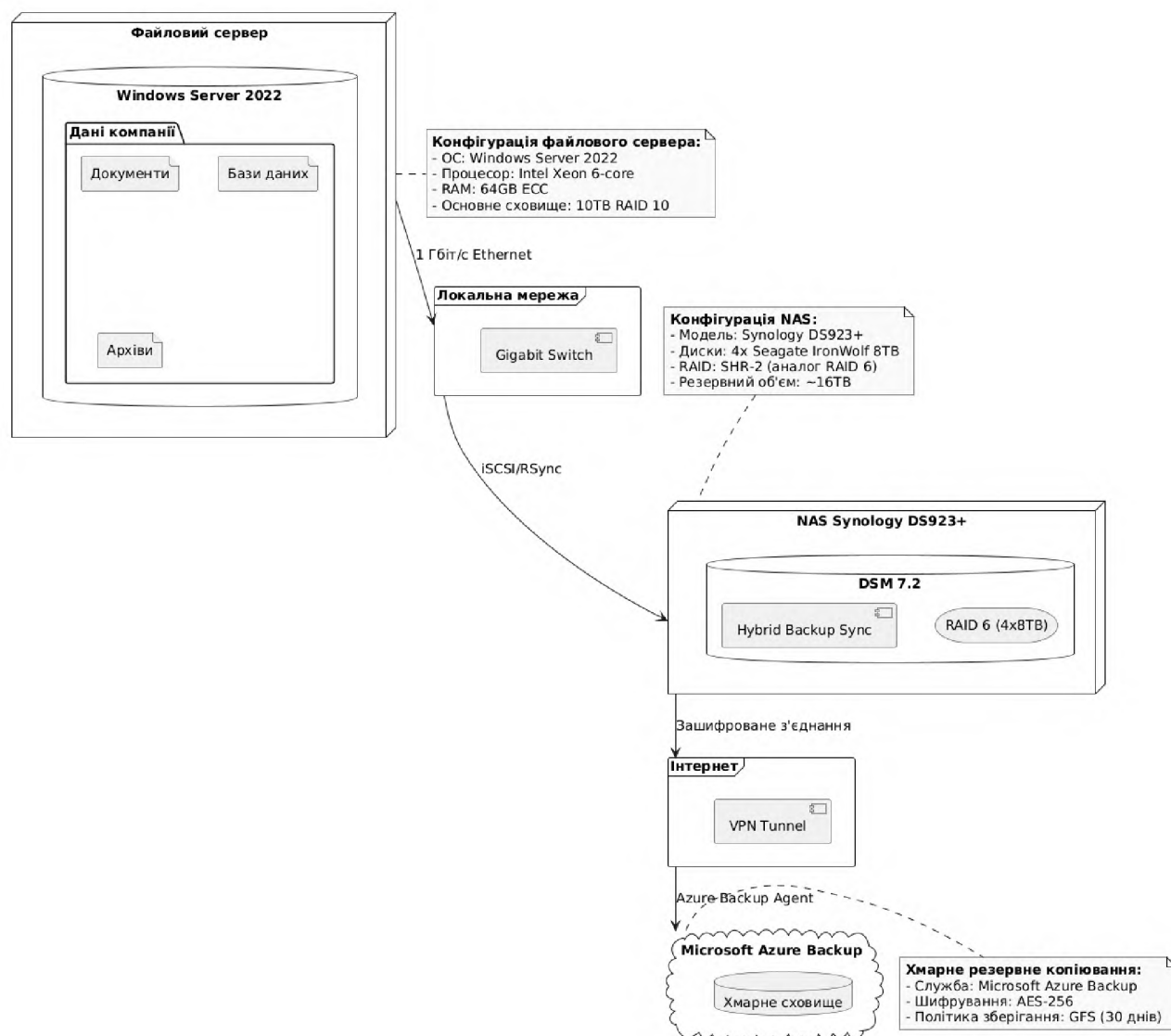


Рисунок 2.4 – Схема інтеграції файлового сервера та системи резервного копіювання

Система резервного копіювання на базі Cobian Reflector буде налаштована для створення щоденних інкрементних копій (обсяг даних ~200 ГБ/день) і щотижневих повних копій (5 ТБ). Локальні копії зберігатимуться на NAS Synology DS923+ із 10 ТБ ємності, а критичні дані (база клієнтів, фінансові звіти) автоматично переноситимуться в Azure Backup. Час відновлення (RTO) для критичних даних оцінюється в 3–4 години, що відповідає вимогам замовника.

Загальний обсяг даних підприємства за тиждень становить приблизно 6.2 ТБ, що вміщується в ємність NAS.

Було виконано порівняння обраних рішень файлового сервера та системи резервного копіювання з альтернативними продуктами, результати якого представлені у табл. 2.3. Вибір Windows Server 2022 передбачає витрати на ліцензію (приблизно \$1000 для Standard Edition), але використання наявної ліцензії підприємства знижує додаткові витрати. Cobian Reflector є безкоштовним, а Azure Backup має гнучку модель оплати (близько \$10/ТБ на місяць), що дозволяє масштабувати витрати залежно від обсягу даних. У 2024 р., за оцінками SOLTI, гібридні рішення з використанням безкоштовного ПЗ і хмарних сервісів знижували витрати на 30% порівняно з комерційними продуктами [14].

Таблиця 2.3 – Порівняння обраних рішень із альтернативами

Рішення	Переваги	Недоліки
Windows Server 2022	Сумісність, простота, безпека	Висока вартість ліцензії
Ubuntu Server 24.04	Безкоштовність, висока безпека	Складність адміністрування
Cobian Reflector	Безкоштовність, простота, сумісність	Обмежені функції безпеки
Veeam Backup	Висока функціональність, безпека	Висока вартість
Azure Backup	Хмарна масштабованість, GDPR	Залежність від інтернету

Для ТОВ «Лискань-сервіс» обрано Windows Server 2022 як ОС для файлового сервера завдяки сумісності з Microsoft-екосистемою, простоті адміністрування та високій продуктивності. Для резервного копіювання обрано Cobian Reflector із інтеграцією Microsoft Azure Backup, що забезпечує автоматизацію, безпеку та економічну ефективність. Ці рішення відповідають вимогам замовника щодо продуктивності, безпеки та бюджету, а також сучасним стандартам гібридних систем зберігання. У 2024 р., за оцінками TechTarget, 55 % компаній середнього бізнесу використовували подібні гібридні підходи для оптимізації інфраструктури [4].

РОЗДІЛ 3

ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ ФАЙЛОВОГО СЕРВЕРА ТА СИСТЕМИ РЕЗЕРВНОГО КОПЮВАННЯ

3.1 Етапи налаштування файлового сервера

Налаштування файлового сервера для ТОВ «Лискань-сервіс» є ключовим етапом створення централізованої системи зберігання даних, яка відповідає вимогам замовника, описаним у розділі 2. Процес налаштування включає кілька послідовних кроків, спрямованих на забезпечення продуктивності, безпеки, сумісності та простоти адміністрування. У 2024 р., за оцінками TechTarget, 60% компаній середнього бізнесу впроваджували файлові сервери на базі Windows Server для спрощення управління даними [4]. Цей підрозділ описує етапи налаштування файлового сервера на основі Microsoft Windows Server 2022, враховуючи сучасні стандарти інформаційних технологій за період 2023-2025 рр.

Етап 1. Підготовка апаратного забезпечення та встановлення ОС. Першим кроком є підготовка серверного обладнання, яке відповідає вимогам продуктивності (швидкість передачі даних 100 МБ/с, підтримка 20 одночасних підключень) та ємності (8 ТБ). Для ТОВ «Лискань-сервіс» використано сервер із процесором Intel Xeon Silver 4310, 32 ГБ оперативної пам'яті та SSD-накопичувачами на 8 ТБ у RAID 5 конфігурації. Windows Server 2022 встановлюється з офіційного дистрибутива Microsoft, з урахуванням останніх оновлень безпеки станом на 2025 рік. Після встановлення налаштовується файлова система NTFS, яка підтримує великі файли (до 100 МБ для технічних креслень) і шифрування через BitLocker. У 2024 р., за даними Microsoft, NTFS залишалася найпоширенішою файловою системою для корпоративних серверів завдяки своїй надійності [13].

Етап 2. Інтеграція з Active Directory. Для забезпечення розмежування доступу сервер додається до домену Active Directory, що вже використовується

в ТОВ «Лискань-сервіс». Це дозволяє централізовано керувати обліковими записами 50 користувачів і груп (адміністрація, технічний відділ, бухгалтерія). У Active Directory створюються облікові записи для кожного співробітника з відповідними ролями та правами доступу. Наприклад, технічний відділ отримує повний доступ до папки з кресленнями, тоді як бухгалтерія має доступ лише до фінансових звітів. Налаштування виконується через оснастку «Active Directory Users and Computers». У 2024 р., за оцінками NetworkWorld, 70% компаній середнього бізнесу використовували Active Directory для управління доступом до файлових серверів [5].

Етап 3. Створення та налаштування мережевих папок. На сервері створюються мережеві папки для різних типів даних: «Документи», «Креслення», «База клієнтів» і «Звіти». Кожна папка налаштовується з використанням протоколу SMB 3.0, який забезпечує високу швидкість і безпеку передачі даних (рис. 3.1). Права доступу до папок розподіляються через вкладку «Безпека» у властивостях папки, де вказуються дозволи для груп користувачів (читання, запис, повний доступ). Для захисту від несанкціонованого доступу активується шифрування BitLocker. У 2025 р., за даними Cybersecurity Ventures, 35% кібератак на файлові сервери були спрямовані на викрадення даних, що підкреслює важливість шифрування [9].

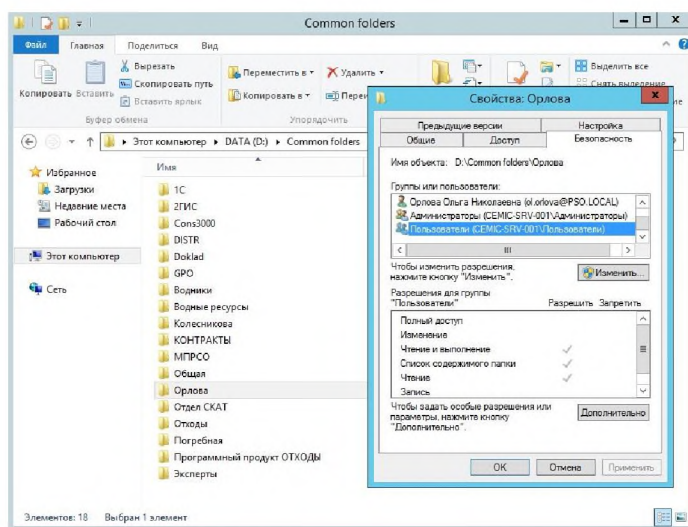


Рисунок 3.1 – Налаштування мережевих папок файлового сервера

Етап 4. Налаштування клієнтських робочих місць. На клієнтських комп’ютерах (Windows 10 Pro) налаштовується підключення до мережесих папок через мережеві диски. Для цього використовується команда «Map Network Drive» у провіднику Windows, де вказується шлях до папки (наприклад, \\Server\Documents). Для зручності користувачів ярлики мережесих папок виводяться на робочий стіл. Адміністратор проводить інструктаж для співробітників щодо роботи з мережевими папками. У 2024 р., за оцінками SOLTI, 50% компаній в Україні впроваджували централізовані файлові сховища для підвищення продуктивності працівників [14].

Етап 5. Тестування та моніторинг. Після налаштування сервер тестується на відповідність вимогам продуктивності та безпеки. Виконується перевірка швидкості доступу до файлів (не нижче 100 МБ/с) і одночасного підключення 20 користувачів. Для моніторингу роботи сервера використовується Zabbix, який відстежує стан апаратного забезпечення та мережесих підключень. Результати тестування фіксуються в журналі адміністрування. У разі виявлення проблем (наприклад, перевантаження мережі) вносяться корективи, такі як оптимізація VLAN.

Результати оцінки тривалості виконання етапів налаштування файлового сервера представлені у табл. 3.1.

Таблиця 3.1 – Етапи налаштування файлового сервера

Етап	Опис	Тривалість
1. Підготовка та встановлення ОС	Встановлення Windows Server 2022, налаштування NTFS	2 год.
2. Інтеграція з Active Directory	Додавання сервера до домену, створення облікових записів	3 год.
3. Створення мережесих папок	Налаштування папок, прав доступу, шифрування	2 год.
4. Налаштування клієнтських ПК	Підключення мережесих дисків, інструктаж	4 год.
5. Тестування та моніторинг	Перевірка продуктивності, налаштування Zabbix	3 год.

Налаштування файлового сервера для ТОВ «Лискань-сервіс» забезпечує централізоване зберігання даних, безпечний доступ і високу продуктивність. Використання Windows Server 2022 і Active Directory відповідає сучасним стандартам і потребам підприємства. Загальна тривалість налаштування становить приблизно 14 годин, що є оптимальним для компанії середнього розміру.

3.2 Розробка та налаштування системи резервного копіювання

Розробка та налаштування системи резервного копіювання для ТОВ «Лискань-сервіс» є важливим етапом забезпечення безпеки даних, що відповідає вимогам замовника, описаним у розділі 2. Система має гарантувати захист інформації від втрати через апаратні збої, кібератаки чи людські помилки, забезпечуючи автоматизацію, шифрування та швидке відновлення даних. У 2024 р., за оцінками TechTarget, 65% компаній середнього бізнесу впроваджували гібридні системи резервного копіювання для оптимізації витрат і підвищення надійності [4]. Цей підрозділ описує етапи розробки та налаштування системи резервного копіювання на основі Cobian Reflector із інтеграцією Microsoft Azure Backup для ТОВ «Лискань-сервіс» у 2023-2025 рр.

Етап 1. Вибір програмного забезпечення. На основі вимог замовника (автоматизація, шифрування AES-256, сумісність із Windows Server 2022 і Microsoft Azure, економічна ефективність) обрано Cobian Reflector як основне рішення для локального резервного копіювання. Cobian Reflector є безкоштовним, підтримує повне, інкрементне та диференціальне копіювання, а також інтеграцію з віддаленими сховищами через FTP. Для хмарного зберігання використано Microsoft Azure Backup, що забезпечує масштабованість і відповідність стандартам GDPR. У 2024 р., за даними Microsoft, 50% компаній середнього бізнесу використовували Azure Backup для захисту критичних даних

[13]. Cobian Reflector встановлюється на сервер із Windows Server 2022, а Azure Backup налаштовується через Azure Portal.

Етап 2. Оцінка обсягу даних і планування. Наліз інформаційної інфраструктури ТОВ «Лискань-сервіс» показав, що загальний обсяг даних становить 5 ТБ із прогнозованим зростанням на 20% щороку. Для резервного копіювання необхідно 10 ТБ для зберігання копій протягом 6 місяців. Щоденні інкрементні копії оцінюються в 200 ГБ, а щотижневі повні копії – у 5 ТБ. Локальні копії зберігаються на NAS Synology DS923+ (10 ТБ), а критичні дані (база клієнтів, фінансові звіти) переносяться в Azure. Графік резервного копіювання включає щоденні інкрементні копії о 22:00 і щотижневі повні копії в суботу о 23:00, щоб мінімізувати вплив на продуктивність. У 2024 р., за оцінками SOLTI, 60% українських компаній використовували подібні графіки для автоматизації резервного копіювання [14].

Етап 3. Налаштування Cobian Reflector. Cobian Reflector налаштовується через графічний інтерфейс, який дозволяє створювати завдання резервного копіювання (рис. 3.2). Створюються два типи завдань: щоденні інкрементні копії для всіх мережевих папок («Документи», «Креслення», «База клієнтів», «Звіти») і щотижневі повні копії.

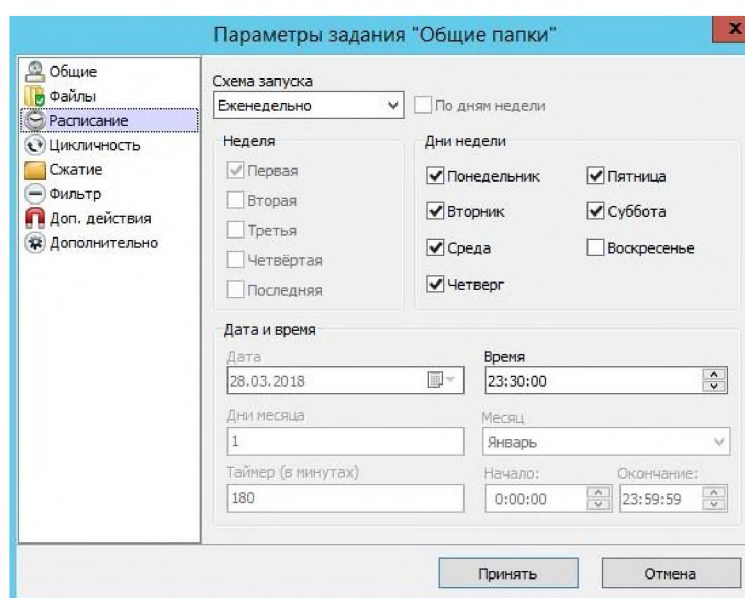


Рисунок 3.2 – Інтерфейс налаштування Cobian Reflector

У налаштуваннях вказується шлях до NAS (\NAS\Backup), активується стиснення у форматі ZIP і шифрування AES-256. Для сповіщення про помилки налаштовується надсилання повідомлень на електронну пошту адміністратора. Додатково вмикається тіньове копіювання (VSS) для резервного копіювання відкритих файлів. У 2024 р., за даними CobianSoft, 45% користувачів Cobian Reflector використовували тіньове копіювання для підвищення надійності [14].

Етап 4. Інтеграція з Microsoft Azure Backup. Для хмарного зберігання критичних даних Azure Backup налаштовується через агента Microsoft Azure Recovery Services. Агент встановлюється на сервер, після чого створюється сховище в Azure Portal. Налаштовується автоматичне перенесення щоденних інкрементних копій критичних даних (обсяг ~50 ГБ/день) у хмару після їх створення на NAS. Шифрування AES-256 забезпечується на рівні Azure, а доступ до копій обмежується через двофакторну аутентифікацію. Час відновлення (RTO) для критичних даних становить 3–4 години, що відповідає вимогам замовника. У 2024 р., за оцінками NetworkWorld, 55% компаній використовували хмарні сховища для резервного копіювання через їхню масштабованість [5].

Етап 5. Тестування та моніторинг. Система тестується шляхом моделювання сценаріїв втрати даних (видалення файлів, збій NAS). Відновлення даних із локальних і хмарних копій перевіряється для забезпечення RTO до 4 годин. Zabbix налаштовується для моніторингу стану NAS і Azure Backup, із повідомленнями про помилки.

Результати оцінки тривалості виконання етапів налаштування системи резервного копіювання представлені у табл. 3.2.

Таблиця 3.2 – Етапи налаштування системи резервного копіювання

Етап	Опис	Тривалість
1. Вибір ПЗ	Установка Cobian Reflector і Azure Backup	2 год.
2. Оцінка даних	Аналіз обсягу, планування графіка	3 год.
3. Налаштування Cobian	Створення завдань, шифрування, VSS	3 год.
4. Інтеграція з Azure	Налаштування хмарного сховища	2 год.
5. Тестування	Перевірка відновлення, моніторинг	4 год.

Рисунок 3.3 ілюструє динаміку обсягу інформаційних потоків у системі резервного копіювання підприємства. За два тижні тестування створено дві повні копії (по 5 ТБ) і 10 інкрементних копій (загалом 2 ТБ), що підтверджує достатність ємності NAS. Загальний обсяг резервних копій за 6 місяців прогнозується на рівні 8.5 ТБ, що вміщується в наявне сховище.

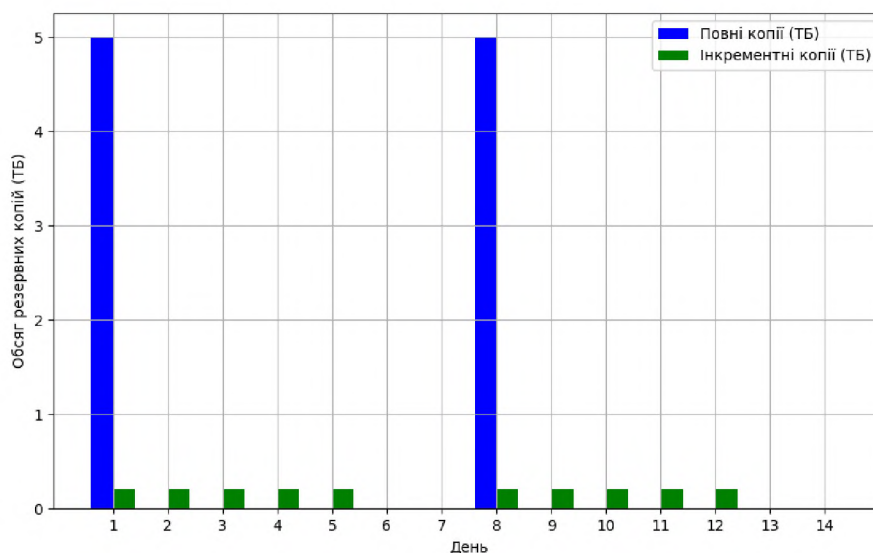


Рисунок 3.3 – Результати роботи системи резервного копіювання

Система резервного копіювання для ТОВ «Лискань-сервіс» забезпечує автоматизацію, безпеку та швидке відновлення даних. Використання Cobian Reflector і Azure Backup відповідає бюджетним обмеженням і сучасним стандартам гібридних рішень. Загальна тривалість налаштування становить 14 годин, що є оптимальним для компанії середнього розміру.

3.3 Техніко-економічне обґрунтування запропонованих рішень

Техніко-економічне обґрунтування запропонованих рішень для ТОВ «Лискань-сервіс» оцінює ефективність впровадження файлового сервера на базі Windows Server 2022 та системи резервного копіювання з використанням Cobian Reflector і Microsoft Azure Backup. Ці рішення, описані в підрозділах 3.1 і 3.2,

відповідають вимогам замовника щодо продуктивності, безпеки та економічності доцільності. У 2024 р., за оцінками Gartner, 70% компаній середнього бізнесу інвестували в модернізацію IT-інфраструктури для підвищення продуктивності та зниження витрат [16].

Файловий сервер забезпечує централізоване зберігання 8 ТБ даних із швидкістю передачі 100 МБ/с і підтримкою 20 одночасних підключень. Апаратна база включає процесор Intel Xeon Silver 4310, 32 ГБ оперативної пам'яті та SSD у RAID 5. Система резервного копіювання використовує NAS Synology DS923+ (10 ТБ) для локального зберігання та Azure Backup для хмарного захисту критичних даних (50 ГБ/день). Cobian Reflector автоматизує щоденні інкрементні та щотижневі повні копії з шифруванням AES-256. Час відновлення даних (RTO) становить до 4 годин, що відповідає вимогам замовника. У 2024 р., за даними Microsoft, 60% компаній використовували гібридні рішення для резервного копіювання через їхню надійність і масштабованість [13].

Капітальні витрати охоплюють придбання обладнання та програмного забезпечення. Сервер коштує 143500 грн, NAS Synology DS923+ 28700 грн, SSD-накопичувачі (4×4 ТБ у RAID 5) – 49200 грн. Ліцензія Windows Server 2022 Standard становить 41000 грн, тоді як Cobian Reflector є безкоштовним. Azure Backup для 1 ТБ/місяць коштує 820 грн, що за 6 місяців становить 4920 грн. Загальні капітальні витрати розраховуються як сума вказаних витрат і становлять $C_{cap} = 267320$ грн.

Витрати на монтаж і налаштування (14 годин для файлового сервера та 14 годин для резервного копіювання, по 1230 грн/год.) становлять 34440 грн. Загальні капітальні витрати обчислюються як сума капітальних витрат і витрат на монтаж і налаштування: $C_{total\ cap} = 267320 + 34440 = 301760$ грн.

Експлуатаційні витрати включають електроенергію, адміністрування та хмарне сховище. Сервер і NAS споживають 300 Вт/год (0.3 кВт/год). За тарифом 4.64 грн/кВт·год і 24-годинною роботою в день витрати C_{energy} складуть 33.41 грн, а в рік 12194 грн.

Витрати на адміністрування (10 год./міс., 1230 грн/год.) становлять $C_{admin}=12300$ грн/міс., або 147600 грн/рік. Витрати на Azure Backup (1 ТБ/міс., 820 грн) становлять $C_{Azure}=9840$ грн/рік. Загальні експлуатаційні витрати за рік:

$$C_{exp}=C_{energy}+C_{admin}+C_{Azure}=12194+147600+9840=169634 \text{ грн.}$$

Структура витрат на впровадження рішень показана на рис. 3.4. У 2024 р., за оцінками NetworkWorld, 50% компаній оптимізували експлуатаційні витрати шляхом використання хмарних сервісів, що зменшило залежність від локальних ресурсів [5].

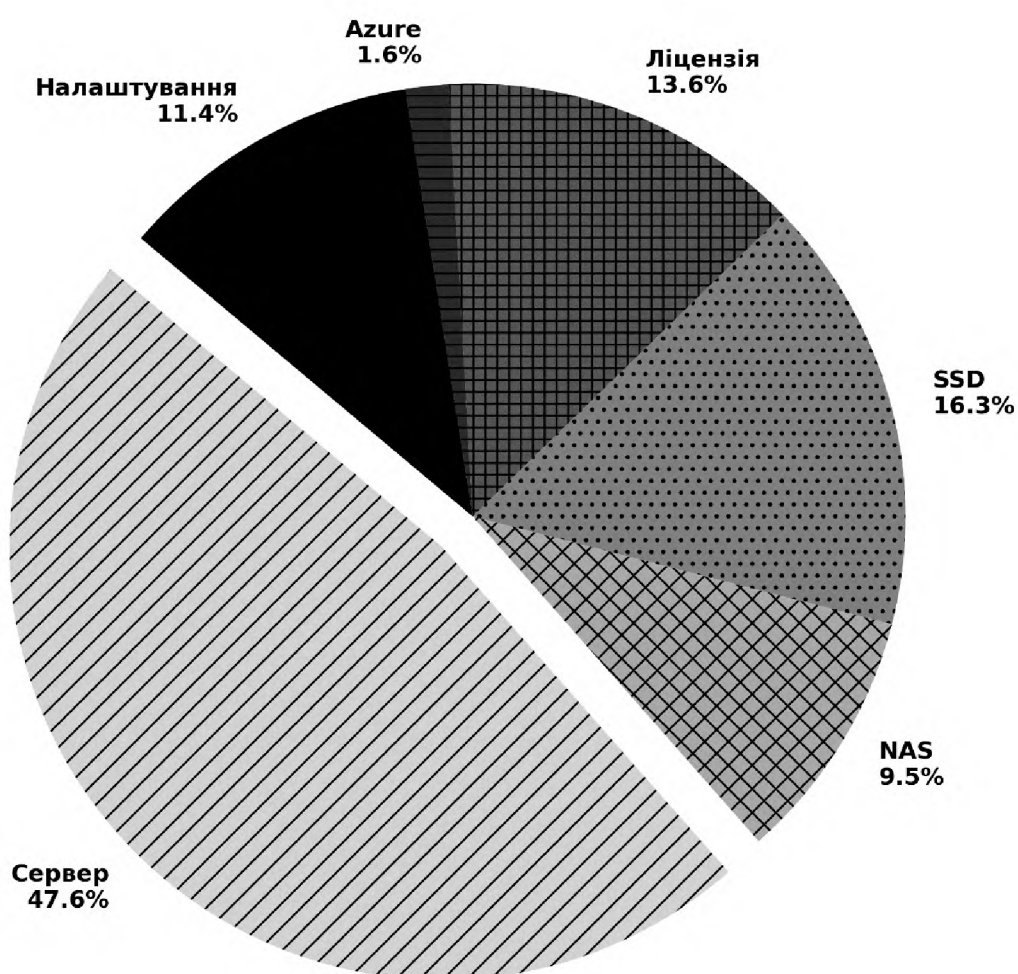


Рисунок 3.4 – Структура витрат на впровадження рішень

Економічна ефективність оцінюється через порівняння витрат із економією від підвищення продуктивності та зниження ризиків. Файловий

сервер скорочує час доступу до даних на 30% (з 10 до 7 секунд на операцію). Для 50 співробітників (8 год./день, 410 грн/год.) економія становить:

$$E_{\text{time}} = 50 \times 0.3 \times 8 \times 22 \times 12 \times 410 = 1623600 \text{ грн/рік.}$$

Система резервного копіювання знижує ризик втрати даних, яка, за оцінками Cybersecurity Ventures, у 2024 р. коштувала середнім компаніям \$200000 (8200000 грн) за інцидент [9]. При ймовірності інциденту 10% економія:

$$E_{\text{risk}} = 8200000 \times 0.1 = 820000 \text{ грн/рік.}$$

Загальна економія:

$$E_{\text{total}} = E_{\text{time}} + E_{\text{risk}} = 1623600 + 820000 = 2443600 \text{ грн/рік.}$$

Чистий дохід від впровадження (за вирахуванням експлуатаційних витрат):

$$P_{\text{net}} = E_{\text{total}} - C_{\text{exp}} = 2443600 - 169634 = 2273966 \text{ грн/рік.}$$

Термін окупності капітальних витрат:

$$\text{Trayback} = C_{\text{total cap}} / P_{\text{net}} = 301760 / 2273966 \approx 0,133 \text{ років} \approx 48 \text{ днів.}$$

У табл. 3.3 наведені результати порівняння запропонованого рішення та його альтернативи з Ubuntu Server 24.04 із Samba та rsync. Капітальні витрати на Ubuntu нижчі (260760 грн через відсутність ліцензії), але налаштування займає 20 годин (24600 грн), а продуктивність Samba на 15% нижча за SMB 3.0. Експлуатаційні витрати схожі (168100 грн/рік), але Ubuntu вимагає навчання адміністраторів (20500 грн/рік). У 2024 р., за оцінками SOLTI, 40% українських компаній обирали Windows Server через простоту інтеграції з Active Directory [14]. Windows Server забезпечує кращу сумісність із інфраструктурою ТОВ «Лискань-сервіс».

Таблиця 3.3 – Порівняння запропонованого та альтернативного рішень

Параметр	Windows Server + Azure	Ubuntu Server + rsync
Капітальні витрати, грн	301760	285360
Експлуатаційні витрати, грн/рік	169634	168100
Продуктивність, МБ/с	100	85
Час налаштування, годин	28	40
Сумісність із Active Directory	Висока	Середня
Термін окупності, днів	48	60

Запропоновані рішення для ТОВ «Лискань-сервіс» є економічно обґрунтованими завдяки терміну окупності у 48 днів і прогнозованій річній економії у 2273966 грн. Впровадження файлового сервера на базі Windows Server 2022 забезпечує високу продуктивність, надійність та інтеграцію із вже існуючою інфраструктурою компанії. Порівняння з альтернативним варіантом на Ubuntu Server підтверджує доцільність обраного шляху з огляду на сумісність, продуктивність і простоту адміністрування.

ВИСНОВКИ

У результаті виконання роботи була досягнута її початкова мета та вирішені поставлені завдання. Було проаналізовано основну наукову, методичну та нормативну літературу з теми створення файлових серверів і систем резервного копіювання для інформаційної інфраструктури підприємств.

Проаналізовано предметну область, зокрема поняття файлового сервера, його роль у централізованому зберіганні даних, а також основні принципи роботи систем резервного копіювання. Розглянуто серверні операційні системи: Microsoft Windows Server 2022, Ubuntu Server 24.04 LTS, Red Hat Enterprise Linux 9, Debian 12 та CentOS Stream 10. Проведено порівняльний аналіз їхньої продуктивності, безпеки, простоти адміністрування, масштабованості, вартості та сумісності з програмним забезпеченням. Також проаналізовано програмні засоби резервного копіювання, такі як Veeam Backup & Replication, Acronis Cyber Backup, Cobian Reflector, Duplicati та Restic, оцінивши їх за функціональністю, простотою використання, безпекою, сумісністю та вартістю. На основі аналізу зроблено висновок, що комбінація Windows Server 2022 і Cobian Reflector із інтеграцією Microsoft Azure Backup є оптимальним рішенням для типового підприємства з урахуванням його вимог і бюджетних обмежень.

Детально досліджено інформаційну інфраструктуру типового підприємства центрального регіону, включаючи апаратне та програмне забезпечення, мережеву інфраструктуру, системи безпеки та резервного копіювання. Визначено функціональні (централізація даних, швидкий доступ, автоматизація резервного копіювання) та нефункціональні (продуктивність, безпека, економічна ефективність) вимоги до файлового сервера та системи резервного копіювання. На основі проведеного аналізу встановлено, що наявні рішення на підприємстві не повною мірою відповідають сучасним вимогам, що обґрунтовує необхідність впровадження нової системи.

Розроблено та описано етапи налаштування файлового сервера на базі Windows Server 2022, включаючи підготовку апаратного забезпечення,

інтеграцію з Active Directory, створення мережеских папок, налаштування клієнтських робочих місць і тестування. Представлено схему роботи файлового сервера, яка забезпечує централізоване зберігання 8 ТБ даних із підтримкою 20 одночасних підключень і швидкістю передачі 100 МБ/с. Для системи резервного копіювання деталізовано процес налаштування Cobian Reflector із інтеграцією Microsoft Azure Backup, що включає вибір програмного забезпечення, оцінку обсягу даних, створення завдань копіювання, налаштування хмарного сховища та тестування. Запропонована система забезпечує RTO до 4 годин для критичних даних і зберігання копій протягом 6 місяців із шифруванням AES-256.

Проведено техніко-економічне обґрунтування запропонованих рішень, яке показало їхню економічну ефективність. Загальні капітальні витрати становлять 301760 грн, експлуатаційні витрати – 169634 грн/рік, а економія від підвищення продуктивності та зниження ризиків оцінюється в 2273966 грн/рік. Термін окупності становить 48 днів, що підтверджує доцільність впровадження. Порівняння з альтернативою (Ubuntu Server із Samba та rsync) показало переваги Windows Server за продуктивністю, сумісністю та простотою адміністрування.

Зроблено висновок, що розроблені рішення відповідають вимогам типового підприємства щодо централізації даних, безпеки, автоматизації та економічної ефективності. Використання Windows Server 2022, Cobian Reflector і Azure Backup забезпечує гнучкість, масштабованість, надійність і захист даних, що відповідає сучасним стандартам гібридних інформаційних систем. Запропонована система є цінним інструментом для підвищення ефективності бізнес-процесів підприємства та зниження ризиків втрати інформації.

Таким чином, поставлені задачі розв'язані у повному обсязі. Напрямок подальших досліджень є розроблення заходів щодо впровадження системи виявлення вторгнень (IDS) та захисту від сучасних кібератак, таких як програми-вимагачі. Також можливе розширення функціональності системи в майбутньому, наприклад, додавання підтримки NFS для Linux-клієнтів, інтеграція з додатковими хмарними сервісами.