

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ І ПРИКЛАДНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ

ГУМЕННИЙ ВАДИМ ОЛЕКСІЙОВИЧ

Допускається до захисту:

в. о. завідувача кафедри
інформаційних систем управління,
д-р екон. наук, професор

_____ Ольга АНІСІМОВА

« _____ » _____ 202__ р.

**РЕГЛАМЕНТАЦІЯ ПРОЦЕСУ ПРИЙМАННЯ ТА ПЕРЕДАВАННЯ
ЕЛЕКТРОННИХ ДОКУМЕНТІВ НА ПОСТІЙНЕ АРХІВНЕ ЗБЕРІГАННЯ**

Спеціальність 029 Інформаційна, бібліотечна та архівна справа

Кваліфікаційна (магістерська) робота

Керівник:

Інга СИВИЦЬКА, канд. екон. наук.,

доцент, доцент кафедри

інформаційних систем управління

Оцінка: ____ / ____ / ____

(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____

(підпис)

АННОТАЦІЯ

Гуменний В. О. Регламентація процесу приймання та передавання електронних документів на постійне архівне зберігання. Спеціальність 029 «Інформаційна, бібліотечна та архівна справа», освітня програма «Документаційна та інформаційна підтримка управлінської діяльності». Донецький національний університет імені Василя Стуса, Вінниця, 2025.

У магістерській роботі здійснено комплексне дослідження теоретико-методичних засад та нормативного забезпечення архівного зберігання електронних документів. Проаналізовано трансформацію поняття «архівний документ» в умовах цифровізації та виявлено проблеми забезпечення довгострокової юридичної сили кваліфікованих електронних підписів (КЕП). На основі міжнародної еталонної моделі OAIS (ISO 14721) розроблено уніфікований алгоритм формування та приймання інформаційних пакетів (SIP), який передбачає диференційований підхід до документів, народжених у, та оцифрованих копій. Обґрунтовано вимоги до спеціалізованого клієнтського програмного забезпечення («SIP Creator») та запропоновано модель централізованого хмарного зберігання для установ з обмеженими ресурсами.

Ключові слова: електронний документ, архівне зберігання, модель OAIS, SIP-пакет, КЕП, оцифрування, електронний архів, інформаційна система.

64 с., 9 табл., 12 рис., 34 джерела.

SUMMARY

Humennyi V. O. Regulation of the Process of Acceptance and Transfer of Electronic Documents for Permanent Archival Storage.

Specialty 029 "Information, Library and Archival Studies", Educational Program "Documentary and Information Support of Management Activities". – Vasyl' Stus Donetsk National University, Vinnytsia, 2025.

The Master's thesis presents a comprehensive study of the theoretical and methodological foundations and the regulatory framework for the archival storage of electronic documents. The transformation of the concept of an "archival document" in the context of digitalization is analyzed, and the problems of ensuring the long-term legal validity of qualified electronic signatures (QES) are identified. Based on the international reference model OAIS (ISO 14721), a unified algorithm for the formation and acceptance of Submission Information Packages (SIP) has been developed, which provides for a differentiated approach to born-digital documents and digitized copies. The requirements for specialized client software ("SIP Creator") are substantiated, and a model of centralized cloud storage for institutions with limited resources is proposed.

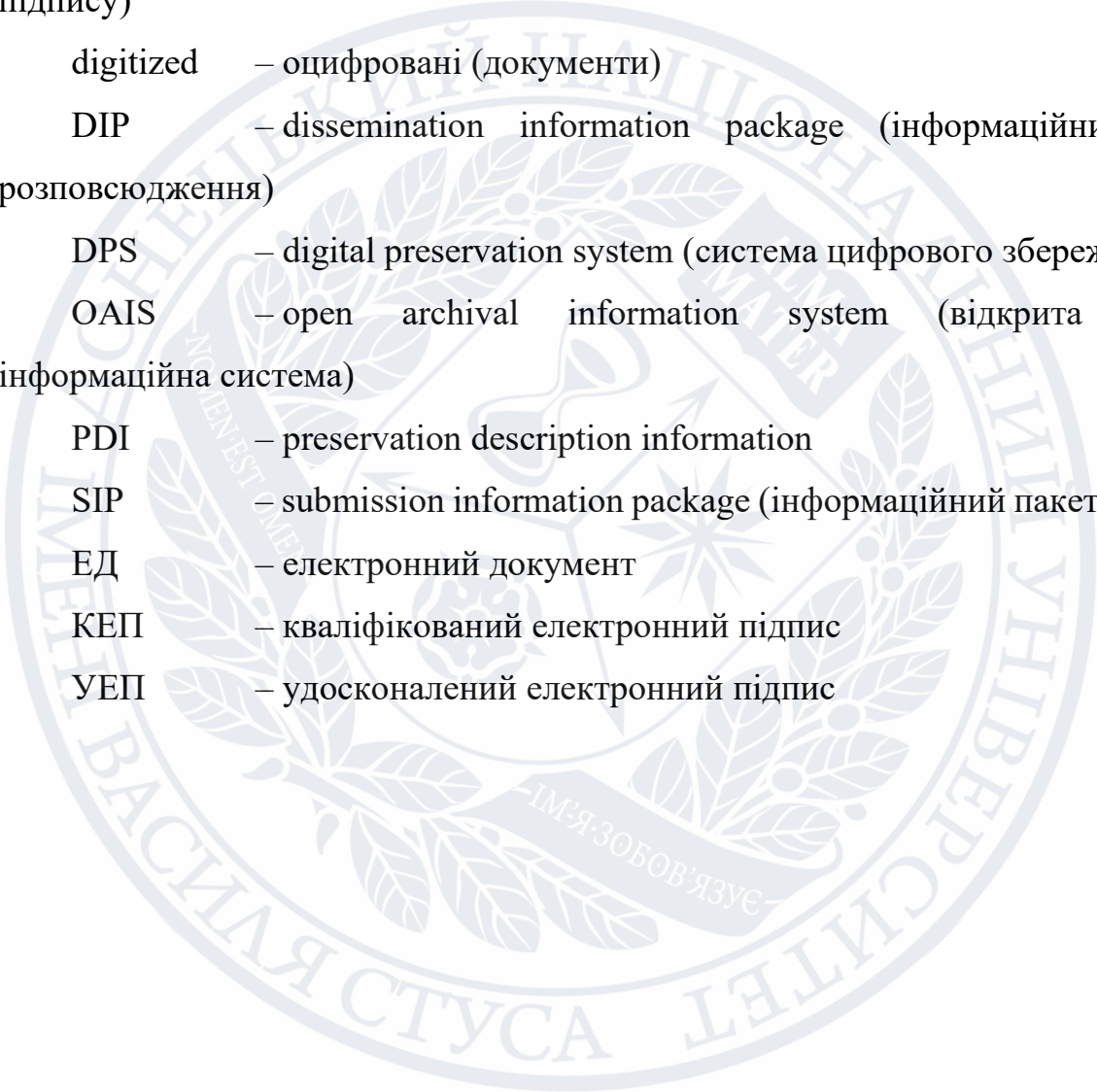
Keywords: electronic document, archival storage, OAIS model, SIP package, QES, digitization, electronic archive, information system.

64 p., 9 tables, 12 fig., 34 sources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	4
ВСТУП	5
РОЗДІЛ 1 ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АРХІВУВАННЯ: ВІД ТРАДИЦІЙНОГО ДО ЕЛЕКТРОННОГО ДОКУМЕНТА.....	10
1.1 Еволюція підходів до управління документами	10
1.2 Становлення та розвиток національної системи управління електронними документами	19
1.3 Трансформація поняття «архівний документ» в умовах цифровізації.....	24
Висновки до розділу 1	30
РОЗДІЛ 2 РЕГЛАМЕНТАЦІЯ ПРОЦЕСІВ ПЕРЕДАВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ НА АРХІВНЕ ЗБЕРІГАННЯ	32
2.1 Концептуальна модель OAIS як методологічна основа регламентації архівних процедур.....	32
2.2 Ключові проблеми забезпечення довгострокового зберігання	41
Висновки до розділу 2	47
РОЗДІЛ 3 УДОСКОНАЛЕННЯ НОРМАТИВНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ПЕРЕДАВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ	49
3.1 Розроблення алгоритму формування та приймання інформаційного пакета SIP	49
3.2 Вимоги до програмно-технічного забезпечення автоматизованої системи архівного зберігання	57
Висновки до розділу 3	59
ВИСНОВКИ.....	60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	62

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ



AIP	– archival information package (архівний інформаційний пакет)
born-digital	– народжені цифровими (про документи)
CAdES	– CMS advanced electronic signatures (стандарт електронного підпису)
digitized	– оцифровані (документи)
DIP	– dissemination information package (інформаційний пакет розповсюдження)
DPS	– digital preservation system (система цифрового збереження)
OAIS	– open archival information system (відкрита архівна інформаційна система)
PDI	– preservation description information
SIP	– submission information package (інформаційний пакет подання)
ЕД	– електронний документ
КЕП	– кваліфікований електронний підпис
УЕП	– удосконалений електронний підпис

ВСТУП

Актуальність теми. В умовах активного розвитку електронного урядування та цифрової трансформації всіх сфер суспільного життя електронні документи (ЕД) набувають статусу базового інформаційного ресурсу держави та поступово стають основним джерелом формування Національного архівного фонду України [1]. Критичним етапом у життєвому циклі ЕД є їхнє приймання та передавання на постійне архівне зберігання, оскільки саме на цьому етапі вирішується питання довгострокового збереження юридичної сили, автентичності та цілісності документальних відомостей. Особливо критичним етапом у життєвому циклі електронних документів є процес їх приймання та передавання на постійне архівне зберігання. Саме на цій стадії вирішується питання збереження юридичної сили, автентичності, цілісності, а також можливості подальшої верифікації електронних підписів і засобів автентифікації. Будь-які технологічні або організаційні порушення під час передавання можуть призвести до втрати значимості документа як доказової інформації, а в окремих випадках – до його повної непридатності.

Попри наявність нормативно-правових актів, що регламентують загальні засади електронного документообігу та архівної справи в Україні, чинна нормативна база все ще не забезпечує цілісної та деталізованої моделі передавання ЕД на архівне зберігання. Вона містить фрагментарні вимоги, які не враховують різноманіття сучасних інформаційних систем, форматів файлів та методів управління метаданими. Через це відсутня уніфікована, стандартизована процедура передавання ЕД, що є критично необхідною для взаємодії між фондоутворювачами та архівними установами. Така ситуація призводить до проблем сумісності (інтероперабельності) між відомчими системами електронного документообігу та інформаційними системами архівних установ. Кожна організація може використовувати власні технологічні рішення, специфічні схеми метаданих, різні формати електронних документів і різні

способи підтвердження цілісності та автентичності. В результаті виникають значні ризики: потенційна втрата або спотворення даних під час експорту-імпорту, несумісність структурних елементів документів, некоректне відтворення контенту, а також проблеми з підтвердженням чинності електронних підписів у довгостроковій перспективі.

Важливо підкреслити, що зазначена проблема проявляється на всіх управлінських рівнях:

- на національному рівні – у вигляді відсутності єдиних державних стандартів та узгоджених методик передавання ЕД;
- на регіональному рівні – у різнорівневості технічної готовності архівних установ та відсутності стандартизованих рішень для взаємодії з місцевими фондоутворювачами;
- на галузевому рівні – у використанні різних відомчих СЕД, що працюють за несумісними правилами та форматами;
- на рівні окремих підприємств і організацій – у фрагментарності процедур, відсутності внутрішніх регламентів, різному рівні цифрової зрілості та застосуванні унікальних внутрішніх технологічних рішень.

Таким чином, проблема не є точковою чи локальною. Вона охоплює всі етапи управління ЕД: від їх створення до передавання на довгострокове архівне зберігання. Це зумовлює нагальну потребу у розробленні та впровадженні уніфікованої регламентації процесу приймання та передавання електронних документів на постійне архівне зберігання, яка має охоплювати технологічні, організаційні, методичні та правові аспекти, забезпечувати інтегровану сумісність систем різних рівнів і гарантувати збереження автентичності та цілісності документів. Отже, відсутність уніфікованих технологічних та організаційних моделей передавання ЕД є ключовою перешкодою на шляху формування повноцінного електронного архівного фонду, що підкреслює високу актуальність обраної теми магістерського дослідження.

Теоретико-методологічні засади документознавства та архівної справи, зокрема питання впровадження новітніх інформаційних технологій, висвітлено

в працях таких вітчизняних вчених, як С. Г. Кулешов, М. Г. Палієнко, В. В. Бездрабко, Л. А. Дубровіна та інші. Правові аспекти обігу електронних документів досліджували О. О. Золотар, А. А. Каламайко, Г. В. Папакін [2-8].

Значний внесок у розробку проблем збереження електронної інформації та стандартів керування документацією зробили зарубіжні дослідники, серед яких керівниця проекту InterPARES Л. Дюранті (Luciana Duranti), Д. Бірман (David Bearman), Ч. Доллар (Charles Dollar), Т. Тібодо (Kenneth Thibodeau) (один із розробників моделі OAIS) та інші [9-12].

Водночас, незважаючи на вагомий науковий доробок, питання створення уніфікованої технологічної моделі регламентації процесу приймання-передавання електронних документів в умовах українського законодавства та різноманітності інформаційних систем залишається недостатньо вивченим, що й зумовило вибір теми магістерської роботи.

Метою роботи є теоретичне обґрунтування та розроблення практичних рекомендацій щодо удосконалення нормативно-методичного забезпечення процесів приймання та передавання електронних документів на постійне архівне зберігання.

Поставлена мета зумовила необхідність вирішення таких логічно пов'язаних теоретичних, науково-методичних та практичних **завдань**:

- дослідити еволюцію підходів до управління документами та визначити специфіку становлення національної системи електронного документообігу;
- проаналізувати трансформацію поняття «архівний документ» в умовах цифровізації, зокрема зміни у вимогах до забезпечення його юридичної сили та автентичності;
- визначити роль і значення міжнародної моделі OAIS та специфікацій E-ARK як методологічної основи для регламентації архівних процедур в Україні;
- обґрунтувати необхідність переходу від локального файлового зберігання до використання спеціалізованих інформаційних систем та централізованих хмарних сервісів;
- розробити уніфікований алгоритм формування та приймання

інформаційного пакета подання (SIP), що враховує специфіку документів, народжених у цифрі, та оцифрованих копій;

– сформулювати вимоги до програмно-технічного забезпечення, необхідного для автоматизації процесів передавання документів до державних архівів.

Об’єкт дослідження – система організації архівного зберігання електронної управлінської документації.

Предмет дослідження – нормативні, організаційні та технологічні засади регламентації процесу приймання та передавання електронної управлінської документації на постійне архівне зберігання.

Наукова новизна роботи полягає у розробленні уніфікованого алгоритму формування SIP-пакета на основі моделі OAIS з розмежуванням потоків для «born-digital» та «digitized» документів; удосконаленні підходів до забезпечення довгострокової автентичності через перехід до моделі активного збереження з регулярним оновленням позначок часу та використанням форматів CAdES-A/ASiC-A; адаптації оновлених положень стандарту OAIS і специфікацій E-ARK для національної архівної практики; а також у запропонуванні організаційно-технологічної моделі «Архів як сервіс» із застосуванням універсального ПЗ «SIP Creator» для подолання цифрової нерівності установ і спрощення формування архівних пакетів.

Методи дослідження, використані в роботі, включають: аналіз і синтез використано для узагальнення теоретичних засад архівного зберігання електронних документів; історико-порівняльний метод – для вивчення еволюції документних практик; системний підхід – для розгляду електронного архіву за моделлю OAIS; термінологічний аналіз – для уточнення ключових понять; моделювання та структурно-функціональний метод – для розроблення алгоритму формування SIP-пакета та визначення вимог до програмно-технічного забезпечення.

Теоретичне значення роботи полягає у поглибленні розуміння механізмів збереження цифрової спадщини та формуванні цілісної концепції регламентації

передавання електронних документів до державних архівів.

Практичне значення роботи полягає у розробленні готового алгоритму дій та формулюванні технічних вимог до програмного забезпечення, що можуть бути використані при вдосконаленні нормативно-правових актів Міністерства юстиції України та проектуванні національних архівних інформаційних систем.

Апробація результатів дослідження. Теоретичні та практичні результати дослідження були опубліковані у збірнику матеріалів матеріали IV Міжнародної науково-практичної конференції «Прикладні аспекти сучасних міждисциплінарних досліджень» (м. Вінниця, 05 листопада 2025 р.), а також на IX Всеукраїнській науково-практичній конференції «Людина в інформаційному просторі» (м. Кременчук, 20 листопада 2025 р.).

Структура кваліфікаційної (магістерської) роботи. Робота складається зі вступу, трьох розділів, висновків і списку використаних посилань (34 найменування). Загальний обсяг роботи складає 64 сторінки друкованого тексту, 9 таблиць, 12 рисунків.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АРХІВУВАННЯ: ВІД ТРАДИЦІЙНОГО ДО ЕЛЕКТРОННОГО ДОКУМЕНТА

1.1 Еволюція підходів до управління документами

Поняття «документ» у сучасній науці має багатогранний і міждисциплінарний характер. Інформація може бути зафіксована у різних формах (текстовій, графічній, образотворчій, аудіовізуальній, електронній, комбінованій) і належати до найрізноманітніших джерел – від історичних пам'яток і особових паперів до творів мистецтва. У таблиці 1.1 наведено декілька визначень поняття «документ» (від лат. documentum – повчання, доказ).

Таблиця 1.1 – Зміст поняття «документ» [15]

Визначення	Зміст поняття
1. Діловий папір, що посвідчує певний юридичний факт, підтверджує право на щонебудь, служить доказом чого-небудь.	Все те, що підтверджує щонебудь
2. Письмове свідоцтво, що офіційно підтверджує особу.	Що офіційно підтверджує особу
3. Письмовий твір, грамота, рисунок і т. ін. як свідчення про щось історичне, важливе.	Свідчення про щось історичне, важливе

Отже, поняття «документ» у сучасній науковій традиції має комплексний характер і поєднує матеріальну, інформаційну та соціально-правову складники. Воно охоплює будь-який зафіксований зміст, здатний бути сприйнятим, відтвореним і використаним у різних сферах діяльності. Водночас центральною, визначальною ознакою документа залишається його доказова природа: документ відображає певний факт, подію або управлінське рішення і може слугувати

підтвердженням їхнього існування. Саме здатність бути доказом у правовому, історичному чи управлінському контексті, дозволяє відрізнити документ від інших інформаційних об'єктів та забезпечує його ключову роль у функціонуванні суспільства.

Етимологічне походження терміна *documentum* також підкреслює, що документ завжди відображає певну реальність та може бути використаний для її підтвердження. У сучасному документознавстві документ розглядається не лише як матеріальний носій інформації чи засіб її передачі, а передусім як засіб підтвердження фактів, дій, прав і обов'язків. Саме доказовість є однією з ключових властивостей документа, без якої втрачається його управлінська, юридична та соціальна сутність.

Підходи до управління документами зазнали суттєвих змін у відповідь на трансформацію суспільства, розвиток технологій та ускладнення управлінських процесів. Те, що колись сприймалося як просте зберігання паперових носіїв, поступово перетворилося на комплексну систему організації інформаційних потоків. Визначення поняття «документ», його властивостей, етапів життєвого циклу та відповідальних за його збереження осіб – усе це змінювалося під впливом історичних умов і адміністративних потреб.

Упродовж доіндустріальної та індустріальної епох домінував традиційний підхід, у межах якого документ ототожнювався з матеріальним об'єктом, що має унікальні фізичні характеристики та потребує впорядкованого зберігання. Архіви виконували насамперед охоронну функцію, а документ після завершення своєї «роботи» вважався статичним та незмінним. Ця модель ефективно працювала в умовах централізованої бюрократії ХХ століття, де чітко регламентований рух паперових документів забезпечував контроль над управлінським процесом. Однак поступове збільшення обсягів документації, зростання вимог до оперативності доступу та поява нових технологічних можливостей продемонстрували обмеженість такого підходу. Це стало поштовхом до пошуку нових моделей управління документами, у яких дедалі більше уваги приділяється інформаційній сутності документів, їхнім функціям у

діяльності організацій та інтегрованому підходу до управлінських процесів.

Після Другої світової війни в США та Канаді почали формуватися нові практики управління документами, зумовлені зростанням обсягів документації. Центральною фігурою став Теодор Рузвельт Шелленберг, який запропонував модель життєвого циклу управління документами «Records Life Cycle». Згідно з цією концепцією, життя документа є лінійним процесом, що складається з чітко розмежованих етапів:

- створення (діловодство);
- активне використання (оперативне зберігання);
- передавання на архівне зберігання або знищення.

Таблиця 1.2 – Опис етапів життєвого циклу, запропонованого архівознавцем Т. Шелленбергом

Стадія	Хто працює з документом	Головні функції
Поточне використання (Current phase / Active stage)	Створювач документа (установа)	Документ щодня використовується у роботі; зберігається в структурних підрозділах
Оперативне/Проміжне зберігання (Semi-current phase / Inactive stage)	Архів установи (служба діловодства)	Документ рідко використовується, але може знадобитись для довідок або повторного звернення
Постійне зберігання (Non-current phase / Archival stage)	Державний (національний) архів	Документ набуває історичної, культурної чи юридичної цінності; забезпечується його збереження для суспільства

Теорія стверджує, що документ не є статичним, він «живе», змінюючи свою роль, значення та місце зберігання залежно від стадії функціонування. На

кожному етапі ним займаються різні установи та фахівці: спочатку діловодні служби, а згодом – архівні. Архів вступав у гру лише на фінальному етапі («смерті» оперативного документа та його «народження» як історичного джерела). Процес передавання був здебільшого фізичним переміщенням матеріальних об'єктів (справ) з відомчого приміщення до архівосховища, що не змінювало внутрішньої сутності самого документа.

Концепція теорії Теодора Шелленберга базується на ідеї подвійної природі цінності документа, яка розмежовує первинну значущість (управлінську, юридичну, фінансову) для самої установи та вторинну (історичну або наукову) для широкого загалу (рисунок 1.1).

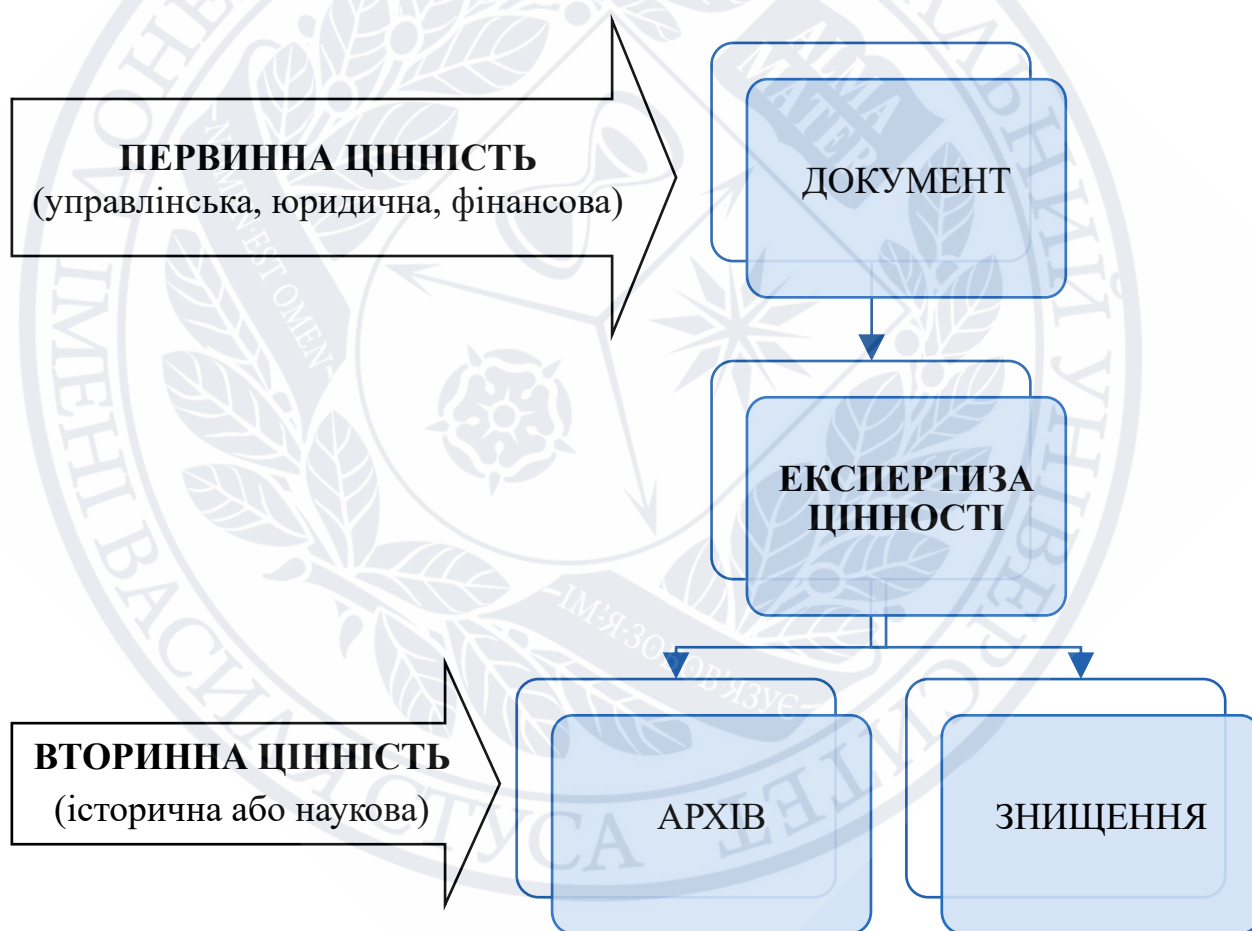


Рисунок 1.1 – Подвійної природі цінності документа у моделі Теодора Шелленберга

Ключовим елементом у цій системі виступає експертиза цінності, що стає

вирішальним етапом переходу між стадіями життя документа: вона визначає, чи буде матеріальний об'єкт передано на постійне зберігання, або знищено після втрати ним практичної потреби. Такий підхід забезпечує раціональне управління ресурсами, гарантуючи, що до архіву потрапляють не всі документи, а лише ті, що мають справжню цінність. Значення цієї теорії для архівної науки є фундаментальним, адже Шелленберг уперше створив системну модель руху документа та чітко розмежував сфери відповідальності поточного діловодства й архівної справи. Його напрацювання стали теоретичним підґрунтям для нормативного регулювання експертизи цінності, перетворивши відбір документів з інтуїтивного процесу на науково обґрунтовану процедуру. Завдяки цьому архіви отримали можливість зосередитися на збереженні найважливішої інформації, формуючи якісну джерельну базу для майбутніх поколінь [16-18].

Розвиток комп'ютерних технологій у другій половині XX століття (1970–1990-ті рр.), зростання кількості управлінських процесів і документальних потоків зумовили перегляд традиційного уявлення про документ як окремого фізичного об'єкта. Поступово формується системний підхід до управління документами, у межах якого документ починає розглядатися як частина ширшої інформаційної системи організації. В цей період закладаються концептуальні засади моделі «Records management» (Управління записами) – керування документами протягом усього їх життєвого циклу.

Результатом комп'ютеризації стало інтегрування процесів документування: створення, реєстрація, оброблення, передавання, використання та зберігання документів перестають бути окремими технічними операціями й утворюють єдину керовану систему (рисунки 1.2). Це сприяє підвищенню оперативності доступу до інформації, мінімізації дублювання та посиленню контролю над інформаційними потоками. У цей період суттєво зростає роль класифікації, систематизації та пошуку, що потребує уніфікації документів. Стандартизація стає важливим інструментом упорядкування документування. Розробляються вимоги до структурних елементів документа, єдині правила оформлення реквізитів, індексації та реєстрації. Це забезпечує можливість автоматизації

діловодства й ефективного взаємообміну інформацією між установами. Документ починає сприйматися не лише як носій, а як структурована інформація, що має визначені атрибути та функції у діяльності організації [18].



Рисунок 1.2 – Інтегрування процесів документування в єдину інформаційну систему

В цей час з'являються перші електронні документи. Хоча більшість із них ще дублює паперові форми й існує в межах паперово орієнтованої логіки, їх використання сприяє переосмисленню сутності документа. Зростає значення метаданих, що забезпечують контекст, доказовість і керованість документів незалежно від носія. Системний підхід став важливим перехідним етапом між традиційною моделлю та сучасним розумінням документів як цифрової інформації. Він сформував інфраструктуру для подальшого розвитку електронного документообігу, а також визначив документ як ключовий ресурс управління, що має важливу юридичну, організаційну, інформаційну та економічну цінність для суспільства і держави.

Таблиця 1.3 – Порівняння двох моделей управління документацією

Критерій	Records Life Cycle (Життєвий цикл документа)	Records Continuum Model (Модель континууму)
Походження	США, сер. XX ст. (Т. Шелленберг)	Австралія, кін. XX ст.
Основний підхід	Документ «живе» і переходить через послідовні стадії	Документ одночасно виконує кілька ролей у різних контекстах
Форма документа	Розроблено переважно для паперових документів	Створено з урахуванням електронних документів
Основна мета	Організувати зберігання від створення → до архіву	Інтегрувати управління та архівну діяльність з моменту створення
Рух документа	Лінійний, «від народження до смерті»	Нелінійний, без жорстких стадій
Експертиза цінності	На <i>пізнішому етапі</i>	На <i>етапі створення</i> або навіть раніше
Відповідальні	Спочатку діловодство → потім архів	Архівісти залучені відразу під час створення документації
Роль автентичності	Перевіряється переважно при передачі в архів	Постійне підтримання автентичності та контексту
Відношення до інформаційного середовища	Носій – визначальний	Носій – вторинний, важливий сам зміст і контекст

Стрімкий розвиток інформаційних технологій наприкінці XX століття (1990–2000-ті) призвів до трансформації традиційних уявлень про документ.

Електронні документи почали виконувати всі функції, властиві паперовим носіям, що зумовило перегляд методів їх створення, опрацювання та зберігання. У межах цього етапу формуються нові теоретичні й технологічні підходи до управління документами, засновані на цифровій природі інформації. Однією з провідних теорій стає «Records Continuum Model», сформована австралійськими науковцями. На відміну від класичної моделі життєвого циклу документа, тут управління розглядається як безперервний процес, що охоплює створення, використання, організацію, збереження та забезпечення суспільної значущості інформації. Документ одночасно розглядається в кількох сутностях: організаційної, правової та культурної. Якщо раніше вважали, що документ спочатку потрібен для роботи, пізніше – для архіву (таблиця 1.4). Тепер – він від моменту створення має потенційне значення для управління, захисту прав, збереження історії.

Таблиця 1.4 – Потенційне значення документа в концепції «Records Continuum Model»

Сутність	Що означає?	Приклад питання
Організаційна	Документ виконує функції в роботі установи: підтверджує рішення, фіксує діяльність	Як документ допомагає керувати процесами?
Правова	Документ може бути доказом у юридичному полі, підтверджує права й обов'язки	Чи має документ юридичну силу?
Культурна / соціальна	Документ стає частиною історичної пам'яті, надбанням суспільства після завершення практичного використання	Чи має документ цінність для майбутніх поколінь?

Паралельно розвиваються електронні системи управління документами (ERM, EDRMS), які автоматизують ділові процеси та забезпечують:

- реєстрацію та контроль виконання документів;
- фіксацію службових метаданих;
- управління доступом і версіями;
- підтримку юридичної сили документа у цифровому середовищі.

Перехід від паперових документів до цифрових спричинив зміну ключових завдань галузі. Якщо раніше важливо було зберегти оригінальний матеріальний носій, то тепер першочерговими стали вимоги до:

- автентичності (підтвердження авторства та незмінності);
- цілісності (відсутність несанкціонованих змін);
- доступності упродовж усього строку зберігання;
- відтворюваності незалежно від технологічних змін.

У цифрову добу документ визначається не носієм, а структурою даних та метаданих, відтворення яких залежить від програмного середовища й технічної інфраструктури. Етап характеризується суттєвими змінами у практиці управління документами:

- архіви змушені працювати з нестабільними цифровими форматами;
- стандартизація стає критично важливою (зокрема, впроваджуються міжнародні норми на кшталт ISO 15489);
- документознавці набувають компетентностей у сфері ІТ безпосередньо для виконання професійних функцій.

Таким чином, інформаційно-технологічний підхід відображає перехід від матеріального до цифрового документального середовища, де збереження інформації залежить не від фізичного носія, а від правильно організованої системи управління даними.

Сучасний етап розвитку управління документами (2010-ті – сьогодні) відображає перехід до розуміння документа як важливого інформаційного ресурсу, що функціонує у мережевому цифровому середовищі. На відміну від попередніх моделей, документ сьогодні не є статичною одиницею, пов'язаною з конкретним носієм. Його цінність визначається можливістю постійної взаємодії, використання, повторного застосування та перенесення між різними

інформаційними системами. Саме тому у центрі уваги опиняються технології інтероперабельності, що забезпечують сумісність метаданих і форматів та дозволяють документам залишатися зрозумілими й автентичними незалежно від програмного середовища. Цифрові документи розміщуються і обробляються не як завершені файли, а як динамічні об'єкти, що постійно змінюються в умовах колективної роботи, мережевих сервісів і хмарної інфраструктури. Вони існують як сукупність версій, контекстів, службових даних та взаємозв'язків із іншими інформаційними ресурсами. У такій ситуації управління документами перетворюється на безперервний процес контролю доступу, фіксації змін та збереження достовірності інформації. Водночас особливої актуальності набуває проблема довгострокового зберігання електронних документів. Швидке моральне старіння технологій робить цифрову інформацію вразливою, а тому архівні установи використовують стратегії міграції форматів, створення цифрових копій, емуляції програмного середовища та побудови спеціалізованих репозиторіїв постійного зберігання. Саме репозиторії поступово замінюють традиційні архіви, оскільки здатні гарантувати збереження документів у зв'язку з їх технічною залежністю від програмних платформ. Отже, сучасний підхід базується на комплексному поєднанні архівознавчих, правових, інформаційних і технологічних принципів. Управління документами перестає бути виключно сферою діловодства: воно включає правові механізми забезпечення доказовості, ІТ-інструменти підтримання автентичності й цілісності, а також інформаційні підходи до оптимізації використання документних ресурсів у діяльності організацій. Таким чином, документ у цифровому суспільстві розглядається як активний елемент комунікаційної екосистеми, а його ефективне управління є умовою прозорості, підзвітності, пам'яті та сталого розвитку установ і держави.

1.2 Становлення та розвиток національної системи управління електронними документами

Розвиток системи управління документами в Україні має свою специфіку,

зумовлену історичним спадком, трансформацією державного апарату та особливостями правового регулювання інформаційної сфери. Якщо у західній практиці перехід до управління записами (Records Management) відбувався еволюційно під впливом ринкових потреб та технологій, то в Україні цей процес мав характер адміністративних реформ «згори», поєднуючи елементи радянської бюрократичної традиції з новітніми євроінтеграційними стандартами.

В еволюції національної системи управління документацією можна виокремити три ключові етапи, що характеризуються зміною технологічних укладів та нормативного регулювання:

Традиційний (паперовий) етап (до 2003 року) – домінування норм Єдиної державної системи діловодства (ЄДСД).

Гібридний етап (2003–2018 роки) – зародження електронного документообігу, паралельне існування паперових та електронних форм.

Цифровий етап (з 2018 року – дотепер) – впровадження системи електронної взаємодії, хмарних технологій та гармонізація з європейським законодавством (eIDAS).

На початковому етапі незалежності України система документування базувалася на радянських стандартах, орієнтованих виключно на паперові носії. Головним об'єктом управління був «документ» як фізична одиниця, а основною функцією діловодства – контроль за виконанням рішень. Ця система відзначалася високим рівнем регламентації (стандартизації форматів, бланків, реквізитів), однак була негнучкою та технологічно застарілою. Комп'ютеризація у 90-х роках використовувалася переважно як засіб виготовлення паперових документів, а не як середовище для їх існування. Електронні файли не мали юридичної сили і сприймалися лише як проекти майбутніх паперових оригіналів.

Переломним моментом стало прийняття у 2003 році Законів України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис» (зараз – «Про електронну ідентифікацію та електронні довірчі послуги»). Ці нормативно-правові акти вперше на законодавчому рівні закріпили визначення електронного документа як документа, інформація в якому

зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [20-22]. Українське законодавство пішло шляхом повного урівняння юридичної сили електронного та паперового документа за умови накладання кваліфікованого електронного підпису (КЕП). Це створило правову основу для відмови від дублювання документів на папері. Проте, незважаючи на прогресивне законодавство, протягом тривалого часу в Україні зберігалася практика «подвійного діловодства». Установи створювали документи в електронній формі, передавали їх каналами зв'язку, але для звітності та архівного зберігання змушені були роздруковувати їх. Це призводило до збільшення навантаження на персонал та неефективного використання ресурсів. Основною причиною гальмування процесів була відсутність інфраструктури довгострокового зберігання електронних документів. Національні архіви технічно та методично не були готові приймати на постійне зберігання цифрові масиви даних, що змушувало установи зберігати паперові оригінали як єдине гарантоване джерело інформації.

Суттєвим кроком у реформуванні національної системи електронного документообігу стало прийняття у 2017 році Закону України «Про електронні довірчі послуги» [23]. Цей нормативно-правовий акт став відповіддю на необхідність гармонізації українського законодавства з європейським Регламентом eIDAS (No 910/2014) [24]. Ключовою новелою закону стала заміна застарілого поняття «електронний цифровий підпис» (ЕЦП) на нову трирівневу систему ідентифікації, вершиною якої є кваліфікований електронний підпис (рисунки 1.3). Ця система класифікує засоби ідентифікації залежно від ступеня захисту персональних даних та вірогідності встановлення особи підписанта.

Простий електронний підпис(ЕП) має низький рівень довіри. До нього належать електронні дані, які додаються до інших даних для ідентифікації особи (логін і пароль, одноразовий код з SMS, позначка «Я погоджуюсь», зображення власноручного підпису). Такий підпис не забезпечує захисту документа від змін і не дає повної впевненості щодо особи підписанта. Застосовується у внутрішньому документообігу компаній, при отриманні посилок, у процесах

авторизації на вебсайтах тощо.

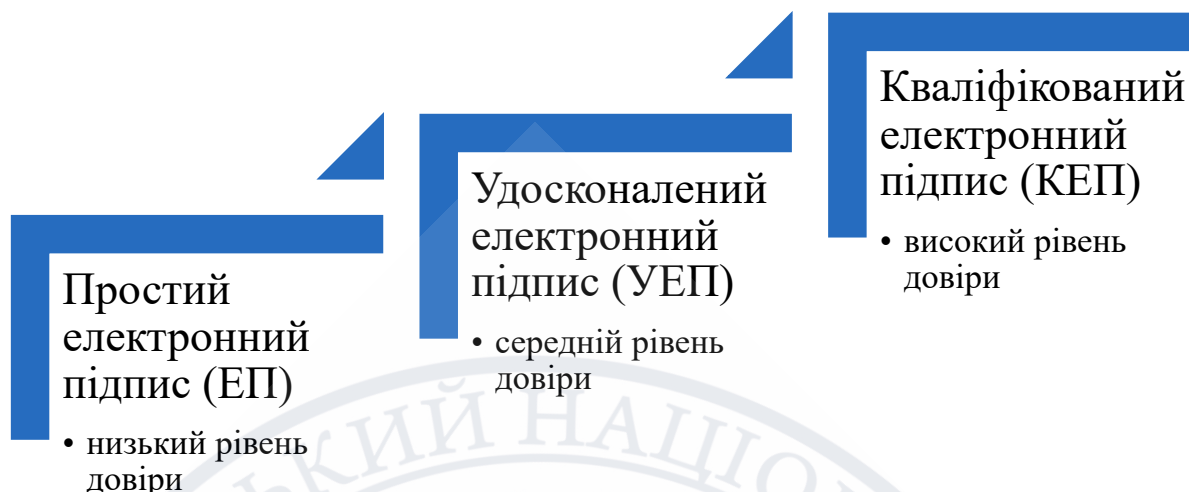


Рисунок 1.3 – Трирівнева система ідентифікації

Удосконалений електронний підпис (УЕП) має середній рівень довіри. Він створюється за допомогою криптографічних алгоритмів, однозначно пов'язаний з підписантом і дозволяє виявити несанкціоновані зміни документа після його підписання. Але особистий ключ зберігається на незахищеному носії (файлі на комп'ютері, флеш-накопичувачі), що може створювати ризик його копіювання сторонніми особами. Застосовується у бізнес-процесах, для подання податкової звітності, у деяких банківських сервісах.

Кваліфікований електронний підпис (КЕП) має високий рівень довіри. Він базується на кваліфікованому сертифікаті відкритого ключа, а особистий ключ зберігається на захищеному носії – засобі кваліфікованого електронного підпису (токені або смарткарті). Ключ генерується всередині пристрою та не може бути скопійований чи перехоплений шкідливим програмним забезпеченням. Застосовується в органах державної влади, судових і нотаріальних діях, для юридично значимих електронних транзакцій, у міжнародному електронному документообігу.

Отже, незважаючи на те, що у побутовій лексиці термін «ЕЦП» досі використовується за інерцією, у фаховому та юридичному полі він є застарілим. Закон вводить чітке розмежування понять, що базується на рівні довіри та

захисту даних. Кваліфікований електронний підпис визначається як удосконалений електронний підпис, що створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. Принципова різниця між старою моделлю ЕЦП та сучасним КЕП полягає не лише у термінології, а й у технології зберігання особистого ключа, що безпосередньо впливає на презумпцію достовірності підпису. КЕП передбачає найвищий рівень захисту, оскільки особистий ключ підписувача має зберігатися на засобі кваліфікованого електронного підпису (токені). Законодавець чітко визначає коло суб'єктів, для яких використання захищених носіїв є обов'язковим. Це критично важливо для формування архівних фондів, адже документи, створені органами влади, мають містити підпис найвищого рівня захисту. До переліку осіб, зобов'язаних використовувати виключно захищені носії (токени), належать:

- представники органів державної влади та місцевого самоврядування;
- працівники державних установ, підприємств, організацій;
- нотаріуси та державні реєстратори;
- суб'єкти, що виконують обов'язки згідно з уповноваженням держави.

Для державних архівів це означає, що при прийманні електронних документів на зберігання необхідно перевіряти не лише валідність сертифіката, а й тип носія, на якому було накладено підпис, щоб підтвердити статус документа як офіційного.

Окрім підпису фізичної особи (посадовця), Закон вводить поняття електронної печатки. Якщо підпис є аналогом власноручного підпису і засвідчує волевиявлення особи, то електронна печатка є аналогом «мокрої» печатки установи. Удосконалена електронна печатка – це інструмент, що забезпечує:

- автентичність походження (підтверджує, що документ видано саме цією організацією);
- цілісність даних (гарантує, що після накладання печатки у зміст документа не вносилися зміни).

Таким чином, у сучасній практиці діловодства формується чітка формула

юридичної сили електронного документа:

Юридична сила = Електронний документ + КЕП (особи) + Електронна
печатка (установи).

Отже, еволюція від ЕЦП до КЕП – це перехід від простого технічного підтвердження даних до юридично значущої системи довірчих послуг, яка гарантує неможливість підробки ключа. Для процедур архівного зберігання це має вирішальне значення, оскільки використання КЕП дозволяє застосовувати механізми довгострокового архівування (формати CAdES-A, ASiC-A) та забезпечувати доказовість документа протягом десятків років [25].

Суттєвий прогрес відбувся із впровадженням Системи електронної взаємодії органів виконавчої влади (СЕВ ОВВ) [26]. Це дозволило відмовитися від пересилання паперових носіїв між міністерствами та відомствами, створивши єдиний захищений простір обміну даними. На сучасному етапі розвиток національної системи управління документами характеризується переходом від поняття «діловодство» до концепції «управління інформаційними ресурсами». Відбувається поступова імплементація міжнародних стандартів серії ISO (зокрема ДСТУ ISO 15489), що змінюють фокус із форми документа на його контекст, цілісність та доступність.

1.3 Трансформація поняття «архівний документ» в умовах цифровізації

Предметом нашого дослідження є управлінський (службовий) документ, що створюється в процесі діяльності органів влади, установ і підприємств та відіграє визначальну роль у фіксації управлінських рішень, процесів і ділових операцій. Історично управлінські документи існували переважно у матеріальній формі, що забезпечувало їхній фізичний контроль, можливість візуальної перевірки автентичності та відносну простоту передачі на архівне зберігання. Цей тип

документа має чітко визначені реквізити, юридичну силу та регламентований життєвий цикл, що робить його ключовим об'єктом архівного обліку й експертизи цінності. У класичному діловодстві та архівній справі документ традиційно визначався через нерозривну єдність трьох складових: змісту (інформації), форми (структури/реквізитів) та матеріального носія (рисунок 1.4).

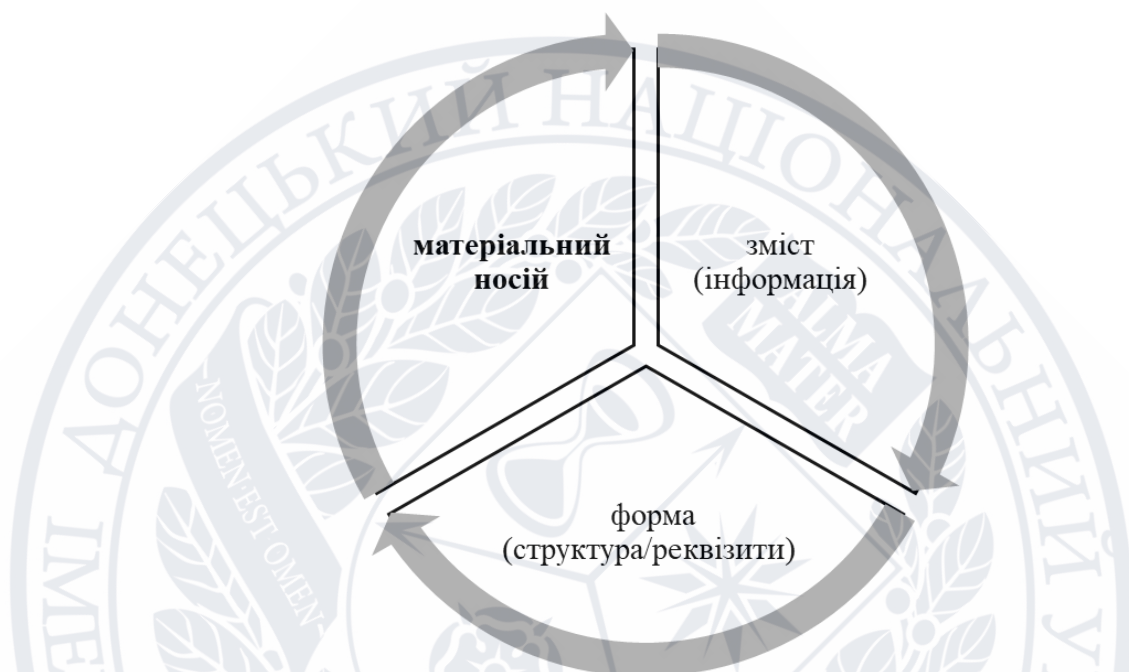


Рисунок 1.4 – Матеріальна фіксація як ключова ознака традиційного документа

Життєвий цикл традиційного управлінського документа охоплює низку послідовних етапів, які забезпечують його створення, рух, використання та завершальне зберігання (рисунок 1.5). Спершу виникає потреба у створенні документа, що зумовлено необхідністю зафіксувати управлінське рішення, підтвердити факт, організувати процес чи виконати нормативну вимогу. На цій основі здійснюється підготовка та складання документа: збираються потрібні відомості, обирається відповідна форма, формується текст і здійснюється його оформлення відповідно до вимог стандартів діловодства. Далі документ проходить узгодження (візування) із зацікавленими підрозділами та фахівцями, після чого набуває юридичної сили через підписання або затвердження

уповноваженою посадовою особою.



Рисунок 1.5 – Життєвий цикл управлінського документа

Підписаний документ підлягає реєстрації, унаслідок чого отримує унікальний індекс, що забезпечує його облік та можливість контролю. Після цього він направляється адресатам або доводиться до виконавців у межах установи для реалізації передбачених дій. На етапі виконання здійснюється практична реалізація завдань, визначених документом, а служби контролю відстежують дотримання строків і фіксують результат виконання. Після завершення роботи документ включається до складу відповідної справи та разом із супровідними матеріалами підшивається згідно з номенклатурою. Подальший етап – зберігання документації в установі протягом визначених строків, після чого проводиться експертиза її цінності. За результатами експертизи документи постійного чи довготривалого зберігання передаються до архіву, а ті, що втратили практичну та юридичну значущість, знищуються в установленому порядку. Така логічно вибудована послідовність забезпечує повний життєвий цикл управлінського документа – від його появи до остаточного завершення. Саме матеріальна фіксація була ключовою ознакою, що відрізняла документ від

простої усної інформації, і саме вона забезпечувала його стабільність у часі [2]. Фізична сутність документа була гарантією його існування: збереження носія автоматично означало збереження інформації.

Однак в умовах цифрового середовища цей зв'язок руйнується. Електронний документ не має жорсткої прив'язки до конкретного матеріального носія. Він стає віртуальним об'єктом, існування якого залежить від програмно-апаратного середовища. Це призводить до трансформації самого розуміння терміна «архівний документ», який набуває нових, раніше не властивих йому характеристик. Згідно із Законом України «Про Національний архівний фонд та архівні установи», архівний документ – це документ, що припинив виконання функцій, для яких був створений, але в силу своєї значущості для суспільства та держави підлягає постійному зберіганню. Для електронних документів це визначення ускладнюється технологічним чинником: щоб документ залишався «архівним» (тобто доступним і читабельним через 50 чи 100 років), над ним необхідно постійно здійснювати технологічні операції (міграцію форматів, емуляцію середовища).

Трансформація поняття відбувається у трьох основних площинах (рисунок 1.6).

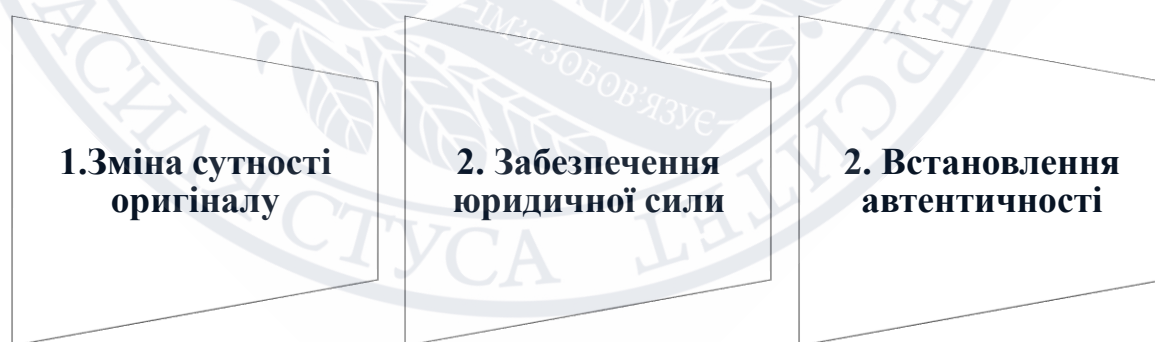


Рисунок 1.6 – Трансформація поняття «архівний документ»

1. У традиційному архівознавстві оригінал – це унікальний матеріальний об'єкт, створений первинно. Його юридична сила нерозривно пов'язана з носієм: втрата паперового носія фактично означає втрату оригіналу документа. Копії,

навіть засвідчені, мають похідний статус і часто обмежену доказову силу.

В електронному середовищі поняття «оригінал» набуває принципово іншого, умовного характеру. Згідно з Законом України «Про електронні документи та електронний документообіг», оригіналом електронного документа вважається його електронний примірник з обов'язковими реквізитами, зокрема електронним підписом автора. Специфіка цифрової природи дозволяє створювати нескінченну кількість ідентичних примірників (копій) без втрати якості, кожен з яких матиме статус оригіналу. Відтак, архівне зберігання зміщує фокус зі збереження унікального носія (як це відбувається з паперовими справами) на збереження унікальної інформаційної сутності та її зв'язків (метаданих).

2. Забезпечення юридичної сили документа традиційно гарантувалося власноручним підписом. Фізичний підпис є біометричною характеристикою особи і, будучи нанесеним на папір, залишається незмінним і доступним для графологічної експертизи протягом усього терміну зберігання носія (десятки або сотні років). Натомість в електронному документознавстві гарантом юридичної сили виступає кваліфікований електронний підпис (КЕП), який базується на криптографічних перетвореннях. Тут виникає фундаментальна колізія, відома як «проблема довгострокового зберігання підписаних даних»:

- термін дії сертифікатів: сертифікати відкритих ключів зазвичай діють 1–2 роки, тоді як термін зберігання архівних документів може бути постійним;
- застарівання криптоалгоритмів: з часом алгоритми шифрування стають вразливими, що ставить під загрозу можливість перевірки підпису через 10–20 років.

Це докорінно змінює методологію архівної роботи: якщо паперовий документ можна просто покласти на полицю («пасивне зберігання»), то електронний документ вимагає «активного збереження» – періодичного перепідписання, додавання міток часу або застосування спеціальних архівних форматів (наприклад, CAdES-A), щоб юридична сила не була втрачена після закінчення дії сертифіката.

3. Традиційний документ є самодостатнім: текст, дата і підпис знаходяться на аркуші. Електронний документ без метаданих (даних про дату створення, формат, структуру, авторів, історію змін) є фактично набором незрозумілих символів. Тому сучасний архівний документ розглядається не як окремий файл, а як «інформаційний пакет» (згідно з моделлю OAIS), що включає сам зміст та супровідні метадані. Як зазначає провідна дослідниця Л. Дюранті, у паперовому світі автентичність встановлюється через експертизу фізичних характеристик (папір, чорнило, водяні знаки) та безперервність фізичного контролю. В цифровому середовищі документ не має стабільних фізичних ознак. Тому автентичність ЕД переходить з площини візуального сприйняття у площину процедурну та математичну.

Вона базується на двох компонентах:

- цілісність (integrity): підтвердження того, що бітова послідовність файлу не була змінена (забезпечується хеш-функціями);
- метадані (metadata): супровідна інформація, яка фіксує зміст створення, історію змін та переміщень документа.

Таким чином, якщо для традиційного архіву головним було зберегти об'єкт недоторканим, то для електронного архіву критично важливим стає фіксація «ланцюга довіри» (Chain of Custody) – документованої історії володіння та управління документом від моменту його створення до передавання в архів. Будь-яка прогалина в цьому ланцюзі (наприклад, несанкціоноване копіювання без фіксації в метаданих) автоматично ставить під сумнів автентичність електронного документа, навіть якщо сам файл технічно не пошкоджений.

Отже, еволюцію поняття «архівний документ» можна розглядати крізь призму переходу від «статичної автентичності» фізичного оригіналу до «динамічної автентичності» електронного запису. Ключовим завданням стає аналіз того, як змінюються вимоги до підтвердження юридичної сили документа, коли він втрачає свою матеріальну форму та стає набором бітових даних, і які нові критерії (метадані, хеш-суми, електронні підписи) стають гарантами довіри до архівної інформації.

Висновки до розділу 1

Аналіз теоретичні аспекти вступу до закладів вищої освіти дозволив узагальнити деякі теоретичні позиції і зробити такі висновки:

1. Здатність бути доказом у правовому, історичному чи управлінському контексті, дозволяє відрізняти документ від інших інформаційних об'єктів та забезпечує його ключову роль у функціонуванні суспільства.

2. Інформаційно-технологічний підхід «Records Continuum Model» відображає перехід від матеріального до цифрового документального середовища, де збереження інформації залежить не від фізичного носія, а від правильно організованої системи управління даними.

3. Швидке моральне старіння технологій робить цифрову інформацію вразливою, а тому архівні установи використовують стратегії міграції форматів, створення цифрових копій, емуляції програмного середовища та побудови спеціалізованих репозиторіїв постійного зберігання. Саме репозиторії поступово замінюють традиційні архіви, оскільки здатні гарантувати збереження документів у зв'язку з їх технічною залежністю від програмних платформ.

4. Для довгострокового архівного зберігання критичне значення мають лише документи з високим рівнем довіри. Тільки використання захищених носіїв та кваліфікованих позначок часу дозволяє гарантувати юридичну силу документа через 10, 50 чи 75 років, забезпечуючи «презумпцію достовірності» підпису, яку неможливо спростувати без технічної експертизи.

5. Для забезпечення майбутнього архівного зберігання ЕД, архівні вимоги (формати, метадані) мають бути враховані ще в момент створення документа.

6. Для електронного архіву критично важливим стає фіксація «ланцюга довіри» (Chain of Custody) – документованої історії володіння та управління документом від моменту його створення до передавання в архів. Будь-яка прогалина в цьому ланцюзі (наприклад, несанкціоноване копіювання без фіксації в метаданих) автоматично ставить під сумнів автентичність електронного документа, навіть якщо сам файл технічно не пошкоджений.

7. Критичний аналіз показав, що головною проблемою залишається забезпечення «динамічної автентичності» документа. Якщо паперовий документ гарантував збереження інформації завдяки довговічності носія, то електронний документ вимагає постійної технологічної підтримки (міграції, конвертації). Чинна нормативна база України лише частково вирішує це питання, фокусуючись переважно на технології КЕП, яка має обмежений термін дії сертифікатів, що створює ризики для документів постійного терміну зберігання.



РОЗДІЛ 2

РЕГЛАМЕНТАЦІЯ ПРОЦЕСІВ ПЕРЕДАВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ НА АРХІВНЕ ЗБЕРІГАННЯ

2.1 Концептуальна модель OAIS як методологічна основа регламентації архівних процедур

Розроблення ефективної системи регламентації процесу передавання електронних документів на архівне зберігання неможливе без надійного теоретико-методологічного підґрунтя. В основі регламентації архівних процесів лежить еталонна модель OAIS, закріплена міжнародним стандартом ISO 14721:2012 [27]. Ряд наукових та професійних публікацій в Україні (зокрема у сфері цифрових архівів, бібліотек, збереження культурної спадщини) посиляються на OAIS / ISO 14721 як на модель для побудови цифрових архівів. В останніх роботах 2024–2025 рр. українськи науковці прямо згадують «OAIS Reference Model (ISO 14721)» як «фундаментальний стандарт для цифрового зберігання» [28]. У теоретичних і прикладних дослідженнях з архівної справи та управління документами OAIS розглядають як орієнтир для проектування систем зберігання [29]. Таким чином, в Україні цей стандарт впроваджено методом підтвердження, що свідчить про інтеграцію вітчизняної архівної системи у світовий інформаційний простір.

OAIS – це не конкретне програмне забезпечення чи інструкція, а концептуальна схема. Вона визначає універсальну термінологію та функціональну архітектуру, яка дозволяє організувати довгострокове збереження цифрової інформації незалежно від технологічних змін. Для регламентації процесів приймання-передавання документів модель OAIS є критично важливою, оскільки вона зміщує фокус з хаотичного переміщення файлів на структурований обмін інформаційними пакетами. Центральним елементом моделі є поняття «інформаційний пакет» (рисунк 2.1). OAIS

стверджує, що для збереження інформації недостатньо мати лише файл із даними. Необхідна також інформація про збереження – метадані, що описують походження, контекст, структуру та права доступу. Згідно з моделлю, у процесі архівування інформація трансформується і існує у трьох формах пакетів.

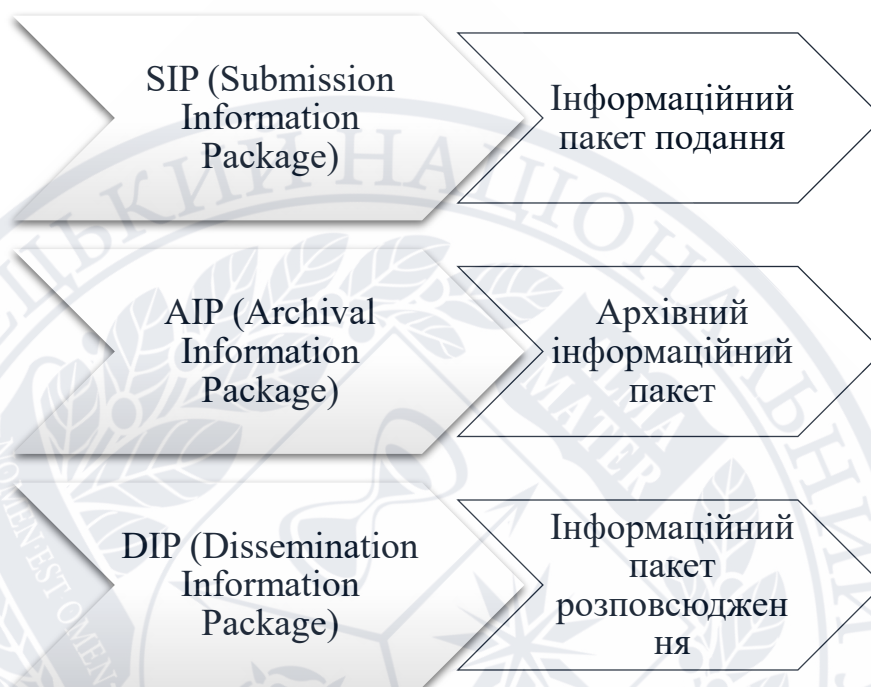


Рисунок 2.1 – Поняття «інформаційний пакет» моделі OAIS

SIP – це сукупність даних та метаданих, яка формується виробником документів (установою) і передається до архіву. Це «контейнер», який фіксує стан документа на момент його відчуження від власника. Головна функція SIP – забезпечити самодостатність документа. Це означає, що архівіст повинен зрозуміти зміст пакета і перевірити його автентичність, не телефонуючи до установи з запитаннями «А що це за файл?» або «Де підпис?».

Пакет SIP складається з двох основних блоків:

- змістова інформація; безпосередньо сам електронний документ (файли *.pdf, *.docx, *.xml) та дані про те, як їх відкрити;
- описова інформація про збереження (preservation description information – PDI): метадані, необхідні для ідентифікації та захисту документа.

PDI в пакеті SIP обов'язково має включати чотири категорії даних:

- унікальний номер (індекс), за яким документ можна знайти (наприклад, реєстраційний номер в СЕВ);
- хто створив документ, хто ним володів, історія змін (хто і коли підписав);
- зв'язок з іншими документами (наприклад, «це відповідь на лист №...»);
- контрольна сума (хеш-значення файлу), яка дозволяє перевірити, чи не був файл пошкоджений при передачі.

Для регламентації процесу передавання поняття SIP є ключовим. Саме вимоги до формування SIP мають бути детально прописані в національних нормативно-правових актах та інструкціях з діловодства. Якщо регламент не визначає чіткої структури SIP (які формати файлів допустимі, який склад метаданих обов'язковий, як пакувати контейнер), архів отримує неструктурований набір даних, який неможливо ефективно обробити та зберегти.

Розглянемо практичну реалізацію концепції SIP на прикладі передавання управлінського документа (наприклад, розпорядження керівника). На відміну від простого копіювання документа в архів, правильний підхід за моделлю OAIS передбачає створення спеціально структурованого контейнера, що забезпечує збереження документа разом з усіма даними, необхідними для підтвердження його автентичності й контексту створення. Такий пакет може бути оформлений як ZIP-архів або впорядкована папка. На рисунку 2.2 показано структура інформаційного пакету SIP, що побудована відповідно до моделі OAIS. Це архівний контейнер (наприклад, ZIP-архів або папка), який має чітку внутрішню структуру.

SIP-пакет містить усі логічні складники документа: основний файл, додатки, підписи та метадані. Це унеможливорює втрату частини інформації, яка була пов'язана з документом у момент його створення. Об'єднання всіх елементів у єдиний контейнер гарантує, що документ зберігається в первісній структурі та в повному складі. Цілісність забезпечується шляхом фіксації контрольної хеш-суми (наприклад, SHA-256), що дозволяє виявити будь-які зміни або пошкодження даних. Додатково використовуються формати, придатні

для довготривалого зберігання, такі як PDF/A, що зменшує ризик втрати доступності через технологічне старіння. SIP містить структуровані метадані про походження документа, його контекст та зв'язки з іншими документами.

Папка Data/ (Власне документ):

- decision_45.pdf (Текст рішення у форматі PDF/A для довгострокового зберігання)
- annex_table.xlsx (Додаток з цифрами бюджету)

Папка Signatures/ (Юридична значущість):

- decision_45.pdf.p7s (Файл кваліфікованого електронного підпису мера – КЕП)
- timestamp.tsr (Мітка часу, що підтверджує дату підписання)

Файл Metadata.xml (Паспорт документа – PDI):

- Reference: ID: UA-SEV-2024-0045.
- Provenance: Автор: Іванов І.І.; Підписант: Петров П.П. (Мер); Дата створення: 2024-11-25.
- Context: Належить до фонду «Міська рада», справа № 01-15 «Рішення сесій».
- Fixity: SHA-256 хеш файлу PDF: a1b2c3d4... (цифровий відбиток).

Файл manifest.xml (Опис структури пакета):

- Список усіх файлів у архіві, щоб переконатися, що нічого не загубилося.

Рисунок 2.2 – Вміст пакета SIP «Rish_45_2024.zip», побудованого відповідно до моделі OAIS

Наявність кваліфікованих електронних підписів і міток часу дозволяє точно

встановити, чи змінювався файл після підписання. Таким чином забезпечується доказ автентичності та можливість формальної перевірки. Юридична значущість документа підтримується збереженням КЕП та позначки часу у вигляді окремих файлів (p7s, tsr). Метадані про підписанта, дату створення та пов'язаний контекст забезпечують відповідність вимогам електронного документообігу й зберігають юридичну доказовість навіть у довгостроковій перспективі. У сукупності ці елементи формують надійний механізм довгострокового зберігання цифрових документів, який підтримує як технічну, так і юридичну їхню автентичність. Отже, SIP-пакет забезпечує повноту, збереженість, перевірюваність і юридичну силу цифрових документів протягом усього часу їхнього існування.

Якщо установа не застосовує модель OAIS, процес архівного збереження цифрового документа може виглядати надто спрощено й некоректно. Наприклад, файл Rish_45_budget.pdf просто копіюють на сервер архіву без додаткового супроводу. На перший погляд це здається достатнім, однак у довгостроковій перспективі виникають серйозні ризики. Уже через 10 років може бути неможливо встановити, хто саме підписував документ, оскільки електронний підпис був зовнішнім і не був збережений разом із файлом. Також залишається незрозумілим, чи є цей файл остаточною, узгодженою версією, чи в архів потрапив чернетковий варіант. До того ж відсутність контрольної хеш-суми не дозволить перевірити цілісність документа: файл може пошкодитися внаслідок технічних збоїв, шкідливого програмного забезпечення або інших факторів, і ніхто про це не дізнається. Таким чином, без дотримання принципів моделі OAIS архівування цифрових документів стає ненадійним і не забезпечує їхнього довготривалого збереження та автентичності.

AIP – це версія інформаційного пакета, яка зберігається всередині архівної системи. Це «еталонна копія» або «майстер-копія» документа. На відміну від SIP – пакету подання, який формується установою-виробником і може містити помилки чи нестандартні формати, AIP формується самим архівом під його повну відповідальність. Якщо установа надіслала документ у форматі *.doc (Word), архів під час створення AIP може автоматично конвертувати його

у *.pdf/a (для довгострокового зберігання), зберігаючи при цьому оригінал. Тобто AIP міститиме дві версії файлу. До опису додаються суто архівні дані: номер фонду, опису, справи, місце фізичного зберігання (шлях на сервері). В AIP записується протокол перевірки: «Прийнято дату X, перевірено антивірусом Y, підпис валідний, перевірів архівіст Z».

У таблиці 2.1 показано суть трансформації SIP-пакета у AIP, які здійснює архів в процесі приймання:

- контроль цілісності;
- антивірусна перевірка;
- перевірка підпису;
- нормалізація форматів;
- створення власних архівних метаданих.

Таблиця 2.1 – Трансформація SIP в AIP

Елемент	Було в SIP	Стає в AIP
Формати	Можуть бути нестабільні (.docx, .xlsx)	Нормалізація до PDF/A, XML та ін.
Структура	Лише службова структура установи	Архівний опис: фонд–опис– справа
Метадані	Мінімальні, для документообігу	Додано архівні та технічні метадані
Перевірка	Можлива наявність помилки	Протокол приймання + Audit Trail
Контроль цілісності	Хеш окремих файлів	Хеш усього пакета та періодична перевірка

Повернемося до нашого прикладу. Установа надіслала пакет SIP (файл + підпис КЕП). Архівна система прийняла його, провела валідацію і створила AIP «UA-Arch-Fund1-Op1-Spr45», як показано на рисунку 2.3.

1. Блок контенту (Content Information):

- original_decision_45.pdf (Те, що надіслала установа – ми це зберігаємо як доказ).
- **preservation_decision_45.pdf (Нормалізована версія PDF/A-3, яку створив сам архів для гарантії читабельності).**
- signature_mayor.p7s (Оригінальний підпис мера).

2. Блок збереження (PDI - Preservation Description Information):

- Інформація про походження (Provenance):
 - Запис: "Документ створено в Міськраді 25.11.2024".
 - **Запис: "Пакет SIP отримано 01.12.2024 о 14:00".**
 - **Запис: "Валідацію КЕП успішно пройдено 01.12.2024 о 14:01 (Протокол № 77)".**
- Інформація про цілісність (Fixity):
 - SHA-256 хеш для оригіналу: a1b2...
 - **SHA-256 хеш для AIP-контейнера: f9e8... (Архів постійно перевіряє саме цю суму).**
- Інформація про контекст (Context):
 - Архівний шифр: Фонд 1, Опис 1, Справа 45.
 - Зв'язки: "Є додатком до Протоколу сесії № 10".

3. Блок пакування (Packaging Information):

- Спеціальний XML-файл (наприклад, у форматі METS), який "склеює" всі ці файли разом і каже системі: "Це все – один документ".

Рисунок 2.3 – Вміст пакета AIP «UA-Arch-Fund1-Op1-Spr45», побудованого відповідно до моделі OAIS

Пакет DIP – це версія архівного документа, сформована системою на запит споживача. Головна особливість DIP полягає в тому, що він не обов'язково є точною копією того, що зберігається в архіві (AIP). Він оптимізований для зручності використання, швидкості передачі та захисту інформації. AIP може зберігатися у «важкому» форматі (наприклад, нестиснутий TIFF для зображень або спеціалізований XML для баз даних). DIP трансформується у «легкий» формат (JPEG, PDF), який відкривається у звичайному браузері. DIP може

містити менше інформації, ніж AIP. Наприклад, з нього можуть бути вилучені персональні дані (знеособлення) або службові технічні метадані, які не цікавлять звичайного користувача. DIP може формуватися як «проста інформаційна копія» (без юридичної сили) або як «електронна архівна довідка/копія» (з накладанням електронної печатки архіву для підтвердження достовірності).

Варто зазначити, що сфера цифрового збереження стрімко розвивається, і нормативна база постійно актуалізується. Станом на сьогодні міжнародна спільнота здійснює перегляд базового стандарту ISO 14721:2012 з метою приведення його у відповідність до сучасних технологічних викликів (хмарні обчислення, кібербезпека, блокчейн). Нова редакція стандарту (ISO 14721:2025), що перебуває на фінальній стадії затвердження, зберігає класичну архітектуру функціональних сутностей, проте значно деталізує вимоги до інформаційної безпеки та інтероперабельності систем. Для української архівної галузі орієнтація на цю оновлену версію є стратегічно важливою, оскільки вона закладає фундамент для побудови цифрових архівів наступного покоління. Хоча фундаментальна модель (SIP-AIP-DIP) залишається незмінною, оновлення викликане необхідністю адаптації до нових реалій:

1. Версія 2012 року писалася, коли архіви були переважно локальними серверами. Версія 2025 враховує реалії Cloud Computing.
2. Значно посилено вимоги до захисту від кіберзагроз, чого не було в старій версії.
3. виправлено неточності у термінології, які викликали суперечки протягом останніх 12 років, на кшталт, «цілі збереження», формалізація функції «Моніторинг», уточнення поняття «Інформаційна властивість» тощо [30].

Важливо також зазначити, що модель OAIS виділяє шість функціональних сутностей архіву, серед яких першочергове значення для процедури передавання має функція Ingest («Приймання»). Саме вона є «вхідними воротами» архіву та охоплює процеси отримання SIP від виробника, перевірку їхньої якості, формування AIP та підготовку матеріалів до довгострокового зберігання. На її основі мають бути розроблені регламентовані процедури вхідного контролю

(перевірка на віруси, цілісність, відповідність форматам і стандартам), валідації метаданих (коректність і повнота описових полів) та формування акта приймання–передавання. Разом із тим модель OAIS передбачає, що функція Ingest – лише один із шести рівноцінних блоків архівної системи. Інші п'ять визначають повний цикл довгострокового збереження та так само потребують нормативної регламентації:

– «Архівне зберігання» забезпечує фізичне та логічне розміщення AIP. На нормативному рівні ця сутність визначає вимоги до створення дублювальних копій, географічного резервування, контролю цілісності, періодичних перевірок хеш-сум та процедур відновлення після збоїв.

– «Керування даними» відповідає за супровід метаданих: їх структуру, актуальність, повноту та зв'язки між об'єктами. Регламенти повинні визначати стандартизовані словники, таксономії, XML-схеми, правила ведення реєстрів та журналів змін і підтримку зв'язку між SIP, AIP та DIP.

– «Адміністрування» охоплює управління всією системою: політиками збереження, документацією, правами доступу, аудитами та взаємодією з Producer і Consumer. Саме тут регулюються питання відповідальності, затверджуються протоколи моніторингу, визначаються показники надійності та процедури реагування на інциденти.

– «Планування збереження» прогнозує ризики технологічного застарівання та визначає стратегії міграції. Регламент повинен фіксувати перелік прийнятих форматів, політику міграції та конвертації, принципи тестування нових технічних рішень і методи оцінювання ризиків втрати доступності.

– «Доступ» забезпечує формування та видачу DIP користувачам. У нормативній базі ця сутність визначає вимоги до автентифікації, порядок надання електронних копій, формати для видачі, правила фіксації фактів доступу та умови збереження юридичної сили документів.

Таким чином, значення моделі OAIS для визначення регламентних процедур полягає не лише в стандартизації функції Ingest, а у створенні комплексної «архітектурної карти» для всієї системи електронного архівування.

Модель вимагає регламентувати не окремий файл (*.docx чи *.pdf), а цілісний інформаційний контейнер (ZIP, XML), що містить як контент, так і метадані. Це стимулює розробників нормативної бази (Міністерство юстиції, Укрдержархів) створювати формати обміну даними, які відповідають структурі SIP, зокрема XML-схеми. Модель розмежовує ролі «Власника» – установи, що передає документи, і «Архіву». Регламент має фіксувати момент переходу відповідальності: до успішної валідації SIP відповідальність за збереження несе Виробник; після прийняття та формування AIP – Архів. Використання OAIS як основи для національних регламентів забезпечує сумісність українських цифрових архівів із міжнародними системами. Це дозволяє інтегрувати перевірені практики та програмні рішення (наприклад, системи класу e-Archive), які побудовані відповідно до архітектури OAIS. Модель вимагає наявності у пакеті метаданих про збереження (Fixity, Provenance, Context). Це означає, що регламент передавання повинен зобов'язувати установу не просто «скинути файли», а надати докази їхнього походження та цілісності (хеш-суми, протоколи перевірки КЕП). Без цих вимог, закладених у модель, архів отримає набір файлів, які через декілька років втратять юридичну силу. Отже, модель OAIS виступає не просто теоретичною схемою, а необхідною «архітектурною картою» для створення нормативної бази. Будь-яка спроба регламентувати передавання електронних документів в обхід логіки «SIP – Ingest – AIP» призводить до створення нежиттєздатних систем, які не можуть гарантувати цілісність та доступність Національного архівного фонду в майбутньому.

2.2 Ключові проблеми забезпечення довгострокового зберігання

У практиці національних установ поширена думка, що для архівування електронних документів достатньо лише конвертувати їх у відповідний формат (наприклад, PDF/A з підписом CAdES-A) та розмістити на сервері чи зовнішньому носії, є хибною та небезпечною. Такий підхід, який можна

охарактеризувати як «пасивне зберігання», ігнорує фундаментальні загрози цифрового середовища: фізичну амортизацію носіїв («bit rot») та моральне старіння криптографічних алгоритмів.

Аналіз технологічних вимог показує, що надійне зберігання можливе лише в умовах функціонування спеціалізованих інформаційних систем (Архівних сховищ даних), які забезпечують активну підтримку цілісності об'єктів.

1. Електронний підпис (навіть у форматі довгострокового зберігання) є математично залежним від цілісності кожного біта файлу. Зміна навіть одного байта внаслідок збою жорсткого диска, дії вірусу або помилки копіювання призводить до повної втрати юридичної сили документа (помилка верифікації підпису). Звичайні файлові системи (NTFS, FAT32) не мають вбудованих механізмів постійного контролю цілісності. Тому архівна система повинна автоматично виконувати процедуру «fixity check» – регулярну перевірку контрольних сум кожного файлу та автоматичне відновлення пошкоджених об'єктів із резервних копій.

2. Формати CAdES-A або PAdES-LTV фіксують статус підпису на певний момент часу. Однак криптографічні алгоритми хешування (наприклад, SHA-256), на яких базуються ці підписи, з часом стають вразливими до кібератак (зокрема, з появою квантових обчислень). Зберігання файлу «де завгодно» не дозволяє реагувати на ці загрози. Натомість, повноцінна система електронного архіву повинна реалізовувати функцію «періодичного перештамування» (Timestamp renewal). Система автоматично моніторить термін життя алгоритмів і, до моменту їх компрометації, накладає поверх старого архівного підпису нову мітку часу, створену на базі більш стійкого алгоритму.

Цей процес дозволяє подовжувати юридичне життя документа нескінченно довго, створюючи ланцюжок довіри, який неможливо забезпечити при простому зберіганні файлів на диску.

3. Логічний контроль доступу. На відміну від звичайного файлового сховища, де права доступу легко змінити, архівна система повинна реалізовувати політику WORM (Write Once, Read Many). Це унеможливорює видалення або

модифікацію архівного документа навіть привілейованими користувачами (адміністраторами), гарантуючи його незмінність для майбутніх поколінь [31].

Отже, існує принципова різниця між «резервним копіюванням файлів» та «електронним архівуванням». Перше – це лише збереження байтів, друге – це комплексний технологічний процес збереження юридичної значущості, який вимагає впровадження спеціалізованого програмного забезпечення, побудованого за моделлю OAIS.

Аналіз вимог до довгострокового зберігання електронних документів (підтримка форматів OAIS, забезпечення бітової цілісності, постійна актуалізація криптографічних підписів) свідчить про високу вартість та технічну складність створення власних систем електронного архівування. Для більшості установ – фондоутворювачів Національного архівного фонду (шкіл, лікарень, органів місцевого самоврядування, малого бізнесу) розгортання локальних OAIS-сумісних систем є економічно недоцільним або неможливим через відсутність IT-інфраструктури та кваліфікованого персоналу. Вирішенням цієї проблеми є перехід від децентралізованої моделі (де кожна установа будує свій маленький цифровий архів) до централізованої сервісної моделі.

Світовий досвід пропонує чотири основні шляхи для таких установ:

1. Модель «Архів як сервіс». Це хмарна модель, за якої установа не купує сервери та програмне забезпечення, а отримує доступ до централізованої платформи через веб-інтерфейс.

Установа формує пакети SIP на своєму комп'ютері та через захищений канал завантажує їх у «хмару» державного архіву або сертифікованого провайдера. Установа відповідає лише за правильне формування та опис документів. Всі складні технічні процедури (резервне копіювання, міграція форматів, оновлення міток часу LTV) виконує центральна система автоматично. Це зрівнює у можливостях великі міністерства та маленькі сільські ради, надаючи їм однаковий рівень захисту даних без капітальних витрат [31].

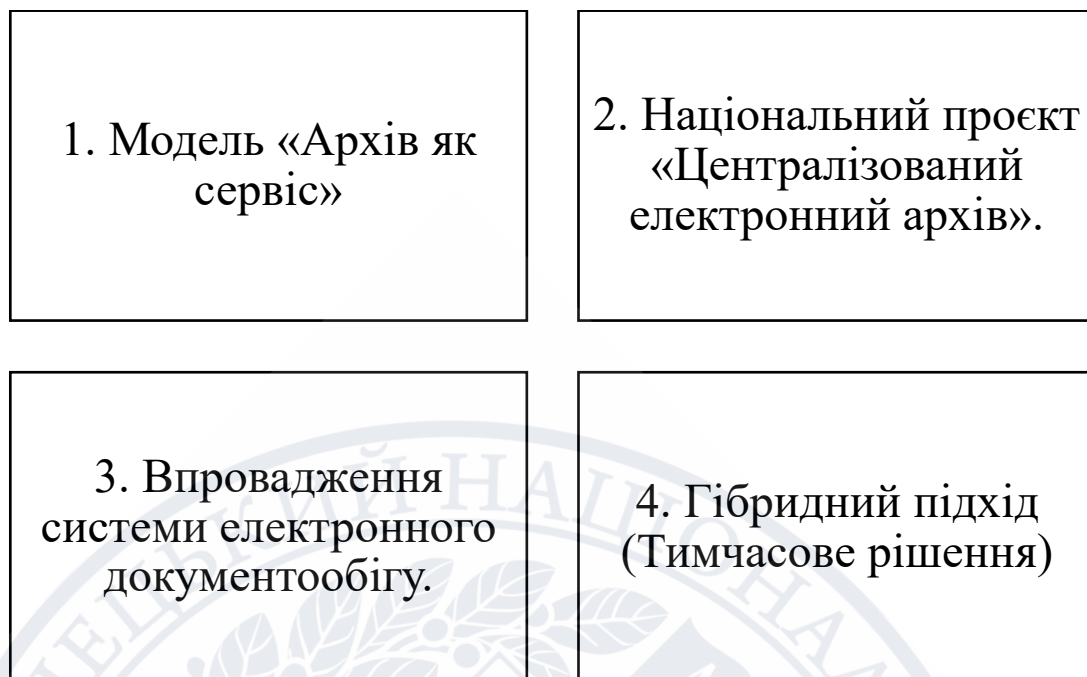


Рисунок 2.4 – Шляхи переведення установ на електронні документи

2. В Україні Державна архівна служба спільно з Міністерством цифрової трансформації реалізує пілотний проєкт зі створення платформи, яка виконуватиме функції галузевого державного архіву цифрової документації. Ця система передбачає, що установи передають документи не на фізичних носіях (дисках/флешках), а завантажують їх безпосередньо в єдину державну систему. Це дозволяє реалізувати принцип «єдиного ядра», де всі механізми перевірки підписів та забезпечення цілісності зосереджені в одному місці, яке обслуговують професійні фахівці [32].

3. Професійні системи електронного документообігу забезпечують повноцінне управління життєвим циклом електронних управлінських документів. На етапах створення, погодження та виконання вони автоматично формують і підтримують необхідні метадані, що гарантують юридичну силу, автентичність, цілісність і простежуваність документа. Завдяки підтримці накладання кваліфікованого електронного підпису підтверджується відповідальність посадових осіб і зберігається доказовість документа у довгостроковій перспективі. Однак системи електронного документообігу первинно не призначені для довгострокового зберігання документів, а їх основна

функція обмежується етапом активного використання. Після завершення бізнес-процесів знижується частота звернення до документів, і в цей момент починають проявлятися суттєві обмеження СЕД, зокрема:

- відсутність механізмів забезпечення бітової цілісності на протязі десятків років (регулярна перевірка контрольних сум, автоматичне відновлення з резервів);

- залежність довговічності електронного підпису від незмінності файлу, а також від актуальності криптографічних алгоритмів, які потребують періодичного оновлення (перештампування LTV);

- відсутність гарантій незмінності – адміністратор або розробник може змінити або видалити документ;

- зберігання в робочих форматах (DOCX, XLSX), які не гарантують довготривалого відтворення;

- локальна залежність від платформи, версії СЕД та ІТ-інфраструктури установи, що з часом змінюється;

- брак архівних метаданих, необхідних для подальшої передачі документа до державного архіву;

- відсутність підтримки архівних процедур, визначених міжнародними стандартами (формування SIP/AIP/DIP за моделлю OAIS).

Отже, системи електронного документообігу оптимально застосовувати на етапі оперативного управління документами: створення, погодження, виконання, контроль термінів. Саме для цього вони розроблені. Однак після завершення робочих процесів частина документів має довгострокові строки зберігання або ж підлягає передачі до архівних установ. У більшості українських установ ще відсутня технічна можливість гарантувати цифрове зберігання впродовж десятків років, тому законодавство наразі передбачає тимчасовий компроміс: якщо установа не може забезпечити довгострокове зберігання електронних документів, вона повинна створити засвідчену паперову копію. У таблиці 2.2 здійснено порівняння СЕД і Електронного архіву.

Таблиця 2.2 – Порівняння характеристик СЕД і Електронного архіву

Критерій	Система електронного документообігу (СЕД)	Електронний архів (OAIS-сумісний)
Призначення	Оперативна робота з документами, погодження, виконання процесів	Довгострокове (10–100+ років) забезпечення збереження та юридичної цінності
Юридична значимість у часі	Підписи старіють → можливість втрати чинності	Підтримка LTV, періодичне перештампування, збереження ланцюга довіри
Цілісність даних	Залежить від надійності файлового сховища, немає fixity checks	Постійна перевірка контрольних сум, відновлення з резервних копій
Незмінність документів	Документи можна змінити/видалити адміністратором	Політика WORM – неможливість модифікації об'єктів
Формати зберігання	Робочі формати: DOCX, XLSX, JPEG	Архівні формати: PDF/A, XML, TIFF, стандартизована структура AIP
Метадані	Метадані орієнтовані на бізнес-процеси	Архівні метадані: контекст створення, зберігання, доступу, перевірок
Контроль доступу	Гнучкий, але змінний (можливі ризики знищення)	Строгий контроль, ведення історії доступів та дій
Управління життєвим циклом	Орієнтована на активні документи	Робота з напівактивними і неактивними документами
Передача документів	Немає механізмів формування архівних пакетів	SIP → AIP → DIP, підтримка процесів передачі в держархів
Нормативна база	ISO 15489 (records management)	OAIS (ISO 14721), ISO 16363, моделі довгострокової автентичності
Аудит та довіра	Доказовість обмежена часом чинності КЕП	Верифікація походження та історії документа протягом усього строку зберігання
Вартість впровадження	Нижча, спрямована на щоденну роботу	Вища, потребує спеціальної інфраструктури та персоналу

У майбутньому, після запуску державної інфраструктури цифрового архівування, ці паперові документи можуть бути повторно оцифровані з

накладанням електронного підпису уповноваженої особи. Але важливо розуміти:

- оцифрований папір – це вже не той самий електронний документ, що був у СЕД;
- юридично він набуває статусу електронної копії з паперового оригіналу;
- втрачається частина первинних технічних атрибутів автентичності.

Це необхідний перехідний механізм, але його не можна вважати ідеальним рішенням.

4. До моменту повноцінного запуску централізованих сервісів, для установ, які не можуть забезпечити цифрове збереження, законодавство залишає можливість використання паперових копій. Згідно з чинними нормами, якщо установа не має можливості гарантувати збереження електронного документа протягом встановленого строку (наприклад, 75 років для кадрових документів), вона зобов'язана створити засвідчену паперову копію електронного документа. Ця копія передається в архів у традиційний спосіб. Такий підхід є вимушеним компромісом ("милицею"), який, хоч і суперечить ідеї безпаперового офісу, але гарантує фізичне збереження інформації в умовах технологічної невизначеності.

Майбутнє регламентації для «звичайних установ» полягає не в написанні інструкцій «як купити сервер», а в розробці регламентів підключення до централізованих хмарних сховищ. Стратегічним завданням держави є створення єдиної інфраструктури, яка візьме на себе тягар довгострокового збереження, залишивши за установами лише функцію фондоутворювачів.

Висновки до розділу 2

1. Для регламентації процесу передавання електронного документа на архівне зберігання поняття SIP (пакета подання) є ключовим. Саме вимоги до формування SIP мають бути детально прописані в національних нормативно-правових актах та інструкціях з діловодства. Якщо регламент не визначає чіткої

структури SIP (які формати файлів допустимі, який склад метаданих обов'язковий, як пакувати контейнер), архів отримує неструктурований набір даних, який неможливо ефективно обробити та зберегти.

2. Значення моделі OAIS для визначення регламентних процедур полягає не лише в стандартизації функції Ingest, а у створенні комплексної «архітектурної карти» для всієї системи електронного архівування. Вона уніфікує об'єкт передавання (відокремлений інформаційний контейнер SIP, а не окремі файли), чітко розподіляє відповідальність між Виробником і Архівом, забезпечує інтероперабельність національних систем збереження з міжнародними та гарантує довгострокову доступність і автентичність Національного архівного фонду. Будь-яка спроба регламентувати передавання електронних документів в обхід логіки «SIP – Ingest – AIP» неминуче призводить до створення нежиттєздатних систем, які не здатні забезпечити збереження цифрової спадщини в довготривалій перспективі.

3. На сьогодні системи електронного документообігу ефективно забезпечують лише активну фазу життєвого циклу документа. Довгострокове ж зберігання потребує спеціалізованих архівних систем та централізованої державної інфраструктури. Тимчасове рішення у вигляді створення паперових копій не є оптимальним, але дозволяє гарантувати збереження інформації до повного переходу на цифрову модель архівної справи.

РОЗДІЛ 3

УДОСКОНАЛЕННЯ НОРМАТИВНО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ПЕРЕДАВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

3.1 Розроблення алгоритму формування та приймання інформаційного пакета SIP

Аналіз нормативної бази та технологічних проблем, проведений у другому розділі, дозволяє стверджувати, що головною перешкодою для ефективного комплектування Національного архівного фонду є відсутність чітко регламентованих процедур. Однак розроблення уніфікованого алгоритму ускладнюється тим, що сама процедура формування пакета SIP не є лінійною. Вона критично залежить від первісного джерела походження документів і визначає подальшу технологічну траєкторію їхнього оброблення.

У сучасній архівній практиці співіснують два принципово відмінні потоки інформації, які вимагають диференційованого підходу до регламентації:

1. Документи, народжені в цифрі – створюються в системах електронного документообігу, мають накладений КЕП автора і не мають паперового оригіналу.
2. Оцифровані документи – є електронними копіями паперових оригіналів, отриманими шляхом сканування.

Джерело походження документа безпосередньо впливає на ключові параметри алгоритму формування SIP, а саме:

– на вибір формату зберігання: для «народжених у цифри» пріоритетом є збереження структури (PDF/A, XML), тоді як для «оцифрованих» критичним є збереження візуальної точності образу (TIFF, PNG);

– на склад метаданих: народжені в цифрі документи автоматично успадковують метадані з СЕД, тоді як оцифровані потребують ручного або напіваавтоматичного індексування та прив'язки до фізичного оригіналу;

– на процедуру підтвердження юридичної сили: у першому випадку

перевіряється криптографічний підпис автора, у другому – засвідчувальний підпис оператора оцифрування, який гарантує правильність копії.

З огляду на це, пропонується комплексний алгоритм формування та приймання інформаційного пакета SIP, побудований на принципах моделі OAIS, який враховує специфіку обох документальних потоків.

Процес передавання поділяється на три логічні етапи:

1. Етап формування. Відбувається на боці установи-власника.
2. Етап передачі: Захищений канал передачі даних.
3. Етап приймання та валідації відбувається на боці архіву.

Етап 1 «Формування пакета SIP» реалізується в інформаційній системі установи-фондоутворювача. Його метою є перетворення розрізних файлів або паперових аркушів на уніфікований архівний об'єкт (рисунок 3.1). Запропонований алгоритм передбачає розгалуження процесів залежно від первісної природи документа.

Крок 1.1. Класифікація вхідного потоку. Система автоматично або за участі оператора визначає тип джерела:

- Потік А: Електронні документи, створені в СЕД, які мають кваліфікований електронний підпис (КЕП) автора.
- Потік Б: Паперові документи, що підлягають оцифруванню.

Крок 1.2. Нормалізація та створення контенту. На цьому кроці забезпечується уніфікація форматів файлів для довгострокового зберігання.

- Для Потoku А: Здійснюється конвертація робочих файлів (DOCX, RTF) у формат PDF/A (ISO 19005). При цьому система перевіряє, щоб візуальне відображення конвертованого файлу відповідало оригіналу.
- Для Потoku Б: Здійснюється сканування паперового оригіналу.

Формується два файли:

1. Майстер-копія (TIFF): Висока роздільна здатність (300–600 dpi), без стиснення, для збереження точного візуального образу.
2. Робоча копія (PDF/A): Стиснена версія з розпізнаним текстовим

шаром (OCR) для забезпечення повнотекстового пошуку.

Крок 1.3. Забезпечення юридичної значущості.

- Для Потoku А: Система перевіряє наявність та валідність КЕП автора документа. Якщо підпис недійсний або пошкоджений, документ не допускається до архівування.
- Для Потoku Б: Уповноважена особа (працівник архівного підрозділу) накладає на електронну копію свій КЕП засвідчення, підтверджуючи відповідність цифрової копії паперовому оригіналу (згідно з Інструкцією з діловодства).

Крок 1.4. Генерація метаданих та хешування. Це критичний етап для забезпечення цілісності.

1. Система обчислює контрольну суму (хеш) кожного файлу за алгоритмом SHA-256. Цей унікальний цифровий відбиток дозволить у майбутньому виявити будь-яку, навіть найменшу, зміну у файлі.
2. Формується XML-паспорт (маніфест) пакета. До нього автоматично записуються: індекс справи, заголовок, дата створення, імена файлів та їхні обчислені хеш-суми.

Крок 1.5. Інкапсуляція (Packaging). Усі компоненти об'єднуються в єдиний контейнер (ZIP-архів). До контейнера включаються:

- файли контенту (PDF/A, TIFF);
- файли відокремлених підписів (P7S);
- XML-паспорт.

Крок 1.6. Фінальне засвідчення пакета. На сформований ZIP-контейнер накладається Кваліфікована електронна печатка установи з обов'язковою позначкою часу.

- *Мета:* Зафіксувати склад пакета та точний час його формування, закривши його від будь-яких подальших змін.

Результатом Етапу 1 є готовий до передавання пакет SIP, який є самодостатнім, захищеним та юридично оформленим об'єктом.

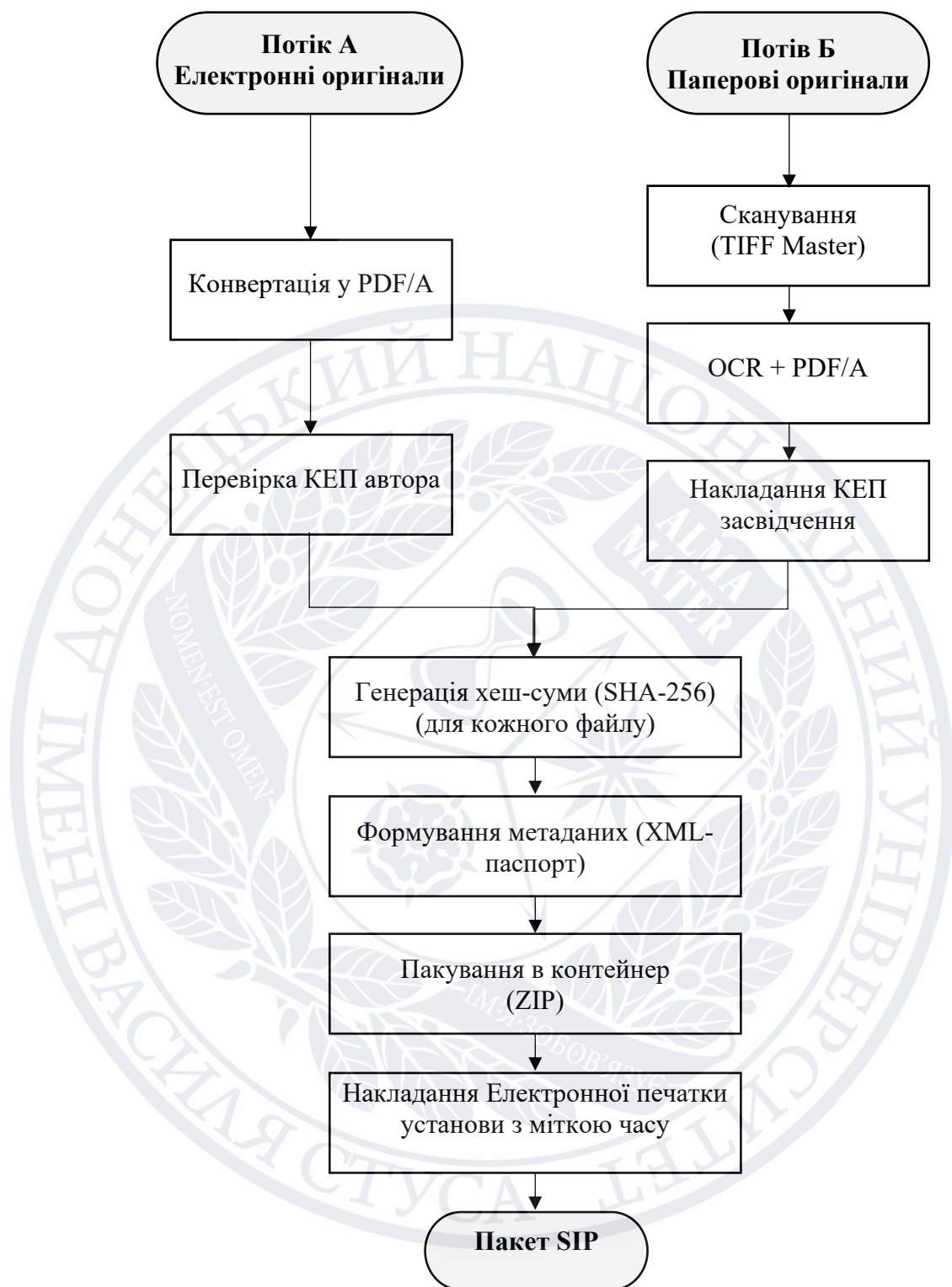


Рисунок 3.1 – Етап «Формування пакета SIP»

У таблиці 3.2 показано відмінності алгоритму формування SIP для різних типів документів, що дозволяє наочно продемонструвати специфіку процедури для кожного окремого виду документації.

Таблиця 3.1 – Відмінності алгоритму формування SIP для різних типів документів

Етап процесу	«Народжені цифровими»	Оцифровані
Джерело	Система електронного документообігу (СЕД)	Паперова справа на полиці
Формат файлу	Конвертація DOCX PDF/A	Сканування Paper TIFF (Master) + PDF/A
Суть контенту	Текст + вбудовані об'єкти	Растрове зображення + OCR шар
Метадані	Автоматично витягуються з картки документа	Вносяться вручну або напівавтоматично (опис фізичного стану)
Електронний підпис	Підпис автора (Мер, Директор). Засвідчує <i>зміст.</i>	Підпис оператора/архівіста. Засвідчує <i>вірність копії.</i>
Головний ризик	Старіння форматів та криптографії	Низька якість сканування, помилки розпізнавання (OCR)

Отже, при розробці регламенту передавання необхідно чітко розмежовувати потоки «born-digital» та «digitized» документів. Для оцифрованих копій алгоритм формування SIP ускладнюється етапами технічного контролю якості зображення (ISO 19264) та процедурою засвідчення відповідності електронної копії паперовому оригіналу. Регламент має передбачати включення до SIP-пакета оцифрованого документа двох версій файлів:

Майстер-копії (TIFF) – для забезпечення максимальної збереженості візуальної інформації;

Робочої копії (PDF/A) – для забезпечення текстового пошуку та доступу користувачів. Ігнорування етапу створення майстер-копії є поширеною помилкою, яка унеможливорює якісне відтворення документа в майбутньому.

Етап 2 передачі пакета SIP часто недооцінюють, вважаючи його простою технічною процедурою («скопіював файл»). Але з точки зору регламентації та безпеки – це критична ланка, де документ виходить із захищеного контуру установи і стає вразливим. Цей етап забезпечує фізичне та логічне переміщення сформованого пакета SIP із середовища установи-виробника до середовища архіву. З огляду на ризики перехоплення, підміни або пошкодження даних під час транзиту, регламентація цього етапу вимагає застосування захищених протоколів.

Крок 2.1. Вибір каналу передачі. Запропонований алгоритм передбачає два сценарії транспортування, залежно від технічних можливостей сторін та обсягу даних (таблиця 3.2).

Таблиця 3.2 – Характеристики каналів передачі пакетів SIP

Характеристика	Онлайн-передача	Офлайн-передача
Застосування	Для регулярного передавання невеликих та середніх масивів документів	Для передавання особливо великих масивів (наприклад, терабайтів оцифрованих фондів) або секретної документації, яку заборонено передавати мережею Інтернет
Технологія	Використання захищених каналів зв'язку (VPN-тунелі) або спеціалізованих веб-інтерфейсів (API) із шифруванням трафіку за протоколом TLS 1.2/1.3	Використання фізичних носіїв інформації (зовнішні жорсткі диски, захищені флеш-накопичувач
Процедура	Установа завантажує SIP-пакет через кабінет користувача в системі «Електронний архів» або передає його автоматично через шлюз системи електронної взаємодії (СЕВ)	Носій має бути відформатований у файловій системі, що підтримує контроль цілісності та великі файли (наприклад, NTFS або exFAT), та попередньо перевірений на відсутність вірусів

Крок 2.2. Ідентифікація та автентифікація. Перед початком передачі архівна система повинна ідентифікувати відправника. Використовується двофакторна

автентифікація (КЕП посадової особи + логін/пароль системи). Система перевіряє, чи має дана установа право передавати документи саме до цього архівного фонду (перевірка повноважень згідно з Планом комплектування).

Крок 2.3. Фіксація часу відправлення. У момент початку завантаження (або передачі носія) фіксується точний час транзакції. Це важливо для дотримання нормативних строків передавання справ.

Крок 2.4. Передача супровідного повідомлення. Разом із пакетом SIP (або групою пакетів) передається електронне супровідне повідомлення (аналог супровідного листа), яке містить:

- кількість переданих пакетів;
- загальний обсяг даних (у байтах);
- загальну контрольну суму (хеш) усього масиву передачі.

Цей крок дозволяє архіву на наступному етапі миттєво виявити можливу втрату частина даних під час передавання.

Етап 3 «Приймання та валідація» – це критичний етап контролю якості. Архівна система не повинна сліпо довіряти тому, що прийшло. Вона виконує функцію «фільтра», відсіюючи пошкоджені або некоректно оформлені пакети.

Запропонований алгоритм вхідного контролю наведено на рисунку 3.2 і включає такі кроки перевірки.

Крок 2.1. Карантинна перевірка. Отриманий пакет SIP поміщається в ізольовану зону («пісочницю») і сканується на наявність шкідливого програмного забезпечення.

Крок 2.2. Перевірка цілісності передачі. Система обчислює хеш-суму отриманого контейнера і звіряє її з тією, що була зафіксована у момент відправки. Якщо суми не збігаються – передача відбулася з помилками, пакет автоматично відхиляється.

Крок 2.3. Синтаксична валідація. Система розпаковує контейнер і перевіряє:

- Чи відповідає XML-паспорт затвердженій схемі (XSD schema)?
- Чи є всі файли, зазначені в паспорті, наявними в архіві?
- Чи відповідають файли заявленим форматам (чи це справді PDF/A, а не

перейменований вірус)?

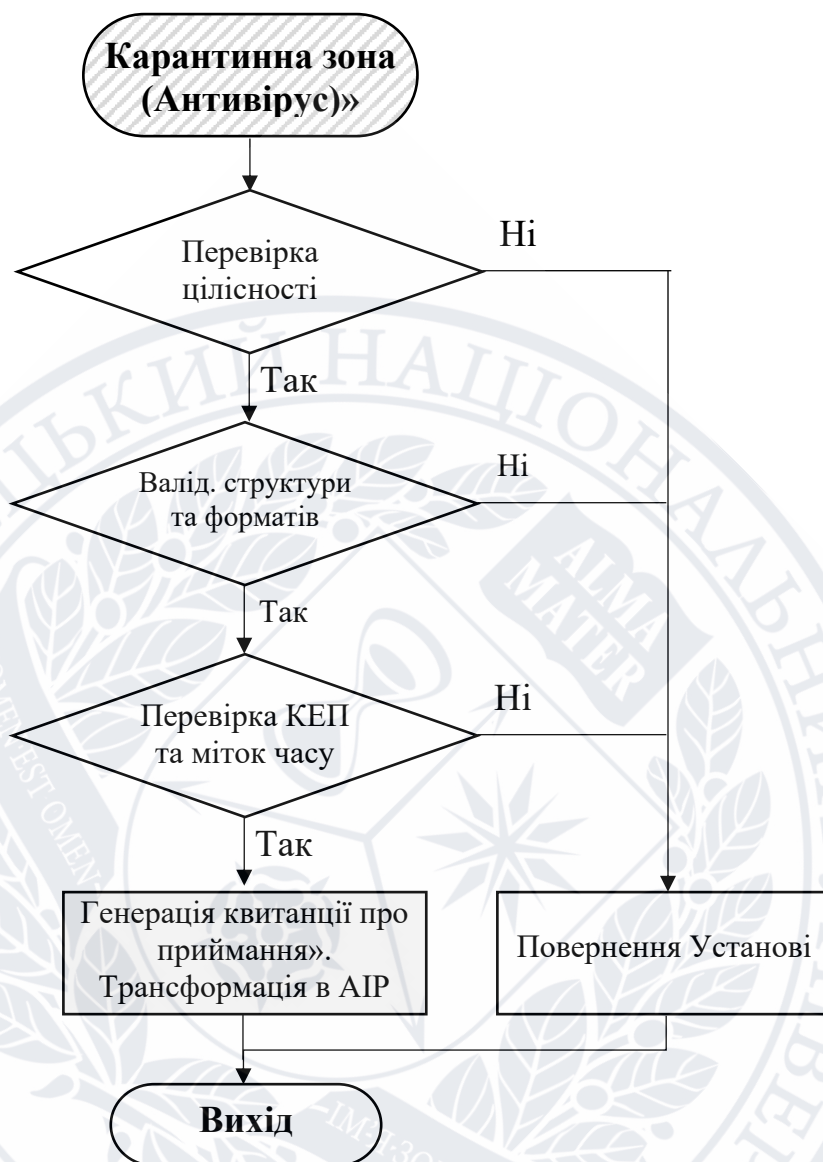


Рисунок 3.2 – Етап «Приймання та валідації»

Крок 2.4. Перевірка юридичної сили. Найскладніший етап. Система перевіряє валідність усіх накладених КЕП:

- Чи був сертифікат чинним на момент підписання?
- Чи не був він у списку відкликаних (CRL)?
- Чи коректна мітка часу? Результат перевірки записується у спеціальний протокол валідації, який стає частиною архівного зберігання.

Крок 2.5. Прийняття рішення.

Якщо всі перевірки пройдено, системі присвоює пакету статус «Прийнято»,

генерує квитанцію про отримання для установи і розпочинає процес створення архівного пакета AIP.

Якщо хоча б одна перевірка не пройшла, пакет повністю відхиляється. Установі надсилається протокол з кодом помилки (наприклад, «Помилка хеш-суми файлу № 2»). Часткове приймання (коли прийняли тільки «хороші» файли) є неприпустимим, оскільки це порушує цілісність справи.

3.2 Вимоги до програмно-технічного забезпечення автоматизованої системи архівного зберігання

Реалізація першого етапу алгоритму вимагає впровадження в установі спеціалізованого програмного модуля – «Генератора SIP». Це ПЗ може бути реалізоване як окрема десктопна програма (для малих установ) або як інтегрований модуль системи електронного документообігу (для великих фондоутворювачів).

Функціональна архітектура такого ПЗ повинна включати чотири ключові компоненти:

1. Модуль нормалізації та конвертації – це «двигун», який відповідає за підготовку файлів. Звичайний Word або Excel не вміють створювати валідні архівні формати автоматично у промислових масштабах. Програма повинна мати вбудовані бібліотеки для конвертації (наприклад, на базі LibreOffice SDK або Ghostscript), які дозволяють пакетно перетворювати файли *.doc/*.docx, *.xls/*.xlsx, *.ppt/*.pptx у стандартизований формат PDF/A-1b або PDF/A-2a.

Також має бути програмна перевірка того, що у PDF/A вбудовано всі шрифти і немає заборонених елементів (JavaScript, шифрування), які заблокують доступ до тексту в майбутньому.

2. Модуль криптографічної обробки – це програмний компонент, який взаємодіє з апаратними носіями ключів (токенами) або хмарними сервісами підпису (CloudID). ПЗ повинно підтримувати роботи з українськими криптографічними бібліотеками (наприклад, бібліотеки АТ «ІТ» або

EndUser.dll), що забезпечують накладання КЕП згідно з ДСТУ 4145-2002.

Критично важливою функцією є можливість створення відокремлених підписів (CAdES-Detached) та, що найважливіше, підтримка масового підписання. Програма має дозволяти керівнику або архівісту підписати 1000 сформованих справ однією операцією (введенням PIN-коду один раз), інакше процес передавання буде заблоковано людським фактором.

3. Модуль опису та пакування – це «мозок» системи, який формує структуру пакета. ПЗ повинно автоматично генерувати XML-файли (METS, EAD або національний формат опису) на основі карток документів. Програма має зчитувати поля з бази даних СЕД («Заголовок», «Дата», «Індекс») і переносити їх у відповідні теги XML без ручного введення.

Критично важливою функцією такого ПО є розрахунок контрольних сум. ПЗ повинно автоматично вираховувати хеш (SHA-256) для кожного файлу і записувати його в маніфест пакета перед закриттям ZIP-архіву.

4. Валідатор – це інструмент самоперевірки. Перш ніж відправити пакет в архів, програма має сама себе перевірити і мати інтеграцію з інструментами ідентифікації форматів (наприклад, DROID або Siegfried). Це дозволяє установі переконатися, що вона відправляє саме те, що вимагає архів.

Приклади наявних програмних рішень (Open Source), які Україна може адаптувати наведені у таблиці 3.3.

Таблиця 3.3 – Приклади програмних рішень [34]

ПО	Призначення
E-ARK SIP Creator	Безкоштовна утиліта з відкритим кодом, розроблена в ЄС. Дозволяє вручну завантажити файли, додати метадані та отримати готовий валідний SIP. Ідеально підходить для малих установ (сільради, музеї), які не мають потужних СЕД.
RODA-in	Інструмент для масового створення SIP-пакетів з папок на комп'ютері. Автоматично сканує директорії, створює структуру і пакує в ZIP.
DocuWare / Scriptum (Українські реалії)	Вітчизняні розробники СЕД (АСКОД, Мегаполіс) повинні доопрацювати свої системи, додавши кнопку «Експорт в Архів», яка запускає описаний вище алгоритм «під капотом».

Для реалізації Етапу 1 установи не потребують складних серверів, але потребують клієнтського ПЗ класу «SIP Creator». Стратегічним завданням держави є розробка та безкоштовне розповсюдження уніфікованої програми-клієнта, яка дозволить будь-якій установі сформувати стандартизований архівний пакет, сумісний з державною системою зберігання.

Висновки до розділу 3

1. Під час розроблення регламенту передавання слід окремо визначати потоки «born-digital» і «digitized» документів. Для оцифрованих матеріалів формування SIP ускладнюється потребою контролю якості (ISO 19264) та засвідчення відповідності копії оригіналу. У SIP потрібно включати дві версії: майстер-копію у TIFF для гарантованого збереження візуальної інформації та робочу копію у PDF/A для пошуку й доступу. Пропуск створення майстер-копії є типовою помилкою й позбавляє можливості якісного відтворення документа в майбутньому.

2. Для формування SIP-пакету установам не потрібна потужна серверна інфраструктура, однак необхідне клієнтське програмне забезпечення типу «SIP Creator».

3. Стратегічним пріоритетом держави має стати створення й безоплатне поширення уніфікованого клієнтського застосунку, який забезпечуватиме формування стандартизованих архівних пакетів, повністю сумісних із державною системою зберігання.

ВИСНОВКИ

У магістерській роботі здійснено комплексне дослідження теоретико-методологічних та практичних аспектів регламентації процесу приймання та передавання електронних документів на постійне архівне зберігання. За результатами проведеного дослідження зроблено такі висновки:

1. Встановлено, що в умовах цифрової трансформації відбувається фундаментальна зміна сутності архівного документа. Він трансформується зі статичного матеріального об'єкта (паперового носія) у динамічний інформаційний об'єкт, існування якого залежить від програмно-апаратного середовища. Доведено, що традиційні підходи до регламентації, орієнтовані на фізичне збереження, є неефективними. Сучасна регламентація має базуватися на управлінні метаданими, забезпеченні бітової цілісності та підтримці логічної структури документа незалежно від носія.

2. Аналіз національної нормативної бази показав, що ключовим інструментом забезпечення юридичної сили електронних документів в Україні є Кваліфікований електронний підпис (КЕП). Однак виявлено критичну проблему «технологічного старіння» криптографічних засобів. Стандартні підписи мають обмежений термін дії, що створює загрозу втрати юридичної значущості архівних документів у довгостроковій перспективі. Обґрунтовано необхідність нормативного закріплення обов'язкового використання форматів архівного підпису (CAdES-A/ASiC-A) з підтримкою технології LTV (Long-Term Validation) та періодичного оновлення позначок часу.

3. Визначено, що безальтернативною основою для побудови ефективної системи регламентації є міжнародна еталонна модель OAIS (ISO 14721). Доведено, що спроби регламентувати архівування без урахування архітектури «SIP – Ingest – AIP» призводять до створення нежиттєздатних систем, несумісних з європейським цифровим простором.

4. У роботі розроблено комплексний алгоритм формування та приймання

пакета SIP, який, на відміну від існуючих практик, чітко розмежовує два технологічні потоки: для документів, народжених у цифрі, пріоритетом визначено збереження структури та конвертацію у формат PDF/A; для оцифрованих документів висунуто вимогу створення еталонної майстер-копії (TIFF) та процедуру засвідчення відповідності електронної копії паперовому оригіналу. Такий підхід дозволяє уніфікувати процес передавання незалежно від джерела походження документації.

5. Встановлено, що реалізація вимог OAIS потребує спеціалізованого програмного забезпечення класу «E-Archive», яке є недоступним для більшості установ-фондоутворювачів через високу вартість та технічну складність. Запропоновано перехід до централізованої моделі «Архів як сервіс» (SaaS). Стратегічним рішенням визначено створення єдиного державного хмарного сховища та розробку безкоштовного клієнтського застосунку «SIP Creator», що дозволить установам з обмеженими ресурсами формувати валідні архівні пакети без розгортання власної складної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національний архівний фонд та архівні установи. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/3814-12#Text>.
2. Кулешов С.Г. Управлінське документознавство: Навчальний посібник. – К.: ДАККіМ, 2003. 57 с.
3. Палієнко М. Українські архіви, війна та збереження національної ідентичності. *Архіви України*. 2022. Вип. 1. № 330. С. 12–38.
4. Бездрабко В. В. Зарубіжний досвід архівації електронних документів: е-пошта та твіти / В. В. Бездрабко // *Сумська старовина*. – 2018. – №52. – С. 80-89
5. Дубровіна Л. А. Основні положення концепції комп'ютеризації архівної справи в Україні. *Студії з архівної справи та документознавства*. Київ, 1998. Т. 3. С. 6–17.
6. Золотар О.О. Правова охорона як складова інформаційної безпеки: моногр. – Київ: ТОВ «ПанТот». 2011. 100 с.
7. Каламайко А. Ю. Електронні засоби доказування в цивільному процесі : автореф. дис. ... канд. юрид. наук : 12.00.03 / А. Ю. Каламайко ; кер. роботи К. В. Гусаров ; Нац. юрид. ун-т ім. Ярослава Мудрого. – Харків, 2016. – 20 с.
8. Папакін Г. «Цифровий поворот» у джерелознавстві: реальність, перспектива чи ілюзія? *Український історичний журнал*. 2021. № 1. С. 153-169.
9. InterPARES Project. *InterPARES Project*. URL: <https://www.interpares.org/>.
10. Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years. *CLIR*. URL: <https://www.clir.org/pubs/reports/pub107/thibodeau/>.
11. <https://ccsds.org/Pubs/650x0m3.pdf>
12. Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years. *CLIR*. URL: <https://www.clir.org/pubs/reports/pub107/thibodeau/>.

13. CCSDS.org - Consultative Committee for Space Data Systems.
URL: <https://ccsds.org/Pubs/650x0m3.pdf>.
14. Dollar C.M., Bucci O. Archival Theory and Information Technologies: The Impact of Information Technologies on Archival Principles and Methods / ed. by Bucci O. University of Macerata, 1992. 117 p.
15. ДОКУМЕНТ - тлумачення, орфографія, новий правопис онлайн.
СЛОВНИК - тлумачний словник української мови, орфографічний словник онлайн. URL: <https://slovnyk.ua/index.php?swrd=документ>.
16. Schellenberg T.R. Modern Archives Principles and Techniques. The University of Chicago Press, Chicago, 1956.
17. Schellenberg T. R. The Management of Archives. New York: Columbia University Press, 1965.
18. Левченко Л. Архіви і архівна справа Сполучених Штатів Америки: історія та організація : монографія / Лариса Левченко. – Миколаїв : Іліон, 2013. – 1204 с.
19. Бездрабко, В. В. Управлінське документознавство: Навчальний посібник. К.: Четверта хвиля, –2006.–208 с.
20. Про електронні документи та електронний документообіг. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/851-15>.
21. Про електронний цифровий підпис. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/852-15#Text>.
22. Про електронну ідентифікацію та електронні довірчі послуги. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.
23. Про електронні довірчі послуги. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005#Text>
24. Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС. *Офіційний вебпортал парламенту України*.

URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text.

25. Cryptomathic. Introduction into CAdES for Trust Service Providers. *Cryptomathic: Empowering Secure Cryptographic Solutions*.

URL: <https://www.cryptomathic.com/blog/introduction-into-cades-for-trust-service-providers>.

26. Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ) | ДП «ДІА». Державне підприємство «ДІА». URL: <https://se.dia.gov.ua/sev-ovv>.

27. ISO 14721:2012. ISO. URL: <https://www.iso.org/ru/standard/57284.html>.

28. Ковтанюк Ю. Актуальні питання створення цифрових колекцій історико-культурної спадщини Національної бібліотеки України імені В. І. Вернадського в контексті цифрової трансформації гуманітарної галузі / Ю. Ковтанюк, З. Шевченко // Наукові праці Національної бібліотеки України імені В. І. Вернадського. - 2024. - Вип. 72. - С. 208-245. doi: <https://doi.org/10.15407/np.72.208>

29. Калінічева Г. І. Міжнародні стандарти у сфері архівної справи та керування документаційними процесами: проблеми гармонізації в Україні / Г. І. Калінічева, Р. В. Романовський // Архіви України. - 2015. - № 4. - С. 54-73. - Режим доступу: http://nbuv.gov.ua/UJRN/ay_2015_4_5.

30. ISO 14721:2025. ISO. URL: <https://www.iso.org/standard/87471>.

31. Про затвердження та впровадження методичних рекомендацій "Забезпечення збереженості електронних документів Національного архівного фонду". Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/rada/show/v0013842-20#Text>.

32. Розробка та створення електронного архіву | UAC. UAC. URL: <https://uac-archive.com.ua/digital-services/rozrobka-konczepczyi-i-stvorennya-elektronnogo-arhivu/>.

33. В Україні запрацюють електронні архіви: деталі проекту. *InBase*. URL: <https://inbase.com.ua/v-ukrayini-zapraczyuyut-elektronni-arhivy-detali-proyektu/>.

34. Gemini / Google. 2025. URL: <https://gemini.google.com>