МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. І. ВЕРНАДСЬКОГО
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

На правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА НА ЗДОБУТТЯ СТУПЕНЯ ВИЩОЇ ОСВІТИ «БАКАЛАВР»
ЕЛЕКТРОННІ АРХІВИ: СУЧАСНІ МОДЕЛІ ОРГАНІЗАЦІЇ, ДОСТУПУ ТА ЗБЕРЕЖЕННЯ

Здобувачки вищої освіти
Дзюби Аліни Сергіївни
спеціальності «Інформаційна, бібліотечна та архівна справа»
Навчально-наукового інституту муніципального управління та міського господарства

_____
(підпис)

Науковий керівник:
к.філ.н., доцент Данькевич Ю.В.

_____
(підпис)

Національна шкала добре
Кількість балів 75
Оцінка: ECTS C

Київ – 2026

АНОТАЦІЯ

Дзюба Аліна. Електронні архіви: сучасні моделі організації, доступу та збереження.

У роботі розглядаються сучасні моделі електронних архівів та доступ до них. Під час написання роботи було розглянуто теоретико-правові основи функціонування електронних архівів; проаналізовано практичні моделі організації електронних архівів, виявлено шляхи оптимізації та перспективи розвитку сучасних е-архівів.

Ключові слова: електронні архіви, штучний інтелект, блокчейн-технології, цифрове середовище, кіберзахист.

SUMMARY

Dziuba Alina. Electronic archives: modern models of organization, access and preservation.

The paper examines modern models of electronic archives and access to them. During the writing of the paper, the theoretical and legal foundations of the functioning of electronic archives were considered; practical models of organization of electronic archives were analyzed, ways of optimization and prospects for the development of modern e-archives were identified.

Keywords: electronic archives, artificial intelligence, blockchain technologies, digital environment, cyber security.

ЗМІСТ

ВСТУП

Актуальність теми дослідження зумовлена масштабною цифровою трансформацією, яка охопила всі сфери діяльності сучасної держави та бізнесу. У результаті стрімкого впровадження інформаційно-комунікаційних технологій традиційні методи архівного зберігання документів поступово втрачають свою ефективність, поступаючись місцем гнучким цифровим рішенням. Сучасне суспільство генерує колосальні обсяги інформації, значна частина якої створюється виключно в електронному вигляді, що ставить перед архіваріусами нові виклики щодо її автентичності та довготривалості. Особливої гостроти це питання набуває в Україні, де реалізація стратегії «держава у смартфоні» вимагає створення надійної національної інфраструктури для збереження цифрової спадщини [53, с.163].

Перехід на електронний документообіг на рівні державних установ та комерційних структур створює потребу в уніфікованих моделях організації е-архівів. Проблема збереження даних ускладнюється швидким застаріванням апаратного забезпечення та форматів файлів, що може призвести до явища «цифрового вимирання» інформації. Крім того, в умовах повномасштабної агресії та постійних кібератак питання кіберзахисту та створення катастрофостійких хмарних сховищ стають критично важливими для національної безпеки [25, с.123]. Доцільність розробки даної теми підтверджується необхідністю гармонізації українського законодавства з європейськими стандартами, зокрема у сфері електронної ідентифікації та довірчих послуг. Над проблемою електронного архівування працювали численні вітчизняні та зарубіжні вчені, чиї дослідження стали фундаментом для цієї роботи. Серед провідних західних інституцій слід виокремити Національне управління архівів та документації США (NARA), яке ще у 1960-х роках почало розробляти перші регламенти для машиночитаних записів [4, с.82].

Теоретичні засади цифрової доказовості та функціональні вимоги до систем управління документами досліджували фахівці Піттсбурзького університету та розробники специфікацій MoReq в Європі. Важливий внесок у розвиток теорії «континууму документів» зробили нідерландські науковці, що дозволило інтегрувати архівні процеси у ранні етапи життєвого циклу документа. Сучасна західна школа представлена глобальним дослідницьким проєктом InterPARES, який об'єднує зусилля Канади, США та ЄС у пошуках надійних цифрових репозиторіїв. Фундатором вітчизняної кібернетичної думки та ідеологом автоматизованих систем обліку був В. М. Глушков, чиї ідеї щодо Загальнодержавної системи обробки інформації випередили свій час [25, с.89].

На сучасному етапі вагому роль у розвитку галузі відіграє Центральний державний електронний архів України, фахівці якого розробляють методичні рекомендації для роботи з цифровими фондами [55]. Попри значну кількість напрацювань, недослідженими залишаються аспекти широкого впровадження штучного інтелекту для автоматизованої класифікації великих масивів неструктурованих даних. Також потребують глибшого вивчення правові та технічні механізми використання технології блокчейн для гарантування незмінності архівних записів у приватних хмарах [6]. Малодослідженим є питання забезпечення юридичної значущості документів при їхній міграції між різними юрисдикціями в умовах глобального ринку.

Теоретична значимість теми полягає у систематизації та порівняльному аналізі сучасних моделей організації е-архівів, що дозволяє виявити найбільш життєздатні стратегії для українських реалій.

Практичне значення роботи визначається можливістю впровадження розроблених рекомендацій у діяльність державних підприємств та комерційних установ для оптимізації їхніх бізнес-процесів. Вивчення стану питання показало, що Україна вже має міцну нормативну базу, закладену Законами від 2003 року, але потребує нових підходів до документів. Перспективи, які відкриває дослідження, пов'язані з можливістю створення

єдиної екосистеми цифрових архівів, інтегрованої в європейський простір даних, що забезпечить прозорий доступ громадян до інформації та підвищить рівень довіри до цифрових державних сервісів.

Метою кваліфікаційної роботи є комплексний аналіз сучасних моделей організації, доступу та збереження електронних архівів з метою обґрунтування оптимальних шляхів їх впровадження в Україні. Для досягнення цієї мети було поставлено та вирішено такі **завдання:**

- досліджено історію виникнення та еволюцію концепції електронного архівування у світі та Україні;
- проаналізовано сучасне нормативно-правове забезпечення функціонування е-архівів;
- проведено порівняльний аналіз моделей організації архівів у державному та комерційному секторах;
- вивчено перспективи технологічної модернізації е-архівів за допомогою штучного інтелекту та блокчейну;
- розроблено стратегії довготривалого збереження та міграції даних у цифровому середовищі.

Об'єктом дослідження є процес організації, забезпечення доступу та тривалого збереження документів в електронному архівному середовищі.

Предметом дослідження є сучасні моделі побудови, технологічні рішення та нормативні засади функціонування електронних архівів у державних та комерційних структурах.

Можливість розробки обраної теми підтверджується наявністю широкої емпіричної бази на матеріалах Центрального державного електронного архіву України та аналізом практичного досвіду провідних інформаційних установ. У процесі дослідження застосовано **комплекс наукових методів**, зокрема: історичний метод для відстеження еволюції носіїв інформації; системний аналіз для вивчення архітектури е-архівів як цілісних об'єктів; порівняльно-правовий метод для оцінки українського та міжнародного законодавства; метод моделювання для прогнозування розвитку галузі під впливом новітніх

технологій. Отримані результати дослідження містять обґрунтування доцільності переходу до гібридних хмарних моделей зберігання, які забезпечують баланс між безпекою та доступністю даних.

Нами доведено, що впровадження систем автоматизованої класифікації на основі нейромереж дозволяє суттєво підвищити швидкість архівного пошуку та обробки документів.

Практичне значення отриманих результатів полягає у тому, що вони можуть бути використані архівними підрозділами підприємств для розробки внутрішніх регламентів експлуатації цифрових фондів. Зокрема, рекомендації щодо конвертації форматів та управління метаданими допоможуть уникнути втрати інформації при оновленні програмного забезпечення. Результати роботи також можуть знайти застосування у навчальному процесі при підготовці фахівців зі спеціальності «Інформаційна, бібліотечна та архівна справа».

Структура роботи відповідає поставленим завданням та логіці дослідження. Повний текст складається зі вступу, трьох розділів, які поділені на підрозділи, висновків, списку використаних джерел та додатків. Список використаних джерел налічує 62 найменування, включаючи нормативно-правові акти, монографії та електронні ресурси. Додатки містять зразки форм описів електронних справ та схеми життєвого циклу цифрового документа.

Виконане дослідження є завершеною працею, що розкриває актуальні питання трансформації сучасної архівної справи в умовах глобалізації інформаційного простору. Кожен розділ роботи логічно підсумовує певний етап дослідження, формуючи цілісне уявлення про майбутнє електронних архівів.

РОЗДІЛ І. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННИХ АРХІВІВ

1.1. Історія виникнення та еволюція концепції електронного архівування

Історія електронного архівування є невід'ємною частиною загального розвитку інформаційних технологій та цифрових обчислювальних машин. Витоки цього процесу сягають середини XX століття, коли людство почало шукати альтернативу громіздким паперовим масивам. Перші кроки у створенні прототипів цифрових архівів були зроблені в 1940–1950-х роках із появою перших комп'ютерів типу ENIAC та UNIVAC. Тоді концепція «архіву» обмежувалася лише тимчасовим збереженням даних на перфокартах та перфострічках [14, с.36]. Ці носії мали вкрай низьку щільність запису та були надзвичайно вразливими до фізичних пошкоджень. Справжня революція в архівній справі розпочалася із впровадженням магнітних стрічок у 1951 році, що дозволило вперше в історії зберігати великі обсяги інформації на компактному носії, який можна було перезаписувати. Проте магнітні стрічки мали суттєвий недолік — послідовний доступ до даних, що робило пошук потрібного документа довготривалим процесом.

У 1960-х роках розвиток технологій призвів до появи магнітних дисків, що стало фундаментом для створення систем прямого доступу до інформації. Саме в цей період науковці почали замислюватися над довготривалим збереженням машиночитних записів. Важливим етапом стало усвідомлення того, що цифровий документ — це не просто набір бітів, а структура, що потребує контексту. У 1970-х роках державні установи США та Європи почали стикатися з проблемою накопичення великої кількості статистичних даних на магнітних носіях. Національні архіви почали розробляти перші регламенти щодо приймання та зберігання таких записів. Тоді ж з'явилося

поняття «машиночитний архів», яке стало попередником сучасного терміну «електронний архів» [14, с.37].

Становлення електронного архівування в країнах Заходу було зумовлене стрімкою комп'ютеризацією державного апарату та бізнесу в другій половині XX століття. Сполучені Штати Америки стали першими у цій галузі, оскільки саме там виникла критична маса машиночитних даних. Вже у 1960-х роках Національне управління архівів та документації США (NARA) зіткнулося з необхідністю збереження магнітних стрічок із даними перепису населення, що стало поштовхом до створення першого у світі спеціалізованого підрозділу для роботи з електронними записами у 1968 році [4, с.82]. Американська модель спочатку базувалася на принципі збереження «чистих даних», відокремлених від програмного забезпечення. Фахівці NARA швидко зрозуміли, що фізичне збереження носія не гарантує можливості прочитати інформацію в майбутньому. У цей же час провідні європейські країни, зокрема Велика Британія та Німеччина, почали розробляти власні стратегії цифровізації архівів. Британський досвід відрізнявся глибоким теоретичним підходом до визначення «електронного рекорду» як доказового об'єкта.

У 1970-х роках у Європі акцент змістився на створення великих наукових баз даних, що потребували архівного супроводу. Французькі архіваріуси в цей період активно працювали над концепцією «Constance» — першою системною спробою архівування державних цифрових реєстрів [4, с.83]. Разом з тим, у США тривали дискусії щодо юридичного статусу електронних документів у судових справах. Важливим кроком стало прийняття у США Закону про свободу інформації, який змусив архіви шукати шляхи швидкого доступу до цифрових даних. Європейська архівна традиція натомість більше фокусувалася на захисті персональних даних, що пізніше відобразилося у суворих директивах ЄС. У 1980-х роках американські дослідники з Піттсбурзького університету сформулювали функціональні вимоги до доказовості електронних записів, дослідження стало підґрунтям для створення перших автоматизованих систем управління документами.

Європейський Союз у 1990-х роках ініціював програму «DLM-Forum», метою якої була координація зусиль національних архівів у цифровій сфері [59]. Саме в рамках цієї ініціативи було розроблено специфікації MoReq (Model Requirements for the Management of Electronic Records). MoReq став справжнім «золотим стандартом» для розробників програмного забезпечення в Європі та за її межами. Паралельно у США активно розвивався проєкт ERA (Electronic Records Archives), спрямований на створення глобального репозиторію для всіх урядових файлів. Американський підхід завжди був більш технологічно орієнтованим та прагматичним у питаннях міграції даних. У Скандинавських країнах, зокрема у Швеції, було впроваджено стратегію «відкритості за замовчуванням», що потребувало тотальної цифровізації поточного діловодства [59].

У свою чергу, Нідерланди зробили значний внесок у розвиток теорії «континууму документів», яка заперечувала лінійний життєвий цикл файлу. Ця теорія допомогла архівам інтегруватися у процеси створення документів на ранніх етапах. На межі тисячоліть міжнародна співпраця призвела до появи стандарту ISO 15489, який уніфікував вимоги до керування записами. У США в цей період особлива увага приділялася архівам електронної пошти після гучних корпоративних скандалів. Європейські інституції, такі як Національний архів Великої Британії, зосередилися на проблемі «цифрового вимирання» через застарівання форматів. Було створено реєстр форматів PRONOM, який став світовим ресурсом для ідентифікації типів файлів.

Німеччина впровадила проєкт DOREMUS, спрямований на довготривале збереження мультимедійних архівів та складних об’єктів [59]. У 2000-х роках США розпочали масштабну програму з архівації соціальних мереж та вебсайтів державних діячів. Європейська комісія підтримала проєкт CASPAR, що вивчав збереження наукових даних за допомогою метаданих моделі OAIS. Сучасна західна модель е-архівів базується на принципах InterPARES — глобального дослідницького проекту за участю Канади, США та ЄС [59]. Сьогодні американські архіви активно експериментують із

хмарними технологіями Amazon та Microsoft для зберігання петабайтів інформації. У Європі ж робиться акцент на створенні національних цифрових платформ, інтегрованих у єдиний цифровий ринок. Швейцарські фахівці розробили систему SIARD для архівування реляційних баз даних, що стала стандартом у багатьох країнах. Таким чином, досвід США надав світу технологічні інструменти, а європейська школа — методологічну та нормативну базу [59].

Сучасний стан галузі на Заході характеризується переходом до автоматизованої класифікації даних за допомогою штучного інтелекту. Архівні установи обох континентів сьогодні працюють над створенням «trustworthy digital repositories» (надійних цифрових сховищ). Історія становлення е-архівів у цих регіонах доводить, що успішна цифровізація неможлива без синергії техніки, права та архівної науки. Цей шлях був тернистим, але він дозволив виробити механізми, які сьогодні використовує вся світова спільнота.

Паралельно з розвитком апаратного забезпечення відбувалася еволюція програмних засобів керування даними. Поява перших баз даних (СКБД) у 1980-х роках дала поштовх до структурування архівних описів у цифровому форматі. У цей час почали активно використовувати оптичні диски (CD-ROM), які вважалися ідеальним засобом для довгострокового зберігання через їхню стійкість до магнітних полів [4, с.83]. 1990-ті роки принесли із собою масове поширення персональних комп'ютерів та мережевих технологій, що докорінно змінило парадигму архівування. Концепція електронного архіву трансформувалася від ізольованого сховища до динамічної системи, доступної через локальні мережі. У той самий час Інтернет стає каталізатором розробки стандартів метаданих, адже виникала потреба в уніфікованому описі цифрових об'єктів.

Становлення електронного архівування в Україні має глибоке коріння, що сягає періоду 1960–1970-х років у межах загальнорадянської системи автоматизації. Перші кроки були пов'язані з діяльністю Інституту кібернетики

імені В. М. Глушкова, де розроблялися концепції Загальнодержавної автоматизованої системи обліку та обробки інформації (ЗДАС) [25, с.59]. У цей час архіви розглядалися переважно як інформаційні масиви для потреб планової економіки та науково-технічного прогресу. На великих підприємствах УРСР створювалися обчислювальні центри, які оперували даними на магнітних стрічках та дисках великої місткості. Проте архівування цифрових даних тоді не мало самостійного юридичного статусу, а сприймалося як допоміжний процес. Зі здобуттям незалежності Україна успадкувала потужну технічну базу, але потребувала власної нормативної рамки для цифрових документів. У 1990-х роках почалося активне впровадження персональних комп'ютерів у державні установи, що призвело до хаотичного накопичення файлів. Національний архівний фонд (НАФ) зіткнувся з викликом: як обліковувати інформацію, що існує лише в електронному вигляді [25, с.68].

Першим вагомим кроком стало прийняття у 2003 році Законів України «Про електронні документи та електронний документообіг» [35] та «Про електронний цифровий підпис» (втратив чинність). Маємо наголосити, що аналіз нормативно-правової бази буде зроблений нами у підрозділі 1.2. Ці акти де-юре зрівняли паперовий та електронний документи, що стало фундаментом для створення е-архівів. У середині 2000-х років розпочалася розробка спеціалізованого програмного забезпечення для державних архівних установ. Важливу роль відіграв Центральний державний електронний архів України (ЦДЕА), створений у 2007 році як профільна установа для зберігання цифрової спадщини [55]. ЦДЕА став методичним центром, який почав розробляти регламенти приймання електронних документів на постійне зберігання. У цей період активно впроваджувалися системи класу EDMS (Electronic Document Management Systems) у міністерствах та відомствах. Проте тривалий час існувала проблема розриву між поточним діловодством та архівним зберіганням. Багато документів роздруковувалися для «архівної копії», що нівелювало переваги цифровізації.

Ситуація почала змінюватися з 2014 року в межах загальної стратегії реформування державного управління та переходу до «держави у смартфоні». Поява Міністерства цифрової трансформації України дала потужний імпульс для створення єдиної екосистеми цифрових архівів. Проєкт «е-Архів», ініційований урядом, передбачав повний відхід від паперових дублікатів у державному секторі [29]. Важливим етапом стало впровадження системи електронної взаємодії органів виконавчої влади (СЕВ ОВВ), яка забезпечила прозорий шлях документа від створення до архіву [12]. Сучасна українська модель орієнтована на централізацію та хмарне зберігання даних у захищених дата-центрах. Особлива увага приділяється кібербезпеці, що стало критично важливим в умовах повномасштабної агресії та постійних кібератак. Сьогодні українські архіви активно інтегруються з порталом «Дія», що дозволяє громадянам отримувати архівні довідки в режимі онлайн. Розвиток технологій електронного підпису (КЕП) забезпечив юридичну значущість архівних копій на довгі роки [12].

В академічному середовищі України активно обговорюються питання впровадження міжнародних стандартів, таких як OAIS та ISO 16363. Створюються цифрові колекції аудіовізуальних документів, що потребують специфічних методів конвертації та опису. Проблемою залишається фінансування технічного оновлення регіональних архівів, які все ще мають значні обсяги несистематизованих даних. Проте Україна вже демонструє унікальні кейси «архівування війни» за допомогою волонтерських цифрових ініціатив. Впровадження штучного інтелекту для розпізнавання давніх рукописів та їх автоматичної індексації є наступним пріоритетом розвитку. На рівні комерційних підприємств спостерігається масовий перехід на хмарні рішення типу SharePoint або спеціалізовані українські розробки (наприклад, Megapolis.DocNet). Еволюція українських е-архівів пройшла шлях від ізольованих баз даних до інтегрованої національної інфраструктури [29].

У 1999 році було опубліковано проєкт моделі OAIS (Open Archival Information System), яка стала фундаментальним стандартом для всіх сучасних

е-архівів. Ця модель чітко розмежувала процеси приймання, зберігання та надання доступу до цифрової інформації. Початок XXI століття ознаменувався переходом від оцифрування паперових документів до зберігання документів, що «народилися цифровими» (born-digital) [4, с.88]. Зростання обсягів неструктурованих даних призвело до створення систем класу ECM (Enterprise Content Management). Ці системи дозволили автоматизувати життєвий цикл документа від моменту створення до знищення або передачі на постійне зберігання. Розвиток технологій віртуалізації у 2010-х роках відкрив шлях до хмарного архівування, яке ми бачимо сьогодні.

Зараз Україна претендує на роль одного з лідерів цифрової трансформації архівної справи у Східній Європі [29]. Важливою частиною стратегії є забезпечення сумісності українських цифрових архівів з європейським простором даних, що дозволить у майбутньому легко обмінюватися інформацією з міжнародними інституціями. Державна архівна служба України постійно оновлює вимоги до форматів тривалого зберігання, надаючи перевагу відкритим стандартам. Процес «депаперизації» стає невідворотним, охоплюючи навіть найбільш консервативні галузі промисловості. Таким чином, український досвід поєднує в собі радянську системність та сучасну гнучкість IT-рішень. Кожне нове покоління програмного забезпечення робить електронний архів більш доступним та надійним для користувача. Підсумовуючи, можна стверджувати, що вітчизняні е-архіви стали невід'ємною частиною цифрового суверенітету держави. Подальший розвиток галузі залежатиме від стабільності інфраструктури та оперативності оновлення законодавчої бази.

Сучасний етап еволюції характеризується відмовою від фізичних серверів на користь розподілених хмарних інфраструктур (SaaS, PaaS) [60]. Хмарні сховища забезпечують небачений раніше рівень доступності та катастрофостійкості даних завдяки реплікації. Сьогодні концепція електронного архівування включає не лише збереження файлів, а й забезпечення їхньої автентичності та цілісності протягом десятиліть. Ми

спостерігаємо перехід до «інтелектуальних архівів», де пошук здійснюється не лише за ключовими словами, а й за змістом за допомогою нейромереж. Історія е-архівів — це шлях від фізичного носія до абстрактного сервісу, де головною цінністю є інформація, а не її оболонка. Еволюція триває, і наступним кроком стане використання блокчейну для гарантування незмінності архівних записів. Отже, за півстоліття електронні архіви пройшли шлях від експериментальних систем до критично важливої інфраструктури сучасного суспільства. Кожен етап цієї еволюції був відповіддю на виклики зростаючого обсягу інформації та потреби в її швидкому опрацюванні.

1.2. Нормативно-правове забезпечення функціонування електронних архівів в Україні та світі

Формування правового поля для електронних архівів в Україні розпочалося як відповідь на виклики інформаційного суспільства на межі тисячоліть. Початковий етап характеризувався відсутністю спеціалізованого законодавства, що змушувало архівістів керуватися загальними нормами діловодства. Перші спроби нормотворення були спрямовані на визначення статусу машиночитних документів у межах класичного архівного фонду. Важливим підґрунтям став Закон України «Про Національний архівний фонд та архівні установи», який згодом зазнав суттєвих змін для адаптації до цифрових реалій [44]. Державна архівна служба України (Укрдержархів) почала розробляти перші галузеві стандарти, що регулювали порядок оцифрування паперових масивів. У середині 2000-х років виникла гостра потреба у регламентації процесів передавання електронних документів на державне зберігання. Було розроблено низку наказів Міністерства юстиції, які крок за кроком описували процедури експертизи цінності цифрових об’єктів.

Становлення бази відбувалося в умовах постійного технологічного оновлення, що вимагало від законодавця гнучкості та оперативності. Поступово акцент змістився від простого збереження файлів до забезпечення

їхньої довготривалої юридичної значущості [5, с.57]. Важливу роль у цьому процесі відіграв Центральний державний електронний архів України, який став головним майданчиком для апробації нормативних новацій [55]. Створення правового поля супроводжувалося гармонізацією вітчизняних норм із європейськими директивами у сфері цифровізації. Сьогодні ми спостерігаємо перехід до комплексної нормативної системи, яка охоплює всі етапи життєвого циклу електронного документа. Цей процес є безперервним, оскільки поява нових технологій, як-от блокчейн чи штучний інтелект, потребує нових правових трактувань [6].

Фундаментом сучасного електронного архівування в Україні є пакет базових законів, прийнятих у 2003 році. Закон «Про електронні документи та електронний документообіг» встановив основні принципи створення, відправлення та зберігання е-документів. Він чітко визначив, що юридична сила електронного документа не може бути заперечена лише через його цифрову форму. Наступним став Закон «Про електронну ідентифікацію та електронні довірчі послуги», який прийшов на зміну закону про ЕЦП у 2017 році [36]. Цей акт запровадив поняття кваліфікованого електронного підпису, що є обов'язковим для архівування офіційної документації. Важливе значення має Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затверджений наказом Мін'юсту № 1886/5 [38]. Документ детально описує процес формування електронних справ та створення описів для е-архівів.

Також необхідно виокремити Правила організації діловодства та архівного зберігання документів у державних органах, які містять окремі розділи щодо цифрових носіїв [39]. Закон України «Про захист персональних даних» накладає на електронні архіви додаткові зобов'язання щодо конфіденційності та обмеження доступу [40]. Питання кіберзахисту архівних ресурсів регулюються Законом «Про основні засади забезпечення кібербезпеки України» [48]. Нормативна база також включає ДСТУ 4144, який встановлює вимоги до структури та змісту метаданих архівних документів.

Важливим є і Постанова Кабінету Міністрів України «Про функціонування Реєстру публічних електронних реєстрів», що забезпечує їх облік на загальнодержавному рівні [50]. Сукупність цих актів створює багаторівневу систему, яка дозволяє електронному архіву функціонувати як повноцінна юридична інституція. Проте, на нашу думку, законодавство потребує подальшої деталізації в питаннях конвертації форматів та міграції даних між різними системами.

Нормативно-правове регулювання сфери електронного архівування в Україні є багаторівневою системою, що поєднує загальнодержавне законодавство, галузеві стандарти та локальні акти установ. Вихідною точкою правового регулювання є Конституція України, яка гарантує право кожного на інформацію та доступ до архівних документів. Базовим актом, що визначає загальні засади архівної справи, є Закон України «Про Національний архівний фонд та архівні установи» [44]. Закон встановлює правові відносини щодо формування, обліку та зберігання документів, незалежно від їхнього носія. Ключову роль у легітимізації цифрового сегмента архівів відіграє Закон «Про електронні документи та електронний документообіг», що запроваджує рівнозначність електронного документа паперовому за умови дотримання встановлених реквізитів [35]. Важливим елементом юридичної сили архівного документа є наявність кваліфікованого електронного підпису або печатки. Регулювання цих питань здійснюється відповідно до Закону «Про електронні довірчі послуги», який гармонізований із європейським регламентом eIDAS [36]. Це дозволяє забезпечити автентичність та цілісність документів протягом усього терміну їхнього зберігання.

На підзаконному рівні ключовим документом є Наказ Міністерства юстиції № 1886/5 «Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання». Цей Порядок є фактично «дорожньою картою» для будь-якої установи, що впроваджує е-архів [38]. Він регламентує процедуру створення електронних справ, їхнього індексування та формування описів. Окрему увагу

в нормативній базі приділено експертизі цінності електронних документів, яка має свої специфічні критерії. Відповідно до Порядку, електронні документи постійного та тривалого зберігання повинні бути представлені у форматах, що забезпечують їхнє відтворення у майбутньому [38]. Наказ № 1000/5 «Про затвердження Правил організації діловодства та архівного зберігання документів...» встановлює вимоги до технічного оснащення архівних сховищ [39]. Ці правила визначають стандарти зберігання знімних носіїв інформації та умови експлуатації серверного обладнання. Важливим аспектом є нормативне закріплення процедури конвертації та міграції даних у разі застарівання програмного забезпечення.

Питання захисту інформації в електронних архівах регулюються Законом «Про захист інформації в інформаційно-комунікаційних системах» [41]. Архівні установи зобов'язані впроваджувати комплексну систему захисту інформації (КСЗІ) для запобігання несанкціонованому доступу. Питання персональних даних, що містяться в архівних справах, підпадають під дію Закону «Про захист персональних даних» [40]. Це створює певний правовий конфлікт між принципом відкритості архівів та правом на приватність, що потребує чіткої регламентації доступу. Типові інструкції з діловодства, затверджені Кабінетом Міністрів, встановлюють уніфіковані вимоги до складання та оформлення електронних документів. Державна архівна служба України видає методичні рекомендації, які деталізують процес приймання документів на державне зберігання. Зокрема, існують окремі регламенти для роботи з аудіовізуальними та науково-технічними електронними документами. Важливу роль у системі регулювання відіграють національні стандарти України (ДСТУ) [13, с.19].

Метадані дозволяють ідентифікувати документ, підтвердити його походження та відстежити історію його використання. Без належного опису на рівні метаданих електронний документ втрачає свою архівну цінність та стає просто набором даних. Регулювання доступу до архівів також здійснюється через Закон «Про доступ до публічної інформації», що стимулює створення

онлайн-платформ [34]. Правовий режим електронних архівів на приватних підприємствах визначається їхніми внутрішніми статутами та положеннями, але не повинен суперечити загальним нормам. Важливою інновацією останніх років стала нормативна підтримка хмарних технологій для зберігання державних інформаційних ресурсів. Це дозволяє архівам використовувати потужності захищених дата-центрів замість утримання власних серверних кімнат. Законодавство також передбачає відповідальність за навмисне знищення або пошкодження електронних архівних документів [34].

Спеціалізовані накази Мін'юсту визначають переліки документів із зазначенням строків їх зберігання, що є обов'язковими для всіх форм власності. Окремо регулюється питання надання архівних довідок у цифровому форматі, що мають таку ж юридичну силу, як і виписки з паперових книг. Розвиток нормативної бази в Україні сьогодні спрямований на максимальну інтеграцію в європейський цифровий простір. Це потребує подальшої адаптації норм щодо довготривалого збереження за стандартами ISO [13, с.46]. Існує необхідність у прийнятті окремого закону про електронні архіви, який би об'єднав розрізнені норми в єдиний кодекс. Сучасні правові виклики включають також регламентацію використання штучного інтелекту в архівному пошуку. Питання авторського права на оцифровані копії документів також потребує чіткішого законодавчого визначення. Таким чином, нормативно-правове забезпечення е-архівів в Україні є динамічним процесом, що постійно вдосконалюється [13, с.47]. Вона створює необхідний юридичний фундамент для трансформації паперової пам'яті у цифрову спадщину. Кожна нова нормативна зміна наближає українську архівну систему до світових стандартів прозорості та надійності. Аналіз поточної бази свідчить про готовність держави до повної цифровізації архівного сектору. Ефективність цих норм залежить від їхньої реалізації на місцях та готовності архівістів до роботи в новому правовому полі.

Сучасний стан нормативного регулювання електронних архівів характеризується глибоким розривом між динамічним розвитком технологій

та консервативною природою права. Найбільш гострою юридичною колізією є невідповідність термінів дії кваліфікованого електронного підпису (КЕП) термінам зберігання архівних документів [36]. Зазвичай сертифікат відкритого ключа видається на один або два роки, тоді як значна частина документів має зберігатися десятиліттями або довічно. Після завершення терміну дії сертифіката перевірка автентичності документа стає юридично складною процедурою. Закон вимагає, щоб документ був цілісним та автентичним протягом усього періоду зберігання, але технології перевірки підпису застарівають швидше, ніж спливає строк зберігання справи. Це створює ситуацію «юридичного вакууму», коли документ фактично існує, але його процесуальний статус як доказу ставиться під сумнів. Проблема посилюється тим, що криптографічні алгоритми, які вважалися надійними десять років тому, сьогодні можуть бути легко зламані.

Нормативна база України поки що не містить чіткого механізму «перепідписування» документів або накладання нових часових міток без порушення первинної цілісності файлу. Крім того, виникає колізія щодо формату зберігання: закон вимагає збереження оригіналу, але оригінал у застарілому форматі (наприклад, .doc чи .xls старого зразка) може не відкритися на сучасному обладнанні [58, с.129]. Процедура конвертації документа в інший формат (наприклад, у PDF/A) з точки зору класичного архівного права може розцінюватися як створення копії, а не збереження оригіналу. Юридично не врегульовано питання, як забезпечити незмінність змісту документа під час його міграції з однієї інформаційної системи в іншу. Більшість вітчизняних нормативних актів досі орієнтовані на «статичний» документ, тоді як сучасні бази даних є динамічними об'єктами. Архівування баз даних як цілісних об'єктів потребує специфічних процедур, які наразі відсутні в інструкціях з діловодства [58, с.129].

Ще однією проблемою є правовий статус метаданих, які часто існують окремо від самого файлу документа. Якщо метадані, що підтверджують контекст створення документа, будуть втрачені або змінені, документ втрачає

свою доказову силу, навіть якщо сам файл залишився незмінним. Чинне законодавство не дає однозначної відповіді на питання, хто несе відповідальність за технічне старіння носіїв інформації в приватних архівах. Колізія також виникає у сфері доступу до персональних даних, що містяться в електронних справах. Автоматизований пошук у цифрових архівах дозволяє миттєво знаходити інформацію, яка за паперової епохи була фактично захищена «труднощами пошуку». Це вимагає розробки нових правових механізмів анонімізації даних в архівних документах перед їх наданням у публічний доступ [58, с.130].

Закон України «Про захист персональних даних» часто вступає у протиріччя з принципом всебічності формування Національного архівного фонду [40]. Юридично не визначено статус «хмарних» архівів, якщо сервери фізично знаходяться за межами юрисдикції України. Це породжує ризики втрати контролю над державною інформацією та створює загрозу національній безпеці. Існує також проблема правового регулювання видалення інформації — так званого «права на забуття» в контексті обов'язкового архівного зберігання. Якщо особа вимагає видалити дані про себе, архівіст опиняється перед вибором між порушенням закону про захист даних та порушенням закону про архіви.

Проблема ідентифікації автора документа також ускладнюється у випадках, коли підпис було накладено від імені установи автоматизованою системою без участі фізичної особи. Нормативні акти не враховують можливість архівування об'єктів, створених за допомогою штучного інтелекту, де авторство є розмитим. Юридична процедура знищення електронних документів також є недосконалою, адже просте видалення файлу не гарантує неможливості його відновлення. Виникає потреба в нормативному закріпленні стандартів «гарантованого знищення» цифрової інформації [58, с.130].

Колізії спостерігаються і в питаннях оплати послуг електронних архівів, оскільки чинні тарифи часто розраховані на аркуші паперу, а не на гігабайти

даних. Правова система не встигає регулювати статус блокчейн-реєстрів як потенційних джерел архівного зберігання. Відсутність єдиного державного стандарту на інтерфейси взаємодії між різними системами е-архівів призводить до «відомчої ізоляції» даних [6]. Це суперечить принципу єдиного інформаційного простору держави. Кожна установа трактує норми щодо безпеки даних по-своєму, що створює бар'єри для обміну інформацією. Міжнародні стандарти, такі як ISO 16363, пропонують вихід через сертифікацію надійних репозиторіїв, але в Україні ця практика ще не набула законної сили [6].

Юридична невизначеність щодо того, що вважати «первинним» у цифровому середовищі, гальмує розвиток історичної науки. Науковці потребують доступу до первинних кодів та алгоритмів, якими оброблялися дані, але право власності на софт часто належить приватним компаніям. Це створює загрозу появи «цифрових темних віків», коли ми матимемо файли, але не матимемо легальних засобів для їхнього коректного відтворення. Вирішення цих колізій потребує не лише косметичних змін до законів, а розробки принципово нової «Цифрової конституції архівів». Необхідно запровадити поняття «технологічної нейтральності» в архівному праві, щоб норми не залежали від конкретного формату чи носія [6].

Автоматизація процесів експертизи цінності за допомогою нейромереж також потребує правової легітимізації, щоб рішення ШІ мали юридичну вагу. Важливо встановити презумпцію надійності для акредитованих цифрових архівів, що спростить судовий розгляд електронних доказів. Тільки через подолання цих правових протиріч можна забезпечити стале функціонування електронних архівів у майбутньому. Кожен крок у напрямку усунення юридичних колізій підвищує рівень довіри суспільства до цифрової пам'яті. Архівісти та юристи мають працювати в синергії, щоб кожна технологічна інновація супроводжувалася відповідним правовим актом. Без подолання «законодавчого лагу» електронний архів залишатиметься вразливою

структурою. Сучасний етап розвитку вимагає від нас сміливості у перегляді застарілих догм архівної справи на користь цифрової реальності [6].

Міжнародна нормативна база є орієнтиром для розвитку національних систем електронного архівування. Центральне місце у світовій практиці посідає серія стандартів ISO, зокрема ISO 15489 «Інформація та документація. Керування записами» [27, с.34]. Цей стандарт визначає загальні принципи створення та контролю за цілісністю документів у будь-якому форматі. Модель OAIS (Open Archival Information System), закріплена стандартом ISO 14721, є концептуальною основою для побудови надійних цифрових сховищ. Вона впроваджує поняття інформаційних пакетів (SIP, AIP, DIP), що забезпечують передачу та збереження даних без втрати контексту. У Європейському Союзі ключовим регулятором є Регламент eIDAS, який забезпечує транскордонне визнання електронних підписів. Специфікації MoReq (Model Requirements for the Management of Electronic Records) широко використовуються для сертифікації програмного забезпечення е-архівів [60].

Досвід США базується на стандартах DoD 5015.2, які висувають надзвичайно суворі вимоги до безпеки та автентичності урядових записів. Міжнародна рада архівів (ICA) активно просуває стандарти опису, такі як ISAD(G), адаптовані для цифрового середовища. Стандарт ISO 19005 визначає використання формату PDF/A як найбільш придатного для довготривалого архівного зберігання. Важливим є також стандарт ISO 16363, який регламентує процедуру аудиту та сертифікації надійних цифрових репозиторіїв. У багатьох країнах діють спеціальні закони про «Цифрову спадщину», що захищають дані, які мають історичну цінність [53, с.169]. Міжнародний досвід доводить, що ефективне архівування неможливе без уніфікації форматів та процедур обміну даними. Впровадження цих стандартів в Україні є обов'язковою умовою для інтеграції у світовий інформаційний простір. Кооперація між країнами дозволяє виробляти єдині підходи до вирішення проблеми «цифрового старіння» програмного забезпечення. Таким

чином, глобальна нормативна система створює безпечне середовище для збереження пам'яті людства у цифрову епоху.

РОЗДІЛ ІІ. АНАЛІЗ ПРАКТИЧНИХ МОДЕЛЕЙ ОРГАНІЗАЦІЇ ЕЛЕКТРОННИХ АРХІВІВ

2.1. Специфіка побудови та функціонування моделей електронних архівів на державних підприємствах

Побудова моделі електронного архіву на державному підприємстві є складним процесом, що вимагає гармонізації управлінських стандартів із сучасними технологічними рішеннями. Сучасні умови функціонування державного сектору економіки України диктують подальший перехід до повноцінного цифрового циклу зберігання документів [38]. Специфіка державних підприємств полягає у їхній підпорядкованості профільним міністерствам та відомствам, що автоматично накладає вимогу до ієрархічності архівної системи. Електронний архів, за Ю. Палехою, розглядається не лише як сховище файлів, а як складна інформаційна система з високим рівнем довіри [28, с.234].

Побудова електронного архіву на державних підприємствах нерозривно пов’язана з суворим дотриманням норм Закону України «Про державну таємницю» [3]. Цей законодавчий акт визначає правові основи захисту інформації, розголошення якої може завдати шкоди національній безпеці. Для державних підприємств, що виконують оборонні замовлення або працюють у стратегічних галузях, цей закон є фундаментом усієї архівної справи. Електронний формат зберігання секретних документів накладає на суб'єктів господарювання додаткові зобов’язання щодо технічного та криптографічного захисту [3]. Закон чітко розмежовує категорії секретності: «таємно», «цілком таємно» та «особливої важливості». Кожна з цих категорій вимагає специфічного підходу до організації електронного архіваріусу та обмеження доступу [3].

Державне підприємство є власником інформації, що зобов’язаний створити умови для її абсолютної недоторканності. Відповідальність за

організацію захисту секретної інформації в архіві покладається безпосередньо на керівника підприємства. Відповідно до статті 5 Закону, державні органи та ДП здійснюють заходи щодо охорони державної таємниці у межах своїх повноважень [3]. Для реалізації цих завдань на підприємствах функціонують режимно-секретні органи (далі — РСО). Саме РСО відіграє роль «контролера доступу» до будь-якої бази даних або електронного сховища. Кожен документ, що потрапляє до електронного архіву, повинен мати відповідний цифровий гриф секретності в метаданих. Автоматизована система зобов'язана блокувати доступ до документа особам, які не мають відповідної форми допуску [3].

Технічна реалізація вимог Закону в електронному архіві базується на впровадженні Комплексної системи захисту інформації (далі — КСЗІ). КСЗІ повинна обов'язково пройти державну експертизу та отримати атестат відповідності від Держспецзв'язку [57]. Без такого атестата функціонування будь-якого електронного архіву з державними таємницями є незаконним. Закон вимагає, щоб обробка секретної інформації здійснювалася виключно в автоматизованих системах з належним рівнем захищеності. Основним викликом для ДП є забезпечення фізичної та логічної ізоляції архівної мережі від загальних каналів зв'язку. Секретний електронний архів не може бути частиною глобальної мережі або мати вихід у відкритий Інтернет. Це створює так званий «повітряний зазор», що є найнадійнішим методом запобігання кібератакам [57].

Використання знімних носіїв інформації в таких системах жорстко регламентоване та перебуває під постійним наглядом РСО. Кожен флеш-накопичувач чи жорсткий диск має бути зареєстрований у спеціальному журналі та мати інвентарний номер. Процес архівування секретних електронних документів включає їх обов'язкове криптографічне шифрування за державними стандартами. Закон передбачає використання лише тих засобів захисту, що пройшли сертифікацію в Україні [3]. Алгоритми шифрування повинні бути стійкими до методів сучасного криптоаналізу протягом усього терміну зберігання документа. У моделі електронного архіву ДП

криптографічні ключі зберігаються на захищених апаратних пристроях, таких як токени. Взаємодія з системою «АСКОД» у таємному сегменті вимагає спеціалізованих модулів для роботи з зашифрованими контейнерами [2].

Будь-яка спроба несанкціонованого копіювання файлу з архіву повинна миттєво фіксуватися системою внутрішнього аудиту. Закон також регулює питання термінів секретності, які для електронних документів зазвичай становлять 5, 10 або 30 років [3]. Модель електронного архіву повинна підтримувати регламентовану процедуру регулярного перегляду грифів секретності. Відповідно до статті 13 Закону, зміна або скасування грифа здійснюється виключно державним експертом з питань таємниць [3]. Електронна система має дозволяти автоматичне оновлення статусів документів після отримання офіційного рішення про розсекречення. При цьому повна історія зміни грифів має зберігатися у захищеному лозі для звітності перед контролюючими органами.

Важливим аспектом є захист від витоку інформації через побічні електромагнітні випромінювання та наводки. Приміщення, де розташовані сервери електронного архіву ДП, обладнуються системами екранування або активного зашумлення. Закон «Про державну таємницю» категорично забороняє передачу секретних відомостей іноземним структурам без спеціального міждержавного дозволу [3]. Це автоматично робить неможливим використання закордонних хмарних сервісів для зберігання секретних архівів. Всі дані повинні фізично розміщуватися на території України на серверах, що належать державі або підприємству. Особливу увагу в Законі приділено процедурі знищення секретних документів після завершення термінів їх зберігання [3].

Звичайне видалення файлу з диска вважається недостатнім з точки зору інформаційної безпеки. Необхідно застосовувати сертифіковані методи гарантованого знищення даних шляхом багаторазового перезапису або фізичного знищення носія. Акти про знищення електронних документів оформлюються комісією, до складу якої обов’язково входить представник

РСО [3]. Закон передбачає персональну кримінальну відповідальність працівників архіву за порушення правил поводження з таємницею. Кожен адміністратор системи підписує зобов'язання про нерозголошення, що діє навіть після його звільнення. Моніторинг дій персоналу в системі архіву здійснюється в режимі реального часу з автоматичним аналізом аномалій [3].

Взаємодія між різними ДП у питаннях обміну секретними архівними даними здійснюється через канали фельд'єгерського зв'язку. Будь-які прямі цифрові канали між архівами різних відомств створюються лише за умови побудови захищених VPN-тунелів. Закон вимагає проведення періодичних аудитів стану охорони державної таємниці фахівцями Служби безпеки України. Перевірки СБУ охоплюють як технічну цілісність системи, так і правильність ведення паперових журналів обліку електронних носіїв [3]. Електронний архів має гарантувати неможливість будь-якої модифікації змісту документа після його депонування в сховище. Використання технологій WORM (Write Once, Read Many) дозволяє забезпечити юридичну достовірність секретних фондів [62]. Кожна цифрова копія документа, що видається з архіву, повинна містити приховані водяні знаки для ідентифікації отримувача [62].

Специфіка ДП полягає також у необхідності підтримувати архівну спадкоємність під час ліквідації чи реорганізації об'єкта. Закон визначає, що в таких випадках секретний архів передається правонаступнику або до центральних державних архівних установ. Розробка програмного забезпечення для таких архівів здійснюється лише компаніями, які мають відповідну ліцензію на роботу з держтаємницею [3]. Закон стимулює впровадження біометричних методів ідентифікації для доступу до особливо важливих сегментів архіву. Доступ до серверних приміщень обмежується складними системами СКУД із обов'язковим відеопротоколюванням. Таким чином, Закон України «Про державну таємницю» формує жорстку, але необхідну рамку для цифрової трансформації державних підприємств [3].

Лише повна відповідність цим нормам дозволяє архіву ДП бути не просто сховищем, а надійним елементом системи національної безпеки.

Основним драйвером розгортання таких систем є необхідність інтеграції з наявними системами електронного документообігу, серед яких ключове місце посідає «АСКОД» [2]. Модель функціонування архіву на базі «АСКОД» передбачає автоматизацію передавання документів із оперативної стадії діловодства до довготривалого зберігання [2]. Важливою особливістю є забезпечення цілісності та автентичності електронних документів протягом усього терміну їхнього перебування в архіві. Державні підприємства змушені впроваджувати моделі, що відповідають вимогам ДСТУ та нормативним актам Державної архівної служби України [57].

Централізація є базовим принципом побудови електронних архівів для великих державних корпорацій та стратегічних підприємств. Централізована модель дозволяє уніфікувати метадані, забезпечити єдину політику безпеки та знизити витрати на ІТ-інфраструктуру. У такій архітектурі всі дочірні підрозділи або філії підприємства використовують спільне серверне середовище для депонування документів. Водночас доступ до даних розмежовується згідно з посадовими обов'язками та рівнями допуску працівників [57].

Особлива увага в моделях державних підприємств приділяється роботі з інформацією, що становить державну таємницю або має гриф «Для службового користування». Специфіка зберігання секретних електронних документів вимагає створення фізично ізольованих контурів архівної системи. Такі підсистеми не повинні мати виходу до мережі Інтернет для запобігання несанкціонованому витоку даних. Використання криптографічних засобів захисту інформації є обов’язковим атрибутом функціонування подібних моделей. Державний стандарт вимагає, щоб кожен документ у секретному електронному архіві був зашифрований з використанням сертифікованих алгоритмів.

Взаємодія з системою «АСКОД» дозволяє автоматично формувати архівні описи та акти про вилучення документів для знищення [2]. Програмні модулі системи забезпечують міграцію файлів у формати тривалого зберігання, такі як PDF/A-1. Це критично важливо для забезпечення читабельності документів через 10, 25 або 75 років [2]. Процес конвертації супроводжується перевіркою кваліфікованого електронного підпису та накладанням архівної позначки часу. Моделі електронних архівів ДП передбачають регулярне резервне копіювання даних на територіально віддалені майданчики. Це гарантує живучість архівної інформації у випадку техногенних катастроф або військових загроз [2].

Функціонування архіву на державному підприємстві неможливе без чітко регламентованої процедури експертизи цінності документів у цифровому форматі. Система має підтримувати можливість створення електронних справ за номенклатурою, що діє на підприємстві. Інтеграція з «АСКОД» забезпечує безшовний перехід метаданих від реєстраційної картки документа до архівної картки [2]. Підхід мінімізує ручну працю та виключає помилки, пов’язані з людським фактором. Модель має передбачати можливість швидкого пошуку інформації за широким спектром атрибутів. Доступ до архівних фондів для співробітників здійснюється через вебінтерфейс або спеціалізовані клієнтські додатки.

Аудит дій користувачів є обов’язковим елементом системи управління державним електронним архівом. Кожна операція перегляду, копіювання чи редагування метаданих повинна логуватися в системі захищеного журналу [2]. Специфіка ДП також передбачає взаємодію з державними архівними установами для передавання документів постійного зберігання. Електронна взаємодія між архівом підприємства та Національним архівним фондом вимагає сумісності форматів обміну даними. Розробка моделі повинна враховувати масштабованість системи при збільшенні обсягів цифрового контенту. Використання хмарних технологій у державних архівах наразі обмежене вимогами щодо локалізації даних на території України [60].

Перевага надається приватним хмарам або власним дата-центрам підприємств із відповідним рівнем сертифікації КСЗІ [57].

Складність моделювання полягає у необхідності підтримувати юридичну силу електронного документа протягом багатьох десятиліть. Система повинна автоматично оновлювати електронні підписи на документах до завершення терміну дії сертифікатів. Це реалізується через процедуру «перепідписання» або використання технологій Long Term Validation. Робота з «АСКОД» у цьому контексті дозволяє використовувати вже готові шлюзи для перевірки статусів сертифікатів [2]. Модель має бути адаптивною до змін у законодавстві щодо електронного урядування та архівної справи. Функціонування електронного архіву на ДП також включає роботу з аудіовізуальними документами та специфічними форматами (CAD-креслення тощо). Для таких файлів створюються спеціальні контейнери зберігання з детальним описом технічних характеристик. Важливим аспектом є забезпечення енергонезалежності серверного обладнання архіву [2]. Державні підприємства критичної інфраструктури впроваджують моделі з найвищим рівнем відмовостійкості. Управління життєвим циклом документа в архіві має бути повністю прозорим для контролюючих органів. Система повинна генерувати звіти про стан фондів у режимі реального часу.

Використання аналогів «АСКОД», таких як «Megapolis.DocNet» чи «Megalopolis», також поширене серед державних структур [53, с.168]. Всі ці системи мають схожі принципи побудови архівних модулів, орієнтованих на державні стандарти. Ключовою відмінністю між ними є інтерфейсні рішення та методи інтеграції з СУБД. Проте концептуальна модель електронного архіву залишається незмінною: надійність, секретність, централізація. Впровадження таких моделей дозволяє державним підприємствам перейти до концепції «підприємства без паперу» [53, с.164]. Це значно підвищує ефективність державного управління та прозорість бізнес-процесів. Фінальним етапом побудови моделі є навчання персоналу роботі з

інструментами електронного архівування. Лише поєднання технологій, регламентів та кваліфікованих кадрів забезпечує життєздатність системи.

Отже, аналіз практичних моделей підтверджує, що для ДП оптимальним є гібридний підхід. Він поєднує високий рівень автоматизації рутинних операцій із суворим контролем доступу до стратегічної інформації. Майбутній розвиток таких моделей пов'язаний із впровадженням елементів штучного інтелекту для автоматичної класифікації документів.

2.2. Особливості впровадження та експлуатації електронних архівів у сучасних комерційних структурах

Впровадження електронних архівів у комерційному секторі суттєво відрізняється від аналогічних процесів у державних установах за рахунок пріоритетності бізнес-цілей. Сучасна комерційна структура розглядає електронний архів не як пасивне сховище, а як активний інструмент управління корпоративним контентом [58, с.133]. Основними рушійними силами цифровізації в бізнесі є прагнення до зниження операційних витрат та пришвидшення прийняття управлінських рішень. Гнучкість архітектурних рішень дозволяє компаніям адаптувати архівні системи під специфічні потреби ринку та внутрішні регламенти. На відміну від жорстко регульованих державних моделей, комерційні архіви часто будуються на засадах модульності та масштабованості.

Ключовою особливістю є глибока інтеграція архівних модулів із системами управління взаємовідносинами з клієнтами та планування ресурсів підприємства. У моделі сучасного офісу документ автоматично потрапляє до архіву безпосередньо з інтерфейсу ERP-системи, наприклад, SAP, Oracle, що забезпечує безперервність бізнес-процесів, де фінансова документація, договори та акти зберігаються в єдиному цифровому контурі. CRM-системи, такі як Salesforce або Bitrix24, виступають джерелами метаданих для формування персоналізованих клієнтських справ в архіві [12]. Автоматичне

тегування документів дозволяє менеджерам знаходити історію взаємодії з контрагентом за лічені секунди. Такий підхід мінімізує ризики втрати важливої інформації при зміні персоналу або реорганізації відділів.

Важливою рисою комерційних моделей є широке використання хмарних технологій (SaaS та PaaS) для розміщення архівних фондів [60]. Хмарні рішення забезпечують високу доступність даних з будь-якої точки світу, що є критичним для міжнародних та дистриб'юторських компаній. Використання гібридних моделей зберігання дозволяє компаніям тримати критично важливі дані на власних серверах, а менш пріоритетні — у публічних хмарах. Це значно оптимізує витрати на IT-інфраструктуру, оскільки бізнес платить лише за фактично використаний обсяг пам’яті. Гнучкість налаштувань дозволяє швидко змінювати права доступу для проектних команд або зовнішніх аудиторів.

Вибір архітектурної моделі хмарних обчислень є фундаментом, на якому будується вся стратегія довготривалого зберігання цифрових документів. У сучасному світі електронний архів уже давно перестав бути просто набором папок на локальному сервері підприємства [60]. Публічна хмарна модель (Public Cloud) пропонує компаніям безпрецедентну масштабованість та швидкість розгортання архівних потужностей. Використання сервісів від таких гігантів, як AWS, Microsoft Azure або Google Cloud, дозволяє бізнесу платити лише за фактично використаний обсяг дискового простору. Це ідеальне рішення для малих та середніх комерційних структур, які не мають бюджету на утримання власного дата-центру. Публічні хмари забезпечують високу доступність даних із будь-якої точки світу, що критично важливо для віддаленої роботи. Однак для державних підприємств цей шлях часто закритий через вимоги щодо локалізації даних у межах національних кордонів [60].

Приватна хмара (Private Cloud) є повною протилежністю, оскільки вона створюється виключно для потреб однієї організації. У такій моделі підприємство має повний контроль над фізичною інфраструктурою,

мережевими налаштуваннями та протоколами безпеки. Для державних установ та стратегічних підприємств приватна хмара є єдиним безпечним способом реалізації вимог КСЗІ. Вона дозволяє інтегрувати систему «АСКОД» у захищений периметр, де доступ ззовні практично неможливий [2]. Приватна модель гарантує, що конфіденційні архівні документи не будуть знаходитися на одному фізичному обладнанні з даними інших компаній. Це мінімізує ризики витоку інформації через вразливості в технологіях віртуалізації. Головним недоліком приватної моделі є висока вартість володіння (TCO), що включає витрати на закупівлю серверів, ліцензій та оплату праці IT-фахівців. Оновлення такої системи вимагає значного часу та капітальних інвестицій, що знижує гнучкість бізнес-процесів [60].

Гібридна хмарна модель (Hybrid Cloud) виступає «золотою серединою», поєднуючи надійність приватної хмари з гнучкістю публічної. У цій моделі найбільш критичні архівні фонди, що містять державну або комерційну таємницю, залишаються у внутрішньому контурі. Менш чутлива інформація, наприклад публічні звіти чи маркетингові матеріали, виноситься у публічну хмару для економії ресурсів. Гібридний підхід дозволяє реалізувати стратегію «cloud bursting», коли під час масового архівування система автоматично орендує додаткові потужності, що забезпечує стабільну роботу архіву навіть при екстремальному зростанні обсягів вхідної документації [60]. Важливою перевагою гібридної моделі є можливість створення віддалених бекапів у публічній хмарі для забезпечення живучості архіву. Сучасні банківські установи активно використовують цей підхід для балансування між безпекою та економічною ефективністю.

Процес міграції даних між різними хмарами вимагає використання складних інструментів оркестрації та єдиної системи управління ідентифікацією (IAM). Гібридна модель вимагає від організації високого рівня технологічної зрілості та наявності чітких регламентів класифікації даних. У контексті «АСКОД» або аналогів, гібридна хмара дозволяє створювати шлюзи для безпечного обміну документами з зовнішніми контрагентами [2]. Вибір

моделі також залежить від вимог регулятора щодо термінів зберігання та методів знищення цифрових об'єктів. Публічні хмари часто пропонують спеціалізовані «холодні» сховища, як-от Amazon S3 Glacier, де вартість зберігання терабайта даних є мінімальною. Однак вилучення даних із таких архівів може бути тривалим та потребувати додаткових витрат [60].

Для державних підприємств критично важливо, щоб хмарний провайдер мав відповідні сертифікати Держспецзв'язку [57]. Управління метаданими в хмарі стає складнішим завданням, оскільки вони повинні бути синхронізовані між усіма сегментами сховища. Комерційні структури часто віддають перевагу мультихмарним стратегіям (Multi-cloud), щоб уникнути залежності від одного постачальника послуг. Це підвищує відмовостійкість архітектури та дозволяє обирати найкращі умови на ринку. Безпека в будь-якій хмарній моделі базується на принципі «Zero Trust», де кожне звернення до архіву перевіряється незалежно від розташування користувача. Використання шифрування на стороні клієнта (Client-side encryption) гарантує, що навіть провайдер хмари не зможе прочитати зміст документів [60].

Кінцевий вибір моделі для електронного архіву завжди є компромісом між ризиками, ціною та продуктивністю. Гнучкість хмарних рішень дозволяє підприємствам починати з малих обсягів і масштабуватися разом із ростом бізнесу. Впровадження хмарного архіву значно спрощує процедури аудиту та відповідності стандартам ISO. Тобто, хмарні моделі стали невід'ємною частиною інфраструктури сучасного електронного архівування. Вони забезпечують технічний фундамент для переходу до концепції повністю цифрового державного та приватного сектору. Розуміння специфіки кожної моделі дозволяє керівникам підприємств уникати критичних помилок при проєктуванні архівних систем. Майбутнє електронних архівів однозначно пов'язане з подальшим розвитком хмарних технологій та штучного інтелекту [5, с.78].

Захист комерційної таємниці в таких архівах реалізується через багаторівневі системи ідентифікації та системи запобігання витоку даних

(DLP). На відміну від державної таємниці, захист комерційної інформації базується на політиках конфіденційності (NDA) та внутрішніх стандартах безпеки. Програмне забезпечення електронних архівів у бізнесі часто оснащується модулями поведінкового аналізу для виявлення підозрілої активності користувачів. Шифрування даних проводиться не лише на рівні зберігання, а й під час їхньої передачі через відкриті мережі. Комерційні структури активно впроваджують двофакторну автентифікацію для всіх працівників, що мають доступ до архіву [60].

Окрему увагу в комерційних моделях приділяють юридичній значущості документів, що підтверджується кваліфікованим електронним підписом. Експлуатація архіву передбачає автоматичну перевірку валідності підписів під час завантаження документів від постачальників чи партнерів. Для міжнародних компаній актуальним є питання відповідності формату електронних документів вимогам різних юрисдикцій. Моделі архівів часто підтримують декілька стандартів електронного підпису для роботи з іноземними контрагентами. Важливим аспектом є функція автоматичного нагадування про завершення термінів дії договорів або необхідність оновлення сертифікатів [6].

Експертиза цінності в комерційних архівах часто автоматизована за допомогою алгоритмів машинного навчання та OCR-технологій. Система може самостійно розпізнавати тип документа, витягувати з нього ключові реквізити та призначати відповідну категорію зберігання. Це дозволяє великим рітейлерам або банкам обробляти мільйони первинних документів без залучення великої кількості персоналу. Архівна модель бізнесу орієнтована на концепцію «гарячого» та «холодного» зберігання даних. «Гарячі» дані — це активні контракти та поточні рахунки, до яких потрібен миттєвий доступ. «Холодні» дані — це архівна звітність минулих років, яка переміщується на дешевші та повільніші носії [21, с.46].

Комерційні структури активно використовують електронні архіви для підготовки до податкових перевірок та судових розглядів. Можливість

швидкого формування електронного реєстру документів за запитом контролюючих органів є вагомою конкурентною перевагою. Модель функціонування архіву повинна враховувати вимоги Закону України «Про бухгалтерський облік та фінансову звітність» [32]. Відповідність стандартам ISO 27001 (інформаційна безпека) є маркером надійності компанії для інвесторів. Також архіви в бізнесі часто інтегруються з системами електронного обміну даними (EDI), що популярно у сфері логістики.

Робота з персональними даними клієнтів у межах архіву вимагає суворого дотримання GDPR або національного законодавства про захист персональних даних [40]. Комерційні архіви впроваджують функції автоматичного знеособлення (анонімізації) даних після завершення терміну їхнього використання. Це мінімізує ризики великих штрафів за порушення приватності. Гнучкість інтерфейсу дозволяє створювати «кабінети клієнта», де користувачі можуть самостійно переглядати свої архівні договори або виписки. Експлуатація таких систем вимагає наявності кваліфікованої служби технічної підтримки, що працює в режимі 24/7 [5, с.79].

Масштабування архіву в комерційному секторі відбувається динамічно відповідно до зростання бізнесу. При злитті та поглинанні компаній постає завдання міграції та консолідації розрізнених електронних архівів у єдину систему. Успішна модель експлуатації передбачає регулярне навчання співробітників новим методам роботи з цифровими фондами. Використання мобільних додатків для доступу до корпоративного архіву стає нормою для керівників середньої та вищої ланки, що дозволяє візувати документи або перевіряти архівну інформацію безпосередньо під час переговорів [5, с.78].

Аналіз показує, що комерційні моделі є більш інноваційними та відкритими до впровадження штучного інтелекту для аналітики документів [54]. Автоматичне виявлення дублікатів та очищення архіву від інформаційного «сміття» дозволяє підтримувати систему в актуальному стані. Фінальна мета експлуатації електронного архіву в бізнесі — перетворення накопиченої інформації на інтелектуальний капітал. Комерційні структури,

що ігнорують цифрову архівізацію, швидко втрачають конкурентоспроможність через низьку швидкість бізнес-процесів. Функціонування електронного архіву в банківській установі є еталоном цифрової трансформації комерційного сектору. Банківська модель базується на необхідності миттєвого доступу до мільйонів одиниць зберігання при забезпеченні абсолютного захисту персональних даних. Ключовою особливістю банківського архіву є його повна інтеграція з Автоматизованою банківською системою (АБС) та фронт-офісними додатками [6]. Кожен кредитний договір або анкета клієнта потрапляє до електронного сховища автоматично відразу після накладання Кваліфікованого електронного підпису, що виключає ризик втрати документів на етапі передачі між відділеннями та центральним офісом. Специфіка банківського сектору вимагає зберігання документів протягом різних термінів, що регулюються нормативами Національного банку України. Модель архіву дозволяє автоматично класифікувати справи за категоріями: від поточної звітності до документів із терміном зберігання 75 років [35].

Центральним елементом системи є «Електронне досьє клієнта», яке консолідує всю інформацію про взаємодію банку з фізичною або юридичною особою. Завдяки використанню CRM-систем, архів автоматично підтягує історію комунікацій, скарги та результати фінансового моніторингу. Це дозволяє банківським працівникам здійснювати швидку перевірку контрагентів у межах процедур «Знай свого клієнта» (KYC). Висока гнучкість моделі проявляється у здатності системи масштабуватися під час пікових навантажень, наприклад, у періоди масового видавання кредитів. Банківський архів використовує гібридну інфраструктуру, де найбільш актуальні документи зберігаються у «швидкій» пам'яті для миттєвого доступу [12]. Старіші записи переміщуються в «холодні» хмарні сховища для оптимізації витрат на підтримку серверів. Важливим аспектом є забезпечення банківської таємниці, що вимагає впровадження жорстких протоколів шифрування даних [12]. Доступ до архівних фондів суворо розмежований на основі рольової

моделі (RBAC), де кожен менеджер бачить лише дозволені йому сегменти даних.

Система автоматично фіксує кожен факт перегляду документа, створюючи незмінний журнал аудиту. У разі виникнення судових спорів банк може надати електронний документ із повним ланцюжком доказів його автентичності. Впровадження технологій OCR дозволяє проводити повнотекстовий пошук навіть у відсканованих паперових архівах минулих десятиліть [12]. Автоматизація роботи з архівом дозволяє банку скоротити штатний розклад архівних підрозділів на 60% або навіть 80%. Економічна ефективність моделі також підтверджується відмовою від оренди величезних фізичних площ для зберігання паперу [12]. Для забезпечення відмовостійкості банківські архіви використовують технологію геореплікації даних між декількома дата-центрами. Це гарантує, що навіть у разі повної відмови одного з серверів, банк зможе відновити доступ до клієнтських справ за лічені хвилини.

Банківська модель також передбачає інтеграцію з державними реєстрами для автоматичної верифікації наданих клієнтами документів. Як ми зазначали вище, використання технології Long Term Validation забезпечує юридичну силу підписів на документах навіть через багато років після завершення терміну дії сертифікатів. Це критично важливо для іпотечних договорів, термін дії яких може сягати 30 років. Електронний архів банку є також інструментом для роботи відділів стягнення заборгованості (collection). Менеджери мають можливість миттєво сформувати пакет документів для подання позову до суду без звернення до фізичного архіву. Програмні модулі системи автоматично відстежують терміни позовної давності та нагадують про необхідність актуалізації даних [12].

Кейс великого банку демонструє, що електронний архів стає базою для впровадження штучного інтелекту. Алгоритми AI аналізують архівні дані для виявлення патернів шахрайства та прогнозування ризиків неповернення кредитів. Гнучкість інтерфейсу дозволяє клієнтам банку через мобільний

додаток самостійно отримувати архівні виписки або копії договорів. Це значно підвищує лояльність клієнтів та знижує навантаження на контакт-центри. При впровадженні такої моделі банківські установи звертають увагу на кіберзахист та запобігання внутрішнім витокам інформації. Системи DLP (Data Loss Prevention) автоматично блокують спроби масового вивантаження клієнтських баз з електронного архіву. Регулярні стрес-тести та аудити безпеки є невід'ємною частиною експлуатації банківського архіву [12].

Сучасні банки активно переходять на безпаперові технології в усіх внутрішніх процесах, від кадрів до бухгалтерії. Архів стає єдиною точкою істини для всіх корпоративних даних, що виключає дублювання інформації. Модель також включає функцію автоматичного знищення документів, термін зберігання яких закінчився, з оформленням відповідних актів. Це допомагає дотримуватися норм захисту персональних даних та уникати зберігання зайвої інформації. Тобто, кейс банківського архіву підтверджує, що інвестиції в цифрову інфраструктуру приносять дивіденди у вигляді швидкості, безпеки та довіри клієнтів. Електронний архів у банку перетворюється з допоміжної функції на стратегічний актив бізнесу. Лише така модель дозволяє фінансовій установі успішно конкурувати в епоху цифрових технологій та швидких фінансів. Банк, що володіє досконалим електронним архівом, є максимально прозорим для регуляторів та надійним для вкладників.

Отже, сучасна модель електронного архіву в комерції — це поєднання високих технологій, правової безпеки та економічної ефективності. Вона забезпечує фундамент для побудови цифрової екосистеми сучасної компанії.

РОЗДІЛ ІІІ. ШЛЯХИ ОПТИМІЗАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СУЧАСНИХ МОДЕЛЕЙ Е-АРХІВІВ

3.1. Технологічна модернізація: впровадження штучного інтелекту та блокчейн-технологій для забезпечення автентичності документів

На нашу думку, сучасний розвиток електронних архівів вимагає переходу від пасивного збереження даних до активного управління їхньою автентичністю та структурою. Стрімке зростання обсягів цифрової інформації робить традиційні методи каталогізації та верифікації малоефективними та вразливими до людського фактора [58, с.132]. Саме тому технологічна модернізація архівних установ стає пріоритетним завданням для забезпечення юридичної значущості е-документів у довгостроковій перспективі.

Ключовим інструментом у цьому процесі виступає штучний інтелект (далі — ШІ), який докорінно змінює підходи до інтелектуального аналізу даних [54]. Впровадження алгоритмів машинного навчання дозволяє автоматизувати процеси розпізнавання та класифікації документів за їхнім змістом, а не лише за формальними ознаками. Використання нейронних мереж забезпечує високу точність ідентифікації типів документів, виокремлюючи структурні елементи, такі як заголовки, реквізити та підписи. Завдяки семантичному аналізу ШІ здатний самостійно генерувати метадані, що значно прискорює процес індексації великих масивів інформації. Це дозволяє архівістам зосередитися на експертній оцінці, довіривши рутинне сортування автоматизованим системам.

ШІ також ефективно вирішує проблему «темних даних» (dark data), які зберігаються в архівах без належної ідентифікації [54]. Алгоритми кластеризації групують документи за контекстною схожістю, створюючи логічні зв’язки між розрізненими файлами. Важливою перевагою ШІ є здатність до самонавчання: чим більше документів проходить через систему, тим точнішими стають результати класифікації — це мінімізує ризик помилок,

пов'язаних із суб'єктивним сприйняттям інформації людиною. Окрім того, технології обробки природної мови (NLP) дозволяють здійснювати повнотекстовий пошук із врахуванням морфології та контексту, що забезпечує принципово новий рівень доступності архівної інформації для користувачів. Проте швидкість обробки даних — лише одна сторона модернізації, тоді як інша полягає у забезпеченні їхньої недоторканності [54].

Тоді застосовується технологія блокчейн, яка виступає гарантом незмінності та автентичності цифрового контенту. За своєю суттю, блокчейн — децентралізований реєстр, де кожен запис нерозривно пов'язаний із попереднім через криптографічні хеш-функції. Впровадження блокчейну в е-архіви дозволяє створити систему, в якій неможливо непомітно підробити або видалити документ [6]. Кожна операція з документом, від його створення до кожної зміни метаданих, фіксується у ланцюжку блоків. Це створює надійний аудиторський слід, який доступний для перевірки у будь-який момент. Маємо наголосити, що сучасні технології, які визначають майбутнє електронних архівів, сягають корінням у середину XX століття, коли людство вперше замислилося над автоматизацією інтелектуальних процесів.

Історія штучного інтелекту розпочалася з теоретичних розробок Алана Тюрінга, який у 1950 році поставив фундаментальне питання про здатність машин мислити. Офіційне народження галузі відбулося на Дартмутській конференції 1956 року, де було вперше вжито термін «штучний інтелект» та окреслено амбітні плани щодо імітації людського розуму. Перші кроки були зосереджені на створенні систем, здатних вирішувати логічні завдання та доводити теореми. У 1960-х роках з'явилися перші програми для обробки природної мови, такі як ELIZA, що заклали основу для майбутньої взаємодії людини з машиною. Проте невдовзі галузь зіткнулася з періодом «зими штучного інтелекту», зумовленим обмеженістю тодішніх обчислювальних потужностей [54].

У 1980-х роках інтерес до ШІ відродився завдяки успіху експертних систем, які використовували бази знань для прийняття вузькоспеціалізованих

рішень. Саме в цей період розпочалися перші спроби автоматизації документообігу через системи розпізнавання символів (OCR). Справжній технологічний вибух стався на початку XXI століття з появою великих даних та розвитком алгоритмів глибокого навчання (Deep Learning). Сучасні нейронні мережі змінили підхід до класифікації документів, навчившись розпізнавати не лише знаки, а й контекстуальні смисли. Паралельно з еволюцією «розуму» машин розвивалася потреба в забезпеченні абсолютної довіри до цифрової інформації [54].

Витоки технології блокчейн можна відстежити з кінця 1970-х років, коли було винайдено дерево Меркла — структуру даних для ефективної верифікації інформації. У 1991 році Стюарт Хабер та Скотт Сторнетта представили концепцію криптографічно захищеного ланцюжка блоків для зберігання часових міток документів. Їхня мета полягала в тому, щоб зробити неможливим змінення дати створення цифрового файлу «заднім числом». Це була перша пряма історична передумова застосування блокчейн-принципів в архівній справі. Проте до 2008 року ці ідеї залишалися переважно в академічній площині [54].

Революційним моментом став маніфест Сатоші Накамото, який об'єднав існуючі криптографічні методи в цілісну систему децентралізованого реєстру. Поява біткоїна у 2009 році довела життєздатність концепції розподілених баз даних без центрального органу управління. Згодом, із появою платформи Ethereum у 2015 році, світ дізнався про смарт-контракти — програмний код, що автоматично виконує умови угоди. Це відкрило нові горизонти для автоматизації архівних регламентів та прав доступу. Для архівної науки це означало перехід від довіри до інституції (архівіста) до довіри до математичного алгоритму [54].

Протягом останнього десятиліття шляхи розвитку ШІ та блокчейну почали стрімко перетинатися. ШІ навчився генерувати та структурувати контент, а блокчейн став інструментом для фіксації авторства та незмінності цього контенту [54]. В історичному контексті це можна порівняти з винаходом

друкарського верстата, який одночасно прискорив розповсюдження знань і вимагав створення нових засобів підтвердження справжності видань. Сьогодні ми спостерігаємо період конвергенції, де ШІ виступає як «двигун» обробки даних, а блокчейн — як «панцир» їхнього захисту [6].

Державні установи в усьому світі почали усвідомлювати, що цифровізація архівів без належної технологічної бази веде до втрати юридичної значущості спадщини. Еволюція ШІ пройшла шлях від простих алгоритмів сортування до складних моделей, що розуміють зміст державних актів. Блокчейн, у свою чергу, еволюціонував від фінансового інструменту до фундаменту цифрової ідентичності та довіри [6]. Поєднання цих технологій у третьому десятилітті XXI століття стало відповіддю на виклики епохи «постправди» та дипфейків. Архівна справа історично завжди адаптувала передові технології свого часу — від папірусу та пергаменту до мікрофільмування та магнітних стрічок. Сучасна модернізація через ШІ та блокчейн є закономірним етапом цієї тисячолітньої еволюції. Вона дозволяє подолати головну вразливість цифрового документа — його легку змінюваність без залишення видимих слідів [12].

Тобто, історія розвитку аналізованих нами технологій — історія боротьби за збереження автентичності людського знання в умовах технологічного прогресу. Розуміння цього шляху дозволяє нам краще оцінити потенціал запропонованих методів оптимізації сучасних е-архівів. Сьогодні ми стоїмо на порозі створення систем, де історія кожного документа фіксується навічно в цифровому коді. Найбільш критичним аспектом для архівної справи є підтвердження дати створення документа та його незмінності з моменту реєстрації. Традиційні мітки часу в централізованих базах даних можуть бути скомпрометовані адміністратором або зловмисником. Блокчейн-технологія пропонує механізм розподіленого часового штампування, який не залежить від єдиного центру керування. Коли документ завантажується в систему, створюється його унікальний цифровий відбиток — хеш [6].

Хеш записується в блокчейн разом із часовою міткою, що стає незаперечним доказом існування документа в конкретний момент часу [6]. Будь-яка, навіть найменша зміна в самому файлі призведе до повної зміни його хешу, що миттєво виявить факт несанкціонованого втручання. Підхід забезпечує абсолютну автентичність, оскільки система дозволяє порівняти поточний хеш документа з тим, що був записаний при його створенні. Користувачі архіву отримують можливість самостійно перевірити цілісність документа без звернення до третіх сторін. Використання смарт-контрактів у блокчейн-мережі дозволяє автоматизувати правила доступу та терміни зберігання документів. Наприклад, смарт-контракт може автоматично знищити доступ до документа після завершення терміну його зберігання або надати права перегляду лише авторизованим особам. Це виключає ризик корупції або випадкового порушення регламентів архівного зберігання.

Поєднання ШІ та блокчейну створює комплексну екосистему «розумного» та безпечного архівування, а саме: ШІ відповідає за інтелектуальну організацію простору, а блокчейн — за верифікацію його безпеки [54]. Разом ці технології вирішують проблему довіри в цифровому середовищі, де інформація може бути легко скопійована або змінена. Це особливо важливо для державних установ та юридичних осіб, чия діяльність базується на правовій силі документів. Перехід на таку модель дозволяє архівним установам трансформуватися у високотехнологічні сервісні центри.

Впровадження інновацій вимагає розробки відповідних стандартів та протоколів взаємодії. Окрім технічних аспектів, необхідно враховувати й енерговитратність блокчейн-мереж, обираючи оптимальні алгоритми консенсусу [6]. Також архітектура системи повинна бути масштабованою, щоб витримувати постійно зростаюче навантаження. Інтеграція ШІ у процеси блокчейн-верифікації дозволяє також виявляти аномалії у діях користувачів, запобігаючи кіберзагрозам. Наприклад, ШІ може розпізнати нетипову активність, яка свідчить про спробу масового копіювання даних. У такий спосіб формується багаторівневий захист архівної спадщини.

Аналіз поточної діяльності типового державного підприємства свідчить про те, що архівний фонд є критично важливим активом, який забезпечує юридичну тяглість та прозорість управління державним майном [21, с.56]. Проте традиційні моделі електронних архівів у державному секторі часто страждають від фрагментарності, де дані зберігаються у розрізнених базах без єдиного стандарту метаданих. Оптимізація такої системи вимагає переходу від простого цифрового сховища до інтелектуальної екосистеми управління життєвим циклом документа. Першим кроком у модернізації має стати аудит існуючих бізнес-процесів, який виявить «вузькі місця» у швидкості обробки вхідної та внутрішньої кореспонденції.

Впровадження штучного інтелекту на етапі реєстрації документів дозволяє усунути суб'єктивізм та помилки ручного введення даних. Система, оснащена модулями комп'ютерного зору, автоматично розпізнає скановані копії, вилучаючи ключові реквізити, такі як номер, дата, підписант та предмет договору [5, с.83]. Завдяки алгоритмам семантичного аналізу, е-архів державного підприємства зможе самостійно розподіляти документи за тематичними папками та фондами. Це значно спрощує підготовку до перевірок контролюючими органами, оскільки пошук необхідного пакета документів за конкретним проєктом триватиме лічені секунди. Більше того, ШІ здатний виявляти дублікати та пов'язані документи, створюючи цілісну історію взаємодії з контрагентами [3, с.32].

Наступним рівнем оптимізації є забезпечення абсолютної довіри до архівних даних, що критично для державного сектора в контексті антикорупційної політики. Використання технології блокчейн дозволяє кожну транзакцію в системі е-архіву зробити прозорою та незворотною. У моделі оптимізованого архіву ДП кожен документ при реєстрації отримує унікальний криптографічний ідентифікатор, який записується у розподілений реєстр. Це унеможливлює практику підміни сторінок у контрактах або зміну дат «заднім числом», що часто є предметом судових розглядів. Для державного

підприємства це означає створення надійного доказового поля, яке захищає інтереси держави в правових спорах.

Важливим аспектом оптимізації є інтеграція е-архіву з загальнодержавними системами електронної взаємодії, такими як «Трембіта» або сервіси електронного підпису [53, с.168]. Автоматична верифікація КЕП (кваліфікованого електронного підпису) безпосередньо в архівній системі дозволяє підтримувати юридичну силу документів протягом усього терміну їхнього зберігання [36]. Оптимізована модель передбачає також використання смарт-контрактів для управління правами доступу до конфіденційної інформації. Це дозволяє автоматично надавати або обмежувати доступ співробітників залежно від їхньої посади чи терміну виконання конкретного завдання. Така автоматизація знижує адміністративне навантаження на службу діловодства та архіву.

Крім технічних переваг, модернізація е-архіву несе значний економічний ефект за рахунок скорочення витрат на фізичне зберігання паперу та логістику. Штучний інтелект також може прогнозувати обсяги накопичення даних, допомагаючи ІТ-відділам вчасно масштабувати серверні потужності [3, с.34]. Завдяки блокчейну, внутрішній аудит підприємства стає безперервним процесом, оскільки будь-яке втручання в систему фіксується і не може бути приховане, що підвищує інвестиційну привабливість державних підприємств та рівень довіри з боку міжнародних партнерів.

У контексті кібербезпеки оптимізована система використовує нейронні мережі для моніторингу аномальної активності користувачів. Якщо система фіксує спробу масового вивантаження документів у неробочий час, вона автоматично блокує доступ і надсилає сповіщення службі безпеки. Відбувається створення додаткового периметру захисту навколо інтелектуальної власності та комерційної таємниці підприємства [41]. Процес класифікації документів за ступенем конфіденційності також стає автоматизованим, що мінімізує ризик витоку інформації через людську необачність. Оптимізація передбачає створення мобільних інтерфейсів, що

дозволяє керівництву ДП отримувати доступ до архівних довідок та звітів у режимі реального часу з будь-якої точки світу.

Підсумовуючи аналіз, можна стверджувати, що трансформація архіву державного підприємства — це перехід від моделі «складу» до моделі «бази знань». Використання ШІ для інтелектуального пошуку перетворює архів з пасивного сховища на активний інструмент підтримки прийняття управлінських рішень [54]. Блокчейн, у свою чергу, забезпечує цифрову суверенність та недоторканність державних даних [6]. Впровадження такої моделі вимагає оновлення нормативної бази підприємства та навчання персоналу роботі з новими інструментами. Однак довгострокові вигоди у вигляді прозорості, безпеки та ефективності повністю виправдовують інвестиції в технологічну модернізацію. Таким чином, оптимізований е-архів стає фундаментом для побудови сучасної цифрової держави на мікрорівні окремого підприємства.

На завершення варто зазначити, що технологічна модернізація — це не просто данина моді, а необхідна умова виживання інституту архівування. Без впровадження ШІ та блокчейну сучасні е-архівні моделі ризикують стати кладовищами неперевіреної та хаотичної інформації. Автоматизація класифікації та криптографічне підтвердження автентичності повертають цифровому документу статус «оригіналу». Це закладає міцний фундамент для розвитку електронного урядування та цифрової економіки. Перспективи використання цих технологій відкривають шлях до створення глобальної мережі довірених архівів. Таким чином, симбіоз штучного інтелекту та блокчейну є ключовим вектором оптимізації сучасних е-архівів.

3.2. Стратегії довготривалого збереження та міграції даних у цифровому середовищі

Проблема збереження цифрової інформації у часовому проміжку 50 років і більше кардинально відрізняється від традиційного архівування

паперових носіїв. Головна небезпека полягає не лише у фізичному руйнуванні носія, а й у «технологічному старінні» форматів файлів та програмного забезпечення [7, с.78]. Цифрові дані є ефемерними за своєю природою, оскільки вони потребують посередника у вигляді специфічного обладнання та софту для інтерпретації бітового потоку. Коли програмне забезпечення, що створило файл, зникає з ринку або стає несумісним з новими операційними системами, дані перетворюються на «цифровий шум». Саме тому стратегія довготривалого збереження повинна фокусуватися на забезпеченні постійної читабельності та змістовної цілісності об'єктів.

Ми стикаємося з парадоксом: що складнішим є формат файлу, то вища ймовірність його швидкої втрати. Формати, права на які належать корпораціям, створюють найбільші ризики через закритість вихідного коду та специфікацій. Якщо компанія припиняє підтримку продукту, користувач залишається з архівом, який неможливо відкрити без застарілого «заліза». Таким чином, боротьба з технологічним старінням вимагає відмови від залежності від конкретних постачальників послуг х7б сю90ъ. Основна мета підрозділу — визначити механізми, які дозволять майбутнім дослідникам через пів століття отримати доступ до сучасних даних так само легко, як ми сьогодні читаємо друковану книгу. Першим і найважливішим кроком у стратегії збереження є правильний вибір форматів файлів на етапі створення або архівування.

Для текстових документів золотим стандартом є формат PDF/A, який спеціально розроблений для довготривалого зберігання х35ъ. Він виключає використання зовнішніх посилань та вбудовує всі необхідні шрифти безпосередньо у файл, що гарантує ідентичність відображення через десятиліття. У сфері зображень перевагу слід віддавати формату TIFF без стиснення або з відкритими алгоритмами стиснення, оскільки він зберігає максимальну кількість візуальної інформації. Для табличних даних та баз даних найкращим рішенням є формат CSV або XML, які є людиночитаними та легко імпортуються у будь-яку майбутню систему обробки даних.

Важливо уникати форматів із цифровим керуванням правами (DRM), оскільки механізми шифрування можуть стати нездоланним бар'єром після завершення терміну підтримки ключів активації. Відкриті стандарти (Open Standards) мають перевагу, оскільки їхні специфікації доступні публічно і можуть бути реалізовані будь-яким розробником у майбутньому. Кожен формат, обраний для архіву, повинен мати високий рівень «самодокументованості» х53б сю168ъ. Це означає, що структура файлу має бути логічною та описаною у супровідній документації. Використання простих, поширених та стандартизованих форматів знижує витрати на майбутню конвертацію. Таким чином, ми створюємо «технологічну страховку» для наших цифрових активів.

Міграція — керований процес перенесення цифрових об'єктів з однієї апаратно-програмної конфігурації до іншої або конвертація файлів із застарілих форматів у сучасні, активний метод, який вимагає регулярного моніторингу технологічного ландшафту. Міграція має відбуватися кожні 5–10 років, залежно від темпів оновлення ПЗ [7, с.102]. Головним ризиком тут є втрата інформації або зміна автентичності документа під час перекодування. Кожна ітерація міграції повинна супроводжуватися суворим контролем якості та перевіркою цілісності даних за допомогою контрольних сум. Важливо зберігати не лише останню версію файлу, а й оригінальний бітовий потік, щоб мати змогу повернутися до першоджерела у разі виявлення помилок конвертації.

Міграція дозволяє підтримувати дані в «активному» стані, роблячи їх доступними для сучасних користувачів без додаткових зусиль. Проте цей процес є ресурсомістким, оскільки потребує постійної уваги фахівців та обчислювальних потужностей [7, с. 102]. Для великих архівів автоматизація процесів міграції стає життєво необхідною. Розробка скриптів для пакетної обробки дозволяє мінімізувати людський фактор. У результаті успішної міграції ми отримуємо дані, що повністю інтегровані в актуальне робоче

середовище. На відміну від міграції, яка змінює сам файл, емуляція зосереджується на відтворенні середовища, у якому цей файл був створений.

Підхід передбачає створення програмних оболонок, що імітують роботу застарілого апаратного забезпечення (процесорів, відеокарт) та операційних систем [12]. Емуляція є критично важливою для збереження складних об'єктів, таких як інтерактивне програмне забезпечення, відеоігри або бази даних зі складними зв'язками. Завдяки емуляції ми можемо запустити оригінальне ПЗ 1990-х років на сучасному комп'ютері та побачити файл саме таким, яким його бачив автор. Метод дозволяє зберегти «досвід користувача» та контекст взаємодії з інформацією. Проте розробка та підтримка надійних емуляторів є складним технічним завданням, що потребує глибоких знань архітектури минулих поколінь.

Емуляція часто використовується в музеях комп’ютерної техніки та цифрового мистецтва. Вона дозволяє уникнути ризиків, пов’язаних із багатократною конвертацією даних. Водночас емуляція потребує наявності образів дисків оригінальних систем, що також потребує довготривалого зберігання. Поєднання міграції для простих даних та емуляції для складних систем створює комплексну систему захисту [12]. Дані без контексту втрачають свою цінність, тому стратегія збереження повинна включати розширену систему метаданих. Метадані мають описувати не лише зміст файлу, а й історію його змін, технічні параметри та умови доступу.

Стандарт PREMIS (Preservation Metadata: Implementation Strategies) є основою для фіксації подій у життєвому циклі цифрового об'єкта. Ми повинні документувати, хто, коли і за допомогою якого інструмента проводив міграцію файлу. Важливо зберігати інформацію про походження даних (provenance), щоб підтвердити їхню автентичність у майбутньому. Метадані мають зберігатися як усередині файлу, так і в зовнішніх реєстрах для дублювання [61]. Опис об’єкта повинен бути зрозумілим навіть без використання спеціалізованого ПЗ, що досягається шляхом використання текстових форматів для супровідних записів. Важливо також враховувати

юридичні аспекти, зокрема авторські права, які можуть обмежити можливість міграції або доступу через 50 років.

Чітко структуровані метадані перетворюють набір файлів на структурований інтелектуальний архів. Без них майбутні користувачі можуть знайти дані, але не зможуть зрозуміти їхнє призначення. Технологічне старіння форматів неможливе без забезпечення фізичної цілісності бітів. Використання правила «3-2-1» є обов'язковим: мінімум три копії даних на двох різних типах носіїв, одна з яких зберігається в іншому географічному місці [7, с.145]. Сучасні хмарні сховища забезпечують високу доступність, але вони не є гарантією довготривалого збереження через ризик банкрутства провайдера або зміни умов сервісу. Для «холодного» зберігання варто розглядати спеціалізовані носії, такі як M-DISC або магнітні стрічки LTO, які мають підтверджений термін служби у кілька десятиліть.

Перспективним напрямком є зберігання даних у молекулах ДНК або на кварцовому склі, що може забезпечити збереження інформації на тисячі років. Регулярна перевірка цілісності даних дозволяє вчасно виявити «бітову гниль» — мікропошкодження носія. У разі виявлення помилки пошкоджена копія повинна бути негайно замінена еталонною з іншого сховища. Автоматизовані системи керування архівами повинні самостійно виконувати ці перевірки за розкладом. Фізична безпека включає захист від пожеж, повеней та електромагнітних імпульсів. Тобто, ми створюємо багаторівневу систему відмовостійкості. Технології самі по собі не гарантують збереження — це завдання для менеджменту та інституцій. Організація повинна мати офіційно затверджену Політику збереження цифрових даних, яка визначає відповідальних осіб та джерела фінансування. Довготривале збереження — це не разовий проєкт, а безперервний процес, що вимагає щорічного бюджетування [21, с.67].

Важливо забезпечити спадковість знань у команді ІТ-фахівців та архіваріусів. Навчання персоналу роботі з архівними форматами та процедурами міграції є критичним. Інституційна відданість гарантує, що дані

не будуть видалені через зміну керівництва або пріоритетів. Ми повинні розглядати збереження даних як частину культурної спадщини або капіталу організації. Співпраця з міжнародними консорціумами, такими як Digital Preservation Coalition, дозволяє використовувати кращі світові практики. Документування всіх процесів забезпечує прозорість та можливість аудиту системи збереження [61].

На нашу думку, лише системний підхід, поєднаний з технологічною експертизою, дає шанс на виживання цифрової інформації. Якщо ми дотримувалися стратегії відкритих форматів, то навіть через 75 років можна буде прочитати специфікацію PDF/A або XML навіть на комп'ютерах, архітектура яких ще не винайдена. Якщо дані були вчасно мігровані, вони будуть частиною актуальної на той час інформаційної екосистеми. У разі використання емуляції дослідник запустить віртуальну машину «Old-Tech 2020-s» і побачить софт у дії [61]. Контрольні суми підтвердять, що жоден біт не змінився за пів століття, гарантуючи достовірність інформації. Особливості цифрового збереження в межах приватних підприємств зумовлені насамперед орієнтацією на комерційну доцільність та операційну ефективність, що часто суперечить ідеї довготривалого архівування [61].

На відміну від державних установ, де існують чіткі регламенти передачі документів, приватні компанії часто розглядають свої цифрові архіви як внутрішню інтелектуальну власність із обмеженим доступом. Проблема «технологічного старіння» тут посилюється економічною нестабільністю та високою ймовірністю раптового припинення діяльності суб'єкта господарювання. У випадку банкрутства або ліквідації підприємства його цифрові активи опиняються під загрозою миттєвого знищення через несплату рахунків за хмарні сервіси або фізичну утилізацію серверного обладнання. Найбільш критичним аспектом є відсутність чітко визначеного механізму передачі е-архіву правонаступнику або державним архівним установам [61]. Коли юридична особа припиняє існування, виникає правовий та технічний вакуум, у якому цінні дані можуть бути втрачені назавжди.

Ризик банкрутства створює ситуацію, коли цифровий архів стає «сиротою» — він існує фізично, але не має законного володільця, який би підтримував його життєздатність. У процесі ліквідації підприємства ліквідаційна комісія зазвичай фокусується на фінансових активах та нерухомості, часто ігноруючи складність перенесення та збереження терабайтів цифрової інформації [14, с.63]. Питання про те, хто є правонаступником е-архіву, стає особливо гострим, якщо компанія не має прямого спадкоємця в межах корпоративної структури. Якщо дані містять інформацію про тривалі зобов'язання перед клієнтами або результати наукових досліджень, їхня втрата має негативні наслідки для всього ринку. Відсутність автоматичного механізму передачі ключів шифрування та паролів доступу до ліквідаторів робить архів недоступним навіть за наявності фізичних носіїв. Ми спостерігаємо тенденцію, де цифрова спадщина приватного сектора є значно вразливішою за паперову, оскільки потребує безперервного фінансування для підтримки працездатності серверів.

Для мінімізації ризиків приватні підприємства повинні впроваджувати стратегію «вихідного плану» для своїх цифрових архівів ще на етапі їхнього створення. Це передбачає укладення договорів про метод безпечного зберігання даних, де третя незалежна сторона (наприклад, спеціалізований цифровий депозитарій) бере на себе зобов'язання підтримувати доступ до архіву в разі банкрутства власника [14, с.57]. Важливим кроком є інтеграція е-архіву підприємства до Національного архівного фонду, якщо документи мають культурну чи історичну цінність [44]. У такому разі держава виступає гарантом збереження даних після зникнення приватної компанії. Проте технічна сумісність форматів між приватним архівом та державним сховищем залишається серйозним бар'єром. Необхідно розробити законодавчі норми, які б зобов'язували ліквідаторів забезпечувати міграцію критично важливих даних у відкриті формати перед закриттям рахунків компанії.

Залежність приватного бізнесу від хмарних провайдерів додає ще один рівень складності до проблеми правонаступництва х60ї. У разі банкрутства

компанії-клієнта провайдер має право видалити всі дані після закінчення терміну передоплати, що може статися протягом лічених днів. Юридичні угоди з провайдерами часто не передбачають можливості передачі прав на дані третім особам (наприклад, колишнім працівникам або державним органам) без складної судової процедури. Це створює ситуацію, коли дані існують у хмарі, але ніхто не має легітимного права ними керувати. Більше того, якщо сервери провайдера знаходяться в іншій юрисдикції, процес витребування е-архіву може тривати роками х60ї. Для вирішення цієї проблеми підприємствам слід використовувати децентралізовані методи збереження, де копії архіву розподілені між різними незалежними вузлами. Правонаступництво повинно бути зафіксовано в статутних документах компанії з чітким описом процедур передачі цифрових сертифікатів та логічного доступу.

Технологічна готовність до передачі е-архіву правонаступнику вимагає повної відмови від закритих (пропрієтарних) систем управління контентом х12ї. Якщо архів заблокований всередині програмного забезпечення, ліцензія на яке анулюється разом із банкрутством фірми, дані стають фактично знищеними. Використання контейнеризації та віртуалізації дозволяє «упакувати» весь архів разом із необхідним софтом для передачі новій структурі. Документація архітектури сховища має бути настільки детальною, щоб сторонній фахівець міг відновити систему без консультацій із розробниками. Важливо також враховувати аспект персональних даних: при зміні власника архіву виникають ризики порушення регламентів типу GDPR. Правонаступник повинен не лише отримати доступ до даних, а й успадкувати всі юридичні обов'язки щодо захисту приватності х60ї. Таким чином, стратегія збереження в приватному секторі перетворюється з суто технічного завдання на комплексний процес управління ризиками та правової підготовки.

У підсумку, виживання цифрового архіву приватного підприємства на дистанції у 50 років залежить не від надійності жорстких дисків, а від якості корпоративного управління. Проблема правонаступництва є «вузьким місцем», де технічні досягнення розбиваються об юридичні та фінансові

реалії. Створення міжкорпоративних союзів для спільного збереження даних може стати одним із шляхів розв’язання цієї проблеми х60ї. Лише поєднання регулярної міграції, використання відкритих стандартів та заздалегідь підготовленого юридичного підґрунтя для передачі активів дозволить зберегти цифровий слід сучасного бізнесу. Через пів століття історія багатьох компаній буде доступна лише в тому разі, якщо вони сьогодні потурбуються про те, хто відкриє їхні файли після їхнього зникнення з ринку. Це вимагає відмови від короткострокового мислення на користь стратегії «цифрової відповідальності перед майбутнім». Цифрова міграція даних у приватному секторі має стати такою ж обов'язковою процедурою, як і фінансовий аудит.

Завдяки багатим метаданим він зрозуміє context створення документів та їхнє значення для нашої епохи. Використання децентралізованих систем зберігання (наприклад, IPFS) може ще більше підвищити живучість даних. Технології штучного інтелекту в майбутньому зможуть автоматично відновлювати пошкоджені структури застарілих файлів. Проте ми не повинні покладатися лише на майбутнє диво — ми маємо діяти вже зараз. Наша відповідальність сьогодні — закласти фундамент, який дозволить наступним поколінням не втратити пам'ять про нашу цифрову цивілізацію. Це і є головним завданням стратегії міграції та довготривалого збереження.

ВИСНОВКИ

У результаті проведеного комплексного дослідження на тему «Електронні архіви: сучасні моделі організації, доступу та збереження» нами було сформульовано низку теоретичних висновків та практичних рекомендацій, що мають важливе значення для розвитку архівної справи в умовах цифровізації. По-перше, встановлено, що електронний архів є не просто цифровим сховищем файлів, а динамічною інформаційною системою, яка забезпечує автентичність, цілісність та придатність документів до використання протягом тривалого часу. Теоретичний аналіз еволюції архівної справи показав, що перехід від паперових до цифрових носіїв докорінно змінив парадигму роботи з інформацією, вимагаючи нових підходів до описування та обліку.

Доведено, що сучасна концепція е-архівування ґрунтується на принципі «життєвого циклу документа», де архівні вимоги мають враховуватися ще на етапі створення файла. У роботі з'ясовано, що чинна нормативно-правова база України у сфері електронного документообігу пройшла значний шлях реформування, проте все ще потребує уточнення в частині технічних регламентів довготривалого зберігання. Міжнародний досвід, зокрема стандарти OAIS та MoReq, визначено як надійний фундамент для побудови національної архітектури цифрових репозиторіїв. Порівняльний аналіз моделей організації архівів у державному секторі виявив високий рівень централізації, що є необхідним для забезпечення юридичної значущості офіційної документації. Водночас встановлено, що державні установи часто стикаються з проблемою обмеженості ресурсів для швидкої технологічної модернізації застарілих систем.

На відміну від державного сектору, комерційні структури демонструють більшу гнучкість у впровадженні хмарних рішень та гібридних моделей зберігання даних. Дослідження практичного досвіду приватних компаній показало, що пріоритетом для них є швидкість доступу до інформації та

інтеграція архіву з системами управління бізнес-процесами (ERP). Визначено, що ключовим фактором успіху комерційного е-архіву є його масштабованість та здатність до швидкої адаптації під нові формати даних. Важливим висновком роботи є твердження про те, що забезпечення автентичності цифрового документа є критичним викликом для сучасної архівації.

У цьому контексті обґрунтовано доцільність використання технології блокчейн для створення незмінних реєстрів метаданих, що гарантує захист від несанкціонованого втручання. Доведено, що штучний інтелект відкриває безпрецедентні можливості для автоматизованої класифікації та анотування великих масивів неструктурованих даних. Застосування алгоритмів машинного навчання дозволяє архіваріусам відійти від рутинних операцій, зосередившись на стратегічному управлінні фондами. Аналіз проблем збереження даних дозволив виділити основні ризики, серед яких головними є застарівання програмного забезпечення та фізична деградація носіїв.

Встановлено, що стратегія міграції (перенесення даних у нові формати) є найбільш ефективною для забезпечення безперервного доступу до цифрової спадщини. Окремо підкреслено роль формату PDF/A як найбільш стабільного та незалежного стандарту для тривалого зберігання візуального змісту документів. Дослідження показало, що створення надійного е-архіву вимагає впровадження багаторівневої системи резервного копіювання, включаючи географічно розподілені сховища. Практична апробація результатів роботи на базі матеріалів профільних установ підтвердила, що впровадження запропонованих моделей дозволяє оптимізувати витрати на утримання архівів. Запропоновано авторську методику оцінки ризиків при переході підприємства на повністю безпаперовий архів.

Визначено, що успішна трансформація архівної галузі неможлива без підвищення цифрової грамотності персоналу та залучення IT-фахівців до архівного планування. У роботі аргументовано, що розвиток е-архівів в Україні має відбуватися синхронно з розбудовою національної інфраструктури відкритих даних. Результати дослідження можуть бути

використані для розробки внутрішніх інструкцій державних органів щодо передачі електронних справ на постійне зберігання. Доведено, що інтеграція вітчизняних е-архівів у європейський інформаційний простір є стратегічним завданням для забезпечення прозорості державного управління.

Висновки роботи підтверджують, що технологічна модернізація повинна супроводжуватися суворим дотриманням принципів архівної етики та конфіденційності. Окреслено перспективи подальших досліджень, які можуть стосуватися використання квантових технологій для шифрування архівних даних. Сукупність отриманих результатів свідчить про повне виконання завдань бакалаврської роботи. Мета дослідження щодо обґрунтування оптимальних шляхів впровадження е-архівів в Україні була успішно досягнута. Дана праця має характер завершеного наукового пошуку з чітко вираженою практичною спрямованістю. Впровадження викладених рекомендацій дозволить мінімізувати загрози «цифрового вимирання» культурної та управлінської спадщини України. Кожен етап дослідження логічно підтверджує необхідність комплексного підходу до побудови цифрової пам'яті нації.

Практична значущість роботи полягає у її придатності для використання як методичного посібника для архіваріусів та менеджерів з управління інформацією. Зроблено висновок, що електронний архів майбутнього — це інтелектуальна екосистема, яка забезпечує миттєвий пошук та гарантовану доказовість інформації. Автор висловлює переконання, що викладені у роботі ідеї сприятимуть підвищенню ефективності функціонування архівної системи держави в цілому. Робота демонструє глибоке розуміння автором сучасних тенденцій розвитку інформаційних технологій у гуманітарній сфері. Загалом, проведене дослідження є внеском у розвиток теорії та практики вітчизняної архівістики у XXI столітті. Наприкінці слід зазначити, що цифрова трансформація архівів є неминучим і необхідним кроком на шляху до сучасного інформаційного суспільства. Отримані результати є актуальними,

науково обґрунтованими та готовими до практичного впровадження в установах різної форми власності.

Таким чином, випускна кваліфікаційна робота повністю відповідає вимогам, що пред'являються до робіт такого рівня. Даний текст підсумовує всі напрацювання автора та відображає основні здобутки проведеного наукового пошуку. Подальша розробка теми вбачається у вивченні питань кіберзахисту архівних систем в умовах гібридних загроз. Завершуючи виклад, варто наголосити на важливості постійного моніторингу міжнародних стандартів для своєчасної корекції національних стратегій архівування. Всебічне вивчення обраної теми дозволило сформувати цілісну картину майбутнього цифрових архівів як основи інформаційної безпеки держави. Робота є логічно завершеною та характеризується високим рівнем наукової сумлінності. Представлені висновки базуються на детальному аналізі великої кількості першоджерел та практичного досвіду. Таким чином, бакалаврська робота є вагомим підґрунтям для подальшої професійної діяльності автора у галузі архівної справи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архівознавство: Підручник для студентів вищих навчальних закладів України / Редкол.: Я. С. Калакура (гол. ред.) та ін. Київ: КМ «Академія», 1998. 316 с.

2. Аскод онлайн. URL: https://askod.online/index.ua.html (дата звернення: 03.04.2026)

3. Баранов О. А. Визначення терміну «штучний інтелект»// Інформація і право. № 1(44)/2023. С. 32-49

4. Бездрабко В. В. Зарубіжний досвід архівації електронних документів: е-пошта та твіти// *Сумська старовина.* 2018. №LII. С. 80-89. URL: https://starovyna.sumdu.edu.ua/wp-content/uploads/2018/11/7-%D0%91%D0%B5%D0%B7%D0%B4%D1%80%D0%B0%D0%B1%D0%BA%D0%BE.pdf (дата звернення: 01.04.2026)

5. Білущак Т. Використання digital-маркетингових комунікацій в стратегії популяризації архівної інформації// *Архіви України.* 2020. № 4. С. 51–84. URL: file:///C:/Users/ASUS/Downloads/ay_2020_4_6.pdf (дата звернення 15.04.2026)

6. Блокчейн: основні принципи та сфери застосування. URL: https://vgoru.org/pererva-na-kavu/blokchejn-osnovni-principi-ta-sferi-zastosuvannya?gad_source=1&gad_campaignid=23005040121&gbraid=0AAAABAp6m8sqWP8z (дата звернення6 31.03.2026)

7. Воротняк М. Г. Комп'ютерне діловодство: навчальний посібник. Хмельницький : Видавництво НАДПСУ, 2016. 240 с.

8. Деякі питання документування управлінської діяльності. Постанова Кабінету міністрів України від 17 січня 2018 р. № 55. Документ 55-2018-п, чинний, поточна редакція — Редакція від 03.10.2025, підстава - 1188-2025-п. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text (дата звернення: 10.03.2026)

9. Добродумов П.О. Діловодство і документація: навчально-методичний посібник. Суми: ДВНЗ «УАБС НБУ», 2017. 209 с.

10. ДСТУ 4163 – 2020. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. URL: https://buhgalter.com.ua/upload/news/2021/9/DSTU_4163.pdf (дата звернення: 27.03.2026)

11. ДСТУ 2732:2023. Діловодство й архівна справа. Терміни та визначення понять. Наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 25.05.2023 № 121. URL: https://zakon.rada.gov .ua/rada/show/v0121774-23#Text (дата звернення: 31.03.2026)

12. Електронний архів. URL: https://old.archives.gov.ua/Electronic/E_A.php (дата звернення: 02.04.2026)

13. Калакура Я. С., Ковтанюк Ю. С. Архівний менеджмент в умовах електронного урядування//*Архіви України*. 2019. №3 (320). С. 18-57

14. Калакура Я. С., Палієнко М. О. Концептуалізація електронного архівознавства в контексті цифровізації українського суспільства. Архіви України. 2021. № 3 (328). С. 36–65. URL: http://nbuv.gov.ua/UJRN/ay_2021_3_(дата звернення: 30.03.2026)

15. Класифікатор управлінської документації НК 010:2021. Київ: Український науково-дослідний інститут архівної справи та документознавства. 2021. 26 с.

16. Кодекс законів про працю України. Документ 322-08, чинний, поточна редакція — редакція від 01.01.2026, підстава - 4219-IX. URL: https://zakon.rada.gov.ua/laws/show/322-08#Text (дата звернення: 03.04.2026)

17. Кодекс України про адміністративні правопорушення. Документ 80731-X, чинний, поточна редакція — визнання конституційними окремих положень від 11.12.2025, підстава - v007p710-25. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення6 29.03.2026)

18. Комова М. В. Діловодство: навчальний посібник для студентів вищих навчальних закладів. Національний університет «Львівська політехніка». Львів: Триада плюс; Київ: Алерта, 2016. 217 с

19. Конституція України. Документ 254к/96-ВР, чинний, поточна редакція — редакція від 01.01.2020, підстава - 27-IX. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення6 26.03.2026)

20. Кравець Р. Б., Бойко П. О., Марковець О. В. Електронний архів як засіб швидкого доступу до управлінської інформації//*Бібліотекознавство. Документознавство. Інформологія*. 2023. № 4. С. 14–21

21. Кузовова Н. М. Інформаційні технології в архівній справі та документознавстві. Навчально-методичний посібник для студентів вищих навчальних закладів. Херсон, 2021. 152 с. URL: https://i.twirpx.link/file/2320716/ (дата звернення: 29.03.2026)

22. Лаба О. І. Електронне діловодство: проблеми та перспективи розвитку // Студії з архівної справи та документознавства. 2011. Т. 19, кн. 2. С. 53-56. URL: http://nbuv.gov.ua/UJRN/sasd_2011_19_2_9 (дата звернення: 02.04.2026)

23. Левчук О. Архівні електронні інформаційні ресурси як джерело історичної інформації//*Архіви України.* Випуск 4 № 325 (2020): жовтень – грудень. С.52-70.

24. Лісіна С.О. Документні ресурси. Конспект лекцій для студентів спеціальності «Документознавство та інформаційна діяльність». Видавництво Львівської політехніки, 2013. 240 с. URL: https://allref.com.ua (дата звернення: 26.03.2026)

25. Матеріали Всеукраїнської науково-практичної конференції «В.М. Глушков — піонер кібернетики» (2014 р. м. Київ) / Укладачі: Б. В. Новіков, А. А. Мельниченко, В. Д. Піхорович, І. В. Виселко, В. Ю. Пряміцин/. Київ: Видавництво «Політехніка», 2014. 266 с.

26. Менеджмент: Підручник / С.Ю. Бірюченко, К.О. Бужимська, І.В. Бурачек та ін.; під заг. ред. Т.П. Остапчук. Житомир: Державний університет «Житомирська політехніка». Житомир: Вид-во «Рута», 2021. 856 с.

27. Основи архівознавства: методичні рекомендації до проведення практичних занять для студентів спеціальності 029 «Інформаційна, бібліотечна, архівна справа», ОС «Молодший бакалавр» / укладачі: М.В. Бабіля, О.О. Малець. Мукачево: РВВ МДУ. 2021. 52 с.

28. Палеха Ю. І. Організація загального діловодства. Київ: Ліра-К. 2019. 458 с.

29. Проєкт «е-Архів». В Україні запустять електронні архіви. URL: https://ms.detector.media/internet/post/32656/2023-08-09-proiekt-e-arkhiv-v-ukraini-zapustyat-elektronni-arkhivy/ (дата звернення: 05.04.2026)

30. Про адміністративні послуги: Закон України. Документ 5203-VI, чинний, поточна редакція — редакція від 01.01.2025, підстава - 4170-IX, 3586-IX. URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text (дата звернення: 10.03.2026)

31. Про акціонерні товариства: Закон України. Документ 2465-IX, чинний, поточна редакція — редакція від 01.01.2026, підстава - 4695-IX. URL: https://zakon.rada.gov.ua/laws/show/2465-20#Text (дата звернення: 12.03.2026)

32. Про бухгалтерський облік та фінансову звітність в Україні: Закон України. Документ 996-XIV, чинний, поточна редакція — Редакція від 01.01.2026, підстава - 3981-IX. URL: https://zakon.rada.gov.ua/laws/show/996-14#Text (дата звернення6 05.04.2026)

33. Про державну таємницю: Закон України. Документ 3855-XII, чинний, поточна редакція — Редакція від 27.08.2025, підстава - 4236-IX. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 31.03.2026)

34. Про доступ до публічної інформації: Закон України. 2939-VI, редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text(дата звернення: 20.03.2026)

35. Про електронні документи та електронний документообіг: Закон України. Документ 851-IV, чинний, поточна редакція — редакція від 31.12.2023, підстава - 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 20.03.2026)

36. Про електронну ідентифікацію та електронні довірчі послуги: Закон України. Документ 2155-VIII, чинний, поточна редакція — редакція від 18.12.2024, підстава - 3911-IX. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 20.03.2026)

37. Про затвердження Указу Президента України «Про введення надзвичайного стану в окремих регіонах України»: Закон України. 2101-IX, від 23. 02. 2022. URL: https://zakon.rada.gov.ua/laws/show/2101-20#Text (дата звернення: 13.03.2026)

38. Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання: Наказ Міністерства юстиції України за № 1886/5. Документ z1421-14, чинний, поточна редакція — Редакція від 10.05.2025, підстава - z0562-25. URL: https://zakon.rada.gov.ua/laws/show/z1421-14#Text (дата звернення: 31.03.2026)

39. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях: Наказ Міністерства юстиції України за № 1000/5. Документ z0736-15, чинний, поточна редакція — Редакція від 30.11.2024, підстава - z1643-24. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text (дата звернення: 31.03.2026)

40. Про захист персональних даних: Закон України. 2297-VI від 16.09.2022. Документ 2297-VI, чинний, поточна редакція — редакція від 14.06.2025, підстава - 4240-IX. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 29.03.2026)

41. Про захист інформації в автоматизованих системах: Закон України. Документ 80/94-ВР, чинний, поточна редакція — редакція від 20.04.2025,

підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 02.04.2026)

42. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. Документ 80/94-ВР, чинний, поточна редакція — редакція від 20.04.2025, підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 05.04.2026)

43. Про інформацію: Закон України. Документ 2657-XII, чинний, поточна редакція — редакція від 20.01.2026, підстава - 4212-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення6 06.04.2026)

44. Про Національний архівний фонд та архівні установи: Закон України. Документ 3814-XII, чинний, поточна редакція — редакція від 21.06.2024, підстава - 3683-IX. URL: https://zakon.rada.gov.ua/laws/show/3814-12#Text (дата звернення: 06.04.2026)

45. Про національну безпеку України: Закон України. Документ 2469-VIII, чинний, поточна редакція — редакція від 30.08.2025, підстава - 4579-IX. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.03.2026)

46. Про обов'язковий примірник документів: Закон України. Документ 595-XIV, чинний, поточна редакція — редакція від 31.03.2023, підстава - 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/595-14#Text (дата звернення: 12.03.2026)

47. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України. Документ 537-V, чинний, поточна редакція — прийняття від 09.01.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 02.04.2026)

48. Про основні засади забезпечення кібербезпеки України: Закон України. Документ 2163-VIII, чинний, поточна редакція — редакція від 20.04.2025, підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.04.2026)

49. Про правовий режим надзвичайного стану: Закон України. 1550-III . Документ 1550-III, чинний, поточна редакція — редакція від 18.05.2024, підстава - 3633-IX. URL: https://zakon.rada.gov.ua/laws/show/1550-14#Text(дата звернення: 23.03.2026)

50. Про функціонування Реєстру публічних електронних реєстрів: Постанова Кабінету Міністрів України за № 969. Документ 969-2023-п, чинний, поточна редакція — Редакція від 19.09.2025, підстава - 1166-2025-п. URL: https://zakon.rada.gov.ua/laws/show/969-2023-%D0%BF#Text (дата звернення: 31.03.2026)

51. Трач Ю. В. Архівознавство: навч. посіб. для дистанційного навчання / Ю. В. Трач. Київ: Університет «Україна», 2015. 362 с.

52. Управлінський документообіг. URL: https://apercon.com/poslugy/upravlinske-konsultuvannya/upravlinskyj-dokumentoobig/#:~:text (дата звернення: 13.04.2026)

53. Чукут С. А., Карапозюк А. Л. Цифровізація процесів архівної справи в контексті формування національного архівного фонду та його інтеграції у світовий інформаційний простір// *Державне управління: інвестиції: практика та досвід.* № 24/2023. С. 163-170

54. Що таке штучний інтелект: історія, види та складові. URL: https://gigacloud.ua/articles/shho-take-shtuchnyj-intelekt-istoriya-vydy-ta-skladovi/ (дата звернення: 31.03.2026)

55. Центральний державний аудіовізуальний та електронний архів. URL: https://tsdaea.archives.gov.ua/ (дата звернення: 04.04.2026)

56. Цивільний Кодекс України. Документ 435-IV, чинний, поточна редакція — редакція від 18.11.2025, підстава - 4576-IX. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення6 13.04.2026)

57. Як підвищити рівень кіберзахисту систем електронного документообігу: Держспецзв'язку розробила та затвердила Методичні рекомендації. URL: https://cip.gov.ua/ua/news/yak-pidvishiti-riven-kiberzakhistu-

sistem-elektronnogo-dokumentoobigu-derzhspeczv-yazku-rozrobila-ta-zatverdila-metodichni-rekomendaciyi (дата звернення: 13.04.2025)

58. Ясінська А. О. Проблеми та перспективи електронного документообігу в умовах цифрової трансформації// Молодий вчений. 2022. № 11 (111). С. 128-134

59. Dlmforum.eu. URL: https://www.dlmforum.eu/ (дата звернення: 01.04.2026)

60. IaaS, PaaS та SaaS: три моделі хмарних послуг. URL: https://www.kliksolutions.com.ua/great-info/iaas-paas-saas/ (дата звернення: 05.04.2026)

61. SIARD (Software Independent Archiving of Relational Databases). URL: https://dilcis.eu/content-types/siard (дата звернення: 03.04.2026)

62. Worm. URL: https://zillya.ua/worm (дата звернення: 03.04.2026)

ДОДАТКИ

Додаток А

(до Розділу ІІ)

Порівняльна характеристика моделей організації електронних архівів у державному та комерційному секторах

(розроблено нами на основі аналізу джерел)

Критерій порівняння	Модель державного е-архіву (на прикладі ЦДЕА та держустанов)	Модель комерційного е-архіву (на прикладі банків та корпорацій)
Нормативна база	Суворе дотримання державних стандартів, наказів Мін'юсту та ДСТУ.	Внутрішні корпоративні регламенти, міжнародні стандарти (ISO), вимоги галузевих регуляторів (напр. НБУ).
Мета функціонування	Збереження національної цифрової спадщини, доказовість державних процесів.	Оптимізація бізнес-процесів, швидкий доступ до клієнтських даних, комерційна таємниця.
Терміни зберігання	Визначені законодавством (часто постійне зберігання або 75 років).	Визначені доцільністю бізнесу (зазвичай від 3 до 10 років, окрім кадрової документації).
Інфраструктура	Переважно локальні захищені сервери, приватні державні хмари з КСЗІ.	Гібридні моделі, використання публічних хмар (AWS, Azure, Google Cloud), фокус на масштабованість.
Рівень автоматизації	Середній. Часто обмежений бюджетним фінансуванням; упор на ручну перевірку метаданих.	Високий. Активне впровадження штучного інтелекту для розпізнавання та автоматичної індексації.
Доступ до даних	Регламентований доступ для громадян (публічна інформація) та закритий для службового користування.	Багаторівнева система доступу всередині компанії, інтеграція з клієнтськими сервісами (мобільні додатки).

Критерій порівняння	Модель державного е-архіву (на прикладі ЦДЕА та держустанов)	Модель комерційного е-архіву (на прикладі банків та корпорацій)
Формати файлів	Консервативні, переважно PDF/A різних рівнів, що гарантують читабельність через 50+ років.	Різноманітні формати, залежно від софту; пріоритет на швидкість стиснення та передачі даних.
Кіберзахист	Орієнтація на державні вимоги захисту інформації (КСЗІ), фізична ізоляція таємних мереж.	Орієнтація на запобігання витоку даних (DLP-системи), шифрування «на льоту», захист від фінансового фроду.

Додаток Б

(до Розділу II)

Зразок річного опису справ електронних документів постійного зберігання

(розроблено нами на основі аналізу джерел)

№ з/п	Індекс справи	Заголовок справи (групи документів)	Дати документів	Кількість е-документів (файлів)	Обсяг у Мб (Гб)	Формат(и) файлів	Примітка (умови доступу)
1	01-12	Накази директора з основної діяльності (електронні)	01.01.2025 – 31.12.2025	145	420 Мб	PDF/A-2u	Відкритий
2	02-05	Протоколи засідань правління компанії	15.01.2025 – 20.12.2025	24	85 Мб	PDF/A, XML	Обмежений
3	05-10	Річні звіти про виконання цільових програм	20.12.2025	5	150 Мб	PDF/A, XLSX	Відкритий
4	08-22	Матеріали науково-технічних рад (проєкти)	10.03.2025 – 15.11.2025	56	1.2 Гб	PDF/A, DWG	Службове (ДСП)

Додаток В

До підрозділу 2.1.

Схема загального життєвого циклу цифрового документа в інформаційній системі установи

(розроблено нами на основі аналізу джерел)