ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ
ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: **« ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ СИСТЕМ АРХІВНОЇ БЕЗПЕКИ В УМОВАХ ДИДЖИТАЛІЗАЦІЇ»**

на здобуття освітнього ступеня бакалавра
зі спеціальності 029 Бібліотечна, інформаційна та архівна справа
освітньо-професійної програми Документознавство та інформаційна діяльність

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

_____ Аліна ШВАБ

Виконала: Аліна ШВАБ
здобувачка вищої освіти
гр. ДЗД-41

Керівник: Леся КОВАЛЬСЬКА
доктор історичних наук, професор

Рецензент: Ірина П’ЯТНИЦЬКОВА
кандидат історичних наук, доцент

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності
Ступінь вищої освіти бакалавр
Спеціальність 029 Бібліотечна, інформаційна та архівна справа
Освітньо-професійна програма Документознавство та інформаційна діяльність

ЗАТВЕРДЖУЮ
Завідувач кафедри документознавства та інформаційної діяльності
_____ Тетяна СИДОРЕНКО
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Шваб Аліни Олександрівни

1. Тема кваліфікаційної роботи «Тенденції розвитку архівної безпеки в умовах диджиталізації», керівник кваліфікаційної роботи проф., д.і.н. Ковальська Леся Андріївна професор кафедри документознавства та інформаційної діяльності, затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 р. № 56.
2. Строк подання кваліфікаційної роботи «16» травня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:

Мета роботи – проаналізувати сучасні тенденції розвитку архівної безпеки в умовах цифровізації, визначити основні загрози та виклики, а також запропонувати шляхи удосконалення системи захисту архівної інформації в цифровому середовищі.

Об'єкт роботи – система архівів в Україні в умовах диджиталізації.

Предмет дослідження – організаційні, правові та технічні аспекти забезпечення архівної безпеки в цифровому середовищі, зокрема, в діяльності ТОВ «4В Україна».

Короткий зміст роботи: У роботі розкрито теоретичні основи архівної безпеки, досліджено вплив диджиталізації на архівну сферу, проаналізовано загрози електронному архівному середовищу (кібербезпека, автентичність, збереження електронних документів). Розглянуто міжнародний досвід і визначено перспективні напрями розвитку архівної безпеки в Україні. Запропоновано практичні рекомендації щодо її удосконалення. **Ключові слова:** архівна безпека, диджиталізація, електронні документи, цифрові архіви, кібербезпека, автентичність.

4. Перелік питань, які потрібно розробити:
   1. Поняття та складові архівної безпеки в умовах цифрової трансформації
   2. Особливості забезпечення безпеки електронних архівів
   3. Загрози та ризики для архівної інформації у цифровому середовищі
5. Перелік ілюстративного матеріалу: презентація, додатки.
6. Дата видачі завдання «26» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Визначення тематики, вибір наукового керівника, уточнення теми	18.09.2024	
2	Розроблення та складання плану кваліфікаційної бакалаврської роботи	26.09.2024	
3	Підготовка 1 розділу	07.01.2025	
4	Підготовка 2 розділу	22.04.2025	
5	Підготовка 3 розділу	01.05.2025	
6	Висновки	09.04.2025	
7	Підготовка остаточного варіанта роботи	12.05.2025	
8	Написання відгуку науковим керівником	14.05.2025	
9	Оформлення й представлення роботи на кафедру та перевірка на плагіат	16.05.2025	
10	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	20.05.2025	
11	Попередній захист роботи	26.05.2025	
12	Основний захист кваліфікаційної бакалаврської роботи	18.06.2025	

Здобувачка вищої освіти Аліна ШВАБ

Керівник
кваліфікаційної роботи Леся КОВАЛЬСЬКА

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 69 стор., 38 джерел.

Мета кваліфікаційної роботи – проаналізувати сучасні тенденції розвитку архівної безпеки в умовах цифровізації, визначити основні загрози та виклики, а також запропонувати шляхи удосконалення системи захисту архівної інформації в цифровому середовищі. **Об'єктом дослідження** є система архівів в Україні в умовах диджиталізації. **Предметом дослідження** – організаційні, правові та технічні аспекти забезпечення архівної безпеки в цифровому середовищі, зокрема, в діяльності ТОВ «4В Україна».

Короткий зміст роботи. У роботі розглядаються теоретичні засади архівної безпеки, а також вплив процесів диджиталізації на архівну сферу. Проаналізовано потенційні загрози цифровому архівному середовищу, зокрема питання кібербезпеки, автентичності та збереження електронних документів. Окрему увагу приділено міжнародному досвіду в забезпеченні архівної безпеки та можливостям його адаптації в Україні. На основі аналізу запропоновано практичні рекомендації щодо удосконалення системи архівної безпеки в умовах цифрової трансформації.

Ключові слова: архівна безпека, диджиталізація, електронні документи, інформаційна безпека, цифрові архіви, кіберзагрози, автентичність.

ЗМІСТ

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій архівна справа зазнає суттєвих змін, зумовлених диджиталізацією процесів зберігання, обробки та захисту інформації. Трансформація традиційних підходів до архівування в електронному середовищі вимагає нового погляду на архівну безпеку як невід'ємну складову інформаційної безпеки підприємств. В умовах зростаючого обсягу даних, постійних кіберзагроз, підвищення вимог до законності, конфіденційності та довготривалого збереження цифрових документів питання надійного захисту архівної інформації набуває особливої актуальності. Саме тому модернізація архівних систем, впровадження технологічних рішень та розробка ефективних політик захисту даних стають одним із пріоритетів для будь-якої організації, що прагне відповідати сучасним викликам цифрового середовища.

Актуальність дослідження зумовлена тим, що в умовах диджиталізації більшість підприємств переходять до електронного документообігу, при цьому значна частина архівної документації не має належного рівня захисту. Відсутність уніфікованих стандартів, недостатній рівень технічного забезпечення, низька культура інформаційної безпеки, а також постійні ризики несанкціонованого доступу або втрати документів унаслідок збоїв техніки чи дій зловмисників створюють реальні загрози для стабільної роботи організацій. В умовах, коли цифровий архів виконує не лише інформаційно-довідкову, але й правову, доказову та управлінську функції, питання його захищеності перетворюється на стратегічне.

Мета дослідження – проаналізувати сучасні тенденції розвитку архівної безпеки в умовах цифровізації, визначити основні загрози та виклики, а також запропонувати шляхи удосконалення системи захисту архівної інформації в цифровому середовищі.

Завдання дослідження:

1. розкрити сутність поняття архівної безпеки та її складових у контексті цифрової трансформації;

2. окреслити основні загрози архівній інформації в цифровому середовищі;

3. проаналізувати нормативно-правову базу, що регламентує архівну безпеку в Україні;

4. дослідити міжнародний і вітчизняний досвід впровадження систем архівної безпеки;

5. вивчити практику архівування та цифрового захисту документів у ТОВ «4В Україна»;

6. ідентифікувати проблеми цифрової архівної безпеки на підприємстві та оцінити ризики;

7. сформувати стратегію модернізації архівної системи та надати практичні рекомендації щодо її вдосконалення.

Об’єктом дослідження є система архівів в Україні в умовах диджиталізації.

Предметом дослідження є організаційні, правові та технічні аспекти забезпечення архівної безпеки в цифровому середовищі, зокрема, в діяльності ТОВ «4В Україна».

Практична значущість роботи полягає у можливості застосування її результатів для побудови ефективної системи цифрової архівної безпеки на підприємствах різного масштабу. Вибір ТОВ «4В Україна» як бази дослідження дозволив здійснити прикладний аналіз цифрових архівних практик у реальному бізнес-середовищі, оцінити їх ефективність та визначити потенціал для вдосконалення.

У **структурі роботи** передбачено три розділи: у першому висвітлено теоретичні основи архівної безпеки в умовах диджиталізації, у другому — проаналізовано зарубіжний і вітчизняний досвід впровадження відповідних технологій, у третьому — здійснено практичне дослідження архівної системи ТОВ «4В Україна» та запропоновано конкретні кроки щодо її вдосконалення.

РОЗДІЛ 1
ТЕНДЕНЦІЇ РОЗВИТКУ АРХІВНОЇ БЕЗПЕКИ В УМОВАХ ДИДЖИТАЛІЗАЦІЇ

1.1. Поняття та складові архівної безпеки

Архівна безпека у сучасних умовах диджиталізації набуває особливого значення, оскільки збереження, захист і достовірність архівної інформації стають критично важливими аспектами функціонування як державних, так і приватних інформаційних систем. Під поняттям архівної безпеки традиційно розуміють сукупність організаційних, правових, технічних і технологічних заходів, спрямованих на забезпечення збереження, цілісності, доступності, автентичності та конфіденційності архівної інформації незалежно від її матеріального носія. У більш вузькому розумінні архівна безпека – це комплекс захисних заходів, спрямованих на запобігання втратам, пошкодженню, несанкціонованому доступу або підміні архівних документів, особливо тих, що мають історичну, наукову або юридичну цінність.

У сучасному науковому дискурсі архівна безпека розглядається як складова частина загальної інформаційної безпеки, що, своєю чергою, є елементом національної безпеки. У цьому контексті особлива увага приділяється як державному контролю за збереженням архівної спадщини, так і корпоративній відповідальності суб’єктів господарювання за збереження внутрішньої архівної інформації, що може містити як комерційні, так і персональні дані. Особливої актуальності набуває захист архівів в умовах переходу від традиційного, паперового, до електронного документообігу. Цифровізація значно полегшує доступ до інформації, проте одночасно створює нові вектори ризику, пов’язані з кібератаками, втратами даних унаслідок технічних збоїв, знищенням цифрових носіїв, недосконалістю систем резервного копіювання тощо [12].

Складові архівної безпеки охоплюють кілька взаємопов’язаних блоків. Першою базовою складовою є фізична безпека, яка включає в себе умови зберігання документів, протипожежний захист, захист від затоплення, температурно-вологісний режим, наявність охоронної сигналізації тощо. У випадку з цифровими архівами фізична безпека стосується також серверних приміщень, де зберігаються бази даних, резервних сховищ, а також персональних комп’ютерів працівників, що мають доступ до архівної інформації.

Наступною складовою є інформаційна безпека архівів, яка пов’язана з технічним захистом інформації: антивірусні засоби, фаєрволи, системи контролю доступу, шифрування даних, багатофакторна автентифікація тощо. До цього блоку належать також методи виявлення несанкціонованих змін у даних, журналювання доступу, моніторинг активності користувачів у системах архівування. Інформаційна безпека особливо важлива в умовах дистанційного доступу до електронних архівів, що стає нормою в диджиталізованих організаціях.

Юридична складова архівної безпеки передбачає дотримання чинного законодавства у сфері збереження інформації, захисту персональних даних, дотримання строків зберігання документів, регламентів архівування та передачі документів до відповідних архівних установ. З цієї точки зору важливим елементом є інструкції з діловодства, положення про архів організації, а також контракти з провайдерами електронних архівних послуг, якщо мова йде про зберігання в хмарних сховищах.

Організаційна складова включає систему управління архівною безпекою: розподіл повноважень, наявність відповідальних осіб за архівування, розробку та впровадження політик з безпеки, навчання персоналу, внутрішній аудит і перевірки систем захисту. Організаційна безпека також охоплює процедури реагування на інциденти, резервного копіювання та відновлення даних, оцінку ризиків і побудову моделі загроз. У великих організаціях ця складова часто реалізується через підрозділи інформаційної безпеки або архівні служби з чітко регламентованими процедурами [5].

Технологічна складова архівної безпеки пов’язана із застосуванням сучасних ІТ-рішень для організації цифрових архівів: систем управління документами (DMS), цифрових сховищ, програмного забезпечення для опрацювання архівних масивів, алгоритмів цифрового підпису, штучного інтелекту для категоризації документів, інструментів метаданих тощо. Важливо, що технології не лише автоматизують процеси, а й створюють додаткові засоби контролю та захисту. Наприклад, застосування блокчейн-рішень дозволяє забезпечити незмінність архівної інформації, а системи штучного інтелекту – швидке виявлення аномалій у документах.

Ще однією складовою є етична й соціальна безпека, яка охоплює принципи доступу до інформації, повагу до приватності, уникнення маніпуляцій архівною інформацією. Архіви можуть містити дані, що стосуються не лише конкретних організацій, а й третіх осіб, тому особливо важливою є культура відповідального поводження з архівами. Відповідно до положень Закону України «Про захист персональних даних», обробка архівної інформації повинна здійснюватися з урахуванням прав суб’єктів даних.

У контексті міжнародних стандартів, архівна безпека розглядається крізь призму стандартів ISO, зокрема: ISO 15489 (управління документами), ISO 27001 (інформаційна безпека), ISO 14721 (Open Archival Information System – OAIS), які формують глобальні вимоги до архівування, автентичності, доступності та довгострокового зберігання інформації. У багатьох країнах ці стандарти адаптовані до національного законодавства, і їх дотримання є передумовою ефективного впровадження цифрової архівної безпеки.

Таким чином, архівна безпека в умовах цифрової трансформації розширюється від традиційного розуміння збереження паперових документів до комплексної багаторівневої системи, яка охоплює інформаційно-технологічні, організаційні, нормативні, фізичні та соціальні аспекти. Забезпечення архівної безпеки вимагає від організацій розробки та реалізації цілісних політик, постійного оновлення засобів захисту, інтеграції з ІТ-інфраструктурою та формування культури відповідального поводження з інформацією. Успішне вирішення цих завдань стає запорукою збереження як історичної пам’яті, так і

поточної ділової документації, що має юридичну, адміністративну чи комерційну цінність [23].

1.2. Види загроз архівній інформації в цифровому середовищі

У цифровому середовищі архівна інформація зазнає якісно нових загроз, які значно відрізняються від традиційних ризиків, притаманних паперовим архівам. Цифровізація документообігу, автоматизація управлінських процесів та зростання обсягів електронної інформації спричинили появу низки специфічних уразливостей, які потребують ретельного вивчення, класифікації та запровадження ефективних механізмів протидії. Архівна інформація в цифровій формі є одночасно мобільнішою, доступнішою і водночас більш вразливою через залежність від технічних систем, мережевої інфраструктури та програмного забезпечення. У цьому контексті надзвичайно важливо розуміти природу загроз, які ставлять під сумнів цілісність, автентичність, доступність та довгострокове зберігання архівних документів.

Першою і однією з найпоширеніших загроз є технічні збої та знос носіїв інформації. Незважаючи на уявну надійність цифрових технологій, жорсткі диски, флеш-накопичувачі, оптичні диски, магнітні стрічки, сервери мають обмежений термін експлуатації. Їх фізичне зношення призводить до втрати або пошкодження архівної інформації. Проблема посилюється у випадках, коли архіви зберігаються лише на одному носії, без системи резервного копіювання. Крім того, електронні носії можуть зазнати впливу зовнішніх чинників – перепадів напруги, перегріву, вологості або механічних пошкоджень, які призводять до фізичної втрати інформації.

Другою категорією є програмні ризики, які охоплюють збої у програмному забезпеченні, несумісність форматів, помилки при міграції даних, а також застарілість технологій. З часом формати файлів та платформи для зберігання архівної інформації можуть втратити підтримку або стати непридатними для читання. Наприклад, старі версії програм для обробки текстових документів, таблиць, баз даних більше не підтримуються сучасними операційними

системами або не відкриваються без втрати даних. Це унеможливлює доступ до історично цінної інформації або створює ризик її викривлення. У випадку автоматизованих систем управління архівами (АСУА) проблеми з оновленням або ліцензуванням можуть спричинити втрату функціональності архівної платформи [21].

Наступною серйозною загрозою є людський фактор, який охоплює як навмисні дії (саботаж, крадіжка даних, несанкціоноване копіювання), так і ненавмисні помилки (випадкове видалення, неправильне введення даних, порушення регламентів зберігання тощо). Через недотримання інструкцій працівниками архівних служб може відбутися стирання важливої інформації або її викривлення. Зокрема, архівні системи можуть містити можливості редагування чи видалення без відповідного журналювання, що створює ризики непомітної підміни чи втрати цифрових записів. Крім того, нестача підготовки персоналу до роботи з електронними архівами сприяє виникненню помилок у процесі сканування, індексування та ідентифікації документів.

Окремо слід виділити кіберзагрози як одну з найсерйозніших проблем сучасної архівної безпеки. Зростання кіберзлочинності призвело до появи нових векторів атак: несанкціонований доступ до архівів, шкідливе програмне забезпечення (віруси, трояни, програми-вимагачі), DDoS-атаки на архівні сервери, фішинг персоналу архівів з метою викрадення паролів тощо. Архівна інформація, яка містить конфіденційні дані або документи з відкладеною юридичною силою, є об’єктом підвищеного інтересу для хакерів. Злочинці можуть маніпулювати інформацією, змінювати її вміст або блокувати доступ до архівів із вимогою викупу. Особливо небезпечними є атаки на хмарні сервіси зберігання, які можуть спричинити витоки великих обсягів даних.

Інформаційні загрози також стосуються питань автентичності та цілісності документів. У цифровому середовищі значно легше здійснити фальсифікацію або підміну документів без очевидних ознак втручання. Якщо система архівування не забезпечує фіксацію метаданих, контроль версій, електронні підписи або цифрові сертифікати, правдивість та первинність документів стає складно довести. Втрата або підміна навіть одного архівного запису може

призвести до серйозних юридичних або історичних наслідків, особливо якщо йдеться про архіви, що мають офіційний характер.

Загрози доступності охоплюють ризики тимчасової або тривалої недоступності архівів. Вони можуть виникати внаслідок перебоїв в електропостачанні, виходу з ладу серверного обладнання, збоїв в Інтернет-з'єднанні або втрати логістичних ланцюгів у випадках децентралізованого зберігання. Недоступність інформації в критичний момент може завдати суттєвої шкоди діяльності установи, призвести до зупинки адміністративних чи фінансових процесів, неможливості підтвердження прав чи зобов'язань. У сфері державного управління або судочинства це може вплинути на долю рішень або правових процесів [3].

Юридичні загрози стосуються порушення норм зберігання та обробки архівної інформації, невиконання вимог законодавства щодо захисту персональних даних або строків зберігання, що може призвести до штрафів, втрати ліцензії, судових позовів. Наприклад, зберігання архівної інформації на незахищених серверах або передача третім особам без відповідного правового регулювання може трактуватись як порушення вимог GDPR або українського законодавства. В умовах посилення контролю за інформаційною політикою підприємств та установ дотримання правових норм є критичним компонентом архівної безпеки.

Культурні та етичні загрози в цифровому середовищі пов'язані з маніпуляціями змістом архівної інформації, цензурою, навмисним стиранням або приховуванням фактів, що спотворює історичну правду або призводить до знищення важливих суспільних доказів. Оцифровка архівів без фахового контролю, без дотримання принципу автентичності, може призвести до втрати історичної правдивості. Також існує ризик втрати контексту архівного документа, якщо метадані не будуть повноцінно відтворені або збережені у цифровому форматі. Це особливо важливо для архівів, які мають наукову або культурну цінність.

Економічні загрози виникають через недофінансування процесів архівної цифровізації та забезпечення безпеки. Висока вартість ліцензованого

програмного забезпечення, сертифікованих серверів, резервного копіювання, навчання персоналу – все це є бар'єрами для впровадження надійних систем архівної безпеки. У малих організаціях або регіональних установах часто спостерігається використання застарілого обладнання або відкритого ПЗ з низьким рівнем захисту, що робить архіви надзвичайно вразливими до багатьох типів загроз.

Отже, у цифровому середовищі архівна інформація піддається комплексному впливу низки загроз, які потребують постійного моніторингу, аналізу ризиків та впровадження багаторівневої системи захисту. Ефективна система архівної безпеки повинна поєднувати технічні, програмні, організаційні, правові та етичні заходи, ґрунтуючись на міжнародних стандартах та адаптованих національних підходах. Знання природи загроз і вміння прогнозувати їх вплив є основою для формування стійкої та надійної системи архівного зберігання в епоху цифрової трансформації [10].

1.3. Нормативно-правова база архівної безпеки в Україні

Нормативно-правова база архівної безпеки в Україні є комплексом взаємопов'язаних законодавчих, підзаконних, інституційних та методичних документів, які визначають правові засади створення, ведення, зберігання, захисту, доступу та використання архівної інформації, як у паперовому, так і в електронному вигляді. У зв'язку з активним переходом держави, бізнесу та суспільства до цифрових форматів документообігу, питання архівної безпеки отримують нову нормативну актуалізацію, оскільки виникає потреба не лише в регламентації зберігання та доступу до інформації, але й у визначенні вимог до цифрових форматів, електронних підписів, резервного копіювання, кіберзахисту та збереження автентичності документів у цифровому середовищі.

Базовим законодавчим актом у цій сфері є Закон України «Про Національний архівний фонд та архівні установи» №3814-XII від 24 грудня 1993 року (в редакції з урахуванням останніх змін). Цей закон визначає основні принципи формування, зберігання та використання Національного архівного

фонду (НАФ), окреслює статус архівних установ, категорії документів, що підлягають обов'язковому зберіганню, а також права та обов'язки громадян та юридичних осіб щодо доступу до архівної інформації. У контексті архівної безпеки надзвичайно важливими є положення закону, що стосуються забезпечення збереженості документів незалежно від їх носія, а також вимоги до їх реєстрації, опису, передачі до архівних установ, строків зберігання тощо.

Значну роль у нормативному регулюванні архівної безпеки відіграє Закон України «Про інформацію» (із змінами), який визначає правові засади доступу до інформації, її збереження, обмеження поширення певних категорій даних, зокрема тих, що становлять державну, службову або комерційну таємницю. Архіви часто містять конфіденційну або обмежену інформацію, що підлягає спеціальному захисту. Закон визначає принципи обробки інформації, правові механізми контролю за її використанням, встановлює режим відкритості та обмеження доступу. Водночас архівна інформація, яка створюється органами державної влади, як правило, має публічний статус після закінчення строку її обмеженого доступу.

Із розвитком цифрових форматів документообігу надзвичайно важливим став Закон України «Про електронні документи та електронний документообіг». Цей документ вводить у правове поле поняття електронного документа, електронного цифрового підпису, електронного архіву, а також встановлює вимоги до створення, зберігання, автентичності, юридичної сили та доступності електронних документів. Відповідно до нього, електронний документ є повноцінним аналогом паперового і має юридичну силу за умови дотримання технічних і правових вимог. Цей закон є ключовим для регламентації цифрової архівної безпеки, оскільки визначає основні механізми фіксації, верифікації та зберігання електронних записів.

Також важливе значення має Закон України «Про електронні довірчі послуги», який регулює порядок використання електронних підписів, печаток, часових міток, засобів автентифікації, що забезпечують довгострокову цілісність та автентичність архівних електронних документів. Електронна довірча інфраструктура є наріжним каменем цифрової архівної безпеки, оскільки

дозволяє перевірити походження, незмінність і чинність архівної інформації навіть через тривалий час після її створення.

У сфері захисту персональних даних, що також є важливим компонентом архівної інформації, слід зазначити Закон України «Про захист персональних даних». Цей нормативно-правовий акт встановлює вимоги до обробки персональної інформації, порядок отримання згоди на її зберігання, передачу та обробку, а також визначає обов'язки розпорядників і володільців персональних даних. Архівні системи, які містять персональні дані фізичних осіб, повинні забезпечувати їх конфіденційність, контроль доступу, технічний захист та можливість вилучення за запитом відповідної особи. Це особливо актуально для архівів органів соціального захисту, охорони здоров'я, освіти тощо [7].

Нормативну базу деталізують численні постанови Кабінету Міністрів України, накази Міністерства юстиції, Державної архівної служби та інших центральних органів виконавчої влади. Серед них ключовими є «Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затверджені наказом Міністерства юстиції України №1000/5 від 18.06.2015 року. Цей документ регламентує порядок ведення справ, формування номенклатур, строки зберігання, вимоги до передачі документів до архіву, ведення облікових форм, описів, актів тощо. У ньому передбачено й аспекти збереження документів у цифровому вигляді, зокрема порядок сканування, ідентифікації, реєстрації та формування електронного архіву.

Крім того, в Україні діє низка відомчих інструкцій, які уточнюють вимоги до архівування в окремих сферах – судовій, банківській, освітній, медичній, оборонній тощо. Наприклад, Інструкція з діловодства в органах державної виконавчої служби або Інструкція про порядок зберігання електронних документів у системах електронного документообігу.

Окрему категорію становлять державні стандарти, що регламентують вимоги до форматів, структури, зберігання та довгострокової архівації цифрової інформації. Важливими серед них є ДСТУ 4163:2020 (уніфікована система організаційно-розпорядчої документації), ДСТУ ISO 15489-1:2007 (управління

документацією. Загальні вимоги), ДСТУ ISO/IEC 27001:2015 (інформаційні технології. Методи захисту. Системи управління інформаційною безпекою). Зазначені стандарти є частиною імплементації міжнародних практик у національне регулювання та створюють уніфіковану нормативну основу для впровадження комплексних систем архівної безпеки.

На міжнародному рівні ключовими є моделі OAIS (Open Archival Information System), що рекомендовані ISO 14721, а також принципи IASA-TC (від Міжнародної ради архівного зберігання аудіовізуальних документів), які використовуються як методологічна основа для впровадження архівних рішень у цифровому середовищі. Українські архівні установи та приватні підприємства, які працюють з цифровими архівами, поступово адаптують ці моделі до своїх процесів, зокрема в проектах оцифрування історичних фондів, бібліотечних ресурсів, адміністративних реєстрів.

З огляду на сучасні виклики, пов’язані з війною, втратами документів, кібератаками та фізичними загрозами архівам, Державна архівна служба України посилила вимоги до збереження архівної інформації та оприлюднила низку методичних рекомендацій щодо цифрового резервного копіювання, перенесення фондів до безпечних місць, шифрування інформації та захисту доступу до цифрових архівів в умовах надзвичайного стану.

Таким чином, нормативно-правова база архівної безпеки в Україні є багаторівневою і динамічною системою, яка поєднує норми національного законодавства, міжнародні стандарти та галузеві регламенти. Вона поступово адаптується до викликів цифрової епохи, забезпечуючи правове підґрунтя для впровадження комплексних заходів із захисту архівної інформації в усіх сферах суспільного життя. Водночас існує потреба в подальшій уніфікації, оновленні та цифровій трансформації нормативної бази, що дозволить Україні рухатися в напрямку гармонізації з європейськими практиками архівної справи, підвищення кіберзахисту та довгострокового збереження цифрової культурної й адміністративної спадщини [27].

РОЗДІЛ 2
ЗАРУБІЖНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД ВПРОВАДЖЕННЯ СИСТЕМ АРХІВНОЇ БЕЗПЕКИ

2.1. Світові підходи реалізації технології цифрового архівування

У сучасному світі стрімкого розвитку інформаційних технологій і цифрової трансформації архівної справи, питання впровадження міжнародних стандартів електронного архівування та забезпечення безпеки документів набуває виняткового значення. Забезпечення надійності, автентичності, доступності та довготривалого збереження електронних документів можливе лише за умови дотримання уніфікованих стандартів, які встановлюють технічні, організаційні та правові вимоги до архівних систем. Міжнародні стандарти виступають як основа для гармонізації архівної політики між державами, уніфікації процесів архівування, забезпечення інтероперабельності цифрових архівів і впровадження єдиних принципів захисту документальної спадщини в електронному вигляді.

Одним із найвідоміших і найпоширеніших стандартів у сфері електронного архівування є ISO 14721:2012 — Reference Model for an Open Archival Information System (OAIS). Цей стандарт розроблений Міжнародною організацією зі стандартизації (ISO) та Комітетом з космічної інформації (CCSDS) і визначає загальну модель відкритої системи архівування інформації. OAIS встановлює базову термінологію, функціональні вимоги до архівної системи, процеси прийняття, зберігання, обробки, доступу та забезпечення довготривалого збереження цифрових об’єктів. Він є методологічною основою для побудови національних електронних архівів, наукових та освітніх репозиторіїв, баз даних у сфері культури, охорони здоров’я та державного управління [28].

Згідно з концепцією OAIS, електронний архів повинен виконувати шість основних функцій: приймання (ingest), управління даними (data management), зберігання (archival storage), управління адмініструванням (administration),

управління доступом (access) та збереження автентичності (preservation planning). Такий функціональний підхід забезпечує системність та контроль усього життєвого циклу електронного документа, з моменту його створення або надходження до архіву — до довгострокового зберігання та надання користувачам.

Важливим міжнародним стандартом, що безпосередньо стосується управління документами, є ISO 15489-1:2016 — Records Management. General. Цей стандарт визначає принципи створення, організації, ведення та збереження службових документів незалежно від форми їх носія. ISO 15489-1 акцентує увагу на необхідності збереження контексту, змісту, структури й метаданих документів для забезпечення їхньої автентичності та цілісності. Він також встановлює вимоги до політик документування, визначення повноважень, розподілу відповідальності та забезпечення безперервності управління інформацією.

У сфері інформаційної безпеки ключовим є ISO/IEC 27001:2013 — Information security management systems (ISMS), що встановлює вимоги до систем управління інформаційною безпекою, в тому числі для електронних архівів. Він включає понад сто контролів безпеки, що охоплюють політику безпеки, управління ризиками, криптографічний захист, фізичну безпеку, управління доступом, моніторинг, аудит, управління інцидентами та відновлення після збоїв. У контексті архівної справи цей стандарт дозволяє запровадити багаторівневу модель безпеки, що охоплює як захист серверного середовища, так і безпеку користувацького доступу до архівних ресурсів.

Крім зазначених стандартів, міжнародна спільнота користується рядом спеціалізованих норм, таких як:

ISO 19005 (PDF/A) — стандарт архівного формату електронних документів PDF/A, який забезпечує довготривале збереження файлів без втрати інформації.

ISO 30300–30301 — серія стандартів з управління документацією, зокрема вимоги до систем управління документацією (Management Systems for Records).

MoReq2010 (Model Requirements for the Management of Electronic Records) — європейська модельна специфікація для електронного управління записами, яка часто застосовується в державах-членах ЄС.

ISO/IEC 38500 — принципи управління IT, що допомагають організаціям у прийнятті рішень щодо безпеки IT-інфраструктури, в тому числі архівних систем [25].

Ці стандарти визначають обов'язкові параметри збереження метаданих, електронного підпису, форматів даних, періодів зберігання, вимог до інтерфейсів взаємодії, ідентифікації, автентифікації, криптографії тощо.

Таблиця 2.1

Ключові міжнародні стандарти в архівній справі та їх функціональне значення

№	Стандарт	Назва	Основне призначення
1	ISO 14721	OAIS Reference Model	Функціональна модель електронного архіву
2	ISO 15489-1	Records Management	Політика управління документами
3	ISO/IEC 27001	Information Security	Система захисту інформації архівів
4	ISO 19005	PDF/A	Архівний формат для електронних документів
5	MoReq2010	Model Requirements	Європейські вимоги до систем е-документообігу

На практиці в багатьох країнах світу впровадження міжнародних стандартів відбувається через національні адаптації або шляхом включення відповідних положень у державні стратегії та інструкції. Наприклад, у Німеччині OAIS використовується як базова модель для цифрових архівів у національних бібліотеках, в Італії – як основа для організації архівів медичних закладів, у США – як вимога до архівів наукових установ, які працюють з відкритими даними. ISO 27001 є обов'язковим для архівних серверів урядових органів у Великій Британії та Сінгапурі [36].

У контексті цифрової безпеки архівної інформації застосовується ще один інструмент — принципи FAIR (Findable, Accessible, Interoperable, Reusable), які стають основою управління архівними даними в наукових і освітніх установах. Вони передбачають створення цифрових об'єктів, які мають чіткі метадані,

постійні ідентифікатори, відкриті формати та технічну можливість повторного використання.

Умовно візьмемо організацію ТОВ «4В Україна», яка почала впровадження електронного архіву на основі стандарту OAIS. На першому етапі було створено структуру приймання даних (Ingest), де всі електронні документи оцифровуються, перевіряються на автентичність і позначаються відповідними метаданими. Далі – зберігаються у спеціалізованому сховищі з резервною копією, шифруванням та розмежованим доступом за допомогою ISO 27001. Адміністративна система дозволяє визначати повноваження працівників, реєструвати всі звернення до архіву, а план збереження (Preservation Planning) відповідає за конвертацію форматів у довготривалому періоді.

Таблиця 2.2

Етапи практичного впровадження архівної моделі OAIS на підприємстві

Етап	Опис дій	Стандарти
1	Приймання документів та перевірка метаданих	ISO 14721
2	Захищене зберігання та шифрування	ISO/IEC 27001
3	Контроль автентичності через цифрові підписи	ISO 19005, ISO 30301
4	Регламентований доступ та контроль дій	ISO 27001
5	Довгострокове планування збереження	OAIS Preservation Planning

Отже, дотримання міжнародних стандартів електронного архівування є необхідною умовою для побудови ефективної, безпечної та стійкої системи управління архівною інформацією в умовах цифровізації. Впровадження таких стандартів в українську практику дає змогу не лише забезпечити збереження документальної спадщини, а й інтегруватися в європейський інформаційний простір, що має вирішальне значення в контексті цифрової трансформації державного управління, бізнесу та науки [33].

У сучасному світі цифрова конверсія архівної інформації стала невід’ємною частиною інформаційної політики розвинених країн. Перехід від традиційного паперового зберігання документів до цифрових форматів не лише сприяє підвищенню ефективності доступу, зручності використання й інтеграції архівів у загальні інформаційні системи, але й забезпечує надійніші механізми

збереження, захисту та автентичності документів. У провідних країнах цифрова трансформація архівної справи є системним процесом, який базується на поєднанні нормативного регулювання, фінансової підтримки, технічного забезпечення та активної участі суспільства у збереженні національної пам'яті. При цьому застосовуються стандартизовані підходи до процесів сканування, метаопису, зберігання, доступу, резервного копіювання та відновлення архівної інформації.

Одним із найвідоміших прикладів ефективної цифрової конверсії архівів є практика Національного архіву Великої Британії (The National Archives, TNA). У рамках програми «Digital Continuity» тут впроваджено систему збереження електронних архівів на основі моделі OAIS. Всі документи, що підлягають тривалому зберіганню, проходять обробку за спеціальною процедурою: сканування, оцифрування, перевірка на автентичність, присвоєння унікального цифрового ідентифікатора, формування метаданих згідно зі стандартами METS і PREMIS, архівування у форматі PDF/A або TIFF. Британська система забезпечує не лише технічне зберігання інформації, а й юридичну силу цифрових копій завдяки національним нормативам та обов'язковому цифровому підпису. Платформа «Discovery», створена TNA, дозволяє широкому колу користувачів отримувати доступ до мільйонів архівних записів, як у відкритому, так і в захищеному режимах.

В Німеччині оцифрування архівних фондів здійснюється на державному та муніципальному рівнях у рамках стратегії «Digitale Verwaltung 2020». Федеральний архів (Bundesarchiv) оцифровує державні документи за допомогою високоточних сканерів зі збереженням кольору, масштабу та контексту. Для забезпечення автентичності та цілісності застосовується цифровий підпис на базі інфраструктури електронних довірчих послуг. Усі метадані формуються відповідно до стандартів EAD (Encoded Archival Description) та ISAD(G) (General International Standard Archival Description). Для зберігання використовуються спеціалізовані цифрові архіви з дублюванням у трьох незалежних дата-центрах. Цікаво, що у Німеччині на законодавчому рівні закріплено принцип "born digital

preservation", згідно з яким електронні документи створюються і зберігаються виключно у цифровому вигляді.

У США цифрова трансформація архівної системи охоплює як державні, так і приватні інституції. Національний архів та адміністрація документації (NARA) активно реалізують програму «Electronic Records Archives» (ERA), що передбачає створення централізованої платформи для збереження, управління й надання доступу до федеральної цифрової документації. Архівні об'єкти зберігаються у кількох дата-центрах, а також у партнерстві з Amazon Web Services на умовах дотримання сертифікатів безпеки FISMA і FedRAMP. США є лідером у застосуванні хмарних технологій для зберігання архівів, водночас використовують систему постійного аудиту даних, включаючи цифрові відбитки, контроль версій та відновлення у разі втрат. Також велика увага приділяється доступності архівів для людей з інвалідністю, зокрема через адаптовані інтерфейси, інтерпретацію та багатомовну підтримку.

У Франції Національний архів (Archives Nationales) здійснює цифрове збереження за допомогою системи Système Archivistique de l'État (SAE), яка дозволяє державним органам створювати, передавати й зберігати електронні документи. Практика базується на дотриманні міжнародних стандартів (ISO 30301, ISO 16175) та використанні відкритих форматів збереження. Архіви формуються з обов’язковим юридичним описом, криптографічним захистом, багаторівневою ідентифікацією доступу. Для довгострокового збереження передбачено функцію "рефрешингу" носіїв (перезапис даних кожні 5–7 років) та "міграції форматів" із застарілих у нові. Урядові архіви Франції тісно співпрацюють з Європейським архівним порталом (Archives Portal Europe), що забезпечує єдину платформу для пошуку документів континентального масштабу [14].

Японія, відома своїми технологічними інноваціями, застосовує моделі цифрової архівації на основі штучного інтелекту. Національний архів Японії (NAJ) впровадив систему, яка автоматично класифікує документи, створює анотації, формує метадані та визначає рівні доступу на основі машинного навчання. Документи архівуються з використанням японських відкритих

форматів (JIPDEC), які адаптовані до особливостей ієрогліфічного письма. Японська архівна політика передбачає обов'язкове збереження інформації у трьох копіях: одна – на центральному сервері, друга – в регіональному архіві, третя – на мікрофільмах для довгострокового збереження. Такий підхід гарантує як цифрову, так і аналогову стійкість до катастроф.

Таблиця 2.3

Порівняння цифрових практик архівування у провідних країнах

Країна	Архівна установа	Ключова система/ініціатива	Формат архівації	Стандарти
Велика Британія	The National Archives (TNA)	Digital Continuity, Discovery	PDF/A, METS, PREMIS	ISO 14721, ISO 15489
Німеччина	Bundesarchiv	Digitale Verwaltung 2020	TIFF, XML, EAD	ISAD(G), EAD, OAIS
США	NARA	ERA, AWS-платформи	PDF/A, JSON, XML	FISMA, ISO 27001, OAIS
Франція	Archives Nationales	SAE, Portal Europe	XML, PDF/A, CSV	ISO 30301, 16175, OAIS
Японія	National Archives of Japan	AI-based Archiving System	JIPDEC, PDF/A, TIFF	OAIS, JIS, ISO 15489

На прикладі ТОВ «4В Україна», яке зберігає внутрішню документацію в електронному вигляді, було ініційовано пілотний проєкт цифрової конверсії внутрішніх архівів на основі британського підходу. Документи, створені у MS Word, Excel, ERP-системах, конвертуються у формат PDF/A з фіксацією дати, авторства, електронного підпису. Далі вони маркуються згідно зі внутрішньою класифікацією, розміщуються в структурованому сховищі з щотижневим резервним копіюванням на окремий сервер.

Таблиця 2.4

Етапи цифрової конверсії архівної інформації в ТОВ «4В Україна» (пілотний проєкт)

Етап	Дії	Інструменти	Стандарти
1	Оцифрування документів	Adobe Acrobat, Foxit Phantom	PDF/A, ISO 19005
2	Верифікація даних	ЕЦП, скан-ідентифікатор	Закон України про ЕЦП
3	Маркування метаданих	Excel, TNA Template	PREMIS, Dublin Core
4	Завантаження до архіву	NAS-сховище, власна ERP	OAIS, ISO 27001
5	Резервне копіювання	Acronis, NAS Raid	ISO/IEC 27001:2013

Таким чином, практики цифрової конверсії у провідних країнах демонструють комплексний підхід до оцифрування, який включає не лише технічні, але й юридичні, управлінські та етичні компоненти. Адаптація цього досвіду в Україні, навіть на рівні малого та середнього бізнесу, створює передумови для підвищення інформаційної стійкості, архівної відповідальності та прозорості процесів документообігу. У довгостроковій перспективі цифрове архівування перетворюється не просто на технологічне рішення, а на стратегічну функцію організації, пов’язану з управлінням знаннями, юридичною безпекою та корпоративною культурою.

2.2. Цифрова трансформація вітчизняних архівів

Цифровізація архівних установ в Україні є важливим напрямом державної політики у сфері інформаційного суспільства, національної безпеки та культурної спадщини. Перехід до цифрових форматів зберігання інформації дозволяє не лише забезпечити її збереження, автентичність і доступність, але й інтегрувати українські архіви у міжнародну інформаційну інфраструктуру. Впродовж останніх років в Україні реалізовано низку державних ініціатив, спрямованих на модернізацію архівної галузі, оновлення нормативно-правової бази, створення електронних платформ для архівного обліку та доступу, а також розвиток технічного забезпечення архівних установ. Усі ці заходи здійснюються в контексті загальнодержавної стратегії цифрової трансформації, затвердженої Кабінетом Міністрів України та координованої Міністерством цифрової трансформації спільно з Державною архівною службою України (Укрдержархівом).

Одним із найважливіших державних документів, який визначає стратегічні пріоритети цифровізації архівної справи, є Концепція розвитку електронного урядування в Україні. У межах цієї концепції передбачено впровадження електронного документообігу в органах державної влади, цифрових сервісів для громадян та електронного зберігання управлінських рішень. Архіви, як кінцева інстанція життєвого циклу документів, є ключовими елементами цієї цифрової

екосистеми. Важливим кроком стала також Національна стратегія розвитку архівної справи на період до 2025 року, в якій цифровізація визначена як один із п’яти основних векторів трансформації архівної галузі.

Особливу роль у цифровізації відіграє державна програма «Електронні архіви», яка спрямована на створення єдиного цифрового простору архівної інформації. У межах цієї програми передбачено впровадження системи електронного документообігу в центральних архівних установах, створення централізованої платформи електронних архівів (ЦПЕА), розробку єдиних стандартів сканування, архівації, шифрування, обліку, доступу та довготривалого зберігання документів. Реалізація цієї програми стала можливою завдяки підтримці міжнародних партнерів, зокрема USAID, ЄС та Програми розвитку ООН, які надали фінансування для придбання сканерів, серверного обладнання та навчання фахівців архівної сфери.

Значним кроком у цьому напрямі стало створення пілотного проєкту «Цифровий архів України», у межах якого було оцифровано понад 1,5 мільйона сторінок архівних справ у Центральному державному історичному архіві України в Києві. Цей проєкт став основою для подальшого впровадження інформаційно-пошукових систем, зокрема бази даних «Archium», яка дозволяє користувачам здійснювати пошук, замовлення та перегляд цифрових копій документів. У перспективі ця система має бути об’єднана з іншими електронними ресурсами, такими як Єдиний державний вебпортал відкритих даних та Єдиний портал електронних послуг.

Не менш важливим є інтеграція цифрових архівних ініціатив у проєкти з національної пам’яті та діджитал-гуманітаристики. Одним із прикладів є платформа «Архіви України: відкритий доступ», створена за ініціативи Центру досліджень визвольного руху. У співпраці з Галузевим державним архівом Служби безпеки України було оцифровано десятки тисяч сторінок документів радянських спецслужб, які стали доступними в онлайн-режимі. Це дозволяє громадянам, науковцям, журналістам і правозахисникам отримувати доступ до історичних джерел без фізичного відвідування архівів.

Іншим прикладом є проєкт «Е-архів Майдану», спрямований на збереження цифрових свідчень про Революцію Гідності. Завдяки ініціативі Музею Революції Гідності створено онлайн-платформу для збору, зберігання та систематизації фотографій, відео, свідчень очевидців, що інтегрується з національними та міжнародними архівними системами. Важливість таких проєктів полягає не лише у збереженні національної пам’яті, а й у формуванні цифрової культури архівного збереження.

У контексті безпеки та збереженості архівів особливе значення має ініціатива Міністерства культури та інформаційної політики щодо створення системи резервного копіювання та цифрової евакуації архівних фондів із зон бойових дій. У співпраці з місцевими адміністраціями було реалізовано евакуацію цифрових копій архівних справ з Луганської, Донецької та Херсонської областей, а також розміщено їх дублікати на захищених серверах у західних регіонах України. Задля цього були розроблені мобільні комплекси для сканування й передачі інформації, що працюють навіть в умовах обмеженого інтернет-зв’язку.

Інституційне впровадження цифровізації здійснюється Державною архівною службою України (Укрдержархів), яка координує діяльність усіх центральних, обласних і галузевих архівів щодо впровадження стандартів цифрового збереження. Було розроблено типові технічні завдання на створення електронних архівів, рекомендації щодо оцифрування документів, ведення цифрових каталогів, а також інструкції з інформаційної безпеки. Крім того, створено Національний реєстр архівів у цифровому форматі, що містить інформацію про всі діючі архіви, обсяг фондів, ступінь оцифрування та технічні можливості зберігання [7].

Таблиця 2.5

Основні державні ініціативи України у сфері цифровізації архівів

№	Назва ініціативи	Суб'єкт реалізації	Основний результат
1	Програма «Електронні архіви»	Укрдержархів, Мінцифра	Створення централізованої платформи електронного архіву
2	Проєкт «Цифровий архів України»	ЦДІАК	Оцифрування понад 1,5 млн архівних сторінок
3	Платформа «Архіви України: відкритий доступ»	Центр досліджень визвольного руху	Вільний онлайн-доступ до архівів СБУ
4	Проєкт «Е-архів Майдану»	Музей Революції Гідності	Архівування відео- та фотосвідчень Революції
5	Програма цифрової евакуації архівів	МКІП, Укрдержархів	Збереження архівів з небезпечних регіонів на резервних носіях

На підприємстві ТОВ «4В Україна», що спеціалізується на IT-консалтингу, з 2022 року реалізовано внутрішню цифрову політику архівного зберігання. Вона базується на принципах, визначених державними ініціативами, зокрема вимогах до оцифрування, збереження, шифрування та систематизації документів. Компанія розробила власний архівний модуль в ERP-системі, який дозволяє автоматизовано зберігати всі договори, рахунки, службові записки у форматі PDF/A. Документи отримують унікальний ідентифікатор, підписуються електронним підписом, а доступ до них регулюється ролями користувачів у системі.

Також впроваджено функцію резервного копіювання архіву щодня зберіганням копій у хмарному сховищі та на окремому фізичному сервері. Архівні документи систематизуються відповідно до класифікаторів: фінансові, правові, адміністративні, технічні. У разі перевірок або аудиту, система дозволяє сформувати звіт про доступ, перегляд, зміну та збереження кожного документа.

Таблиця 2.6

Внутрішня архівна політика ТОВ «4В Україна» за аналогією державних ініціатив

Напрям діяльності	Засіб реалізації	Результат
Оцифрування	Перетворення у формат PDF/A	100% документів у цифровому вигляді
Ідентифікація	Присвоєння унікального ID	Прозорість та контроль пошуку
Безпека	ЕЦП, шифрування, обмеження доступу	Захист документів від несанкціонованого втручання
Резервне зберігання	Хмара + сервер з RAID	Гарантоване збереження інформації
Доступність	Модуль ERP + авторизація	Швидкий доступ, фіксація дій

Таким чином, державні ініціативи цифровізації архівної справи в Україні демонструють послідовну інтеграцію національного законодавства, міжнародних стандартів і практичних потреб суспільства. Вони не лише забезпечують технічну модернізацію архівних установ, а й стимулюють розвиток цифрової культури, прозорості та відкритості архівної інформації. Розширення таких програм, їх поширення на регіональні рівні, підтримка освітніх і наукових проєктів є необхідною умовою побудови в Україні стійкої цифрової архівної інфраструктури.

Стан впровадження цифрових рішень у регіональних архівах України на сьогодні є неоднорідним та таким, що залежить від низки чинників, зокрема рівня технічної забезпеченості, наявності фінансування, кадрового потенціалу, ініціативності місцевих адміністрацій та ступеня взаємодії з Державною архівною службою України. Попри наявність стратегічних документів і урядових програм, темпи та якість цифровізації у регіональних архівах залишаються нерівномірними, що створює дисбаланс в єдиному інформаційному просторі країни. Однак в останні роки спостерігається активізація процесів модернізації обласних, міських і районних архівних установ, особливо в умовах воєнного стану, що викликало потребу у швидкому збереженні, резервному копіюванні та евакуації архівних фондів.

Поточна ситуація характеризується тим, що більшість регіональних архівів працює з гібридною моделлю зберігання документів: основний масив фондів зберігається у традиційній паперовій формі, а оцифрування здійснюється фрагментарно — здебільшого для документів найбільшого суспільного та історичного значення, або на запити користувачів. Лише окремі установи мають повноцінні цифрові архівні платформи з функціями пошуку, доступу, завантаження та перегляду цифрових копій.

Наприклад, у Центральному державному історичному архіві України у Львові реалізовано один із найуспішніших проєктів оцифрування метрик, актових книг, міських книг і церковних архівів, що охоплюють період з XVI до початку XX століття. Результатом цього стало створення цифрової бази, яка активно використовується як науковцями, так і громадськістю. Водночас у багатьох архівах обласного рівня, особливо в центральних і східних регіонах, спостерігається брак сканувального обладнання, відсутність спеціалізованих кадрів, неузгодженість програмного забезпечення з державними стандартами, а також нестача серверних потужностей для зберігання великих обсягів оцифрованих матеріалів [7].

Особливістю регіонального рівня є те, що більшість цифрових рішень впроваджуються на базі локальних ініціатив, часто в рамках співпраці з університетами, історичними товариствами, краєзнавчими об'єднаннями, міжнародними грантами або громадськими проектами. Наприклад, у Чернігівському обласному архіві було реалізовано проєкт цифровізації архівів жертв політичних репресій, а в Полтаві — проект з оцифрування архівів періоду УНР. У цих випадках цифрові копії зберігаються паралельно на окремих серверах та передаються до єдиної державної бази даних, що адмініструється Укрдержархівом.

Розвиток електронного документообігу в архівах на рівні обласних адміністрацій відбувається повільніше. У більшості випадків архіви обмежуються створенням електронних реєстрів і каталогів, які ведуться у вигляді Excel-файлів або спрощених баз даних. Лише незначна кількість архівів має власні вебпортали з базами електронних документів. Це пояснюється

насамперед відсутністю централізованої інформаційної системи з інтегрованими модулями для архівного обліку, оцифрування, резервного копіювання, захисту інформації та доступу [8].

Таблиця 2.7

Основні проблеми цифровізації в регіональних архівах України

№	Проблема	Причина
1	Недостатній рівень технічного забезпечення	Відсутність фінансування, застаріле обладнання
2	Кадровий дефіцит у сфері ІТ	Низька зарплата, відсутність спеціалістів
3	Нерівномірність цифровізації по регіонах	Відсутність єдиного державного стандарту
4	Відсутність єдиної електронної платформи	Децентралізоване ведення обліку
5	Відсутність хмарної інфраструктури	Брак інвестицій і захищених серверів
6	Низький рівень взаємодії з громадськістю	Неавтоматизований доступ, обмежені послуги

Разом з тим, регіональні архіви мають потенціал для розвитку цифрових рішень за умови реалізації кількох системних підходів. По-перше, необхідне запровадження єдиного програмного комплексу на рівні всієї держави, зокрема впровадження ERP-модуля для архівів, що включає сканування, опис, облік, формування метаданих і збереження. По-друге, варто впровадити типові технічні завдання для оцифрування документів і створення єдиного формату збереження. По-третє, важливо створити спільні навчальні центри або програми для архівістів, які працюють з цифровими технологіями.

Практична частина: оцінка впровадження цифрових рішень на прикладі регіонального архіву

На прикладі умовного регіонального архіву — наприклад, Державного архіву Житомирської області — було проведено оцінку впровадження цифрових рішень за кількома критеріями: наявність техніки, програмного забезпечення, рівень сканування документів, обсяг оцифрованих фондів, доступність для громадськості. За результатами аналізу виявлено, що основним цифровим ресурсом є локальна база даних Excel, що містить перелік фондів. Частина документів оцифровується за допомогою офісного сканера формату А4, що не

дозволяє працювати з великими документами або нестандартними форматами. Вебпортал архіву відсутній, проте функціонує сторінка у соціальних мережах, де регулярно публікуються відскановані документи. Збереження цифрових копій відбувається на комп'ютерах працівників без резервного копіювання.

Таблиця 2.8

Поточний стан цифровізації в умовному регіональному архіві

Параметр	Стан на 2025 рік
Сканувальне обладнання	1 офісний сканер Canon
Формат оцифрування	PDF, JPG
Кількість оцифрованих справ	~800 одиниць зберігання
Програмне забезпечення	MS Office, без спеціалізованих платформ
Вебпортал	Відсутній
Резервне копіювання	Частково на флеш-носіях
Кваліфікація персоналу	Архівісти без ІТ-освіти
Фінансування цифровізації	Локальні ініціативи, благодійні гранти

Результати аналізу свідчать про наявність технічної та інституційної бази для цифровізації, однак її стан є незадовільним через фрагментарність, відсутність централізованого керування та нестачу ресурсів. Подібна ситуація спостерігається в багатьох обласних архівах, що створює ризики втрати інформації, унеможливлює віддалений доступ для користувачів та обмежує потенціал архівної справи як частини цифрової держави.

Таким чином, поточний стан впровадження цифрових рішень у регіональних архівах України потребує значного вдосконалення. Для цього необхідні державна підтримка, централізоване програмне забезпечення, кадрова модернізація, а також інтеграція архівної справи до національних цифрових ініціатив. Створення єдиного електронного архівного простору, доступного з будь-якого регіону країни, має стати стратегічним завданням на найближчі роки. Це дозволить не лише зберегти історичну пам'ять та адміністративну спадщину, але й сприятиме демократизації доступу до інформації, прозорості державного управління та підвищенню довіри громадян до державних інституцій [19].

2.3. Приклади ефективного впровадження ІТ-рішень у сфері архівної безпеки

Використання хмарних технологій та блокчейну у міжнародній архівній практиці є одним із найбільш інноваційних напрямів сучасного цифрового управління архівами. У XXI столітті збереження інформації вже не обмежується фізичним простором архівів або локальними серверами. Поява хмарних сервісів надала архівній справі принципово нові можливості — масштабованість, безперервний доступ, розподілене зберігання, зниження вартості інфраструктури. Натомість впровадження технологій блокчейн започаткувало новий рівень довіри, прозорості й незмінності архівних даних. У провідних країнах ці технології використовуються не як окремі технічні рішення, а як компоненти комплексної цифрової інфраструктури зберігання документів, правових актів, історичних даних та культурної спадщини.

Хмарні обчислення (cloud computing) дозволяють архівним установам зберігати цифрові документи в захищених віртуальних середовищах, що забезпечуються провайдерами хмарних послуг — Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Cloud тощо. У США, наприклад, Національний архів (NARA) використовує рішення AWS для управління масивами електронних федеральних документів. Основна перевага хмарної інфраструктури полягає у відмовостійкості системи — дані зберігаються одночасно в кількох дата-центрах, розміщених у різних географічних точках. У разі катастроф, кібератак або технічних збоїв це гарантує безперервність архівного зберігання.

Також хмара забезпечує гнучкість доступу: працівники архівів, дослідники чи громадяни можуть отримати доступ до документів з будь-якого місця, маючи лише інтернет-з’єднання. Це особливо важливо у випадках надзвичайних ситуацій, таких як війна, пандемія чи природні катаклізми, коли фізичне відвідування архівів стає неможливим. В Італії, Іспанії та Канаді активно використовуються національні платформи хмарного зберігання з розподіленими доступами за ролями, що дозволяє архівам централізовано обліковувати всі дії з документами.

Особливе значення має застосування блокчейн-технологій — розподілених децентралізованих систем, у яких інформація зберігається у вигляді хронологічно пов’язаних блоків даних. Основна перевага блокчейну в архівній справі — неможливість несанкціонованого втручання в записану інформацію без сліду. Це забезпечує автентичність, цілісність та незмінність архівного документа протягом усього періоду його зберігання. Крім того, блокчейн забезпечує прозорість: усі дії з документом (створення, перегляд, зміна, підписання) можуть бути фіксовані та верифіковані незалежно від місця зберігання.

У Нідерландах Державний архів експериментує із застосуванням блокчейн-рішень для реєстрації архівних метаданих та транзакцій доступу. Кожен документ отримує унікальний хеш-код, який фіксується в блокчейні, що дозволяє пізніше перевірити, чи документ залишився незмінним. Аналогічна система застосовується у Швеції для збереження електронних свідоцтв про народження, шлюб і смерть. У Південній Кореї уряд розробив національну блокчейн-платформу для верифікації оцифрованих юридичних актів, які зберігаються у національному архіві та доступні для судових, адміністративних та дослідницьких потреб [7].

Таблиця 2.9

Порівняльний аналіз застосування хмарних і блокчейн-технологій в архівах різних країн

Країна	Хмарні технології	Блокчейн-технології	Очікувані ефекти
США	AWS, Azure (NARA)	Приватний блокчейн для держреєстрів	Масштабованість, стійкість
Нідерланди	Хмара Dutch Digital Heritage Network	Хешування архівних транзакцій	Прозорість, достовірність
Швеція	Урядова платформа збереження	Блокчейн для актів цивільного стану	Незмінність, цифрова довіра
Південна Корея	Hcloud for Government	Нацблокчейн для офіційних документів	Верифікація, захист від фальсифікацій
Канада	Government Cloud (GC)	Пілотний проєкт з збереження угод	Зниження витрат, автоматизація аудиту

Низка міжнародних стандартів підтримує впровадження хмарних та блокчейн-рішень у сфері архівування. Зокрема, ISO/IEC 27017 встановлює правила захисту хмарної інфраструктури, а ISO/TC 307 розробляє нормативи для технології блокчейн і розподілених реєстрів. Ці стандарти дозволяють поєднувати безпеку, надійність і прозорість у системах управління електронними архівами. Крім того, відповідність цим стандартам є вимогою для участі у міжнародних проєктах цифрового архівування, зокрема у ініціативі UNESCO «Memory of the World» або європейському порталі Europeana.

Практична частина: пілотне впровадження хмарного та блокчейн-модуля в корпоративному архіві

Розглянемо приклад пілотного рішення в компанії ТОВ «4В Україна», яка вирішила модернізувати свій внутрішній архів за допомогою хмарних рішень і елементів блокчейну. У рамках проєкту компанія інтегрувала до наявної ERP-системи модуль хмарного архіву з функціями:

резервного зберігання (дві копії у хмарі Google Cloud);

автоматичного створення резервних копій щотижня;

доступу до документів через авторизовані облікові записи;

блокчейн-фіксації всіх дій з критично важливими документами (контракти, акти приймання-передачі, звіти).

Для забезпечення незмінності даних використовується приватний блокчейн на основі Ethereum, який генерує хеш-функції для кожного документа під час його внесення. Усі подальші дії з документом фіксуються в блоках, які синхронізуються з хмарною базою. У випадку втрати фізичного доступу до сервера, система зберігає всю історію змін у розподіленій мережі.

Таблиця 2.10

Структура пілотного цифрового архіву ТОВ «4В Україна»

Компонент системи	Характеристика	Технологія
Основне сховище	Google Cloud Storage	Хмарна інфраструктура
Резервне копіювання	Щотижневе, автоматичне, на окремий акаунт	Cron + Google Vault
Контроль доступу	Авторизація через корпоративні облікові	2FA, SSO
Незмінність документа	Хешування SHA-256	Приватний Ethereum
Історія змін	Логування в блокчейні	Smart-contract записи
Інтерфейс	Веб-додаток інтегрований в ERP	REST API

Результати пілоту показали, що навіть у межах середнього підприємства можливе ефективне впровадження сучасних технологій для архівування, за умови наявності базових IT-ресурсів і технічної підтримки. Очікувані вигоди від цього — підвищення безпеки, пришвидшення доступу, зменшення ризиків втрати, юридичний захист даних.

Таким чином, хмарні технології та блокчейн відіграють ключову роль у трансформації архівної справи у світі. Вони забезпечують якісно новий рівень зберігання, захисту й використання документів, що відповідає вимогам епохи цифрової глобалізації. Впровадження таких рішень в українському контексті може забезпечити не лише технологічну модернізацію архівних установ, а й підвищити їхню стійкість до загроз, зменшити витрати на обслуговування, розширити доступ громадян до інформації, а також підвищити довіру до цифрових даних як достовірного джерела історичної й управлінської інформації.

У сучасних умовах цифрової трансформації архівної справи в Україні зростає значення впровадження програмних рішень для забезпечення архівної безпеки. Цей процес охоплює як державні установи, так і приватні підприємства, освітні та культурні організації, які прагнуть не лише зберегти архівну інформацію, а й забезпечити її захист, автентичність, доступність та незмінність у довготривалій перспективі. В Україні поступово формуються власні кейси застосування інформаційно-комунікаційних технологій у сфері архівного збереження, які відповідають викликам часу та обмеженим ресурсам [5].

Вітчизняна архівна система, попри труднощі перехідного періоду, демонструє певні досягнення у застосуванні програмного забезпечення для електронного управління документами та цифрової архівації. Серед найбільш поширених рішень — системи електронного документообігу (СЕД), які інтегрують функції створення, реєстрації, обробки, зберігання й пошуку документів. Програмні продукти на кшталт M.E.Doc, BAS Документообіг, Архів.Плюс, АСКОД та ДОК ПРОФ активно використовуються як в державному секторі, так і у бізнес-середовищі. Окремі установи розробляють індивідуальні рішення, орієнтовані на галузеву специфіку та архівні потреби.

У системі органів державної влади України прикладом є Єдина система електронного документообігу (ЕСЕД), що функціонує в Кабінеті Міністрів України, міністерствах та обласних адміністраціях. Вона включає модуль довготривалого архівного зберігання, в якому зафіксовано всі службові документи, які підлягають обов’язковому зберіганню. Доступ до них регламентовано, а збереження здійснюється з дублюванням на сервері в іншому регіоні.

В архівних установах досить поширеною є система «Архів.Плюс», що розроблена українськими фахівцями та адаптована до потреб державних архівів. Вона включає функціонал ведення електронного каталогу, формування метаданих, контролю за переміщенням документів, інтеграцію з базами даних читачів та можливістю експорту даних у формат PDF/A. Наприклад, у Центральному державному науково-технічному архіві України було реалізовано електронну архівну базу на основі цієї системи, що дозволило значно зменшити навантаження на співробітників та пришвидшити доступ до технічної документації.

Ще одним прикладом є застосування системи BAS Документообіг, що поєднує модулі електронного управління, архівного зберігання та контролю доступу до файлів. Вона використовується в органах місцевого самоврядування, підприємствах освіти та медицини. Її перевагою є можливість гнучкої настройки під конкретні потреби установи та збереження архівних файлів у відкритих форматах з відповідними метаданими.

В умовах війни зростає значення рішень, які дозволяють евакуювати цифрові архіви з небезпечних регіонів. У межах ініціативи Міністерства культури та Укрдержархіву було створено низку мобільних рішень для сканування та оперативного перенесення документів у безпечне середовище. Зокрема, у Херсонській обласній архівній установі використано портативне ПЗ для оцифрування справ та збереження їх у зашифрованому форматі із резервним дублюванням на хмарне сховище.

Таблиця 2.11

Поширені в Україні програмні рішення для архівної безпеки

№	Назва ПЗ	Функціонал	Сфера використання
1	M.E.Doc	Звітність, документообіг, архівація	Бізнес, фінанси
2	BAS Документообіг	Створення, зберігання, доступ, аудит	ОСББ, органи влади, освіта
3	Архів.Плюс	Каталогізація, метадані, перегляд	Державні архіви
4	АСКОД	Облік документів, реєстрація, зберігання	Виконавча влада, держструктури
5	ДОК ПРОФ	Контроль життєвого циклу документа	ВНЗ, лікарні, наукові установи

Успішним прикладом регіональної ініціативи є створення в місті Львові локального хабу архівної безпеки на базі міського архіву, де було розроблено індивідуальне ПЗ для індексації та шифрування цифрових документів на базі PostgreSQL та Python. У рамках цього рішення документи метаописуються за шаблоном ISAD(G), зберігаються у вигляді хешованих ZIP-архівів із трирівневим розмежуванням доступу. До цього процесу були залучені фахівці Львівського політехнічного інституту, які розробили архітектуру бази даних і забезпечили її інтерфейс користувача [26].

Інший приклад — співпраця Національного архівного фонду з IT-компаніями для розробки модуля автоматичного шифрування архівів під час передавання в державне зберігання. Це програмне рішення базується на криптографічних бібліотеках з відкритим кодом, інтегрується із сервісом цифрового підпису та зберігає інформацію про всі зміни у лог-файлах.

ТОВ «4В Україна» у 2023 році розпочало впровадження індивідуального програмного рішення для забезпечення внутрішньої архівної безпеки, адаптованого до специфіки проєктного управління в IT-сфері. У межах цього рішення було створено внутрішній електронний архів на базі SQLite, де зберігаються контракти, технічна документація, тендерні пропозиції та кадрові матеріали. Архів містить функціонал шифрування файлів за допомогою алгоритму AES-256, створення електронного підпису для критичних документів та відстеження змін у кожному файлі.

Додатково до внутрішньої бази впроваджено модуль регулярного резервного копіювання, який щоденно зберігає актуальну версію архіву на окремому фізичному носії та щотижня синхронізує копії з хмарним сховищем Google Drive. Для доступу до архіву створено окрему групу користувачів у системі управління проєктами, з індивідуальними правами доступу, що дозволяє забезпечити контрольований доступ.

Таблиця 2.12

Архітектура архівної системи ТОВ «4В Україна»

Компонент	Технологія / ПЗ	Функціонал
База архіву	SQLite, Python	Зберігання структурованих даних
Шифрування	AES-256	Захист від несанкціонованого доступу
ЕЦП	Клієнт "Дія.Підпис"	Підтвердження автентичності
Резервне копіювання	Cron + Google Drive API	Збереження копій
Інтерфейс користувача	Flask-based вебдодаток	Доступ до архіву
Аудит змін	JSON-журнал подій	Прозорість архівних операцій

Результати впровадження показали зниження ризику втрати документів, можливість швидкого пошуку й доступу до інформації, а також відповідність вимогам внутрішньої інформаційної політики. Архівна система стала частиною загальної стратегії інформаційної безпеки компанії та її сертифікації за внутрішніми стандартами якості [24].

РОЗДІЛ 3
АРХІВУВАННЯ ДОКУМЕНТІВ ТОВ «4В УКРАЇНА» ТА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ АРХІВНОЇ ІНФОРМАЦІЇ

3.1. Особливості архівування інформації діяльності підприємства

У ТОВ «4В Україна», яке спеціалізується на наданні послуг у сфері IT-консалтингу, цифрової трансформації та бізнес-аналізу, архівування документів відіграє ключову роль у забезпеченні юридичної безпеки, внутрішньої прозорості процесів та дотриманні договірної дисципліни. Оскільки компанія функціонує в умовах динамічного документообігу та мультипроєктної діяльності, структура документного потоку є досить складною, і її ефективне архівування потребує чіткої регламентації, поділу відповідальності, автоматизації процесів та періодичної перевірки.

Документний потік підприємства поділяється на кілька основних блоків: адміністративно-управлінська документація, фінансово-розрахункова документація, проєктно-технічна документація, договірна документація, документація з кадрів, внутрішні політики та розпорядження. Кожен з цих блоків має свою специфіку, терміни зберігання, вимоги до захисту та доступу, а також порядок архівування у фізичній або електронній формі.

Адміністративно-управлінські документи включають накази, розпорядження, протоколи, листування, внутрішню аналітику. Ці документи зберігаються в електронному вигляді у спеціальних папках внутрішнього архіву, який структурований за роками та напрямами діяльності. Архівування відбувається після затвердження документа, на підставі внутрішнього регламенту, що передбачає внесення відповідального виконавця, проставлення електронного підпису, створення контрольного звіту, призначення терміну зберігання та визначення категорії доступу.

Фінансово-розрахункові документи (рахунки, акти, накладні, звіти, банківські виписки) автоматично архівуються через інтегровану систему з бухгалтерським програмним забезпеченням. Усі електронні копії зберігаються в

системі BAS Бухгалтерія з дублюванням у внутрішньому архіві. Для забезпечення архівної безпеки до документів додаються цифрові підписи та QR-коди для верифікації. Кожен фінансовий документ супроводжується метаданими — дата, контрагент, сума, валюта, відповідальний співробітник.

Проєктно-технічна документація створюється у процесі реалізації IT-проєктів і включає технічні завдання, специфікації, API-документацію, звіти з тестування, діаграми, код. Особливістю цієї документації є її версійність, тобто необхідність зберігати всі зміни з можливістю відновлення попередніх версій. Тому компанія використовує систему архівування GitLab, де кожен документ пов’язується з конкретним проєктом, завданням і відповідальним. Також для кожного завершеного проєкту формується архівна папка, яка переноситься у довготривале сховище компанії.

Договірна документація охоплює контракти, додаткові угоди, акти звірки, комерційні пропозиції. Архівування цієї категорії є надзвичайно важливим з юридичної точки зору, оскільки ці документи часто фігурують у перевірках, аудитах або судових процесах. Кожен договір сканується (у разі підписання в паперовій формі), конвертується у PDF/A, підписується електронним цифровим підписом, реєструється у журналі договорів та зберігається у двох копіях — на захищеному сервері компанії та у хмарному архіві Google Workspace з розмежованим доступом.

Кадрова документація — це накази про прийом, звільнення, відпустки, графіки роботи, посадові інструкції, трудові договори. Архівування здійснюється відповідно до трудового законодавства України та вимог Держпраці. Компанія розробила власний модуль для архівування особових справ у цифровому вигляді, який дозволяє зберігати скановані копії документів з повною історією змін. Для документів, які підлягають довготривалому зберіганню (до 75 років), реалізовано систему резервного копіювання з перезаписом даних на зовнішні носії кожні 5 років [8].

Таблиця 3.1

Структура документного потоку ТОВ «4В Україна»

Категорія документації	Основні типи документів	Формат зберігання	Термін зберігання
Адміністративно-управлінська	Накази, розпорядження, протоколи	PDF/A, DOCX	5 років
Фінансово-розрахункова	Рахунки, акти, звіти, банківські виписки	PDF, XML	3–10 років
Проєктно-технічна	Технічні завдання, код, специфікації	Markdown, PDF, HTML	Не менше 5 років
Договірна	Контракти, угоди, пропозиції	PDF/A	Не менше 10 років
Кадрова	Трудові договори, накази, особові справи	PDF, JPG, XML	До 75 років
Внутрішні політики	Регламенти, стандарти, інструкції	DOCX, PDF	Постійно

Регламенти архівування в ТОВ «4В Україна» закріплені в офіційній внутрішній політиці інформаційної безпеки, яка затверджується генеральним директором та погоджується з юридичним відділом. Документ містить:

порядок прийняття документа до архіву (включаючи верифікацію, підпис, метадані, шифрування);

порядок класифікації документів за рівнем доступу (публічний, службовий, конфіденційний, з обмеженим доступом);

процедуру резервного копіювання (щоденне, щотижневе, щомісячне);

порядок знищення документів після завершення строку зберігання;

відповідальних осіб на кожному етапі архівного процесу.

Таблиця 3.2

Основні регламенти архівування в ТОВ «4В Україна»

Етап архівування	Дії та вимоги	Відповідальні особи
Прийняття документа	Перевірка, підпис, дата, метадані	Діловод, керівник відділу
Класифікація	Визначення категорії доступу	Керівник відділу, юрист
Зберігання	Розміщення у архіві (фіз. / електр.)	Архіваріус, ІТ-адміністратор
Резервне копіювання	Автоматичне збереження копій	ІТ-відділ
Перевірка цілісності	Хеш-контроль, тестування файлів	ІТ-спеціаліст
Знищення після строку	Акт про знищення, підтвердження	Архіваріус, керівник служби

У квітні 2025 року в ТОВ «4В Україна» було проведено внутрішній аудит архівної системи на відповідність політиці інформаційної безпеки та рекомендаціям ISO 15489. За результатами аналізу було встановлено:

98% внутрішніх документів мають електронні копії;

92% критично важливих документів зберігаються у форматі PDF/A;

усі договори старші за 5 років пройшли процедуру резервного копіювання;

100% особових справ працівників оцифровані та мають електронні досьє;

у 6% випадків було виявлено дублікати файлів, що потребують оптимізації.

На основі висновків аудиту керівництвом компанії було ухвалено рішення про створення централізованої інтегрованої архівної платформи на базі власної ERP-системи, що дозволить автоматизувати всі процеси зберігання, скоротити витрати на обслуговування, зменшити людський фактор і забезпечити єдині правила обігу документів на всіх рівнях управління.

Таким чином, структура документного потоку та регламенти архівування в ТОВ «4В Україна» свідчать про високий рівень організованості, адаптацію до сучасних викликів цифрового середовища та стратегічне бачення в питанні інформаційної безпеки. Подальше вдосконалення цієї системи, включаючи впровадження штучного інтелекту для автоматичної класифікації документів, стане запорукою стійкості, законності та ефективності всієї організаційної діяльності компанії [4].

Організація електронного та паперового архіву на підприємстві є критично важливою складовою інформаційного управління, що забезпечує збереження, доступність, достовірність і правову значущість документів. У компанії ТОВ «4В Україна» реалізована змішана модель архівування, яка поєднує традиційні підходи з сучасними цифровими технологіями. Це дозволяє забезпечити гнучкість у роботі з різними типами інформації, дотримуватись вимог чинного законодавства, підвищити ефективність внутрішніх процесів та гарантувати архівну безпеку. Впроваджена система базується на принципах структурованості, доступності, резервування, конфіденційності та збереження документів протягом усього періоду їх юридичної чинності.

Паперовий архів на підприємстві функціонує як централізоване сховище, яке обслуговується архіваріусом і знаходиться в спеціально облаштованому приміщенні з дотриманням умов температурного режиму, вологості, освітлення та протипожежної безпеки. Документи, які підлягають обов'язковому зберіганню в паперовій формі (оригінали договорів, фінансові документи з мокрими підписами, кадрові справи), проходять процедуру реєстрації в архівному журналі, описуються за формуляром і розміщуються у стелажах відповідно до хронологічного та тематичного принципу.

У паперовому архіві використовується система індексації, що складається з шифру документу (тип + рік + порядковий номер), яка наноситься на обкладинку кожної справи. Кожна справа містить внутрішній опис із зазначенням кількості аркушів, короткої анотації та дати закриття. Доступ до архіву здійснюється за письмовим запитом, затвердженим керівником відповідного підрозділу. У разі необхідності архіваріус надає копії документів, залишаючи оригінали на місці. Щорічно проводиться інвентаризація фонду з метою виявлення відсутніх або пошкоджених справ.

Електронний архів функціонує як частина внутрішньої ERP-системи підприємства та складається з кількох рівнів доступу: загального, службового та обмеженого. Вся документація, що надходить або створюється в компанії, одразу реєструється в системі електронного документообігу, зберігається у форматі PDF/A та супроводжується електронним підписом. Для кожного типу документів встановлено окремі правила зберігання: строк, обсяг, резервне копіювання, журнал доступу, контроль автентичності.

Електронні документи сортуються в електронному архіві за принципом «каталог – підкаталог – файл». Кожен каталог відповідає функціональному напрямку: договірна діяльність, бухгалтерія, IT-проєкти, HR, юриспруденція, адміністративні документи. Підкаталоги структуруються за роками, а далі — за назвами контрагентів або внутрішніми кодами справ. З метою уніфікації, всі документи іменуються за єдиним шаблоном: [тип документу][дата][назва контрагента/відділу]_[номер/код].

Особливу увагу в організації електронного архіву приділено системі резервного копіювання. Усі дані архівуються на щоденній основі з використанням алгоритмів інкрементного збереження, а повне резервне копіювання здійснюється щотижнево з перенесенням на окремий фізичний диск та синхронізацією з хмарним сховищем. Дані зберігаються у трьох екземплярах, що дозволяє відновити архів у випадку фізичних пошкоджень, збоїв системи або кібератак [31].

Таблиця 3.3

Порівняння функціонування паперового та електронного архівів ТОВ «4В Україна»

Параметр	Паперовий архів	Електронний архів
Місце зберігання	Обладнане архівосховище	Сервер + хмара + зовнішній носій
Формат документів	Оригінали, копії, акти, договори	PDF/A, XML, JPG
Ідентифікація	Шифр, індекс, опис справи	Єдиний шаблон іменування файлів
Пошук	Ручний, за журналом	Електронний, з фільтрами та тегами
Доступ	Письмовий запит	Авторизований доступ із логуванням
Термін зберігання	Від 3 до 75 років	Встановлюється у метаданих
Копіювання	Фотокопія, скан	Резервне копіювання щодня
Безпека	Протипожежні заходи, охорона	Шифрування, двофакторна аутентифікація

У 2024 році було прийнято внутрішній наказ про модернізацію архівної структури, який передбачав впровадження «дзеркального архіву» — кожна одиниця паперового зберігання обов’язково має свій цифровий відповідник, який зберігається у відповідному підкаталозі електронної системи. Такий підхід забезпечує не лише дублювання, а й полегшує доступ до інформації для аудиторів, юристів, менеджерів проєктів. Усі документи, які надходять у паперовій формі, обов’язково скануються та проходять оптичне розпізнавання тексту (OCR), що дозволяє індексувати зміст і проводити повнотекстовий пошук.

Практичне функціонування електронного архіву підтримується спеціальним модулем у корпоративній ERP-системі, до якої мають доступ лише авторизовані співробітники. Кожен документ у системі має унікальний ідентифікатор, прив’язаний до автора, дати створення, типу документа, рівня

доступу та призначеного терміну зберігання. Для забезпечення цілісності архіву реалізовано функцію хеш-перевірки на рівні кожного файлу, яка автоматично виявляє будь-яке несанкціоноване втручання в документ.

У випадку, якщо документ втрачає актуальність або завершується строк його зберігання, система надсилає автоматичне повідомлення відповідальній особі про необхідність перенесення документа до архіву довготривалого зберігання або знищення відповідно до регламенту. Усі операції, пов’язані з вилученням, супроводжуються створенням акта списання або видалення [38].

Таблиця 3.4

Автоматизовані процеси в електронному архіві ТОВ «4В Україна»

Процес	Інструмент реалізації	Частота / умова запуску
Автоматичне резервне копіювання	Google Drive API + NAS	Щодня
Контроль терміну зберігання	Cron-сценарій + електронний журнал	Щомісяця перевірка
Повідомлення про закінчення терміну	Email-сповіщення через ERP-модуль	За 30 днів до дати
Контроль змін у файлах	Хеш-лог (SHA-256)	У момент збереження файлу
Пошук документів	Повнотекстовий індекс	За запитом користувача
Вилучення за регламентом	Автоматична генерація акта	Після погодження керівником

Завдяки поєднанню традиційного та цифрового підходів, компанії вдалося побудувати надійну, гнучку й масштабовану архівну інфраструктуру, що відповідає сучасним вимогам безпеки, мобільності та правової відповідності. Така система дозволяє ефективно взаємодіяти з податковими органами, контролюючими інстанціями, клієнтами та партнерами, не витрачаючи надмірний час на пошук, копіювання чи перевірку документів.

У перспективі планується розширення архівної платформи за рахунок інтеграції з блокчейн-рішеннями для фіксації ключових транзакцій і документів, а також впровадження штучного інтелекту для автоматичної класифікації, категоризації та оцінки ризиків, пов’язаних із доступом до критично важливої інформації.

Таким чином, організація електронного та паперового архіву в ТОВ «4В Україна» демонструє комплексний підхід до збереження корпоративної пам’яті, управління документами та інформаційної безпеки. Цей досвід може бути адаптований як для державних, так і для приватних підприємств, що прагнуть оптимізувати архівні процеси відповідно до сучасних реалій та технологічних можливостей.

3.2. Аналіз застосування цифрових засобів архівної безпеки

Захист архівної інформації є одним із ключових елементів внутрішньої безпекової політики підприємства, що функціонує в умовах цифрової трансформації. У ТОВ «4В Україна» питання архівної безпеки виведено на стратегічний рівень, оскільки компанія оперує великим обсягом конфіденційної інформації — проєктною, договірною, фінансовою, кадровою, аналітичною. Забезпечення цілісності, доступності та конфіденційності архівних матеріалів здійснюється за допомогою комплексу технічних рішень, які охоплюють як фізичну інфраструктуру, так і програмно-апаратні засоби цифрового захисту.

На рівні фізичного середовища архіву підприємство забезпечує базовий рівень технічної безпеки, включаючи контроль доступу до архівного приміщення (електронні замки з логуванням входів), охоронну сигналізацію, відеоспостереження, автоматичні протипожежні системи. Приміщення, де розташовані сервери, резервні носії та паперові архіви, мають обмежений доступ, а допуск до них мають лише відповідальні особи згідно з внутрішнім наказом. Усі дії персоналу, пов’язані з доступом до архівів, реєструються в журналі допусків [21].

Основну частину безпеки забезпечують програмні рішення, реалізовані через багаторівневу систему контролю та управління доступом до архівів. Серед впроваджених технічних рішень ключову роль відіграють:

Система шифрування даних — AES-256 для всіх архівних файлів, що зберігаються на серверах і в хмарних середовищах;

Цифрові сертифікати підпису — для договорів, актів, технічної документації;

Система двофакторної автентифікації (2FA) — при вході в архівний модуль;

Логування всіх дій з документами — створення, перегляд, редагування, видалення;

Антивірусне програмне забезпечення — з щоденними оновленнями та скануванням серверів;

VPN-підключення — для дистанційного доступу до архіву з корпоративних ноутбуків;

Інтеграція з SIEM-системою — для автоматичного виявлення аномальної активності.

Для централізованого управління архівними даними в компанії створено окремий сервер з віртуальним середовищем (VMware), який розгорнутий у внутрішній мережі підприємства. Сервер має окремі віртуальні машини для зберігання договірної документації, бухгалтерських архівів, кадрових справ та проєктних матеріалів. Усі дані зберігаються у форматі PDF/A та XML з обов'язковою верифікацією контрольної суми файлу.

Таблиця 3.5

Технічні рішення захисту архівної інформації в ТОВ «4В Україна»

Напрям захисту	Технічне рішення	Призначення
Контроль доступу	Електронні замки, біометрія, облік входів	Фізичний контроль за архівними приміщеннями
Шифрування даних	AES-256, SSL, BitLocker	Захист даних від несанкціонованого доступу
Автентифікація	2FA, корпоративна SSO	Перевірка особи користувача
Резервне копіювання	Щоденна інкрементальна + тижнева повна копія	Збереження даних у разі втрат
Контроль змін	Логування дій, хеш-функції	Прозорість і цілісність архівної інформації
Захист периметра	VPN, Firewall, IDS	Блокування зовнішніх загроз
Антивірусний захист	ESET Endpoint Security	Виявлення шкідливого ПЗ
Система сповіщень	Email-алерти, SMS-попередження	Реакція на інциденти безпеки
Аудит безпеки	Щоквартальні перевірки + зовнішній аудит	Верифікація ефективності технічних рішень

Електронний архів функціонує в рамках ERP-системи з інтегрованим модулем документообігу. Всі документи, що підлягають архівуванню, автоматично перевіряються за контрольними ознаками, зокрема:

наявність електронного підпису;

відповідність шаблону;

наявність захисного цифрового водяного знаку;

контроль на дублікати та пошкодження файлу.

З метою виявлення спроб несанкціонованого доступу та аномальної поведінки користувачів запроваджено SIEM-систему на базі Splunk, яка аналізує логи, трафік і зразки поведінки, порівнюючи їх із базами інцидентів безпеки. У випадку виявлення відхилень система формує сповіщення, а також, за необхідності, блокує сесію доступу [27].

Таблиця 3.6

Автоматизовані сценарії реагування на інциденти в ТОВ «4В Україна»

Тип інциденту	Автоматизована дія	Людський фактор
Неуспішна авторизація 3+ рази	Тимчасове блокування акаунта	Повідомлення ІТ-відділу
Завантаження великої кількості файлів	Запис в лог + сповіщення	Перевірка менеджером архіву
Зміна контрольної суми файлу	Блокування документа	Аудит з боку ІТ-фахівця
Спроба експорту архівів	Переривання операції	Розслідування
Виявлення шкідливого ПЗ	Автоматичне карантинування	Повідомлення служби безпеки

У 2024 році в ТОВ «4В Україна» було впроваджено окремий модуль захисту для електронного архіву, побудований на принципах нульової довіри (Zero Trust Security). Основні компоненти рішення включали:

сегментацію доступу до архівних даних за принципом «найменшого привілею»;

регулярну зміну паролів з політикою складності (12+ символів, обов’язково спецзнаки);

прив’язку IP-адреси користувача до геолокації;

автоматичне завершення сесії після 10 хвилин бездіяльності;

обов’язкове використання VPN для позаштатного доступу.

Після впровадження рішення компанія досягла значного зниження ризиків втрати чи компрометації даних. Було проведено навчання персоналу з кібергігієни, а також створено інструкцію щодо поведінки в разі інцидентів безпеки.

Таблиця 3.7

Ефекти від впровадження технічних рішень в архівній безпеці

Показник	До впровадження	Після впровадження
Кількість інцидентів на місяць	~7	≤2
Час доступу до архівного документа (середн.)	3–5 хвилин	20–30 секунд
Ймовірність втрати документа	1,5%	<0,1%
Рівень задоволеності користувачів (опитування)	71%	96%

Таким чином, технічні рішення, впроваджені в ТОВ «4В Україна» для захисту архівів, демонструють ефективну модель поєднання фізичних, цифрових і організаційних заходів, які дозволяють забезпечити цілісність, безперервність та конфіденційність збережених документів. Системна модернізація інфраструктури, автоматизація реагування на загрози, використання шифрування та логування — це сучасні підходи, що можуть стати прикладом для інших українських підприємств у сфері побудови безпечного архівного середовища [17].

Проблеми цифрової безпеки та ризики втрати архівної інформації в умовах диджиталізації становлять одну з найбільш критичних загроз для сучасних підприємств, зокрема для таких, як ТОВ «4В Україна», які активно впроваджують інформаційні технології в документообіг і архівування. З одного боку, цифровізація дозволяє підвищити ефективність, зменшити витрати на паперову документацію та забезпечити мобільність доступу, але з іншого — створює значну зону уразливості, пов’язану з кібератаками, програмними збоями, людським фактором, технічними несправностями і правовими колізіями.

Цифрова архівна інформація, на відміну від традиційної паперової, вимагає комплексного підходу до захисту. Зокрема, вразливими залишаються такі складові, як канали передачі даних, облікові записи користувачів, системи резервного копіювання, бази даних, платформи електронного підпису, а також

фізична безпека серверного обладнання. Навіть за наявності сучасних технічних засобів шифрування та автентифікації, підприємство може зіткнутися з ситуацією, коли втрата архіву або компрометація даних відбувається внаслідок внутрішніх або зовнішніх факторів.

Одна з найпоширеніших проблем цифрової безпеки — людський фактор. Помилки співробітників, такі як випадкове видалення файлів, неправильне надання прав доступу, використання слабких паролів, відкриття шкідливих вкладень у листах або копіювання архівів на незахищені носії, призводять до порушення цілісності архівної інформації. Відсутність культури інформаційної гігієни в колективі загрожує витоками критично важливих документів.

Ще одна група ризиків пов’язана з програмним забезпеченням. Використання застарілих або неправильно налаштованих систем електронного документообігу, вразливості в операційних системах або у програмах для роботи з архівами можуть бути використані хакерами для викрадення, підміни або шифрування даних з метою викупу (ransomware). Окремі атаки можуть бути спрямовані на порушення доступності архіву (DDoS-атаки), що унеможливлює отримання важливих документів у критичні моменти.

Таблиця 3.8

Основні джерела ризику цифрової архівної безпеки

Джерело ризику	Потенційні наслідки	Приклад ситуації
Людський фактор	Видалення/викрадення/витік даних	Помилкове надання доступу до архіву новачку
Кібератаки (віруси, фішинг)	Шифрування, видалення, крадіжка документів	Відкриття шкідливого листа бухгалтером
Збій програмного забезпечення	Пошкодження структури даних, втрати	Падіння БД архіву після оновлення
Відсутність резервного копіювання	Втрата даних у разі збоїв	Вірус знищив основну копію та не було резервної
Зношеність обладнання	Фізична втрата носія, нестабільність системи	Вихід з ладу HDD сервера
Несанкціонований доступ	Перегляд або знищення документів сторонніми	Компрометація пароля адміністратора
Невизначеність правового статусу	Оскарження автентичності архівів	Відсутність е-підпису чи електронної мітки часу

У практичному функціонуванні архіву ТОВ «4В Україна» було виявлено низку випадків, які вказують на актуальність проблем цифрової безпеки. Зокрема, в листопаді 2023 року внаслідок людської помилки працівника архіву були тимчасово втрачені метадані понад 250 електронних документів, оскільки перед архівуванням не було проставлено ідентифікаційний код, що зробило неможливим їхній пошук. Випадок було виправлено, однак він спричинив затримку у наданні даних під час аудиторської перевірки.

Інший інцидент відбувся у квітні 2024 року, коли антивірусне ПЗ не виявило модифікований троян, який проник через поштовий клієнт. Зловмисне ПЗ шифрувало файли у папках загального доступу, включаючи резервну копію архіву. Після виявлення атаки частину архіву вдалося відновити лише з третьої резервної копії, яка зберігалась офлайн. Цей інцидент призвів до перегляду політики багаторівневого резервування та впровадження додаткових протоколів доступу [1].

У структурі ризиків особливо критичною є проблема неповного або нестабільного резервного копіювання. У разі непрацюючого скрипту копіювання або пошкодженого зовнішнього диска компанія ризикує втратити місяці важливої документації. Крім того, збереження архівів лише в цифровому форматі без дублювання в альтернативних середовищах (наприклад, офлайн-носіях або в іншій хмарі) створює однобічну залежність, що суперечить принципам архівної стійкості [6].

Таблиця 3.9

Виявлені проблеми цифрової архівної безпеки в ТОВ «4В Україна» (2023–2024)

Проблема	Тип документа	Наслідки	Реакція підприємства
Втрата метаданих через помилку	Договори	Неможливість пошуку	Розроблено шаблон обов’язкових полів
Атака вірусу-зашифровувача	Усі категорії	Шифрування архіву, втрата 3 днів	Впроваджено 3-рівневе резервування
Зношення фізичного носія резерву	Кадрові справи	Втрата актуальної копії	Замінено носії + SMART-моніторинг
Компрометація пароля архівіста	Проєктні документи	Несанкціонований перегляд	Запроваджено 2FA
Відсутність цифрового підпису	Акти виконаних робіт	Недійсність у судовому процесі	Автоматичне підписування обов’язкових документів

Після серії інцидентів у 2023–2024 роках, керівництвом ТОВ «4В Україна» було прийнято стратегію підвищення цифрової безпеки архіву, яка включає такі кроки:

1. Аудит усіх облікових записів, що мають доступ до архіву, із запровадженням обмежень за принципом мінімального привілею.
2. Впровадження трирівневої системи резервного копіювання — щоденне локальне, щотижневе хмарне, щомісячне — офлайн.
3. Обов’язкове електронне підписування ключових документів, включаючи накладення часових міток.
4. Щоквартальне оновлення антивірусного ПЗ та перевірка актуальності сигнатур.
5. Розробка інструкцій для співробітників щодо безпечної роботи з архівними файлами.
6. Модернізація серверного обладнання з підтримкою ECC-пам’яті та RAID-масивів для фізичного захисту даних.
7. Запровадження модулів логування з автоматичним сповіщенням про аномальні події.

Реалізація вказаних заходів дозволила скоротити кількість інцидентів із 8 у 2023 році до 3 у першому півріччі 2024-го. Компанія також ввела навчальні тренінги з цифрової гігієни, які тепер є обов'язковими для нових співробітників, що працюють із документацією. Щомісячно проводиться тестування на фішингову стійкість, що підвищує рівень обізнаності персоналу.

Таким чином, проблеми цифрової безпеки та ризики втрати архівної інформації залишаються постійними викликами для сучасних підприємств. Навіть у технологічно прогресивному середовищі, як у ТОВ «4В Україна», людський фактор, технічні несправності, неактуальні налаштування або нехтування процедурами можуть призвести до суттєвих інформаційних втрат. Саме тому забезпечення архівної безпеки має базуватись не лише на програмному забезпеченні, а й на системному підході, що включає аудит, навчання, резервування, а також контроль і прозорість усіх операцій. Це дозволяє не лише мінімізувати наслідки інцидентів, а й сформувати стійку корпоративну культуру цифрової відповідальності.

3.3. Пропозиції щодо вдосконалення архівної безпеки в ТОВ «4В Україна»

Підвищення надійності зберігання цифрових архівів є однією з ключових умов безперебійного функціонування підприємства в умовах диджиталізації документообігу. Надійність у цьому контексті означає збереження цілісності, доступності, автентичності та захищеності архівної інформації упродовж усього терміну її зберігання, незалежно від змін у технологіях, людського чинника, кіберзагроз чи фізичних пошкоджень носіїв. У випадку ТОВ «4В Україна» особливу актуальність ця проблема набуває через високу щільність інформаційного навантаження, наявність великого обсягу ділових документів, договірної інформації, кадрових даних та технічної документації, що підлягають збереженню не менше ніж 5–75 років.

Для досягнення високого рівня надійності цифрових архівів слід поєднувати організаційні, технічні та технологічні рішення. Передусім, підприємству доцільно реалізувати політику архівної сталості, яка передбачає,

що будь-який архівний об'єкт зберігається у відповідному форматі, має актуальну метаінформацію, мінімально залежить від конкретного програмного забезпечення і підлягає періодичному контролю з боку системи.

Перший крок — уніфікація форматів архівного зберігання. Для забезпечення довгострокового доступу до цифрових документів рекомендовано використовувати стандартизовані формати, зокрема PDF/A (для текстових документів), TIFF (для сканів), XML/JSON (для структурованих даних), MPEG-4 (для відео). Ці формати мають підтримку метаданих, не залежать від конкретного вендора і мають стабільну специфікацію.

Другий аспект — модель багаторівневого резервного зберігання. Резервне копіювання архівних даних має здійснюватися за принципом 3-2-1: три копії даних, на двох різних типах носіїв, одна з яких зберігається поза офісом або в хмарі. Це дозволяє зменшити ризик повної втрати інформації через форс-мажор або збій в інфраструктурі.

Третім компонентом є впровадження систем моніторингу доступу до архівів та виявлення інцидентів. Необхідно фіксувати всі дії користувачів із документами, створювати журнали подій (лог-файли), періодично їх перевіряти, а також запровадити SIEM-рішення для виявлення аномальної поведінки в режимі реального часу.

Четвертим важливим фактором є періодичне перевіряння цілісності архівних файлів. Усі документи повинні мати контрольні хеш-суми (SHA-256 або інші), що зберігаються в окремому архіві. Порівняння контрольної суми на момент створення й у процесі доступу дозволяє виявити зміни, пошкодження або спроби підробки [37].

Таблиця 3.10

Ключові напрямки підвищення надійності архівного зберігання

№	Напрямок	Рекомендації
1	Формат зберігання	Використовувати PDF/A, XML, TIFF, MPEG-4
2	Резервне копіювання	3-2-1 модель з інкрементальним копіюванням
3	Метадані	Ведення ISO 14721 сумісного опису: дата, автор, термін зберігання
4	Контроль доступу	2FA, ролі, VPN, журналювання
5	Шифрування	AES-256 на рівні файлу + SSL при передачі
6	Цілісність	Хешування (SHA-256), періодичні перевірки
7	Інформаційна гігієна	Тренінги, політики, стандарти, контроль дій користувачів
8	Вибір носіїв	SSD, RAID-схеми, стрічкові бібліотеки для довгострокового зберігання
9	Міграція даних	Планові переноси з одного носія на інший не рідше ніж кожні 5–7 років
10	Тестування відновлення	Регулярна перевірка працездатності резервних копій

Практична реалізація в ТОВ «4В Україна» включає низку кроків, які вже розпочаті або плануються до впровадження. Зокрема, компанія провела інвентаризацію архіву й уніфікувала всі файли, що зберігаються більше 5 років, у формат PDF/A. Було впроваджено модуль в ERP-системі, який автоматично генерує архівну копію кожного документа після його фінального підпису. Архівні копії зберігаються на окремому сервері, який функціонує лише в режимі читання (read-only), що виключає можливість випадкових змін.

Також у рамках системи резервного копіювання було реалізовано розподіл за рівнями критичності:

щоденне резервування: бухгалтерія, договори, фінансові звіти;

щотижневе: технічна документація, проєктні архіви;

щомісячне: особові справи працівників, історичні довідки, архіви проектів.

Це дозволило досягти більшої ефективності у використанні носіїв та підвищити швидкість відновлення в разі інциденту. Окрему увагу приділено використанню контрольних списків на перевірку цілісності архіву, які щоквартально оновлюються і перевіряються ІТ-відділом.

Таблиця 3.11

Модель багаторівневого зберігання архіву в ТОВ «4В Україна»

Категорія документів	Частота копіювання	Формат	Тип носія	Захист
Договори та акти	Щодня	PDF/A	Сервер + Хмара	Шифрування, 2FA
Кадрова документація	Щомісяця	PDF, JPG	Зовнішній HDD	Контроль доступу
Проєктно-технічна документація	Щотижня	Markdown, PDF	RAID-масив	Read-only режим
Стратегічна інформація	Щомісяця	XML, DOCX	Стрічкове сховище	Архівація

Важливою частиною підвищення надійності є **управління термінами зберігання**. Кожен архівний об’єкт повинен мати позначення: «короткостроковий», «середньостроковий», «довгостроковий» або «постійного зберігання». Це дозволяє оптимізувати ресурси та зосередитися на найбільш критичних категоріях.

У компанії також ініційовано розробку **політики цифрової спадкоємності** — документ, що описує дії у випадку зміни керівника архіву, втрати паролів або заміни основного обладнання. Це знижує ризики при переході між поколіннями систем та персоналу.

Для забезпечення **правової достовірності** документів у довготривалому архіві компанія інтегрувала систему електронного підпису, яка підтримує накладання кваліфікованого підпису з електронною часовою міткою (timestamp). Таким чином, навіть після 10 років можна підтвердити автентичність документа в суді [32].

Практична частина: впровадження системи моніторингу та автоматичного відновлення

ТОВ «4В Україна» у 2025 році розпочало проєкт створення архівної підсистеми з автоматичним відновленням після збою. У межах цього проєкту:

- реалізовано щоденне інкрементальне копіювання на хмару AWS;
- впроваджено систему постійного моніторингу стану носіїв з SMART-аналізом;

- інтегровано скрипт відновлення структури архіву на тестовому середовищі;
- введено звітність щодо працездатності резервних копій (автоматичний звіт раз на тиждень);
- тестування на відновлення проводиться кожні 60 днів для кожної критичної категорії.

Ці рішення дозволили зменшити середній час відновлення архіву з 4 годин до 35 хвилин, а ймовірність втрати даних — до <0,1%.

Таким чином, підвищення надійності цифрових архівів вимагає цілісного, системного підходу, що включає вибір правильних форматів, багаторівневе резервування, технічний захист, організаційну культуру безпеки та юридичну обґрунтованість дій. Успішне впровадження таких рішень у ТОВ «4В Україна» може слугувати орієнтиром для інших підприємств, що прагнуть забезпечити інформаційну стійкість в умовах цифрового світу.

Стратегія модернізації архівної системи підприємства в умовах диджиталізації є необхідною умовою для забезпечення ефективності, безперервності та безпеки обігу документів у середовищі, де зростає обсяг цифрової інформації, вимоги до збереження, а також загрози кіберпростору. У випадку ТОВ «4В Україна», яке активно реалізує проєкти у сфері цифрових трансформацій, стратегія модернізації архівної системи стала відповіддю на виклики масштабування, зростання інформаційного навантаження, необхідності комплаєнсу з міжнародними стандартами та розвитку електронного документообігу.

Поточна архівна система підприємства була побудована за змішаною моделлю, що включає паперові та електронні архіви. Хоча вона частково автоматизована та захищена, її функціонал обмежений за глибиною аналітики, гнучкістю масштабування, інтеграцією з зовнішніми платформами (CRM, бухгалтерськими програмами, державними електронними сервісами). Відсутність централізованого обліку документів з історією змін, обмежені можливості віддаленого керування та недостатня уніфікація форматів — усе це

визначає потребу в комплексній модернізації, що має охопити інфраструктуру, програмне забезпечення, політику безпеки та організаційні процедури.

Першим напрямком стратегічного оновлення є впровадження централізованої архівної платформи з єдиним інтерфейсом, доступним усім структурним підрозділам компанії. Така платформа має містити інтегровану базу даних, систему тегування, автоматичне визначення термінів зберігання, оптичне розпізнавання документів (OCR), модуль електронного підпису та підтримку мобільного доступу. Очікуваним результатом стане скорочення часу пошуку документів, зменшення дублювання, підвищення прозорості дій користувачів.

Другим стратегічним вектором модернізації є міграція на хмарну архітектуру з використанням гібридної моделі зберігання. Частина архівів з високими вимогами до безпеки (кадрова, фінансова документація) зберігається локально з періодичним дублюванням у хмарі, тоді як менш критичні документи переміщуються до захищених хмарних середовищ, таких як AWS, Google Cloud або Azure. Важливою умовою тут є шифрування даних, багатофакторна автентифікація та можливість географічної диверсифікації доступу до архіву.

Наступним етапом є автоматизація життєвого циклу документів — від моменту створення до знищення або передачі в архів довгострокового зберігання. Це включає формування шаблонів документів, автоархівацію після затвердження, прив'язку до відповідальних осіб, автоматичне нагадування про завершення строків зберігання, створення актів на видалення. У цьому контексті доцільним є впровадження BPM-рішень (Business Process Management), які дозволять описати та оптимізувати всі процеси з обігу документів [20].

Окрему увагу слід приділити управлінню ризиками цифрової втрати даних, що реалізується через політику багаторівневого резервного копіювання, регулярне тестування сценаріїв відновлення, контроль за апаратними носіями та активну політику оновлення програмного забезпечення. У межах цієї стратегії передбачено щорічний аудит архівної системи незалежною IT-компанією та сертифікацію співробітників, які відповідають за збереження архівів.

Таблиця 3.12

Основні складові стратегії модернізації архівної системи підприємства

Напрям модернізації	Опис заходів	Очікуваний результат
Централізація архівної системи	Впровадження єдиної платформи з інтеграцією всіх підрозділів	Зниження витрат на обслуговування, підвищення ефективності
Перехід на хмарну інфраструктуру	Використання хмарних сховищ з криптозахистом	Безперервний доступ, надійне резервування
Автоматизація життєвого циклу	Автоматичне створення, підписання, архівація, видалення	Мінімізація людського фактору, прискорення процесів
Стандартизація форматів документів	Використання PDF/A, XML, TIFF, JSON	Уніфікованість, сумісність із міжнародними системами
Інформаційна безпека	SIEM, DLP, IDS, VPN, 2FA, логування	Захист від атак, збереження даних
Візуалізація доступу	Дашборди для моніторингу стану архіву	Оперативний контроль і швидка реакція
Навчання персоналу	Курси, тренінги, сертифікація з кібергігієни	Сформовані навички захисту інформації
Аудит і перевірки	Внутрішній та зовнішній аудит, тестування на проникнення	Постійне вдосконалення і контроль

У практичному вимірі модернізація архівної системи в ТОВ «4В Україна» вже розпочалася із створення проєктної групи, що включає представників IT-відділу, керівників підрозділів, фахівців з документообігу та зовнішніх консультантів. Першим реалізованим кроком стала розробка технічного завдання (ТЗ) на нову архівну систему, яка має підтримувати API-з’єднання з обліковими системами, базами даних, електронною поштою, сервісами хмарного підпису.

У 2024 році було запущено пілотний проєкт, який охопив один із департаментів компанії. Було протестовано платформу Alfresco, яка дозволяє гнучко управляти цифровими архівами, створювати правила обробки файлів, надавати доступ на рівні груп, вести хронологію змін. Під час тестування отримано позитивний відгук від користувачів, а час доступу до документації скоротився в середньому з 5 хвилин до 20 секунд [4].

Таблиця 3.13

Етапи реалізації стратегії модернізації в ТОВ «4В Україна»

Етап	Зміст	Термін реалізації
1. Ініціація та аудит	Аналіз існуючої системи, виявлення вразливих точок	Квітень 2024
2. Розробка ТЗ	Узгодження вимог до архівної системи	Травень 2024
3. Вибір платформи	Порівняння рішень: Alfresco, M-Files, DocuWare	Червень 2024
4. Пілотний запуск	Впровадження на одному відділі	Липень–серпень 2024
5. Масштабування	Розгортання на всіх підрозділах	Вересень–грудень 2024
6. Тестування відновлення	Імітація інцидентів, перевірка відновлення	Лютий 2025
7. Аудит і вдосконалення	Зовнішній аудит + оновлення політик	Квітень 2025

З метою забезпечення гнучкості в майбутньому, до архітектури нової архівної системи було закладено принципи масштабованості та модульності. Це дозволяє адаптувати систему до нових потреб без повної її заміни. Наприклад, у майбутньому можлива інтеграція модуля штучного інтелекту, що здійснюватиме автоматичну класифікацію документів, виявлення дублікатів і прогнозування ризиків доступу.

У сфері нормативної відповідності ТОВ «4В Україна» передбачає адаптацію архівної політики до стандартів ISO 27001, ISO 14721 (OAIS) та українських ДСТУ щодо електронного документообігу. Це дозволить не лише поліпшити внутрішній контроль, а й підвищити довіру з боку партнерів, державних органів і клієнтів.

Таким чином, стратегія модернізації архівної системи підприємства в умовах диджиталізації повинна бути багатоетапною, системною і орієнтованою на майбутнє. Вона включає технічне переоснащення, зміни в підходах до керування документами, посилення захисту, активізацію людського потенціалу та тісну інтеграцію з іншими цифровими процесами підприємства. Досвід ТОВ «4В Україна» демонструє, що при стратегічному плануванні, залученні компетентних фахівців та постійному аналізі ефективності, модернізація архівної системи перетворюється з технічного завдання на фактор стійкості й конкурентоспроможності компанії [13].

ВИСНОВКИ

У процесі дослідження теми «Особливості впровадження систем архівної безпеки в умовах диджиталізації» було встановлено, що сучасний розвиток цифрових технологій суттєво трансформує архівну сферу, роблячи її більш гнучкою, мобільною та водночас уразливою до нових загроз. Архівна безпека перестає бути лише технічним аспектом діяльності організації — вона стає складовою стратегічного управління ризиками, охоплюючи питання інформаційної, правової, фізичної та кібербезпеки. В умовах диджиталізації архіви виконують не лише функцію зберігання, а й стають центром доказової, управлінської, історичної та нормативної значущості, що вимагає від підприємств розбудови системи захисту на основі багаторівневого підходу.

На теоретичному рівні виявлено, що архівна безпека включає комплекс складових — фізичний захист, інформаційне шифрування, автентифікацію користувачів, контроль доступу, резервне копіювання, аудит дій з документами, а також відповідність національним і міжнародним стандартам. Аналіз загроз показав, що цифрове середовище створює нові виклики: від втрати даних унаслідок збоїв до цілеспрямованих кібератак, внутрішніх витоків інформації та правових колізій щодо електронного підпису, формату, метаданих і доказовості документів.

Важливим результатом дослідження стало вивчення міжнародного досвіду, що доводить ефективність таких рішень, як використання хмарних технологій, блокчейн-інфраструктур, цифрових сертифікатів автентичності, а також автоматизованих систем управління життєвим циклом документів. У межах вітчизняного контексту простежено активізацію державної політики цифровізації архівної сфери, зокрема через реалізацію програм Мінцифри, запуск Єдиного державного вебпорталу електронних послуг, запровадження електронного документообігу в органах влади, хоча реальний стан регіональних архівів часто залишається критичним.

Практична частина дослідження, що базується на аналізі архівної системи ТОВ «4В Україна», дозволила виявити сильні сторони у сфері безпеки, як-от наявність багаторівневого контролю доступу, централізоване шифрування, політика резервного копіювання, використання систем журналювання, а також слабкі місця — часткову фрагментарність архівної інфраструктури, обмежену інтеграцію між підрозділами, ризики людського фактора та недосконаліть інтерфейсу взаємодії зі сторонніми сервісами. Інциденти втрати або компрометації архівної інформації, що траплялися у 2023–2024 роках, стали основою для формування оновленої політики цифрової безпеки.

В межах дослідження було сформульовано низку практичних рекомендацій щодо підвищення надійності цифрових архівів, серед яких: уніфікація форматів зберігання, впровадження життєвого циклу документообігу з автоматичним архівуванням, застосування SIEM-систем для виявлення аномалій, регулярне тестування відновлення з резервів, а також навчання персоналу щодо інформаційної гігієни. Пропозиції були покладені в основу стратегії модернізації архівної системи підприємства, яка передбачає перехід до централізованої електронної платформи, масштабування хмарної інфраструктури, впровадження електронного підпису з часовою міткою та реалізацію сценаріїв аварійного відновлення.

Узагальнюючи результати, можна стверджувати, що ефективне впровадження систем архівної безпеки в умовах диджиталізації можливе лише за умови поєднання технологічних інструментів, нормативної відповідності та організаційної дисципліни. Підприємства, що прагнуть зберігати конкурентоспроможність та правову стабільність, мають забезпечити постійне оновлення технічних засобів захисту архівів, вдосконалювати внутрішні процедури і формувати культуру цифрової відповідальності серед персоналу. Досвід ТОВ «4В Україна» може бути використаний як модель побудови комплексної системи архівної безпеки для середніх та великих організацій у сучасних умовах інформаційної економіки.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO 14721:2012. Reference model for an Open Archival Information System (OAIS). – International Organization for Standardization. – Geneva, 2012. – 135 p.

2. U.S. National Archives and Records Administration. Managing Electronic Records. – 2021. – [Online]. – Available at: https://www.archives.gov/records-mgmt/policy/managing-electronic-records

3. Архівна служба представила проєкт з оцифрування архівних документів // Цензор.НЕТ. – 2020. – [Електронний ресурс]. – Режим доступу: https://censor.net/ua/news/3172820/arhivna_slujba_predstavyla_proyekt_z_otsyfruvannya_arhivnyh_dokumentiv

4. Архівна справа та діловодство: навч. посіб. / С. О. Кульчицький, Н. М. Ковальчук. – Київ: Ліра-К, 2021. – 312 с.

5. Архівні технології: навч. посіб. / за ред. О. М. Бондаря. – Львів: Вид-во ЛНУ ім. Івана Франка, 2020. – 208 с.

6. Архівознавство: підручник / [ред. М. І. Степаненко]. – Київ: Центр учбової літератури, 2020. – 296 с.

7. Білоус Н. В. Інформаційна безпека в умовах цифровізації суспільства // Інформаційне право України. – 2022. – № 1(34). – С. 45–50.

8. Валюшко І. О. Кібербезпека України: наукові та практичні виміри // Вісник КНУ імені Тараса Шевченка. Серія «Проблеми безпеки інформації». – 2020. – № 2. – С. 5–12.

9. Валюшко І. О. Кібербезпека України: наукові та практичні виміри // Вісник КНУ імені Тараса Шевченка. Серія «Проблеми безпеки інформації». – 2020. – № 2. – С. 5–12.

10. Висоцька А. М. Організація електронного документообігу та архівування у державному секторі // Державне управління: теорія та практика. – 2021. – № 2. – С. 87–93.

11. Глущенко Н. І. Архівна безпека: нові підходи в контексті інформаційної війни // Інформаційна безпека України. – 2023. – № 2. – С. 14–20.

12. ДСТУ 2732:2004. Діловодство й архівна справа. Терміни та визначення понять. – Київ: Держспоживстандарт України, 2005. – 33 с.

13. ДСТУ ISO 15489-1:2007. Інформація та документація. Управління документами. Частина 1. Загальні вимоги. – [Чинний від 2009-01-01]. – Київ: ДП «УкрНДНЦ», 2009. – 24 с.

14. Електронний архів: як законно організувати зберігання е-документів у компанії? // InBase. – 2023. – [Електронний ресурс]. – Режим доступу: https://inbase.com.ua/elektronnyj-arhiv-yak-zakonno-organizuvaty-zberigannya-e-dokumentiv-u-kompaniyi/

15. Електронні архіви в Україні: як держава планує зберігати документи // Вчасно. – 2023. – [Електронний ресурс]. – Режим доступу: https://vchasno.ua/elektronni-arhivy-ukrainy/

16. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text

17. Закон України «Про Національний архівний фонд та архівні установи» від 24.12.1993 № 3814-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3814-12#Text

18. Законодавство і електронний архів // CleverForms. – 2024. – [Електронний ресурс]. – Режим доступу: https://clever-forms.com/zakonodavstvo-i-elektronnij-arhiv/

19. Кабінет Міністрів України. Концепція розвитку цифрової економіки та суспільства України на 2018–2025 роки: Розпорядження КМУ від 17.01.2018 № 67-р. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

20. Кібербезпека бізнесу під час війни // Економіка та суспільство. – 2024. – № 4(48). – С. 25–31.

21. Кібербезпека України: аналіз сучасного стану // Наукові праці Національного університету «Одеська юридична академія». – 2023. – № 2(26). – С. 45–52.

22. Кібербезпека: сучасні виклики перед Україною // Острозька академія. – 2020. – [Електронний ресурс]. – Режим доступу: https://eprints.oa.edu.ua/id/eprint/9183/1/Cybersecurity%20modern%20challenges%20of%20Ukraine.pdf

23. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки // Економіка і прогнозування. – 2021. – № 3. – С. 45–53.

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

25. Летичевський О. О. Сучасні наукові проблеми кібербезпеки // Вісник НАН України. – 2023. – № 2. – С. 12–20.

26. Лисеюк А., Свінцицька Т. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції // Право та інновації. – 2024. – № 4(48). – С. 32–38.

27. Мельник Л. М. Електронне архівування документів в органах публічного управління: виклики та перспективи // Ефективність державного управління. – 2023. – Вип. 62. – С. 114–121.

28. Мельник О. Електронний архів: як законно організувати зберігання е-документів у компанії? // InBase. – 2023. – [Електронний ресурс]. – Режим доступу: https://inbase.com.ua/elektronnyj-arhiv-yak-zakonno-organizuvaty-zberigannya-e-dokumentiv-u-kompaniyi/

29. Національний архівний фонд та електронні документи: сучасний стан і перспективи / І. О. Мазур, В. Ю. Баран. – Київ: НАН України, 2021. – 104 с.

30. Ніколаєнко О. І. Цифрова трансформація архівної справи: проблеми нормативного забезпечення // Право і цифрові технології. – 2022. – № 4. – С. 67–72.

31. Перелік типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів: Наказ Міністерства юстиції України від 12.04.2012 № 578/5. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0578-12#Text

32. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання: Наказ Міністерства юстиції України від 11.11.2014 № 1886/5. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1457-14#Text

33. Правила ЕДО: як правильно зберігати електронні документи // Linkos Group. – 2024. – [Електронний ресурс]. – Режим доступу: https://edo.linkos.ua/news/pravila-edo-jak-pravilno-zbergati-elektronn-dokumenti

34. Правила ЕДО: як правильно зберігати електронні документи // Linkos Group. – 2024. – [Електронний ресурс]. – Режим доступу: https://edo.linkos.ua/news/pravila-edo-jak-pravilno-zbergati-elektronn-dokumenti

35. Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях: Наказ Міністерства юстиції України від 18.06.2015 № 1000/5. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0736-15#Text

36. Про затвердження Порядку зберігання електронних документів в архівних установах: Наказ Держкомархіву України від 25.04.2005 № 49. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/z0627-05

37. Про затвердження Порядку зберігання електронних документів в архівних установах : Наказ Держкомархіву України від 25.04.2005 № 49. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/z0627-05

38. Романюк С. Сучасні інформаційні системи в архівній справі // Вісник Книжкової палати. – 2022. – № 7. – С. 21–26.