Національний університет водного господарства та природокористування
Навчально-науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного врядування

Пояснювальна записка
до дипломної роботи

бакалавр
(освітньо-кваліфікаційний рівень)
на тему:

МОДЕРНІЗАЦІЯ ІТ-ІНФРАСТРУКТУРИ ДЕРЖАВНОГО АРХІВУ: ОПТИМІЗАЦІЯ СИСТЕМ ЗБЕРІГАННЯ ТА РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ

Виконав: студент 4 курсу, групи
ІБАС-41 спеціальності 029
«Інформаційна, бібліотечна
та архівна справа»
Половнєв Микита Ярославович

Керівник: к.е.н., доцентка кафедри
менеджменту та публічного
врядування
Маланчук Лариса Олексіївна

Рецензент: Цецик Ярослав Петрович

Рівне-2026

Форма № Н-9.01

Національний університет водного господарства
та природокористування
(повне найменування вищого навчального закладу)

Навчально-науковий інститут економіки та менеджменту
Кафедра менеджменту та публічного врядування
Рівень вищої освіти бакалавр
Спеціальність 029 «Інформаційна, бібліотечна та архівна справа»
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувачка кафедри
менеджменту та публічного
врядування
_____ (Л.Х. Тихончук)
“26” __червня___ 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ПОЛОВНЄВУ МИКИТІ ЯРОСЛАВОВИЧУ
(прізвище, ім’я, по батькові)

1. **Тема роботи:** Модернізація ІТ-інфраструктури державного архіву: оптимізація систем зберігання та резервного копіювання даних
Керівник роботи: к.е.н., доцентка кафедри менеджменту та публічного врядування Маланчук Лариса Олексіївна
затверджені наказом вищого навчального закладу від “27” квітня 2026 р. С №503
2. Строк подання студентом роботи «26» червня» 2026 р.
3. Вихідні дані до роботи: нормативно-правові акти, розпорядження органів виконавчої влади та місцевого самоврядування, статистичні дані, підручники, посібники, монографії, періодичні видання.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Теоретико-методологічні засади збереження цифрових архівних даних. 2. Аналіз інфраструктури та системи збереження даних державного архіву рівненської області. 3. Проект модернізації системи резервного копіювання, підвищення надійності ІТ-інфраструктури та організаційно-нормативне забезпечення системи зберігання даних.
5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) Таблиця 1.1 Таблиця 1.2 Таблиця 1.3 Таблиця 1.4 Таблиця 2.1 Таблиця 2.2 Таблиця 2.3 Таблиця 2.4 Таблиця 3.1 Таблиця 3.2 Таблиця 3.3 Таблиця 3.4 Рис. 2.1 Рис. 3.1

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Маланчук Л.О доцент	01.05.2026	10.05.2026
Розділ 2	Маланчук Л.О доцент	11.05.2026	25.05.2026
Розділ 3	Маланчук Л.О доцент	26.05.2026	05.06.2026

7. Дата видачі завдання « » 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів	Примітка
1.	Вступ Розділ 1. Теоретичний розділ	До 10.05.2026	
2.	Розділ 2. Аналітичний розділ	До 25.05.2026	
3.	Розділ 3. Проектування, обґрунтування, оптимальні рішення, їх впровадження	До 05.06.2026	
4.	Перевірка випускної кваліфікаційної роботи на наявність текстових збігів, оформлення презентації, документів та підготовка до захисту	До 16.06.2026	

Студент

_____ Микита ПОЛОВНЄВ
(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи

_____ Лариса МАЛАНЧУК
(підпис) (прізвище та ініціали)

StrikePlagiarism.com

Національний університет водного господарства та природокористування

Документ прийнятий

Метадані

ДОКУМЕНТ

Заголовок
Диплом.docx

Автор	Науковий керівник / Експерт	ID документу
Половнєв Микита Ярославович	**Половнєв Микита Ярославович**	**334369806**

ОРГАНІЗАЦІЯ

Назва організації	підрозділ
National University of Water and Environmental Engineering	**National University of Water and Environmental Engineering**

ЗВІТ

Дата звіту	Дата редагування
2026-06-19	—

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

11621
Кількість слів

КЦ

92619
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		13

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз | Колір тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

АКТ
перевірки випускної кваліфікаційної роботи
автора *Половнєва Микити Ярославовича*
на рівень запозичень та можливих маніпуляцій з текстом

Відповідно до даних системи StrikePlagiarism файл «Модернізація ІТ-інфраструктури державного архіву: оптимізація систем зберігання та резервного копіювання даних.»

містить: _2.5_ % коефіцієнта подібності; _2.07_% коефіцієнта цитованості; _0_ замінених букв; _0_ інтервалів; _0_ мікропробілів; _0_ білих знаків; _13_ парафраз.

За результатами перевірки засвідчую, що:
автор кваліфікаційної роботи ***Половнєв Микита Ярославович***:

- самостійно виконала кваліфікаційну роботу;
- коректно посилалась на використані інформаційні джерела;
- в роботі відсутні ознаки академічної недоброчесності.

Керівник кваліфікаційної роботи Лариса МАЛАНЧУК

Дата

ЗАЯВА
щодо самостійності виконання випускної кваліфікаційної роботи

Я, __Половнєв Микита Ярославович_____(ПІБ), студент(ка) _4__курсу ІБАС_ групи 41_ ННІ ЕМ_____

ЗАЯВЛЯЮ:

моя випускна кваліфікаційна робота на тему
«_Модернізація ІТ-інфраструктури державного архіву: оптимізація систем зберігання та резервного копіювання даних.», яка надається в екзаменаційну комісію із захисту кваліфікаційних робіт зі спеціальності «___Інформаційна, бібліотечна та архівна справа__»
для захисту, виконана самостійно і не містить плагіату.

Всі запозичення з друкованих та електронних джерел, у тому числі із захищених раніше випускових кваліфікаційних робіт мають відповідні посилання.

Я не використовував(ла) шахрайські методи маніпуляції з текстом (заміна букв, інтервали, мікропробіли, білі знаки, парафрази та ін.).

Інструменти штучного інтелекту використовував(ла) без порушення академічної доброчесності.

Я ознайомлений(а) з чинним Порядком перевірки навчальних, кваліфікаційних, навчально-методичних та наукових робіт на наявність ознак академічного плагіату в НУВГП та Положенням про академічну доброчесність в НУВГП, за яким виявлення плагіату є підставою для відмови в допуску моєї роботи до захисту та застосування відповідних санкцій (академічної відповідальності).

Дата *Підпис*

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЗБЕРЕЖЕННЯ ЦИФРОВИХ АРХІВНИХ ДАНИХ 5

1.1. Специфіка цифрових фондів в архівних установах: типи даних, їх об'єми та вимоги до довгострокового зберігання 5

1.2. Сучасні стратегії та моделі резервного копіювання: правило 3-2-1, RTO та RPO 9

1.3. Апаратні та програмні рішення для організації архівних сховищ: мережеві масиви NAS, технології RAID та хмарні платформи 13

ВИСНОВКИ ДО РОЗДІЛУ 1 16

РОЗДІЛ 2. АНАЛІЗ ІНФРАСТРУКТУРИ ТА СИСТЕМИ ЗБЕРЕЖЕННЯ ДАНИХ ДЕРЖАВНОГО АРХІВУ РІВНЕНСЬКОЇ ОБЛАСТІ 18

2.2. Оцінка поточного стану зберігання цифрового фонду: аналіз апаратного забезпечення та логічної архітектури масивів 24

2.3. Ідентифікація вразливостей та ризиків втрати даних: наслідки недотримання стратегії 3-2-1 29

ВИСНОВКИ ДО РОЗДІЛУ 2 32

РОЗДІЛ 3. ПРОЕКТ МОДЕРНІЗАЦІЇ СИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ, ПІДВИЩЕННЯ НАДІЙНОСТІ ІТ-ІНФРАСТРУКТУРИ ТА ОРГАНІЗАЦІЙНО-НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ 35

3.1. Розробка нової архітектури резервного копіювання: впровадження стратегії 3-2-1 та автоматизація процесів 35

3.2. Налаштування програмно-апаратного комплексу та впровадження заходів мережевої безпеки 42

3.3. Економічне та ресурсне обґрунтування проєкту модернізації ІТ-інфраструктури ДАРО 47

ВИСНОВОК ДО РОЗДІЛУ 3 53

ВИСНОВКИ 55

ВИКОРИСТАНІ ДЖЕРЕЛА 58

ВСТУП

Актуальність теми: умови стрімкої цифровізації суспільства та перехід до електронного документообігу ставлять перед державними архівними установами нові вимоги щодо збереження Національного архівного фонду. Збільшення обсягів оцифрованих документів у форматах високої якості, таких як TIFF та PDF, вимагає не лише нарощування обсягів дискового простору, але й створення надійних, відмовостійких систем зберігання. На сьогодні у багатьох регіональних архівах ІТ-інфраструктура не повною мірою відповідає сучасним вимогам кібербезпеки та стандартам резервного копіювання.

Відсутність автоматизованих систем резервного копіювання, використання єдиних несегментованих мереж та застарілі підходи до управління даними створюють критичні ризики безповоротної втрати унікальної історичної інформації наприклад, через вихід з ладу апаратних носіїв або кібератаки. Це зумовлює гостру необхідність модернізації ІТ-інфраструктури та впровадження комплексних стратегій резервного копіювання за правилом 3-2-1, що робить обрану тему дослідження актуальною.

Мета дослідження: аналіз поточного стану ІТ-інфраструктури Державного архіву Рівненської області та розробка комплексного проєкту її модернізації для забезпечення надійного зберігання швидкого доступу та безпечного резервного копіювання цифрових фондів.

Для досягнення поставленої мети було визначено такі завдання:

Дослідити теоретико-методологічні засади та міжнародні стандарти зберігання цифрових архівних даних.

Проаналізувати архітектуру існуючих систем резервного копіювання та визначити вимоги до апаратно-програмного забезпечення в архівних установах.

Провести аудит поточної ІТ-інфраструктури, топології мережі та систем зберігання NAS, RAID-масивів Державного архіву Рівненської області.

Виявити основні вразливості та ризики втрати даних.

Розробити проєкт модернізації мережевої інфраструктури та архітектури резервного копіювання на основі стратегії 3-2-1.

Обґрунтувати доцільність та ефективність запропонованих технічних рішень.

Об'єкт дослідження: процес організації ІТ-інфраструктури та управління даними в державних архівних установах.

Предмет дослідження: апаратно-програмні засоби, методи та технології оптимізації систем.

Методи дослідження:

Аналіз та синтез - для вивчення нормативно-правової бази, міжнародних стандартів та наукової літератури.

Системний підхід та аудит - для оцінки поточного стану мережевої топології та апаратного забезпечення ДАРО.

Метод моделювання та проєктування - під час розробки нової архітектури резервного копіювання та сегментації локальної мережі.

Метод порівняльного аналізу - для вибору оптимальних апаратних рішень (RAID-масивів, зовнішніх носіїв) та технологій кіберзахисту.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЗБЕРЕЖЕННЯ ЦИФРОВИХ АРХІВНИХ ДАНИХ

1.1. Специфіка цифрових фондів в архівних установах: типи даних, їх об'єми та вимоги до довгострокового зберігання

Перехід до інформаційного суспільства та цифровізація державного сектору змінили підходи до збереження історичної спадщини. Відповідно до Закону України “Про Національний архівний фонд та архівні установи” [1], електронні документи та цифрові копії паперових носіїв є невід'ємною частиною архівного фонду, що потребує створення специфічної, масштабованої ІТ-інфраструктури.

Сьогодні цифрові фонди державних архівів формуються переважно з двох масивів даних:

1. Електронні документи - це документи, що від самого початку створені в цифровому середовищі за допомогою систем електронного документообігу СЕД та підписані кваліфікованим електронним підписом КЕП.

2. Цифрові копії - це електронні версії традиційних паперових справ, створені шляхом сканування або фотофіксації. Головним викликом в управлінні цифровими архівами є експоненційне зростання обсягів даних, що зумовлено суворими вимогами до форматів їх збереження [5].

У практичній площині архівні установи оперують наступними типами файлів:

1. TIFF (Tagged Image File Format) - рекомендований формат для створення так званих “майстер-копій” або еталонних зображень. Це формат збереження без втрати якості (lossless), який фіксує всі фізичні особливості оригіналу. Нестиснений файл формату TIFF для однієї сторінки документа може досягати десятків мегабайт. Відповідно, збереження навіть невеликої частини оцифрованого фонду вимагає масивів дискового простору обсягом у десятки терабайтів.

2. JPEG (Joint Photographic Experts Group) - використовується як компромісний варіант для зберігання графічних копій високої якості при менших витратах дискового простору, проте має ризики втрати якості при перезаписі.

3. PDF (Portable Document Format) - використовується як “робоча копія” для надання доступу дослідникам, публікації на вебсайтах архівних служб або у спеціалізованих базах даних. Процес пакетної конвертації еталонних TIFF/JPEG-файлів у багатосторінкові PDF є ресурсомістким завданням для обчислювальних потужностей установи [6].

Необхідність одночасного оперування різними форматами файлів створює комплексне навантаження на IT-інфраструктуру архіву. Установа не може відмовитися від надвеликих еталонних файлів TIFF через жорсткі вимоги до збереження історичної якості оригіналів, але водночас вимушена витрачати обчислювальні ресурси на генерацію PDF-копій для забезпечення публічного доступу. Таке багатоцільове дублювання даних неминуче призводить до швидкого вичерпання дискового простору. Слід зауважити, що вимоги до довгострокового зберігання цифрових фондів суттєво відрізняються від корпоративного резервного копіювання. Міжнародний еталонний стандарт ISO 14721 “Відкрита архівна інформаційна система - OAIS” [4] визначає такі критичні критерії до збереження:

1. Автентичність та незмінність - гарантія того, що файл не був пошкоджений з моменту його завантаження в мережеве сховище.

2. Доступність - здатність IT-інфраструктури швидко обробляти запити та видавати об'ємні документи користувачам без перевантаження локальної мережі.

3. Незалежність від технологічного застарівання - модель зберігання повинна передбачати регулярну міграцію даних на нові апаратні носії для уникнення їх деградації так званого (bit rot) та фізичної поломки накопичувачів [8].

Специфіка цифрових архівних фондів полягає в оперуванні статичними даними надвеликих обсягів переважно графічними файлами високої роздільної здатності. Це вимагає відмови від спонтанного накопичення даних на розрізнених носіях та переходу до централізованих, високонадійних архітектур зберігання.

Для більш глибокого розуміння проблематики зберігання цифрових фондів необхідно детально проаналізувати формати файлів, з якими оперують архівні установи. Вибір формату є критичним не лише з точки зору візуальної якості, але й через прямий вплив на навантаження серверної інфраструктури та мережевого обладнання.

У таблиці 1.1 наведено порівняльну характеристику основних форматів, що використовуються в процесі оцифрування та зберігання архівних документів [6].

Формат файлу	Цільове призначення в архіві	Ступінь стиснення	Переваги	Ризики та недоліки
TIFF	Створення еталонних “майстер-копій”	Без стиснення	Максимальна деталізація, відсутність артефактів, точна передача кольору паперу та чорнил	Надзвичайно великий розмір файлів; високе навантаження на дискову підсистему
JPEG 2000	Альтернатива TIFF для еталонних копій	Lossless / Lossy	Краще співвідношення розміру до якості порівняно зі звичайним JPEG	Вимагає більших обчислювальних потужностей процесора для кодування/декодування
JPEG	Проміжні робочі копії, швидкий перегляд	З втратами	Невеликий розмір, швидке відкриття по мережі, низькі вимоги до апаратного забезпечення	Деградація якості при кожному перезбереженні; поява цифрових артефактів
PDF/A	Публікація е-копій, надання	Залежить від	Стандарт ISO для довгострокового зберігання; вбудовані	Складність пакетної конвертації; збільшення розміру

	доступу дослідникам	вбудованих зображень	шрифти та метадані; багатосторінковість	при вбудовуванні великих зображень

Таблиця 1.1 — Порівняльна характеристика форматів файлів для довгострокового архівного зберігання

Аналіз даних таблиці 1.1 демонструє, що архівна установа не може обмежитися використанням лише одного формату. На практиці впроваджується дворівнева або трирівнева модель: важкі TIFF-файли зберігаються на захищених масивах без прямого доступу, а легші PDF-копії генеруються для веб-серверів та читальних залів.

Така багаторівневість генерує колосальні обсяги даних. Для кращого розуміння навантаження на IT-інфраструктуру архіву, проведемо орієнтовний розрахунок необхідного дискового простору для зберігання невеликого пулу документів (таблиця 1.2). За основу візьмемо стандартний аркуш формату A4 210×297 мм, відсканований у кольоровому режимі 24-bit з роздільною здатністю 300 DPI, що є стандартом для архівних установ [7].

Тип збереження	Орієнтовний розмір 1 аркуша	Обсяг для 1 000 аркушів (1 середня справа)	Обсяг для 100 000 аркушів (частина фонду)
Еталонна копія TIFF	~ 25 МБ	25 ГБ	2,5 ТБ
Оптимізована копія JPEG	~ 4 МБ	4 ГБ	400 ГБ
Багатосторінкова копія PDF	~ 5 МБ (на сторінку)	5 ГБ	500 ГБ
СУМАРНО ДЛЯ АРХІВУ:	~ 34 МБ	34 ГБ	~ 3,4 ТБ

Примітка: розрахунки є орієнтовними та можуть змінюватись залежно від особливостей скануючого обладнання та налаштувань програмного забезпечення.

Таблиця 1.2 — Орієнтовний розрахунок обсягів дискового простору для зберігання цифрового фонду на прикладі 100 000 аркушів

Як видно з таблиці 1.2, оцифрування лише 100 000 аркушів що становить незначну частку від загального обсягу справ середнього обласного архіву, вже

вимагає понад 3 ТБ дискового простору. Враховуючи необхідність резервного копіювання а саме дублювання цих даних, реальна потреба в ємності мережевих сховищ зростає в геометричній прогресії.

Окрім проблеми фізичного обсягу, тривале зберігання масивів інформації супроводжується ризиком прихованої деградації даних - так званого “гнитті бітів” (bit rot або data degradation). Це процес непомітного пошкодження цифрових файлів на фізичних носіях HDD, SSD через вплив магнітних полів, зношення комірок пам'яті або мікропомилки контролерів [8].

Для звичайного користувача втрата кількох пікселів на фотографії є некритичною, проте для архівного документа наприклад, креслення або тексту зі згасаючим чорнилом деградація даних означає безповоротну втрату історичної інформації. Це вимагає впровадження в архівах спеціалізованих файлових систем таких як ZFS, які підтримують постійний моніторинг цілісності файлів за допомогою контрольних сум та автоматичне самовідновлення пошкоджених блоків із дзеркальних копій [9].

Таким чином, IT-інфраструктура архіву повинна будуватися з урахуванням не лише поточних обсягів даних, але й їхнього прогнозованого зростання, специфіки архітектури файлів та необхідності превентивного захисту від фізичної деградації носіїв інформації.

1.2. Сучасні стратегії та моделі резервного копіювання: правило 3-2-1, RTO та RPO

Процес збереження цифрових архівних фондів вимагає чіткого розмежування понять “апаратна відмовостійкість” та “резервне копіювання”. Наявність в установі мережевого сховища NAS з налаштованим RAID-масивом забезпечує лише відмовостійкість на випадок фізичної поломки одного з дисків проте не захищає від логічних помилок, випадкового видалення файлів працівниками, збоїв файлової системи або атак вірусів-шифрувальників [10]. Для

гарантованого захисту інформації необхідне впровадження комплексних моделей резервного копіювання.

Золотим стандартом у світовій IT-практиці та індустрії зберігання даних є методологія, відома як “Правило 3-2-1”, вперше сформульована Пітером Крогом. Ця концепція є апаратно-незалежною і визначає архітектурний підхід до розподілу ризиків втрати даних [11]. Відповідно до класичної моделі 3-2-1 надійна система повинна відповідати трьом базовим критеріям:

1. “3” - наявність щонайменше трьох копій даних, одна копія є основною робочою, наприклад файли на комп’ютері або сервері з якими безпосередньо працює завідувач сектору оцифрування, а дві інші - резервними. Це статистично мінімізує ймовірність одночасного пошкодження всіх примірників документа.
2. “2” - використання двох різних типів носіїв, резервні копії не повинні зберігатися на пристроях з однаковою архітектурою або в єдиному масиві. Наприклад, якщо перша копія знаходиться на жорстких магнітних дисках у NAS-сервері, друга копія має зберігатися на стрічковому накопичувачі, зовнішньому SSD-диску або оптичному носії. Це захищає від так званих “вендорних” помилок серійного браку партії дисків та специфічних апаратних збоїв.
3. “1” - зберігання однієї копії поза межами основної локації, найважливіший елемент стратегії що гарантує виживання даних у разі форс-мажорних обставин у будівлі архіву пожежа, затоплення сховища, вилучення обладнання, критичний перепад напруги. Offsite-копія може зберігатися у віддаленому дата-центрі, хмарному сховищі або фізично в іншому корпусі установи, який ізольований від основної локальної мережі.

Враховуючи зростаючу загрозу кібератак, сучасні стандарти кібербезпеки розширили це правило до формату 3-2-1-1-0, де додано вимогу наявності однієї ізольованої або незмінної копії, до якої неможливо отримати доступ з основної мережі, та гарантію “0” помилок під час автоматизованої перевірки цілісності бекапів після їх створення [12].

Окрім архітектурної моделі 3-2-1, проєктування системи резервного копіювання для державної установи базується на двох ключових метриках планування безперервності бізнес-процесів RTO та RPO. Для архівної справи ці показники мають свою специфіку порівняно з комерційним сектором. [13][37]

RPO (Recovery Point Objective або Цільова точка відновлення) - визначає максимально допустимий обсяг даних, який установа може дозволити собі втратити у проміжку між останнім успішним резервним копіюванням та моментом аварії. По суті, це частота створення бекапів.

Приклад: Якщо сектор оцифрування переводить у цифровий формат по 500 аркушів щодня, а бекап налаштований раз на тиждень, то RPO становить 5 днів. У разі поломки сервера в четвер, архів безповоротно втрачає результати роботи за понеділок-середу близько 1500 скан-копій, які доведеться сканувати наново.

RTO (Recovery Time Objective або Цільовий час відновлення) - позначає максимально допустимий час, необхідний для повного відновлення роботи IT-інфраструктури та доступу до даних після збою.

Приклад: Час який потрібен адміністратору для закупівлі нового диска замість згорілого, розгортання операційної системи на сервері та зворотного завантаження 3 терабайтів даних із хмарного резервного сховища що може зайняти кілька діб при обмеженій пропускній здатності інтернет-каналу. [37]

У таблиці 1.3 наведено розроблену матрицю вимог до показників RPO/RTO залежно від типу інформаційних ресурсів архіву.

Категорія даних	Критичність	Цільова точка відновлення (RPO)	Цільовий час відновлення (RTO)	Оптимальний метод бекапування
Еталонні майстер-копії	Критична - втрата дорівнює втраті фонду	24 години	48-72 години	Локальний NAS + ізольований офлайн-носій
База даних обліку та каталог	Висока - зупиняє роботу працівників	1-4 години	До 4 годин	Реплікація на віддалений сервер / Хмара
Веб-сайт архіву	Середня - копії можна згенерувати знову	7 діб	12-24 години	Хмарне сховище

Таблиця 1.3 - Матриця RTO/RPO для різних типів даних цифрового архіву

Аналіз даних таблиці показує, що для еталонних цифрових копій показник RTO є менш пріоритетним, ніж RPO. Для архіву краще чекати тиждень на відновлення терабайтів даних із “холодного” сховища, аніж швидко відновити сервер, але назавжди втратити унікальні скани за останній місяць через рідкісне створення резервних копій [14].

Відповідно впровадження моделі 3-2-1 з урахуванням розрахованих метрик RTO/RPO є грунтом для модернізації IT-інфраструктури архівних установ, що дозволяє перейти від реактивного вирішення проблем а саме ліквідації наслідків поломок до проактивного управління ризиками втрати Національного архівного фонду.

1.3. Апаратні та програмні рішення для організації архівних сховищ: мережеві масиви NAS, технології RAID та хмарні платформи

Реалізація стратегії резервного копіювання та забезпечення відмовостійкості архівних фондів вимагає використання спеціалізованого апаратного та програмного забезпечення. Історичний перехід від зберігання даних на розрізнених персональних комп'ютерах до централізованих рішень зумовив широке впровадження мережевих сховищ - NAS "Network Attached Storage" [15].

NAS являє собою виділений сервер або спеціалізований мікрокомп'ютер, оптимізований виключно для зберігання та надання доступу до файлів через локальну мережу. На відміну від універсальних серверів, сучасні NAS наприклад, виробництва Synology, працюють під управлінням спеціалізованих операційних систем які мінімізують споживання ресурсів та надають вбудовані інструменти для автоматизації бекапів, створення знімків файлової системи та управління правами доступу користувачів інтеграція з Active Directory [16].

Проте ключовим елементом надійності будь-якого мережевого сховища є дискова підсистема, організована за допомогою технології RAID "Redundant Array of Independent Disks - надлишковий масив незалежних дисків". Технологія RAID дозволяє об'єднати кілька фізичних жорстких дисків в один логічний том для підвищення швидкості читання/запису та забезпечення апаратної відмовостійкості на випадок виходу з ладу окремих накопичувачів.

Для зберігання цифрових архівів найчастіше використовують два типи масивів: RAID 5 та RAID 10.

RAID 5 - Чередування з розподіленою парністю: Цей масив вимагає мінімум трьох дисків. Дані та контрольні суми рівномірно розподіляються по всіх дисках масиву.

Переваги: висока економічна ефективність. Масив може пережити вихід з ладу одного будь-якого диска без втрати інформації. Корисна ємність масиву

розраховується за формулою (N - 1) × S, де N - кількість дисків, а S - об'єм найменшого диска. Тобто з трьох дисків по 10 ТБ корисний об'єм складе 20 ТБ.

Недоліки: процес запису інформації наприклад, збереження нових сканів є повільнішим через необхідність постійного обчислення контрольних сум. У разі поломки диска процес відновлення масиву може тривати кілька діб, сильно навантажуючи інші диски, що підвищує ризик виходу з ладу другого носія до завершення відновлення [17].

RAID 10 - Дзеркалювання та чередування: комбінований масив, який вимагає щонайменше чотирьох дисків. Інформація спочатку “дзеркалюється” копіюється на сусідній диск, а потім “чередується” розподіляється частинами.

Переваги: найвища швидкість читання та запису серед захищених масивів, надзвичайно швидке відновлення після заміни зламаного диска системі потрібно просто скопіювати дані з робочого дзеркала, без складних математичних обчислень. Масив може витримати поломку половини дисків головне, щоб не вийшли з ладу два диски з одного “дзеркала”.

Недоліки: висока вартість. Корисна ємність становить лише 50% від загального обсягу закуплених дисків.

Порівняльну характеристику цих масивів у контексті архівного застосування наведено в таблиці 1.4.

Характеристика	RAID 5	RAID 10
Мінімальна кількість дисків	3	4
Корисний обсяг	66% - 90% залежить від кількості дисків	Рівно 50%
Відмовостійкість	1 диск	Від 1 до половини дисків
Швидкість запису	Середня через обчислення парності	Висока
Сфера застосування в архіві	Зберігання “важких” еталонних копій TIFF, де важливий обсяг, а не швидкість запису	Розміщення баз даних та каталогів, де потрібна швидка реакція на запити користувачів

Таблиця 1.4 - Порівняння архітектур RAID-масивів для збереження цифрових архівів

Отже, вибір між типами масивів є компромісом між бюджетом установи та швидкістю доступу до документів. Проте варто наголосити на критичному правилі інформаційної безпеки що RAID не є резервною копією. Він захищає виключно від фізичної поломки накопичувача. Якщо працівник архіву випадково видалить справу, або файл буде зашифровано шкідливою програмою - ці пошкодження миттєво продублюються на всі диски масиву, і фонд буде втрачено [17].

Саме тому сучасна архітектура зберігання для дотримання правила 3-2-1 передбачає інтеграцію локальних NAS-серверів із зовнішніми системами:

Стрічкові бібліотеки - LTO: традиційний метод створення “холодних” офлайн архівів. Картриджі з магнітною стрічкою мають термін придатності до 30 років і найнижчу вартість за терабайт. Проте їх використання вимагає дорогого обладнання для зчитування.

Хмарні платформи - Cloud Storage: сучасна альтернатива для створення віддаленої копії. Хмарні провайдери пропонують об'єктні сховища, спеціально розроблені для архівів. Такі рішення наприклад, класи Amazon S3 Glacier або аналоги від локальних дата-центрів коштують значно дешевше за швидкі хмарні диски, проте мають обмеження на швидкість вивантаження даних [19].

Підсумовуючи, застосування гібридних комплексів є єдиним надійним підходом до збереження Національного архівного фонду. Розміщення первинних документів на швидкому локальному NAS-сервері, з паралельним автоматичним дублюванням їхніх копій на віддалені або хмарні майданчики, дозволяє установі не просто накопичувати електронні справи, а гарантувати виживання цифрової спадщини нації навіть за умови критичних системних аварій.

ВИСНОВКИ ДО РОЗДІЛУ 1

Специфіка функціонування сучасних архівних установ полягає в необхідності оперувати експоненційно зростаючими масивами статичних даних. Одночасне використання еталонних копій без втрати якості “TIFF” для страхового фонду та оптимізованих файлів “PDF/JPEG” для фонду користування створює колосальне навантаження на дискову підсистему установи. Відповідно до міжнародного стандарту OAIS, архівна система повинна не лише забезпечувати фізичне накопичення терабайтів інформації, але й гарантувати її автентичність, безперебійну доступність та превентивний захист від технологічної деградації носіїв.

Водночас забезпечення справжньої надійності цифрового фонду вимагає чіткого розмежування понять апаратної відмовостійкості та повноцінного резервного копіювання. Аналіз технічних рішень доводить, що використання виключно мережевих сховищ “NAS” та масивів технології RAID захищає архів лише від фізичної поломки окремих жорстких дисків. Така архітектура залишається критично вразливою у разі логічних збоїв файлової системи,

помилкових дій працівників чи цілеспрямованих атак шкідливого програмного забезпечення.

З огляду на ці загрози, єдиним надійним підходом до збереження Національного архівного фонду є проєктування інфраструктури на базі міжнародної стратегії резервного копіювання 3-2-1. Зважаючи на специфіку архівних метрик планування безперервності RTO та RPO, де пріоритетом є недопущення втрати історичних даних, оптимальною архітектурною моделлю виступає гібридна система. Вона передбачає розміщення робочих масивів на швидкодіючих локальних серверах із паралельним налаштуванням автоматичного дублювання на ізольовані фізичні носії та віддалені хмарні платформи.

РОЗДІЛ 2. АНАЛІЗ ІНФРАСТРУКТУРИ ТА СИСТЕМИ ЗБЕРЕЖЕННЯ ДАНИХ ДЕРЖАВНОГО АРХІВУ РІВНЕНСЬКОЇ ОБЛАСТІ

2.1. Характеристика існуючої IT-інфраструктури ДАРО: мережева топологія та організація доступу

Будь-який проєкт з модернізації систем зберігання та резервного копіювання цифрових фондів повинен базуватися на комплексному IT-аудиті існуючої інфраструктури установи [20]. Ефективність роботи мережевих сховищ “NAS” безпосередньо залежить від пропускної здатності локальної мережі, архітектури маршрутизації, налаштувань безпеки та політик управління доступом користувачів. У рамках переддипломної практики було проведено дослідження IT-екосистеми Державного архіву Рівненської області з метою виявлення її архітектурних особливостей та потенційних “вузьких місць”.

На сьогодні локальна обчислювальна мережа ДАРО обслуговує до 40 автоматизованих робочих місць “АРМ”, на яких працюють співробітники різних структурних підрозділів, включаючи сектор оцифрування, читальний зал та адміністративний персонал. З точки зору логічної архітектури, мережа архіву побудована за принципом так званої “плоскої мережі” (Flat Network). Це означає, що всі 40 робочих станцій, сервери, мережеві сховища та периферійні пристрої (принтери та сканери) знаходяться в єдиному широкомовному домені та одній підмережі. Відсутність сегментації за допомогою віртуальних локальних мереж VLAN є критичною архітектурною особливістю поточної інфраструктури [21].

Такий підхід має суттєві недоліки в контексті сучасних вимог до збереження архівних даних:

1. Зниження продуктивності - усі широкомовні запити від операційних систем (наприклад, пошук мережевих принтерів чи протоколи виявлення сусідів) розповсюджуються на всі 40 комп'ютерів, створюючи фонове “сміттєве”

навантаження на комутатори та знижуючи корисну пропускну здатність мережі. Це особливо критично під час передачі масивних TIFF-файлів від сканерів до мережевого сховища.

2. Вразливість до латерального переміщення - у разі інфікування одного комп'ютера (наприклад, у читальному залі) шкідливим програмним забезпеченням типу Ransomware (вірус-шифрувальник), шкідливий код має пряму мережеву видимість до всіх інших пристроїв. Це створює загрозу для серверів зберігання цифрового фонду, оскільки між комп'ютерами та мережевим сховищем немає внутрішніх маршрутизаторів або списків контролю доступу, здатних заблокувати поширення загрози [18].

Таким чином, поточна архітектура “плоскої мережі”, хоча й забезпечує базову взаємодію між усіма пристроями установи, але не повною мірою відповідає стандартам безпечного управління інформаційними ресурсами. Спільне перебування в одному мережевому сегменті серверів архіву та комп'ютерів загального користування створює зайве комутаційне навантаження та підвищує ризики випадкового пошкодження даних.

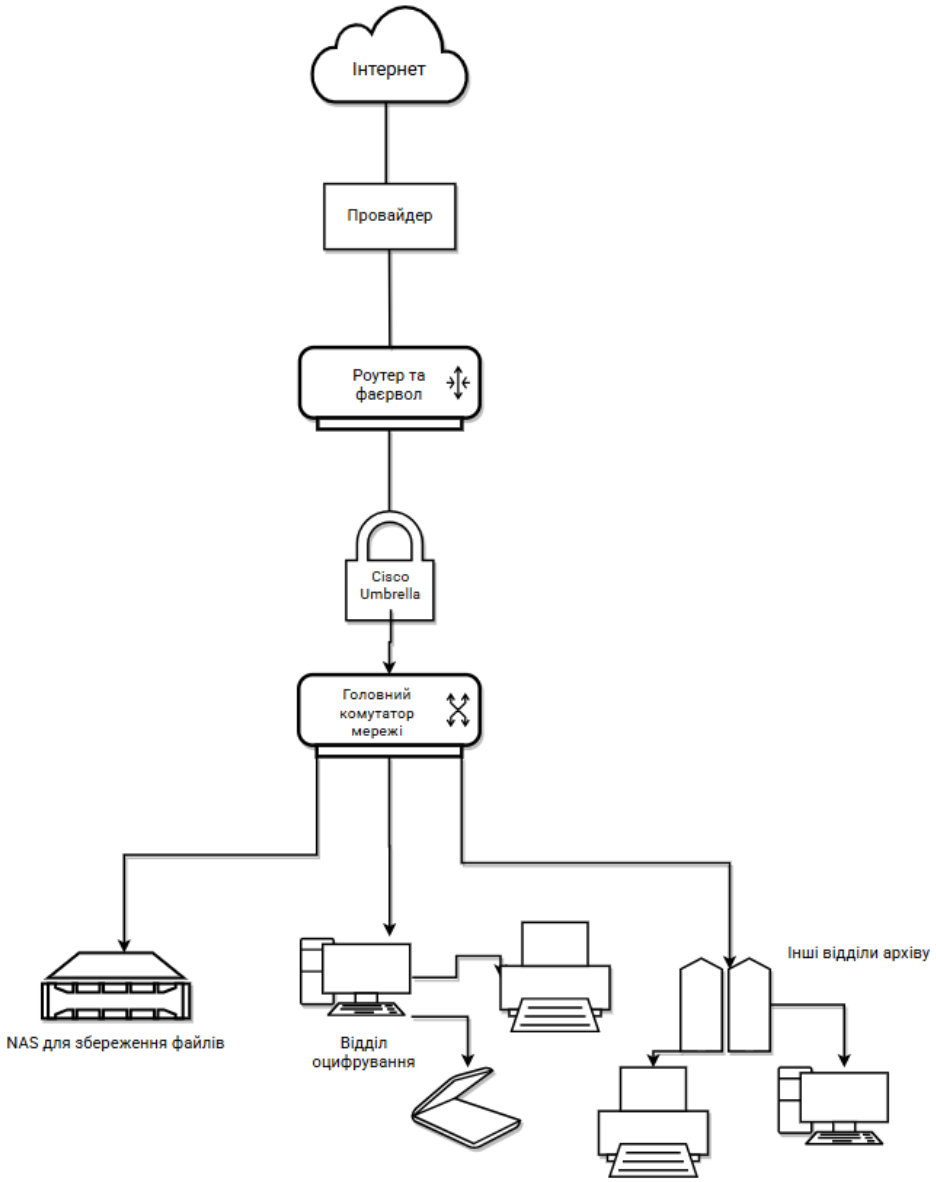

Рис. 2.1. Існуюча логічна топологія мережі ДАРО

Варто підкреслити той факт що, функціонування ДАРО також ускладнюється територіальною розподіленістю установи. Архів фізично розміщується у двох окремих корпусах. Зв'язок між цими будівлями забезпечується не через власну оптичну магістраль, а за допомогою орендованого каналу зв'язку від комерційного інтернет-провайдера. Організація передачі даних між корпусами через інфраструктуру провайдера покладає додаткові фінансові витрати на установу - щомісячна абонентська плата та створює залежність працездатності внутрішньої мережі архіву від стабільності зовнішнього підрядника. У разі аварії на лінії провайдера, співробітники одного

з корпусів повністю втрачають доступ до центрального сервера бази даних та мережевого сховища.

Доступ до глобальної мережі Інтернет та зв'язок із зовнішніми державними реєстрами забезпечується через Регіональний інформаційно-комп'ютерний центр - РІКЦ. Він надає архіву статичну IP-адресу, що є необхідною умовою для налаштування захищених тунелів та доступу до відомчих ресурсів.

Мережевим ядром та головним шлюзом виступає маршрутизатор виробництва латвійської компанії MikroTik, який був наданий з боку РІКЦ. Вибір рішень MikroTik є виправданим для державних установ, оскільки це обладнання дозволяє гнучко налаштовувати брандмауер - Firewall, NAT та правила маршрутизації за відносно низької вартості апаратного забезпечення. [22] Проте ефективність такого маршрутизатора залежить виключно від компетенції адміністратора та правильності написання правил фільтрації трафіку.

Згідно з отриманими даними ДАРО перебуває на початковому етапі розбудови комплексної системи кібербезпеки. Важливим кроком у цьому напрямку стало впровадження хмарного рішення Cisco Umbrella. Cisco Umbrella працює на рівні системи доменних імен - DNS та є першою лінією захисту архіву від інтернет-загроз. Архітектура цього рішення базується на перенаправленні всіх DNS-запитів від 40 комп'ютерів архіву на захищені сервери Cisco.

Механізм дії - Якщо співробітник архіву випадково натискає на фішингове посилання в електронному листі або намагається зайти на скомпрометований сайт, Cisco Umbrella аналізує цей запит до того, як встановиться IP-з'єднання. Якщо домен знаходиться в глобальній базі загроз, доступ блокується, що превентивно захищає локальну мережу від завантаження шкідливого коду. [23]

Також на стадії реалізації знаходиться доручення щодо підключення ДАРО до системи MISP - Malware Information Sharing Platform. [24] MISP - це платформа з відкритим кодом для збору, зберігання, поширення та аналізу індикаторів компрометації та інформації про кіберзагрози. [25]

Рівень захисту	Використовувана технологія	Стан впровадження	Оцінка ефективності
Шлюз	MikroTik - RouterOS, Firewall	Функціонує	Забезпечує базовий захист від зовнішнього сканування портів
Комплексний захист каналу	Рішення від провайдера РІКЦ	Функціонує	Забезпечує захист на магістральному рівні
DNS-фільтрація	Cisco Umbrella	Функціонує	Висока ефективність блокування фішингу та доступу до шкідливих доменів
Threat Intelligence	MISP	У процесі підключення	Дозволить архіву оперативно отримувати дані про нові вектори атак на держсектор
Внутрішня мережа	Відсутня	Критична вразливість	Відсутній захист від поширення загроз всередині архіву

Таблиця 2.1 - Аналіз поточних засобів мережевого захисту ДАРО

Аналіз показує, що хоча зовнішній периметр захищений досить непогано завдяки РІКЦ та Cisco, внутрішня мережа залишається абсолютно відкритою, що становить пряму загрозу для серверів, де зберігаються терабайти цифрового архівного фонду.

Найбільш критичною проблемою в управлінні ІТ-інфраструктурою ДАРО, виявленою під час аналізу, є повна відсутність служби каталогів Active Directory від Microsoft. [26]

На практиці це означає, що мережа з 40 комп'ютерів працює в режимі “Робочої групи” - Workgroup. Ця архітектура призводить до низки серйозних проблем в адмініструванні та безпеці:

1. Децентралізоване управління - для створення нового користувача, зміни його пароля або налаштування прав системний адміністратор повинен фізично підійти до кожного комп'ютера.

2. Відсутність єдиної політики безпеки - без Active Directory неможливо застосувати групові політики - GPO. Неможливо централізовано заборонити підключення особистих USB-флешок до робочих ПК, примусити користувачів змінювати пароль кожні 30 днів або заблокувати доступ до панелі керування Windows. [27]

3. Проблема з авторизацією на серверах сховища - оскільки єдиної бази користувачів немає, мережеве сховище NAS Synology не може автентифікувати співробітників за їхніми доменними іменами.

Саме через відсутність доменної інфраструктури в архіві склалася ситуація, коли доступ до цифрового сховища NAS має виключно адміністратор. Коли сектору оцифрування або іншим працівникам потрібно завантажити нові скановані документи або отримати копію для відповіді на запит громадянина, вони змушені звертатися безпосередньо до IT-спеціаліста. Це створює так зване “вузьке місце” в бізнес-процесах установи. Системний адміністратор витрачає значну частину свого робочого часу на рутинні операції з копіювання файлів замість розвитку інфраструктури, а швидкість надання архівних послуг знижується.

У разі запровадження Active Directory адміністратор міг би налаштувати безпечні мережеві папки на NAS-сервері з жорстко обмеженими правами доступу. Наприклад, сектор оцифрування мав би право запису у папку “Нові надходження”, а працівники читального залу мали б доступ лише на читання до

папки “Фонд користування”, без ризику випадкового видалення еталонних копій. [28]

2.2. Оцінка поточного стану зберігання цифрового фонду: аналіз апаратного забезпечення та логічної архітектури масивів

Центральним елементом ІТ-інфраструктури Державного архіву Рівненської області, що безпосередньо відповідає за збереження оцифрованої історичної спадщини, є підсистема зберігання даних. Для розуміння її ефективності необхідно проаналізувати не лише фізичні характеристики серверного обладнання, але й логічну організацію масивів, а також інтеграцію цих сховищ у щоденні бізнес-процеси сектору оцифрування.

Процес наповнення цифрового сховища ДАРО має чітко виражений циклічний характер, що створює нерівномірне навантаження на сервер та локальну мережу. Згідно з даними, отриманими під час дослідження роботи сектору оцифрування, базовим форматом для збереження відсканованих копій наразі обрано JPEG. Використання формату TIFF який є еталонним для довгострокового зберігання згідно з архівознавчими стандартами, визнається співробітниками як більш якісне рішення, проте на практиці застосовується рідше через критичну нестачу дискового простору. [29]

Життєвий цикл цифрового документа в ДАРО виглядає наступним чином[30]:

1. Генерація: Створення первинних зображень JPEG/TIFF на автоматизованих робочих місцях сектору оцифрування. На цьому етапі файли тимчасово знаходяться на локальних жорстких дисках комп'ютерів.

2. Переміщення на NAS: Ручне або напівавтоматичне перенесення масивів даних на централізоване мережеве сховище по “плоскій” локальній мережі.

3. Конвертація: Для публікації документів на офіційному вебсайті або надання доступу дослідникам, зображення формату JPEG необхідно

конвертувати у багатосторінкові файли формату PDF. Цей процес є найменш автоматизованим етапом роботи. [31]

4. Експорт: Готові PDF-файли відправляються на вебсервер.

Поточний життєвий цикл цифрового документа супроводжується значною часткою ручної праці та вимушеними компромісами щодо якості збереження історичних оригіналів. Нестача серверного простору змушує установу частково відмовлятися від еталонного формату TIFF на користь стиснених копій, а ручна конвертація файлів для публікації нераціонально використовує робочий час працівників. Усе це свідчить про те, що існуюча архітектура масивів виконує функцію переважно простого накопичувача і не забезпечує комплексної автоматизації архівних процесів.

Окремої уваги заслуговує архітектура публічного доступу. Сервер, на якому фізично розміщується вебсайт архіву, територіально знаходиться у м. Києві. Відповідно до договору з хостинг-провайдером для потреб ДАРО виділено жорстко лімітовану квоту дискового простору обсягом до 500 ГБ. Враховуючи специфіку архівних фондів, такий обсяг є критично малим. Це створює парадоксальну ситуацію, архів має фізичну можливість оцифровувати більше справ, але обмежений у можливостях їх публікації через нестачу орендованого простору на вебсервері.

Для часткового вирішення проблеми обміну даними великого обсягу зокрема, при наданні копій за запитами, співробітники використовують хмарний сервіс Google Drive, де доступ до файлів надається користувачам за посиланням з обмеженим терміном дії на 6 місяців. Хоча це тимчасово вирішує комунікаційні завдання, використання публічних неконтрольованих хмарних дисків поза межами єдиної корпоративної IT-політики створює ризики витоку інформації та порушує цілісність управління архівом. [32]

У якості основного вузла зберігання “важких” даних в локальній мережі ДАРО використовується спеціалізоване мережеве сховище виробництва компанії

Synology. Вибір рішень Synology є стандартом для бюджетних та середніх державних установ завдяки зручній операційній системі DiskStation Manager - DSM та підтримці різноманітних протоколів передачі даних SMB, AFP, NFS. [33]

Однак аудит логічної структури дискової підсистеми виявив серйозні обмеження, що загрожують цілісності даних. Наразі інфраструктура зберігання зокрема, фонд “Цифровий НАФ” розділена на декілька логічних томів, серед яких ключовими є масиви на 3 ТБ та 10 ТБ.

Найбільше занепокоєння викликає використання масиву архітектури RAID 5 для зберігання еталонних копій. Як зазначалося в теоретичному розділі, RAID 5 здійснює чередування даних з розподіленою парністю. Для розрахунку корисної ємності такого масиву використовується математична модель:

$C = (N - 1) \times S$, де C - загальна корисна ємність масиву, N - кількість фізичних жорстких дисків, а S - ємність найменшого диска у масиві. [34]

Згідно з цією формулою, для досягнення ефективного обсягу в 3 ТБ або 10 ТБ, сховище ДАРО агрегує кілька фізичних носіїв. Основна проблема RAID 5 в архівних реаліях полягає у процесі відновлення. Якщо один з дисків у масиві на 3 ТБ виходить з ладу, система залишається працездатною, але переходить у критичний стан - Degraded Mode. Після встановлення нового диска контролер Synology починає перераховувати контрольні суми для відновлення втрачених терабайтів даних. Цей процес створює максимальне навантаження на механічні компоненти всіх інших робочих дисків масиву і може тривати від кількох діб до тижня. Практика показує, що ймовірність виходу з ладу другого зношеного диска саме під час процедури відновлення масиву є вкрай високою, що призведе до повного руйнування всього логічного тому і безповоротної втрати всього пулу оцифрованих справ. [35]

Логічний том / Призначення	Використана технологія	Обсяг	Критичність ризику та його обґрунтування
Основний масив NAS - Робочі копії	RAID 5	3 ТБ	Високий. Тривалий час відновлення. Критична ймовірність виходу з ладу другого зношеного диска під час перерахунку контрольних сум, що призведе до повної втрати всього логічного тому.
Масив NAS “Цифровий НАФ” - Еталонні копії	RAID 1	10 ТБ	Середній. Апаратна відмовостійкість вища, проте через відсутність ізольованих офлайн-бекапів залишається ризик повної втрати даних внаслідок логічних помилок або атаки вірусу-шифрувальника.
Зовнішній веб-сервер архіву м. Київ	Орендований дисковий простір дата-центру	500 ГБ	Критичний. Жорсткий ліміт місця повністю блокує планову роботу з публікації нових оцифрованих справ та популяризації архівних фондів у мережі Інтернет.
Тимчасовий обмінник для користувачів	Хмарний сервіс Google Drive	Лімітовано квотою акаунту	Середній. Ризики несанкціонованого поширення посилань, неможливість централізованого аудиту доступу та автоматична втрата файлів через 6 місяців.

Таблиця 2.2 - Оцінка ризиків існуючої логічної структури зберігання даних ДАРО

Наслідком відсутності єдиної служби каталогів Active Directory, яка була детально описана у попередньому підрозділі, є архітектурна проблема в управлінні доступом, прямий доступ до файлової структури NAS-серверів має виключно системний адміністратор. [26]

Цей фактор кардинально змінює логіку взаємодії персоналу з цифровим фондом (таблиця 2.3).

Завдання	Поточна модель ДАРО Монопольний доступ	Оптимальна модель Рольовий доступ / RBAC
Завантаження нових скан-копій на сервер	Співробітник передає файли адміністратору який вручну розміщує їх у потрібні директорії.	Співробітник сектору оцифрування самостійно завантажує файли у виділену мережеву папку “Нові надходження” зі свого ПК.
Пошук документа для видачі копії користувачу	Адміністратор за запитом шукає файл у сховищі і передає його співробітнику читального залу.	Співробітник читального залу має доступ “Тільки читання” до каталогу PDF-файлів і миттєво знаходить потрібний документ.
Видалення тимчасового “сміття”	Виконується адміністратором за фактом критичного переповнення дисків.	Автоматизовані квоти користувачів не дозволяють перевищувати ліміти дискового простору.

Таблиця 2.3 - Порівняльний аналіз моделей управління доступом до архівних фондів

Як видно з таблиці, діюча ІТ-модель перетворює висококваліфікованого ІТ-спеціаліста на звичайного оператора з копіювання файлів. Сховище Synology у даному випадку працює не як динамічний мережевий ресурс для всієї установи, а як закритий “цифровий сейф” з єдиним ключем.

Більше того, керівництвом установи розглядається можливість надання доступу зовнішнім користувачам до частини інформації напряму зі сховища. Технічно це можливо реалізувати засобами операційної системи Synology. Однак, в умовах відсутності сегментації мережі VLAN та повноцінного внутрішнього брандмауера, “відкриття” портів NAS-сервера безпосередньо у глобальну мережу Інтернет створить критичну вразливість нульового дня. Будь-яка атака на веб-інтерфейс сервера може призвести до шифрування всього архіву. [36]

Узагальнюючи аудит апаратного та програмного забезпечення систем зберігання ДАРО, можна констатувати, що існуюча конфігурація досягла межі свого масштабування. Обмеження дискового простору на хостингу у 500 ГБ, повільні масиви RAID 5, монополізований доступ та ручна конвертація форматів є системними бар'єрами, які унеможливлюють перехід архіву до інтенсивного оцифрування фондів та потребують негайної технічної модернізації.

2.3. Ідентифікація вразливостей та ризиків втрати даних: наслідки недотримання стратегії 3-2-1

Завершуючим етапом аудиту IT-інфраструктури Державного архіву Рівненської області є комплексна ідентифікація вразливостей системи зберігання даних. Як було доведено у попередніх підрозділах, наявність мережевих сховищ NAS та використання технологій RAID забезпечують базовий рівень апаратної відмовостійкості, проте не є повноцінною заміною системи резервного копіювання.

Зіставлення фактичного стану IT-інфраструктури ДАРО з міжнародними стандартами архівного зберігання зокрема, моделлю OAIS та концепцією забезпечення безперервності роботи дозволило виявити низку критичних відхилень.

Найбільш критичною вразливістю поточної IT-моделі установи є фактична відсутність регламентованого процесу створення резервних копій. Зафіксовано, що класичне правило 3-2-1 три копії, два різні носії, одна віддалена локація, детально описане в підрозділі 1.2, в архіві не виконується.

Дані, що генеруються сектором оцифрування, після перенесення на NAS-сервери існують фактично в єдиному екземплярі в межах одного логічного тому RAID. Це означає, що показник цільової точки відновлення RPO для установи прагне до нескінченності у разі критичного збою логічної структури масиву, відновлення інформації за попередні періоди буде неможливим, оскільки історичних зрізів даних не існує. [37]

Практичним підтвердженням критичності цієї вразливості є зафіксований в установі інцидент із раптовим виходом з ладу жорсткого диска обсягом 2 ТБ який “згорів” під час експлуатації. У ситуаціях, коли накопичувач не є частиною надлишкового масиву або коли відсутня зовнішня резервна копія, подібні апаратні збої призводять до миттєвої та безповоротної втрати всього масиву інформації, що знаходився на носії. Цей прецедент яскраво ілюструє, що покладання виключно на фізичну надійність окремих дисків у контексті збереження Національного архівного фонду є неприпустимим.

Другий вектор вразливостей пов'язаний із мережевою архітектурою. Як було встановлено, близько 40 комп'ютерів установи та сервери зберігання об'єднані в єдину загальну мережу без сегментації а саме відсутність VLAN. Така топологія створює ідеальне середовище для поширення шкідливого програмного забезпечення, зокрема вірусів-шифрувальників.

Оскільки NAS-сервер знаходиться в одному домені з комп'ютерами читального залу та робочими станціями загального користування, будь-яка успішна атака на кінцевий пристрій наприклад, через відкриття шкідливого вкладення в електронній пошті створює пряму загрозу для архіву. Шифрувальник може просканувати локальну мережу, знайти відкриті мережеві папки на NAS і зашифрувати терабайти еталонних копій у форматі TIFF.

За відсутності ізольованих офлайн-копій - тобто жорстких дисків або стрічкових накопичувачів, які фізично відключені від мережі та струму - ліквідувати наслідки такої атаки буде неможливо. Кіберзахист периметра маршрутизатор MikroTik та Cisco Umbrella, знижує ймовірність проникнення вірусу ззовні, але не захищає дані від внутрішніх загроз або інфікованих USB-носіїв, які можуть бути підключені до робочих станцій безпосередньо в будівлі архіву.

Додатковою вразливістю організаційно-технічного характеру є концентрація повноважень з управління даними. Через відсутність служби Active

Directory доступ до сховища має виключно адміністратор. З одного боку, це мінімізує ризик випадкового видалення файлів некваліфікованим персоналом. З іншого боку, це створює класичну “єдину точку відмови” у бізнес-процесах.

Якщо єдиний адміністратор буде недоступний через хворобу, відпустку тощо, процеси завантаження нових оцифрованих справ або надання доступу до “важких” архівів повністю зупиняються. Крім того, адміністратор отримує на свою електронну пошту звіти від системи моніторингу Synology щодо стану здоров'я дисків - S.M.A.R.T..[38] Якщо ця пошта не інтегрована в загальну систему сповіщень, реакція на деградацію дискової підсистеми залежить виключно від уважності однієї людини.

Для систематизації виявлених загроз розроблено матрицю вразливостей IT-інфраструктури ДАРО (таблиця 2.4).

Вектор загрози	Опис вразливості	Ймовірність	Наслідки для цифрового фонду
Апаратний збій	Вихід з ладу 2-х і більше дисків у масиві RAID 5 наприклад, під час процесу відновлення.	Середня	Катастрофічні. Повна втрата логічного тому на 3 ТБ без можливості відновлення через відсутність бекапів.
Кібернетичний	Проникнення вірусу-шифрувальника через “плоску мережу” з інфікованого АРМ на NAS-сервер.	Висока	Катастрофічні. Шифрування всіх файлів на NAS. Неможливість відновлення через відсутність ізольованих офлайн-копій.
Організаційний	Випадкове видалення масиву файлів адміністратором.	Низька	Тяжкі. Втрата частини фонду, необхідність повторного тривалого

			оцифрування паперових оригіналів.
Інфраструктурний	Фізичне знищення серверної кімнати пожежа, затоплення.	Низька	Катастрофічні. Знищення всього IT-обладнання. Відсутність offsite-копій хмарних або в іншому корпусі, унеможливлює відновлення.
Операційний	Вичерпання ліміту 500 ГБ на зовнішньому вебсервері.	100% Стан, що настав	Помірні. Блокування процесів публікації нових матеріалів, зупинка інформаційного обміну з користувачами.

Таблиця 2.4 - Матриця ідентифікованих вразливостей системи зберігання даних ДАРО

Проведений аудит засвідчив, що поточна IT-інфраструктура Державного архіву Рівненської області перебуває у стані високого ризику. Архітектура мережі відсутність VLAN та Active Directory не відповідає сучасним вимогам безпеки. Обладнання для зберігання даних NAS Synology, хоча і є надійним рішенням базового рівня, налаштоване без урахування правила 3-2-1. Відсутність автоматизованих резервних копій та зовнішніх офлайн/хмарних архівів робить цифрові фонди установи вкрай вразливими до апаратних збоїв (випадок втраченого диска на 2 ТБ). Виявлені недоліки формують технічне завдання для розробки проєкту комплексної модернізації системи зберігання даних, який буде представлено у третьому розділі роботи.

ВИСНОВКИ ДО РОЗДІЛУ 2

Аналіз мережевої топології установи виявив низку критичних архітектурних недоліків. Ключовою проблемою є використання несегментованої “плоскої мережі” у поєднанні з повною відсутністю єдиної служби каталогів (Active Directory). Така організація перетворює внутрішню мережу на вразливе середовище для безперешкодного поширення шкідливого програмного

забезпечення та призводить до організаційної деградації: управління доступом монополізовано, а системний адміністратор виступає єдиною ланкою взаємодії персоналу із цифровим фондом, що суттєво уповільнює бізнес-процеси архіву.

Дослідження підсистеми зберігання даних підтвердило, що існуючі серверні потужності функціонують на межі своїх можливостей. Наявні логічні масиви (RAID 5 на 3 ТБ та RAID 1 на 10 ТБ) використовуються нераціонально через значну частку ручної праці при конвертації еталонних зображень у формати для доступу. Організація основного сховища “Цифрового НАФ” на базі технології дзеркалювання, попри високу відмовостійкість, призводить до втрати половини корисного дискового простору на надлишковість, що за умов відсутності автоматизації лише загострює проблему дефіциту місткості. Крім того, жорсткий ліміт у 500 ГБ дискового простору на зовнішньому вебсервері виступає штучним бар'єром, який фізично блокує можливість інтенсивної публікації архівних матеріалів. Зазначені фактори перетворюють дорогі мережеві сховища (NAS) на прості накопичувачі, що не забезпечують повноцінної автоматизації життєвого циклу цифрових документів.

Найбільш критичною вразливістю ІТ-моделі ДАРО є фактичне ігнорування міжнародної стратегії резервного копіювання 3-2-1. Національний архівний фонд зберігається в єдиному екземплярі на робочих масивах серверів Synology. В умовах відсутності ізольованих офлайн-копій або віддаленого хмарного дублювання це створює максимальний ризик безповоротної втрати терабайтів оцифрованих справ у разі множинного апаратного збою або проникнення в мережу вірусу-шифрувальника. Покладання виключно на технологію RAID як на засіб захисту даних є методичною помилкою, що підтверджується минулими інцидентами з поломкою жорстких дисків.

Підсумовуючи вищезазначене, поточна ІТ-інфраструктура Державного архіву Рівненської області досягла межі свого масштабування і потребує негайної комплексної модернізації. Виявлені вразливості, архітектурні обмеження та операційні неефективності є беззаперечним обґрунтуванням для розробки та

впровадження проєкту оптимізації, який базуватиметься на логічній сегментації мережі, впровадженні рольової моделі доступу, автоматизації обробки копій та побудові відмовостійкої системи резервного копіювання.

РОЗДІЛ 3. ПРОЕКТ МОДЕРНІЗАЦІЇ СИСТЕМИ РЕЗЕРВНОГО КОПІЮВАННЯ, ПІДВИЩЕННЯ НАДІЙНОСТІ ІТ-ІНФРАСТРУКТУРИ ТА ОРГАНІЗАЦІЙНО-НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ

3.1. Розробка нової архітектури резервного копіювання: впровадження стратегії 3-2-1 та автоматизація процесів

На основі результатів аудиту ІТ-інфраструктури Державного архіву Рівненської області, першочерговим завданням модернізації є усунення критичної вразливості - відсутності повноцінних резервних копій цифрового фонду. Метою даного підрозділу є проєктування архітектури зберігання, яка повністю відповідатиме міжнародному стандарту 3-2-1, мінімізує вплив людського фактора та вирішить проблему ручної обробки файлів.

Існуюча конфігурація, за якої єдиними носіями інформації виступають масиви RAID 5 та RAID 1 на NAS-серверах Synology, повинна бути трансформована у комплексну відмовостійку систему. Оскільки закупівля принципово нових серверних стійок в умовах бюджетних обмежень державної установи може бути ускладненою, пропонується максимально ефективно використати наявне обладнання за допомогою його цільової модернізації та використання вбудованого програмного забезпечення Synology.

Для вирішення проблеми неефективного використання дискового простору поточного масиву RAID 1 та усунення критичних вразливостей RAID 5 під час відновлення, проєктом модернізації передбачається реорганізація дискової підсистеми головного NAS-сервера ДАРО. Пропонується здійснити перехід до архітектури масиву RAID 6 (чередування блоків із подвійною розподіленою парністю) шляхом доукомплектування існуючого мережевого сховища двома додатковими жорсткими дисками корпоративного класу Enterprise HDD.

Вибір рівня RAID 6 є оптимальним та економічно обґрунтованим рішенням для архівних установ із високими вимогами до цілісності даних. Математична модель подвійної парності вимагає наявності щонайменше чотирьох накопичувачів, що досягається запропонованою модернізацією [39]. На відміну від RAID 1, який нераціонально резервує 50% загальної ємності під просте "дзеркало", та RAID 5, який є вразливим до каскадних збоїв, масив RAID 6 здатний витримати одночасний або послідовний вихід з ладу будь-яких двох жорстких дисків без жодної втрати доступу до цифрових копій Національного архівного фонду (таблиця 3.1).

Критерій порівняння	Поточна архітектура (RAID 1)	Запропонована архітектура (RAID 6)
Мінімальна кількість дисків	2 жорсткі диски	4 жорсткі диски
Принцип відмовостійкості	Повне дзеркалювання даних	Чередування блоків із подвійною розподіленою парністю
Рівень апаратного захисту	Допускає вихід з ладу лише 1 диска	Допускає одночасний вихід з ладу будь-яких 2 дисків
Корисний об'єм сховища	Рівно 50% від загальної ємності носіїв	Вища ефективність: мінус ємність 2 дисків
Швидкість зчитування даних	Висока (читання з двох дисків одночасно)	Надвисока (паралельне зчитування з усіх дисків масиву)
Ризик каскадної поломки при відновленні	Низький (просте поблокове копіювання)	Повністю нівельований (система захищена другою лінією парності)

Таблиця 3.1 Порівняльний аналіз архітектур дискових масивів RAID 1 та RAID 6

Така архітектура гарантує найвищий рівень апаратної відмовостійкості. Навіть у разі критичної ситуації, коли під час тривалого процесу відновлення після заміни першого пошкодженого накопичувача вийде з ладу другий зношений диск, система збереже свою працездатність, а еталонні файли TIFF залишаться неушкодженими.

Перехід на RAID 6 закладає надійний апаратний фундамент для подальшої безпечної реалізації стратегії резервного копіювання 3-2-1. Для виконання вимог “3” (три копії) та “2” (два різні носії) пропонується наступний алгоритм:

1. Первинні дані (Копія 1): Розміщуються на оновленому масиві NAS (RAID 6 для “Цифрового НАФ”, який забезпечує високу швидкість зчитування даних та максимальний апаратний захист).
2. Локальний бекап (Копія 2): Реалізується шляхом підключення до NAS-сервера зовнішнього жорсткого диска корпоративного класу Enterprise HDD великого обсягу (наприклад, 14-16 ТБ) через високошвидкісний інтерфейс USB 3.0 або eSATA.

За допомогою утиліти Synology Hyper Backup налаштовується автоматичне щоденне створення інкрементних резервних копій у неробочий час (наприклад, о 02:00 ночі). Інкрементне копіювання означає, що система не буде щоразу копіювати всі 10 ТБ даних що перевантажило б мережу та диски, а записуватиме на зовнішній носій лише ті нові скан-копії, які співробітники сектору оцифрування створили за минулу добу.[41]

Для захисту від програм-шифрувальників, цей зовнішній накопичувач налаштовується в режимі (Cold Storage) холодне сховище. У розширеному варіанті адміністратор налаштовує автоматичне логічне відмонтування USB-диска одразу після завершення процесу бекапу. Таким чином, більшу частину доби диск фізично підключений до сервера, але логічно недоступний для операційної системи та будь-яких вірусів.

Реалізація такого підходу повністю вирішує проблему апаратної ізоляції та гарантує установі наявність надійної локальної резервної копії. Однак для повноцінної імплементації стратегії 3-2-1 інфраструктура архіву потребує виконання останнього, критично важливого правила - створення територіально віддаленої копії. Організація цього фінального рубежу захисту, здатного

врятувати цифрові копії Національного архівного фонду навіть у разі надзвичайних ситуацій чи фізичного знищення серверної кімнати ДАРО, реалізується через налаштування автоматичної зашифрованої реплікації даних у хмарне сховище, що є наступним етапом запропонованої модернізації.

Створення віддаленого рівня захисту створення “Копії 3” у хмарі буде також виконуватись через Hyper Backup, але з вибором S3-сумісного хмарного сховища як цільового сервера (Amazon S3 Glacier, Backblaze B2). Критично важливою вимогою на цьому етапі є активація функції Client-Side Encryption (шифрування на стороні клієнта). Дані шифруються за алгоритмом AES-256 та розбиваються на блоки ще процесором NAS-сервера, до того як вони потраплять у маршрутизатор MikroTik та будуть передані через мережу провайдера. [41][45][46]

Впровадження такого багаторівневого підходу формує повністю замкнений контур інформаційної безпеки установи. Синтез апаратної відмовостійкості на рівні RAID 6, автоматизованого локального резервування та зашифрованої хмарної реплікації гарантує стовідсоткове збереження оцифрованих документів. Запропонована архітектура не лише ліквідує критичні вразливості системи, але й перетворює IT-інфраструктуру архіву на сучасне, масштабоване середовище, що повністю відповідає найсуворішим міжнародним стандартам та гарантує безперервність роботи Державного архіву Рівненської області за будь-яких умов.

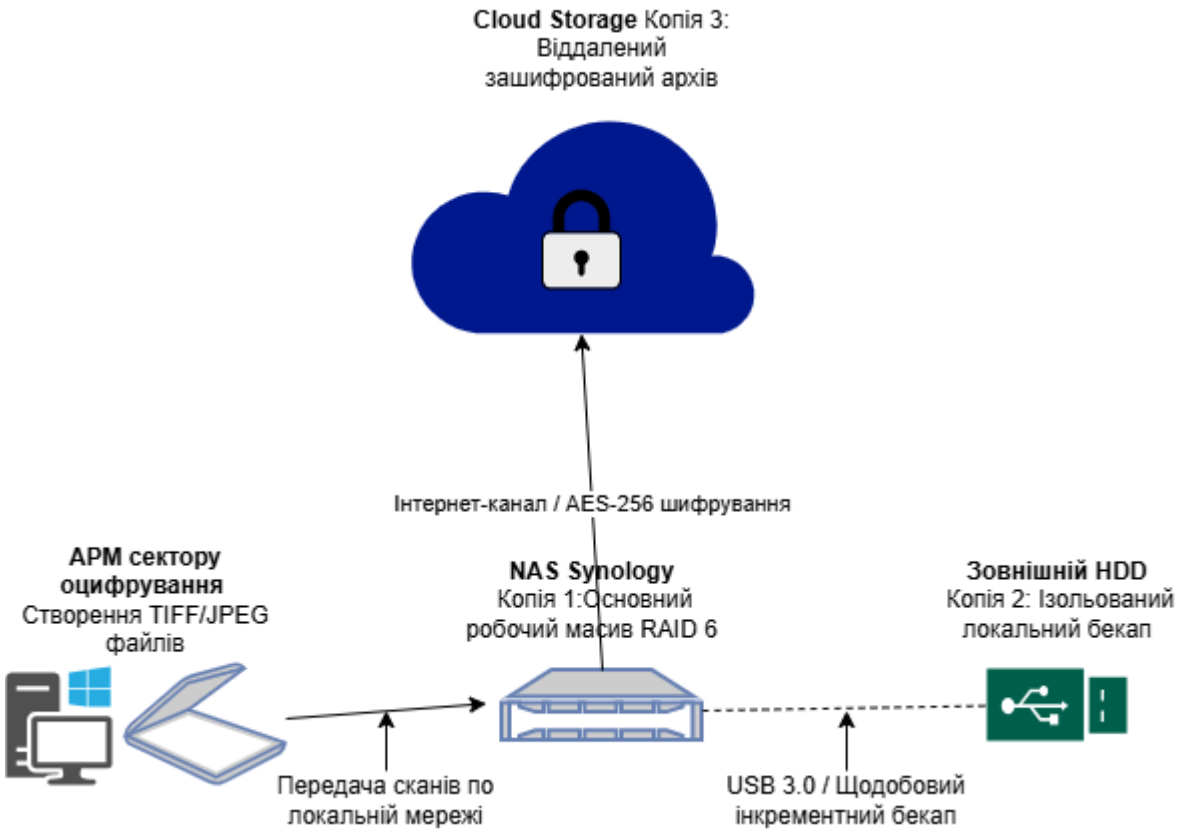

Рис. 3.1. Запропонована архітектура резервного копіювання за правилом 3-2-1 для ДАРО

Окрім модернізації “заліза”, інфраструктурний проєкт має вирішувати операційні “болі” працівників. Оптимізація рутинних процесів оцифрування має базуватися на міжнародних стандартах, зокрема на еталонній моделі Відкритої архівної інформаційної системи “OAIS - ISO 14721”, із застосуванням вбудованих функцій спеціалізованих програмних комплексів.

Відповідно до методології OAIS, для вирішення проблеми нераціонального використання дискового простору та марнування робочого часу персоналу на ручну конвертацію файлів, запропоновано структурувати життєвий цикл цифрового документа в ДАРО шляхом створення трьох типів інформаційних пакетів:

1. Інформаційний пакет передавання (SIP): Первинні, нестиснені зображення у форматі TIFF, які безпосередньо генеруються сканером на автоматизованому робочому місці працівника.

2. Архівний інформаційний пакет (AIP): Еталонні копії (TIFF), які переміщуються на захищений масив NAS-сервера для довгострокового зберігання та підлягають обов'язковому резервному копіюванню. Ці пакети ізолюються від публічного доступу.

3. Інформаційний пакет розповсюдження (DIP): Оптимізовані, зшиті багатосторінкові файли у форматі PDF/A, призначені виключно для публікації на зовнішньому вебсервері та видачі користувачам читального залу.[47]

Головним недоліком існуючих бізнес-процесів архіву є ручне створення пакетів розповсюдження DIP, що є ресурсомістким завданням. Для повної автоматизації цього етапу пропонується використання утиліти ABBYY Hot Folder, яка входить до складу ліцензійного пакета ABBYY FineReader Corporate і спеціально розроблена для потокової "пакетної" обробки документів за розкладом.[40]

Цей інструмент дозволяє налаштувати автономну роботу комп'ютера, який буде самостійно перевіряти визначену директорію, розпізнавати текст та конвертувати графічні файли в архівний формат PDF/A без участі людини.

Алгоритм налаштування автоматизованого конвеєра в ABBYY Hot Folder:

1. Створення мережевих директорій: На NAS-сервері або локальному ПК завідувача сектору створюються дві папки: вхідна (Для_Конвертації) та вихідна (Готові_PDF_Для_Сайту).

2. Налаштування планувальника завдань: В інтерфейсі ABBYY Hot Folder створюється нове завдання. У блоці планування встановлюється параметр *(Повторювати запуск)* із визначеним інтервалом (наприклад, щодня о 18:00,

після завершення сканування поточних справ, щоб обчислювальний процес не заважав роботі персоналу).

3. Налаштування параметрів обробки (OCR та Оптимізація): Задається алгоритм зниження роздільної здатності графічних файлів до 150 DPI (оптимально для веб-публікацій та економії 500 ГБ ліміту на сайті) також Вмикається функція фонового розпізнавання тексту (Optical Character Recognition - OCR) українською та російською мовами (залежно від історичного періоду фонду). Це дозволить дослідникам здійснювати повнотекстовий пошук безпосередньо у завантаженому PDF-файлі.

4. Формування фінального документа: У параметрах збереження обирається формат збереження PDF/A (міжнародний ISO-стандарт для довгострокового архівування електронних документів) та встановлюється опція зшивання всіх виявлених сторінок однієї справи в єдиний багатосторінковий документ. Впровадження такого регламенту кардинально змінює логіку роботи сектору оцифрування (таблиця 3.2).

Етап процесу	Поточна ручна модель ДАРО	Запропонована автоматизована модель
Відбір та сортування зображень	Виконується співробітником вручну (10–15 хв на 1 справу)	Співробітник просто зберігає відскановані файли у “Гарячу папку” (1 хв)
Стиснення та оптимізація розміру	Виконується вручну через сторонні графічні редактори	Виконується програмою автоматично за розкладом
Розпізнавання тексту (OCR) та конвертація	Ручне “склеювання” сторінок без розпізнавання тексту (10–20 хв)	Програма зшиває файли та додає текстовий шар без участі людини
Загальні витрати часу працівника на 1 справу	~ 25–35 хвилин активної роботи	~ 1–2 хвилини активної роботи (решта - машинний час у фоновому режимі)

Таблиця 3.2 - Оцінка ефективності автоматизації підготовки інформаційних пакетів

Як демонструють наведені дані, перехід від ручного адміністрування до автоматизованої пакетної обробки дозволяє ліквідувати операційне “вузьке місце” та вивільнити значний обсяг робочого часу працівників. Замість механічного зшивання файлів, персонал сектору оцифрування може повністю сфокусуватися на своїй базовій задачі - збільшенні темпів переведення паперових історичних справ у цифровий формат. Водночас централізоване стиснення файлів та їх стандартизація у формат PDF/A з текстовим шаром OCR вирішує критичну проблему дефіциту простору на зовнішньому вебсервері та забезпечує повну відповідність кінцевого продукту вимогам міжнародної еталонної моделі OAIS. Таким чином, архів отримує сучасний конвеєр публікації документів без залучення додаткових IT-спеціалістів та втручання у серверну архітектуру.

3.2. Налаштування програмно-апаратного комплексу та впровадження заходів мережевої безпеки

Забезпечення відмовостійкості дискової підсистеми та впровадження надійної стратегії резервного копіювання, розглянуті у попередньому підрозділі, вирішують проблему збереження даних на апаратному рівні. Однак повноцінний захист цифрового фонду архіву неможливий без побудови безпечного мережевого периметра та жорсткого контролю доступу. Навіть найнадійніший масив RAID 6 залишається вразливим, якщо зловмисник або вірус-шифрувальник отримує безперешкодний прямий доступ до нього через локальну мережу установи.

Як було визначено у підрозділі 2.1, поточна топологія “плоскої мережі”, де до 40 комп'ютерів та сервери архіву знаходяться в одному широкомовному домені, є неприпустимою з точки зору кібербезпеки. Для ізоляції критичних активів установи пропонується впровадити технологію віртуальних локальних мереж VLAN на базі існуючого ядра мережі - маршрутизатора MikroTik RouterOS. [42]

Проєкт сегментації передбачає поділ існуючої фізичної інфраструктури на три логічно ізольовані підмережі (таблиця 3.3).

VLAN ID	Назва підмережі	Цільове обладнання	Політика маршрутизації
VLAN 10	MGMT_SERVERS	NAS Synology, інтерфейси управління мережевим обладнанням	Доступ ззовні повністю заборонено. Доступ дозволено лише для IP-адрес адміністратора та сканерів із VLAN 20
VLAN 20	DIGITAL_SECTOR	АРМ сектору оцифрування, мережеві сканери	Мають доступ до VLAN 10 для збереження нових цифрових копій. Обмежений доступ до Інтернету
VLAN 30	GENERAL_STAFF	ПК читального залу, адміністративний персонал	Не мають прямого доступу до VLAN 10. Зв'язок із серверами здійснюється виключно через надання адміністратором тимчасових посилань або через веб-інтерфейс.

Таблиця 3.3 - Проєкт сегментації локальної мережі ДАРО

Реалізація даної моделі на MikroTik виконується шляхом створення віртуальних інтерфейсів на мості (Bridge) та налаштування списків контролю доступу (Access Control Lists - ACL) у розділі IP - Firewall - Filter Rules. [42]

Головним правилом Firewall є дія Drop (відкинути) для будь-якого трафіку, що ініціюється з VLAN 30 у напрямку VLAN 10. Це означає, що навіть якщо комп'ютер у читальному залі буде інфікований вірусом або якщо сторонній користувач спробує просканувати мережу, його пакети будуть знищені маршрутизатором на рівні шлюзу. Переміщення загрози до архівних фондів стає неможливим.

З точки зору управління інформаційними ресурсами, критичним завданням є оптимізація бізнес-процесів оцифрування та вирішення проблеми монополізованого доступу до цифрових фондів, що була виявлена під час аудиту. Оскільки в локальній мережі ДАРО наразі відсутня служба каталогів Active Directory, а весь масив даних контролюється виключно системним адміністратором, пропонується реалізувати Рольову модель контролю доступу (Role-Based Access Control - RBAC) базовими засобами операційної системи Synology DSM.[42]

Цей підхід дозволить делегувати повноваження щодо роботи з цифровими копіями безпосередньо відповідальним працівникам архіву, мінімізуючи ризики випадкового видалення еталонних фондів, які зберігаються на масиві “Цифровий НАФ”. Для цього на мережевому сховищі створюється ієрархія логічних груп користувачів із жорстко регламентованими правами (таблиця 3.4).

Назва групи	Цільова аудиторія	Мережева директорія	Права доступу
Digitization_Staff	Завідувач та працівники сектору оцифрування	\Digitized_New Нові надходження	Право створювати та завантажувати нові скан-копії.
Archive_Reference	Працівники читального залу та столу довідок	\Digital_Fund_PDF Фонд користування	Дозвіл на перегляд та копіювання файлів для видачі дослідникам. Заборона на видалення чи зміну файлів.
Admins	Системний адміністратор	Усі директорії, \Master_TIFF Страховий фонд	Повний контроль, право на налаштування бекапів, відновлення з копій та архівацію фондів.

Таблиця 3.4 - Запропонована рольова модель доступу до цифрових фондів ДАРО

Завдяки впровадженню такої моделі ліквідується “вузьке місце” в особі адміністратора. Працівники сектору оцифрування отримують можливість самостійно зберігати результати своєї роботи на надійний масив NAS, а працівники читального залу - миттєвий доступ до робочих копій без очікування.

Слід зауважити що, надання прямого доступу співробітникам до мережевих папок вимагає впровадження жорстких правил інформаційного аудиту та єдиної політики найменування файлів. Зростання обсягів цифрового фонду призводить до того, що без уніфікованої структури пошук необхідної справи на сховищі обсягом 10 ТБ стає вкрай неефективним.

Для вирішення цієї проблеми пропонується перехід на стандартизовану модель найменування цифрових об'єктів. Кожен файл еталонної копії повинен

мати назву, що чітко ідентифікує його місце в архівній ієрархії: Фонд_Опис_Справа_Сторінка.розширення.

Приклад застосування: F-22_Op-1_Spr-15_001.tiff

Така уніфікація не лише пришвидшує роботу пошукових алгоритмів NAS-сервера, але й унеможливлює виникнення дублікатів файлів під час їх перенесення між підрозділами.

Одночасно з наданням рольового доступу, для забезпечення інформаційної безпеки на мережевому сховищі в обов'язковому порядку активується функція журналювання передачі даних або SMB Transfer Log.[44] Цей інструмент працює у фоновому режимі та фіксує кожну дію користувачів із цифровими фондами.

Завдяки журналам аудиту адміністратор системи має змогу:

1. Точно ідентифікувати, який саме користувач “АРМ” створив, перемістив або спробував видалити архівний документ;
2. Фіксувати точний час доступу до конфіденційних справ;
3. Оперативно виявляти аномальну активність наприклад, масове перейменування файлів, що є першою ознакою дії вірусу-шифрувальника.

Запропонований комплекс організаційно-управлінських заходів гарантує цілісність Національного архівного фонду на програмному рівні. Делегування прав доступу в поєднанні з жорсткою політикою найменування та безперервним аудитом дій користувачів перетворює розрізнені масиви даних на структуровану, захищену та керовану відкриту архівну інформаційну систему.

3.3. Економічне та ресурсне обґрунтування проєкту модернізації IT-інфраструктури ДАРО

Завершальним етапом розробки проєкту модернізації системи зберігання та резервного копіювання цифрового фонду Державного архіву Рівненської області є оцінка його доцільності з точки зору фінансових та ресурсних витрат. Оскільки державні архівні установи функціонують в умовах жорсткого бюджетного фінансування, запропоновані рішення мають бути не лише технічно ефективними, але й економічно виправданими. Запропонована у підрозділі 3.1 комплексна архітектура міграція на RAID 6 та стратегія 3-2-1 базується на максимальному використанні вже наявного в установі обладнання - NAS-сервера Synology та маршрутизатора MikroTik, що дозволяє уникнути масштабних капітальних інвестицій у принципово нові серверні платформи. Витратна частина проєкту складається з двох компонентів:

1. Капітальні витрати - одноразові інвестиції: Включають закупівлю загалом трьох жорстких дисків корпоративного класу Enterprise HDD обсягом 12-16 ТБ. З них два диски необхідні для переведення основного сховища на відмовостійку архітектуру RAID 6, а один зовнішній диск - для реалізації локального холодного бекапу. Орієнтовна ринкова вартість одного такого носія наприклад, лінійки WD Gold або Seagate Exos становить близько 25 000 грн. Відповідно, загальний обсяг капітальних інвестицій складе близько 75 000 грн.[48]

2. Операційні витрати - щомісячні платежі: Оренда об'єктного хмарного сховища класу S3 для зберігання віддаленої копії 3. Використання рішень типу Cold Storage наприклад, Amazon S3 Glacier або Backblaze B2 є найбільш бюджетним варіантом для архівних даних. Середня вартість зберігання становить близько $5-6 за 1 Терабайт на місяць. Відповідно, резервування найбільш критичної частини фонду обсягом 3 ТБ обійдеться архіву приблизно у $15-18 тобто близько 600-750 грн на місяць.[49]

Додаткові витрати на програмне забезпечення відсутні, оскільки функціонал Synology Hyper Backup а також операційна система MikroTik RouterOS розповсюджуються за ліцензіями, які вже включені у вартість раніше придбаного обладнання. Для обґрунтування доцільності витрат близько 75 000 грн одноразово та 750 грн щомісяця необхідно порівняти їх із потенційними збитками у разі настання критичного інциденту - апаратної поломки старих небезпечних масивів або успішної атаки вірусу-шифрувальника, що були змодельовані у другому розділі.

У комерційному секторі втрата даних оцінюється через прямі фінансові збитки - зупинка продажів, штрафи. У державній архівній справі прямий фінансовий збиток розрахувати складніше, проте можна обчислити вартість відновлення повторного оцифрування втраченого фонду.

Згідно з орієнтовними розрахунками, втрата масиву обсягом лише 3 ТБ означає знищення результатів праці завідувача сектору та операторів оцифрування за період від 8 до 12 місяців щоденної роботи. Відповідно, держава зазнає непрямих збитків у розмірі річного фонду заробітної плати цих співробітників, а також зазнає супутніх втрат - амортизація сканерів, витрати на електроенергію, оскільки працівники будуть змушені виконувати ту саму роботу вдруге. Більше того, деякі згасаючі паперові документи можуть не пережити повторного циклу розшивання та сканування, що призведе до втрати історичної інформації назавжди.

Окрім прямого захисту даних, реалізація проєкту забезпечує суттєвий управлінський ефект:

1. Вивільнення робочого часу: Впровадження рольової моделі доступу RBAC та алгоритмів пакетної обробки скорочує час на супровідні IT-операції конвертація PDF, ручне перенесення файлів на 25-30%. Цей ресурс трансформується у збільшення кількості оцифрованих справ за місяць.

2. Нівелювання проблеми ліміту вебсервера: Автоматичне стиснення PDF-файлів збільшує ефективну місткість орендованих 500 ГБ на 15-20%, відтерміновуючи необхідність запитів до профільного міністерства щодо розширення лімітів фінансування послуг дата-центру.

3. Управлінська стійкість: Ліквідація “єдиної точки відмови” в особі системного адміністратора робить роботу сектору оцифрування та читального залу автономною і безперервною.

Запропонований проєкт модернізації є економічно збалансованим. Витрати на придбання зовнішнього носія та оренду хмарного сховища є мізерними у порівнянні з ресурсними, фінансовими та репутаційними втратами установи у випадку руйнування цифрового Національного архівного фонду. Впровадження стратегії 3-2-1, сегментація мережі та оптимізація бізнес-процесів за допомогою рольової моделі дозволяють вивести інфраструктуру Державного архіву Рівненської області на рівень, що відповідає сучасним міжнародним стандартам інформаційної безпеки.

Технічна модернізація інфраструктури Державного архіву Рівненської області, зокрема налаштування стратегії 3-2-1 та рольової моделі доступу, вимагає закріплення нових бізнес-процесів у внутрішніх розпорядчих документах установи.

Відсутність задокументованих інструкцій породжує хаос в управлінні інформаційними ресурсами, розмиває відповідальність співробітників та призводить до помилок, спричинених людським фактором. Для забезпечення безперервності роботи установи розроблено проєкт “Положення про порядок створення, зберігання та доступу до резервних копій цифрового фонду ДАРО”. Цей документ має бути затверджений наказом директора архіву та стати обов'язковим для виконання всіма співробітниками.

Нижче наведено структуру та зміст ключових розділів запропонованого нормативного документа, який адаптує технічні рішення третього розділу до управлінських реалій архівної установи.

ПРОЄКТ ПОЛОЖЕННЯ

1. Загальні положення

1.1. Це Положення визначає єдиний порядок організації збереження цифрових копій документів Національного архівного фонду “НАФ”, а також розмежування прав доступу співробітників ДАРО до мережевого сховища NAS.

1.2. Метою Положення є мінімізація ризиків втрати цифрової інформації внаслідок апаратних збоїв, кібератак зокрема впливу вірусів-шифрувальників та помилкових дій персоналу.

1.3. Система резервного копіювання архіву базується на міжнародному стандарті ISO 14721 “OAIS” та реалізує принцип 3-2-1: створення трьох копій даних на двох різних носіях із розміщенням однієї копії поза межами локальної мережі.

2. Розмежування прав та обов'язків користувачів

2.1. Доступ до файлової структури мережевого сховища здійснюється виключно на основі принципу мінімально необхідних привілеїв.

2.2. Системний адміністратор має виключне право на:

- конфігурацію масивів RAID та налаштування розкладів резервного копіювання;

- додавання нових користувачів та призначення їм дискових квот;

- відновлення інформації з резервних носіїв.

Примітка: Адміністратору забороняється вносити зміни до змісту самих архівних цифрових копій.

2.3. Завідувач та співробітники сектору оцифрування наділяються правами “Читання та Запис” виключно у межах спеціалізованих директорій “Нові надходження”. Вони несуть персональну відповідальність за коректність найменування файлів та своєчасне їх розміщення на NAS-сервері для подальшого резервування.

2.4. Співробітники читального залу та столу довідок отримують доступ до директорії “Фонд користування” виключно з правами “Тільки читання”. Будь-які спроби видалення, переміщення або модифікації файлів з їхніх робочих станцій блокуються операційною системою сховища автоматично.

3. Регламент створення резервних копій

3.1. Усі створені цифрові еталонні копії “формат TIFF” підлягають обов'язковому щоденному резервному копіюванню.

3.2. Локальне резервне копіювання “холодний бекап на зовнішній USB-накопичувач” виконується автоматизовано щодня з 02:00 до 04:00. Відповідальність за моніторинг успішності виконання скрипта покладається на системного адміністратора.

3.3. Віддалене резервне копіювання “відправка зашифрованих копій до об'єктного хмарного сховища” виконується щотижня у ніч з п'ятниці на суботу для зменшення навантаження на інтернет-канал провайдера.

3.4. Зовнішній локальний накопичувач має бути логічно відмонтований від файлової системи сервера у робочий час установи для унеможливлення його зараження мережевими вірусами.

4. Порядок дій при виникненні позаштатних ситуацій

4.1. У разі виявлення ознак апаратного збою “сигнали системи S.M.A.R.T. про деградацію одного з дисків у масиві RAID 6”, адміністратор зобов'язаний:

- негайно зупинити будь-які операції із запису нових даних на сервер;

- ініціювати позачергове зняття резервної копії на зовнішній носій;

- провести фізичну заміну пошкодженого диска та запустити процедуру перерахунку масиву.

4.2. У разі підозри на кібератаку будь-який співробітник зобов'язаний негайно відключити свій комп'ютер від живлення та повідомити адміністратора.

4.3. Адміністратор негайно ізолює мережеві сегменти та блокує доступ до мережевого сховища до повного з'ясування обставин. Відновлення зашифрованих даних здійснюється виключно з ізольованої “холодної” копії на зовнішній HDD після повної перевірки всіх АРМ на наявність шкідливого програмного забезпечення.

Розробка та формалізація внутрішнього Положення перетворює технічні інструменти NAS Synology та мережевого обладнання MikroTik на керований управлінський процес. Це дозволяє Державному архіву Рівненської області не лише відповідати вимогам надійного зберігання інформації, але й успішно проходити аудити з інформаційної безпеки від профільних державних органів, мінімізуючи ризики втрати даних через некомпетентність персоналу або відсутність чітких посадових інструкцій у сфері ІТ.

ВИСНОВОК ДО РОЗДІЛУ 3

Підсумовуючи результати третього розділу, можна констатувати, що розроблений проєкт комплексної модернізації ІТ-інфраструктури Державного архіву Рівненської області повністю вирішує виявлені під час аудиту технічні та організаційні проблеми. Запропонована стратегія дозволяє трансформувати вразливу систему ручного управління даними у сучасне, відмовостійке та автоматизоване цифрове середовище.

По-перше, вирішено проблему апаратної нестабільності та нестачі дискового простору. Шляхом доукомплектування NAS-сервера двома додатковими накопичувачами корпоративного класу обґрунтовано перехід на архітектуру RAID 6. Це рішення нівелює ризик каскадної поломки дисків та створює надійний фундамент для зберігання еталонних копій Національного архівного фонду.

По-друге, розроблено дворівневу архітектуру резервного копіювання, яка стовідсотково відповідає міжнародному стандарту 3-2-1. Впровадження локального “холодного” сховища на базі зовнішнього накопичувача та налаштування автоматичної зашифрованої реплікації у хмарне S3-сховище за допомогою Synology Hyper Backup гарантують збереження даних навіть у разі фізичного знищення серверного обладнання чи атак вірусів-шифрувальників.

По-третє, значно підвищено загальний рівень кібербезпеки установи. Запропоновано сегментацію локальної мережі за допомогою технології VLAN на базі маршрутизатора MikroTik, що ізолює сервери від користувацьких комп'ютерів. Крім того, впровадження рольової моделі доступу (RBAC) та активація журналювання подій (SMB Transfer Log) ліквідують “єдину точку відмови” в особі одного адміністратора та мінімізують ризики внутрішніх загроз.

По-четверте, оптимізовано бізнес-процеси сектору оцифрування на основі еталонної моделі OAIS. Автоматизація створення інформаційних пакетів

розповсюдження (DIP) у форматі PDF/A за допомогою утиліти ABBYY Hot Folder вивільняє колосальний обсяг робочого часу персоналу, який раніше витрачався на ручну конвертацію файлів.

Економічне обґрунтування проєкту довело його абсолютну фінансову доцільність. Одноразові капітальні інвестиції в розмірі близько 75 000 грн є економічно вигідними, оскільки вони унеможливлюють настання критичних інцидентів, ліквідація яких (повторне оцифрування втрачених 3 ТБ або 10 ТБ даних) коштувала б державі майже 600 000 грн, не враховуючи загрозу безповоротної втрати фізичних оригіналів історичних документів.

ВИСНОВКИ

У дипломній роботі вирішено актуальне науково-прикладне завдання щодо підвищення надійності збереження цифрових фондів архівних установ шляхом модернізації ІТ-інфраструктури та впровадження комплексних систем резервного копіювання. За результатами проведеного дослідження сформульовано такі основні висновки:

Досліджено теоретико-методологічні засади зберігання цифрових архівних даних. Встановлено, що експоненційне зростання обсягів оцифрованих документів вимагає переходу від стихійного накопичення файлів до структурованих моделей відкритої архівної інформаційної системи. Доведено, що використання масивів RAID забезпечує лише базову апаратну відмовостійкість, проте не захищає Національний архівний фонд від логічних збоїв, випадкового видалення чи кібератак.

Проаналізовано сучасні моделі резервного копіювання. Визначено, що еталонним архітектурним підходом для державних установ є стратегія 3-2-1 три копії, два різні типи носіїв, одна віддалена локація. Водночас для архівних фондів критично важливим є показник цільової точки відновлення, що вимагає щоденного створення інкрементних резервних копій для недопущення втрати результатів роботи сектору оцифрування.

Проведено комплексний аудит ІТ-інфраструктури Державного архіву Рівненської області. Встановлено, що поточна система зберігання базується на мережевих сховищах NAS Synology масиви на 3 ТБ та 10 ТБ. Виявлено критичні архітектурні недоліки використання “плоскої” несегментованої мережі для 40 робочих станцій, відсутність служби каталогів та монополізацію доступу до цифрових фондів з боку системного адміністратора.

Ідентифіковано вразливості та ризики втрати даних у досліджуваній установі. Аудит підтвердив фактичну відсутність повноцінних резервних копій. Дані зберігаються в єдиному екземплярі на масивах, що робить їх вразливими до

тривалих процесів перерахунку контрольних сум. Відсутність ізольованих офлайн-копій та перебування сховища в єдиному широкомовному домені з іншими ПК створює максимальний ризик безповоротної втрати терабайтів історичних даних у разі проникнення в мережу вірусу-шифрувальника , а також внаслідок апаратних збоїв.

Розроблено проєкт комплексної модернізації системи резервного копіювання ДАРО. На базі наявного обладнання спроєктовано нову архітектуру за правилом 3-2-1:

1. Копія 1 залишається на масивах NAS;
2. Копія 2 реалізується шляхом автоматизованого створення “холодного” щоденного бекапу на зовнішній накопичувач із застосуванням скриптів логічного відмонтування для захисту від кібератак;
3. Копія 3 передбачає зашифровану відправку критичних баз даних у віддалене хмарне сховище.

Впроваджено заходи з мережевої безпеки та автоматизації процесів. Для захисту від латерального переміщення загроз розроблено схему сегментації локальної мережі VLAN на маршрутизаторі MikroTik, що ізолює сервери від робочих станцій читального залу. З метою оптимізації роботи персоналу та подолання жорсткого ліміту в 500 ГБ на зовнішньому вебсервері, запропоновано використання автоматизованого скрипту який створює алгоритм автоматизованого конвеєра для автоматичного стиснення та склеювання PDF-файлів без залучення ручної праці.

Реалізовано оптимізацію управління цифровим фондом. Запропоновано перехід від монопольного контролю до Рольової моделі контролю доступу “RBAC” засобами NAS-сервера. Це дозволило делегувати права на збереження нових сканів сектору оцифрування, а права на перегляд “Фонду користування” - працівникам читального залу, усунувши управлінські перешкоди у доступі до документів.

Економічно та нормативно обґрунтовано доцільність впровадження проєкту. Розраховано, що витрати на придбання зовнішніх накопичувачів та оренду хмарного простору є неспівмірно меншими за вартість втрати результатів річної роботи архівістів. Для закріплення технічних рішень на адміністративному рівні розроблено проєкт внутрішнього нормативного документа - “Положення про порядок створення, зберігання та доступу до резервних копій цифрового фонду ДАРО”, який регламентує зони відповідальності матриця RACI та порядок дій у разі аварії.

Реалізація запропонованого комплексу програмно-апаратних та організаційно-управлінських заходів дозволить Державному архіву Рівненської області вивести ІТ-інфраструктуру на рівень, що гарантує цілісність, автентичність та довгострокове збереження цифрової спадщини нації в умовах сучасних інформаційних та кібернетичних загроз.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Закон України «Про Національний архівний фонд та архівні установи» від 24.12.1993 № 3814-XII (Редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/3814-12 (дата звернення: 21.05.2026).

2. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання: затверджено Наказом Міністерства юстиції України від 11.11.2014 № 1886/5. URL: https://zakon.rada.gov.ua/laws/show/z1421-14 (дата звернення: 21.05.2026).

3. Бездрабко В. В. Електронне документознавство: навчальний посібник. - Київ: Четверта хвиля, 2009. - 536 с.

4. ДСТУ ISO 14721:2015. Системи передавання космічних даних та інформації. Відкрита архівна інформаційна система (OAIS). Еталонна модель (ISO 14721:2012, IDT). - Київ: ДП «УкрНДНЦ», 2016. - 145 с.

5. Ковтанюк Ю. С. Створення та зберігання електронних документів у державних установах. - Київ: УНДІАСД, 2015. - 112 с.

6. Цифровий фонд користування документами Національного архівного фонду: створення, зберігання, облік та доступ до нього: методичні рекомендації / Державна архівна служба України, УНДІАСД. - Київ, 2019. - 45 с.

7. Оцифрування аудіовізуальних документів Національного архівного фонду: методичні рекомендації / Державна архівна служба України. - Київ, 2022. - 34 с.

8. What is Bit Rot? The Silent Enemy of Your Data. *DataCore Software*. URL: https://www.datacore.com/glossary/bit-rot/ (дата звернення: 22.05.2026).

9. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи: Навчальний посібник. - 5-те вид. - Київ: Діалектика, 2020. — 992 с.

10. Preston W. C. Backup & Recovery: Inexpensive Backup Solutions for Open Systems. - Sebastopol: O'Reilly Media, 2007. - 738 p.

11. Krogh P. The DAM Book: Digital Asset Management for Photography. - 2nd ed. - Sebastopol: O'Reilly Media, 2009. - 496 p.

12. Data Protection and Backup Guide / Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov/ (дата звернення: 22.05.2026).

13. ISO/IEC 27031:2011. Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity. - Geneva: ISO, 2011. - 36 p.

14. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. - Київ: ДП «УкрНДНЦ», 2016. - 28 с.

15. Synology DiskStation Manager (DSM) 7.2 White Paper / Synology Inc., 2023. URL: https://www.synology.com/ (дата звернення: 22.05.2026).

16. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури: Затверджено наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601. - Київ, 2021.

17. Patterson D. A., Gibson G., Katz R. H. A Case for Redundant Arrays of Inexpensive Disks (RAID) // ACM SIGMOD Record. - 1988. - Vol. 17, No. 3. - P. 109-116.

18. Кібербезпека державних інформаційних ресурсів: захист від програм-вимагачів (Ransomware) / Урядова команда CERT-UA. - Київ, 2023.

19. Rosenthal D. S. H., Vargas D. L. Distributed Digital Preservation in the Cloud // International Journal of Digital Curation. - 2013. - Vol. 8, No. 1. - P. 107-120.

20. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. - Київ: ДП «УкрНДНЦ», 2016. - 28 с.

21. Оліфер В. Г., Оліфер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи: Навчальний посібник. - 5-те вид. - Київ: Діалектика, 2020. - 992 с.

22. ДСТУ ISO/IEC 27033-1:2015. Інформаційні технології. Методи захисту. Безпека мереж. Частина 1. Огляд і концепції. - Київ: ДП «УкрНДНЦ», 2016. - 65 с.

23. Cisco Umbrella. Офіційна технічна документація / Cisco Systems, Inc. URL: https://umbrella.cisco.com/ (дата звернення: 28.05.2026)

24. Постанова Кабінету Міністрів України «Про затвердження Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки» від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п (дата звернення: 28.05.2026).

25. MISP - Open Source Threat Intelligence Platform. Офіційна документація проєкту. URL: https://www.misp-project.org/ (дата звернення: 23.05.2026).

26. Active Directory Domain Services Overview / Microsoft Technical Documentation. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення: 28.05.2026).

27. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. - Київ: ДП «УкрНДНЦ», 2016. - 95 с.

28. Приєднання NAS Synology до служби каталогів / Synology Knowledge Center. URL: https://kb.synology.com/uk-ua/DSM/help/DSM/AdminCenter/file_directory_service_join (дата звернення: 06.06.2026).

29. ДСТУ ISO/TR 13028:2015. Інформація та документація. Настанови щодо впровадження оцифрування документів (ISO/TR 13028:2010, IDT). - Київ: ДП «УкрНДНЦ», 2016. - 26 с.

30. Порядок створення, зберігання та доступу до цифрових копій документів Національного архівного фонду: затверджено Наказом Міністерства

юстиції України від 16.08.2023 № 2919/5. URL: https://zakon.rada.gov.ua/laws/show/z1428-23 (дата звернення: 06.06.2026).

31. ДСТУ ISO 19005-1:2015. Управління документами. Формат файлу електронного документа для довгострокового зберігання. Частина 1. Використання PDF 1.4 (PDF/A-1). - Київ: ДП «УкрНДНЦ», 2016. - 38 с.

32. ДСТУ ISO/IEC 27017:2019. Інформаційні технології. Методи захисту. Настанови щодо заходів інформаційної безпеки для хмарних послуг. - Київ: ДП «УкрНДНЦ», 2020. - 35 с.

33. Synology DiskStation Manager (DSM) Administrator's Guide / Synology Inc., 2024. URL: https://www.synology.com/uk-ua/support/download (дата звернення: 18.06.2026).

34. RAID Calculator: Storage Planning Tool / Synology Inc. URL: https://www.synology.com/en-global/support/RAID_calculator (дата звернення: 07.06.2026).

35. RAID 5 Data Recovery: Failed Rebuild & Parity Recovery / Gillware Data Recovery. URL: https://www.gillware.com/raid-data-recovery/raid-5-data-recovery/ (дата звернення: 07.06.2026).

36. How to protect your Synology NAS against ransomware? / Synology Knowledge Center. URL: https://kb.synology.com/en-global/DSM/tutorial/How_to_protect_Synology_NAS_against_ransomware (дата звернення: 15.06.2026).

37. RTO та RPO: що треба знати про резервне копіювання даних / Kyivstar Business Hub. - 2024. URL: https://hub.kyivstar.ua/articles/rto-ta-rpo-shho-treba-znati-pro-rezervne-kopiyuvannya-danih (дата звернення: 15.06.2026).

38. Як перевірити стан здоров'я диска (S.M.A.R.T.) на NAS-серверах / Synology Knowledge Center. URL: https://kb.synology.com/en-global/DSM (дата звернення: 15.06.2026).

39. Зміна типу RAID пулу зберігання / Центр знань Synology. URL: https://kb.synology.com/uk-

ua/DSM/help/DSM/StorageManager/storage_pool_change_raid_type (дата звернення: 15.06.2026).

40. Офіційний посібник користувача ABBYY FineReader: Додаток ABBYY Hot Folder для автоматизації завдань. URL: https://help.abbyy.com/uk-ua/finereader/16/user_guide/overview/ (дата звернення: 15.06.2026)

41. Налаштування резервного копіювання даних (Hyper Backup) / Synology Knowledge Center. URL: https://kb.synology.com/en-global/DSM/help/HyperBackup/data_backup_settings?version=7 (дата звернення: 15.06.2026).

42. Базові основи налаштування VLAN у RouterOS на обладнанні Mikrotik: «VLAN для чайників», сегментація мережі підприємства / Блог Lanmarket.ua. URL: https://lanmarket.ua/ua/stats/bazovye-osnovy-nastroyki-vlan-v-routeros-na-oborudovanii-mikrotik-vlan-dlya-chaynikov-segmentatsiya/ (дата звернення: 15.06.2026).

43. Керування доступом на основі ролей // Вікіпедія : вільна енциклопедія.URL:https://uk.wikipedia.org/wiki/Керування_доступом_на_основі_ролей (дата звернення: 15.06.2026).

44. Налаштування SMB: Журнал передавання / Synology Knowledge Center.URL:https://kb.synology.com/uk-ua/DSM/help/DSM/AdminCenter/file_winmacnfs_win (дата звернення: 18.06.2026).

45. Документація Amazon S3 Glacier: довгострокове та відмовостійке зберігання архівів / AWS Documentation. URL: https://docs.aws.amazon.com/s3/ (дата звернення: 15.06.2026).

46. Хмарне об'єктне сховище Backblaze B2 Cloud Storage / Backblaze Documentation. URL: https://www.backblaze.com/b2/cloud-storage.html (дата звернення: 15.06.2026).

47. ISO 14721:2012. Space Data and Information Transfer Systems - Open Archival Information System (OAIS) - Reference Model. 2012.

48. Жорсткий диск WD Gold 14 TB (WD142KRYZ) : порівняння цін та характеристик // Каталог Hotline.ua. URL: https://hotline.ua/ua/computer-zhestkie-diski/wd-gold-14-tb-wd142kryz/ (дата звернення: 15.06.2026).

49. Тарифи на зберігання даних Amazon S3 Glacier (Amazon S3 Glacier Pricing) // Amazon Web Services. URL: https://aws.amazon.com/s3/glacier/pricing/ (дата звернення: 15.06.2026).