УДК 004.056

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТІВ І НОРМАТИВНИХ ДОКУМЕНТІВ У СФЕРІ ДОВГОСТРОКОВОГО ЗБЕРІГАННЯ ТА ПЕРЕВІРКИ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ТА ПІДПИСІВ

Андрій Охріменко, Олександр Стокіпний, Владислав Ковтун

Стаття присвячена порівняльному аналізу міжнародних, європейських та українських стандартів і нормативних документів у сфері довгострокового зберігання електронних документів та забезпечення довгострокової перевірки електронних підписів. Проведено систематизацію чинної нормативної бази на трьох рівнях: глобальному (OAIS/ISO 14721, ISO 16363, IETF RFC 4998/6283, формати AdES), європейському (eIDAS 1.0/2.0, ETSI EN 319 102/421/422, TS 119 511/512, TR-ESOR, NF Z42-013, E-ARK) та національному (Закон України «Про електронну ідентифікацію та електронні довірчі послуги», наказ Мін'юсту № 1886/5, станом на кінець 2025 року, пілот «е-Архів»). Виявлено ключові відмінності у ступені деталізації правового регулювання, зрілості технічної інфраструктури довірчих послуг та практиці застосування механізмів довгострокової валідації електронних підписів (LTV).

Ключові слова: *довгострокове зберігання електронних документів, довгострокова перевірка, електронний підпис, OAIS, eIDAS, LTV, PAdES, XAdES, CAdES, LTA, ETSI, Evidence Record, електронні довірчі послуги.*

ВСТУП

Забезпечення автентичності, цілісності та доступності електронних документів в перспективі десятиліть це одне з ключових завдань інформаційного суспільства. Паперові документи за дотримання певних вимог до носіїв і належних фізичних умов можуть зберігатися сторіччями. Електронні документи ж стикаються з численними ризиками, зокрема з технологічними (наприклад, застарівання форматів даних, носіїв, програмного забезпечення, тощо) та з криптографічними (зникнення надавача, втрата чинності сертифікатів, компрометація алгоритмів підпису і гешування, тощо). Як наслідок, основне завдання, яке постає перед архівістами, юристами та ІТ-фахівцями, полягає в тому, як зберегти довіру до електронного документу, що підписаний сьогодні, через 10 і більше років. Вирішення цього завдання передбачає системний підхід в узгодженості технічних, організаційних і правових заходів (від вибору формату підпису до наявності кваліфікованих довірчих послуг довготривалого зберігання). Хоча й існує ціла низка міжнародних та європейських стандартів, нормативних документів та інструкцій, що покликані вирішити це завдання, проте значна частина наукових досліджень зосереджена або на суто технічних аспектах криптографії, або на правових питаннях визнання підпису, тим самим оминаючи розгляду саме системного підходу. Тому, метою статті є проведення структурованого порівняльного аналізу міжнародних, європейських та вітчизняних стандартів і нормативних документів з довгострокового зберігання та перевірки електронних документів і підписів, виявити ключові відмінності та прогалини, а також окреслити напрями подальшої гармонізації вітчизняної нормативної бази.

Міжнародний рівень

Модель відкритої архівної інформаційної системи (Open Archival Information System, OAIS) де-факто є обов'язковим орієнтиром для всіх архівів, які мають відповідати міжнародним вимогам у сфері довгострокового збереження цифрових даних.

Модель OAIS була обрана у якості стандарту ISO 14721 [1] та визначає архів як систему апаратного та програмного забезпечення, людей і процесів, що відповідають за отримання, довготривале збереження та надання доступу до інформації визначеній спільноті користувачів протягом необмежено довгого періоду часу. Довготривале збереження в контексті OAIS означає проміжок часу, достатній для виникнення змін у технологіях або складі спільноти. Функціональна модель описує шість взаємопов'язаних компонентів [1]: Надходження (Ingest), Архівне зберігання (Archival Storage), Управління даними (Data Management), Адміністрування (Administration), Планування збереження (Preservation Planning) та Доступ (Access).

Ключовою концепцією в OAIS є інформаційний пакет трьох типів:

- Submission Information Package (SIP) або пакет, що надходить до архіву;
- Archival Information Package (AIP) або архівний пакет зберігання;
- DIP (Dissemination Information Package) або пакет що надходить з архіву до користувача.

Кожен AIP включає самі дані, що архівуються, інформацію для збереження (Preservation Description Information, PDI) і описову інформацію для пошуку. PDI, своєю чергою, охоплює метадані цілісності (Fixity), походження (Provenance), контексту та ідентифікації.

OAIS є технологічно нейтральним та не прив'язаний до конкретних форматів даних, протоколів або систем. Саме через це модель OAIS є довговічним концептуальним стандартом, проте потребує доповнення конкретними технічними специфікаціями під час реалізації.

OAIS активно розвивається та доповнюється новими поняттями та функціями. На даний момент актуальною є версія 3 стандарту (CCSDS 650.0-M-3, грудень 2024 р.), що відповідає ISO 14721:2025.

На основі OAIS розроблено стандарт ISO 16363 «Audit and certification of trustworthy digital repositories» [2], що визначає критерії та методику незалежної оцінки відповідності архіву принципам надійності. Стандарт охоплює три категорії критеріїв: організаційну інфраструктуру (управління, фінансова стійкість, правові механізми), управління цифровими об'єктами (прийом, управління даними, збереження та доступ), а також технічну інфраструктуру і систему безпеки.

Стандарт ISO 14641 [3] охоплює практичні вимоги до систем зберігання документів, а стандарт ISO 15489 [4] визначає принципи управління записами, які лежать в основі будь-якої програми архівування, яка відповідає вимогам довгострокового збереження.

На технічному рівні довгострокова перевірка (Long-Term Validation, LTV) електронних підписів забезпечується протоколами і форматами, що дають змогу зберегти доказову базу підпису за межами строку дії сертифіката та надійності криптоалгоритмів.

IETF RFC 3161 [5] (Time-Stamp Protocol) разом з IETF RFC 5816 [6] є базою для всіх форматів позначок часу та визначає протокол взаємодії між клієнтом та службою позначок часу (TSA). Клієнт обчислює геш документа чи даних та надсилає його до TSA, яка в свою чергу додає точний час та підписує своїми ключами. Це забезпечує незаперечний доказ існування даних на зазначений момент часу.

IETF RFC 4998 [7] і IETF RFC 6283 [8], описують синтаксис запису доказів (Evidence Record Syntax, ERS). Evidence Record являє собою контейнер, що містить необхідні геш-образи для групи архівованих об'єктів та послідовність архівних позначок часу, що охоплюють ці геші. ERS дозволяє оновлення шляхом додавання до запису нових архівних позначок часу, коли старий алгоритм гешування або підпис TSA втрачає надійність, створюючи ланцюг доказів. Також ERS дозволяє виконувати масове архівування створюючи спільний доказ існування для багатьох документів одразу згрупувавши їх геші у вигляді геш-дерев.

Де-факто міжнародний стандарт PREMIS (Preservation Metadata: Implementation Strategies) [9] описує формат метаданих для довгострокового збереження та описує модель об'єктів, агентів, прав і подій. Фіксація кожної значущої події з об'єктом (ingest, fixity check, digital signature validation, format migration) в стандартизованій формі PREMIS дозволяє простежити повну історію походження документа і є суттєвим доповненням до технічних доказів довгострокової перевірки. Digital Preservation Handbook [10] це ключовий практичний довідник з цифрового архівування, підготовлений Digital Preservation Coalition. Він є методичним керівництвом з організації довгострокового збереження цифрових даних.

Що стосується криптографічних стандартів гешування, цифрового підпису, шифрування та інших, в тому числі стандарти постквантової криптографії [11], то використовується стек стандартів, що розробляє NIST.

Європейський рівень

Регламент Європейського Союзу (ЄС) №910/2014 (eIDAS) заклав правову основу для електронних довірчих послуг у єдиному цифровому ринку ЄС [12]. Він запровадив правовий режим кваліфікованих електронних підписів, печаток, позначок часу та послуг реєстрованої доставки, визнавши кваліфіковані послуги юридично рівнозначними традиційним аналогам по всьому ЄС. Також eIDAS визначив послуги перевірки та довгострокового зберігання кваліфікованих електронних підписів як окремі категорії кваліфікованих довірчих послуг, однак практичне впровадження цих послуг на ринку ЄС залишалося обмеженим аж до прийняття eIDAS 2.0.

Регламент ЄС №2024/1183 (eIDAS 2.0) став другою версією регулювання електронної ідентифікації та довірчих послуг в ЄС, по суті оновивши базовий регламент eIDAS [13]. Серед оновлень зокрема є зміни, що формують повноцінну регуляторну екосистему для LTV:

- запроваджено кваліфіковану довірчу послугу електронного архівування, що забезпечує тривале зберігання електронних документів із гарантіями цілісності, автентичності та юридичної дійсності.

- запроваджено кваліфіковану довірчу послугу електронних реєстрів (Electronic Ledgers), що легалізує застосування технологій розподілених реєстрів (розподілені реєстри DLT та блокчейн) у правовому полі ЄС.
- запроваджено єдиний цифровий гаманець ідентичності ЄС (EUDI Wallet), що дозволяє громадянам зберігати та пред'являти перевірені атрибути і документи в цифровій формі.
- посилено вимоги до перевірки кваліфікованих електронних підписів.

Європейський інститут телекомунікаційних стандартів (ETSI), що є ключовою організацією зі стандартизації в ЄС, розробив спеціалізовані стандарти, що деталізують технічні вимоги до послуг довгострокового зберігання підписів. Стандарт ETSI TS 119 511 [14] визначає вимоги до політик і безпеки постачальників послуг довгострокового зберігання підписів (вимоги до ізоляції ключів, аудиту, управління змінами та забезпечення неперервності). ETSI TS 119 512 [15] встановлює процедури здійснення послуг збереження, включаючи форматування архівних контейнерів, процедури додавання архівних позначок часу та звітності. ETSI EN 319 421 [16] визначає вимоги до постачальників кваліфікованих позначок часу, такі як точність джерела часу, захист ключів на HSM, формат токену та процедури аудиту. ETSI EN 319 422 [17] є технічним профілем протоколу позначок часу з підтримкою нових алгоритмів і архівних позначок часу.

Європейська технічна специфікація CEN TS 18170 містить вимоги та рекомендації щодо систем електронного архівування [18]. Вона стосується функціональних, технічних та організаційних вимог до систем, призначених для збереження електронних записів з доказовою цінністю та відповідності з плином часу. В свою чергу ETSI SR 019 510 є концептуальним документом [19], що визначає модель, механізми та напрями стандартизації послуг довгострокового збереження електронних даних і цифрових підписів у контексті довірчих сервісів.

Не дивлячись на наявність загальноєвропейської регуляції, деякі країни ЄС розробили власні стандарти та технічні документи, що описують процес LTV. Технічна настанова TR-ESOR (BSI TR-03125), що розроблена Федеральним відомством безпеки інформаційних технологій Німеччини, визначає архітектуру, вимоги та процеси довгострокового зберігання електронних документів і підписів із збереженням їх доказової сили [20]. Він описує використання позначок часу, Evidence Records за IETF RFC 4998 та IETF RFC 6283, дерев гешів, архівних позначок часу, процедури перепідпису та повторного додавання позначок часу, інтерфейси та формати для архівування. Це прикладний стандарт з детальним описом криптографічних механізмів. При цьому TR-ESOR сумісний з набором стандартів від ETSI та eIDAS. Французький національний стандарт NF Z42-013 визначає вимоги до систем електронного архівування, для забезпечення юридичної доказової сили електронних документів [21]. Він описує вимоги до процесів архівування, такі як внесення, зберігання, доступ та видалення електронних документів, організаційні заходи та політики. Фактично це практичний стандарт побудови юридично значимого електронного архіву. NF Z42-013 передбачає сертифікацію NF 461 для відповідних програмних продуктів і послуг.

ЄС фінансував та фінансує ряд ініціатив з розвитку електронного архівування. Так, в рамках загальноєвропейського проекту E-ARK [22] було розроблено ряд технічних специфікацій, еталонну архітектуру архіву та базу знань, визначено схеми метаданих та рекомендовані формати файлів. Ці специфікації підтримуються через програму CEF eArchiving і забезпечують технічну інтероперабельність між національними архівами членів ЄС.

Що стосується криптографічних стандартів гешування, цифрового підпису, шифрування та інших, в тому числі стандарти постквантової криптографії, то використовується власний стек стандартів ETSI [23], які в свою чергу посилаються на стандарти NIST.

Стандарти форматів підписів та документів

Для забезпечення LTV використовуються спеціальні формати підписів AdES (Advanced Electronic Signature), які стандартизовані ETSI відповідно до вимог регламенту eIDAS. Для PDF файлів використовується формат PAdES (ETSI EN 319 142), для XML-документів – формат XAdES (ETSI EN 319 132), а для будь-яких двійкових документів чи даних – формат CAdES (ETSI EN 319 122). Кожен з трьох базових форматів має градацію профілів від базового (B/BES) до довгострокового архівного (LTA/A).

Профіль LTA/LT включає в підписаний контейнер усі необхідні матеріали перевірки, такі як повний ланцюжок сертифікатів, відповіді OCSP або списки відкликаних сертифікатів на момент підпису, а також позначки часу. PAdES-LTA є обов'язковим форматом для

кваліфікованих підписів на PDF-документах у ЄС згідно з вимогами eIDAS. XAdES-LTA та CAdES-LTA забезпечують ті ж гарантії для XML і двійкових документів відповідно, доповнюючи LT-профіль архівними позначками часу.

Активне використання електронних підписів у форматах CAdES та XAdES, призвело до появи відповідних стандартів ETSI TS 119 132-3 [24] та ETSI TS 119 122-3 [25], що визначають специфіку Evidence Record для них.

Формат контейнерів ASiC (Associated Signature Container, ETSI EN 319 162) дозволяє об'єднати один або кілька документів та їхні підписи в єдиний ZIP-контейнер (.asice, .asics). ASiC-E (Extended) підтримує включення Evidence Record для забезпечення LTV всього контейнера, що особливо зручно для архівних процесів, де пакет документів має зберігатися як єдиний об'єкт.

Стандарт ETSI EN 319 102 [26] описує процедури створення та перевірки підписів AdES, архітектуру сервісів перевірки, логіку прийняття рішення про дійсність підпису та формування звіту про результат перевірки електронного підпису.

З метою спростити впровадження електронних підписів, печаток і їх довгострокової перевірки у прикладних системах розробляється референсна реалізація стандартів ETSI і вимог регламенту eIDAS під назвою DSS (Digital Signature Services) [27]. Це бібліотека програмного забезпечення з відкритим кодом, основне призначення якої надати готові механізми для створення, розширення (XAdES, CAdES, PAdES), перевірки підписів, обробки сертифікатів, OCSP/CRL та позначок часу, а також формування доказової бази перевірки відповідно до європейського законодавства.

Для самих документів вітчизняна та міжнародна архівна практика рекомендує формати з низьким ризиком технологічного старіння [28], наприклад:

- PDF/A (ISO 19005) для створення текстових електронних документів,
- TIFF для растрових зображень,
- WAV/FLAC для аудіо,
- SIARD для реляційних баз даних,
- XML/CSV для структурованих даних.

PDF/A відрізняється від звичайного PDF вбудовуванням шрифтів, кольорових профілів і метаданих, що дозволяє забезпечити відтворення зовнішнього вигляду без зовнішніх ресурсів

Національний рівень

Основними орієнтирами у сфері електронних документів і довірчих послуг в Україні є Закон України «Про електронні документи та електронний документообіг» №851-IV від 22.05.2003 (зі змінами) та Закон України «Про електронні довірчі послуги» №2155-VIII від 05.10.2017. Останній замінив Закон України «Про електронний цифровий підпис» № 852-IV від 22.05.2003 і запровадив термінологію eIDAS, таку як кваліфікований електронний підпис, кваліфікована позначка часу, кваліфікований надавач довірчих послуг.

З метою гармонізації українського законодавства з вимогами ЄС (eIDAS) й забезпечення взаємного визнання електронної ідентифікації та довірчих послуг було прийнято Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2801-IX від 2022 р. Фактично він розширив закон 2017 року, додавши повноцінну електронну ідентифікацію і створивши основу для транскордонного електронного документообігу з ЄС [29].

Наказ Міністерства юстиції №1886/5 від 11.11.2014 (зі змінами) встановлює «Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання», який регламентує вимоги до форматів файлів, структури електронних справ та контролю цілісності при передаванні до архіву [30].

Координуючим органом системи довірчих послуг в Україні є Центральний засвідчувальний орган (ЦЗО) при Міністерстві цифрової трансформації України (Мінцифра), який веде Довірчий список кваліфікованих надавачів електронних довірчих послуг (КНЕДП). Крім Мінцифри та ЦЗО, ключові ролі виконують також Національний банк України (здійснює регулювання електронних довірчих послуг у банківській та платіжній сфері), Державна служба спеціального зв'язку та захисту інформації України (формує державну політику у сфері криптографічного та технічного захисту інформації, визначає допустимі алгоритми, вимоги до засобів криптографічного захисту інформації) та Міністерство юстиції України (регулює електронний документообіг та архівне зберігання, встановлюючи правила довготривалого збереження електронних документів і пов'язаних з ними підписів). Станом на 2025 рік в Україні діє близько 30 КНЕДП [31], проте всі вони орієнтовані переважно на надання лише послуг пов'язаних з електронним підписом. КНЕДП, які надають виключно

довірчу послугу кваліфікованої позначки часу, без прив'язки до електронних підписів, немає.

Для взаємного визнання електронної ідентифікації й довірчих послуг Україна має підтримувати технічні стандарти ETSI щодо форматів електронних підписів, які застосовуються в Україні. На теперішній час прийнято державні стандарти України на основі форматів CAdES, XAdES та PAdES, в тому числі і профілі LTA.

Що стосується криптографічних стандартів гешування, цифрового підпису, шифрування та інших, то крім стеку стандартів, що розробляє NIST, Україна має набір національних квантово-захищених стандартів ДСТУ 7624:2014 (блочний симетричний шифр «Калина», ДСТУ 7564:2014 (геш-функція «Купина»), ДСТУ 8845:2019 (потоковий шифр «Струмок»), ДСТУ 8961:2019 (постквантовий алгоритм асиметричного шифрування «Скеля»), ДСТУ 9212:2023 (постквантовий алгоритм електронного підпису «Вершина») та проект стандарту альтернативного постквантового алгоритму електронного підпису «Сокіл».

У 2023 році Міністерство юстиції разом із Державною архівною службою та за підтримки проекту ЄС «Право-Justice» презентувало пілотний проект системи «е-Архів» [32], яка забезпечує централізоване електронне зберігання та доступ до електронних документів органів державної влади. Також Національний банк України реалізує власний електронний архів для документів банківського сектору. Разом з тим, поки що відсутня повноцінна нормативна і технологічна основа для довготривалої криптографічної перевірки LTV.

Аналіз ключових відмінностей

Найбільш комплексну і деталізовану нормативно-правову базу має ЄС завдяки регламенту eIDAS та екосистемі імплементаційних актів. Кожна стадія LTV від створення документу та його підписання до архівного збереження охоплена відповідним нормативним актом.

Україна відповідає стандартам eIDAS на рівні законодавства про довірчі послуги, що є суттєвим досягненням. Більшість нормативних документів гармонізовано з регламентами та стандартами ЄС, проте немає детальних вимог до LTV та не враховано національну специфіку (криптографічних алгоритмів, нормативних документів, тощо). Для більшості пост-квантових криптографічних алгоритмів відсутні об'єктні ідентифікатор (OID) та криптографічні механізми (СКМ) в сенсі PKCS#11.

На глобальному рівні (поза ЄС) правове регулювання залишається частковим. Більшість країн не мають аналога eIDAS, а послуги LTV регулюються галузевими актами або взагалі залишені на розсуд приватних компаній на ринку послуг.

Технічна інфраструктура ЄС є зрілою та конкурентною. Десятки QTSP у кожній країні пропонують свої послуги, які визнаються в усьому ЄС. В Україні рівень практичного застосування довірчих послуг, крім послуг пов'язаних з електронним підписом, залишається низьким.

В Україні відсутнє систематизоване регулювання процесу управління доказами довготривалого зберігання. Також відсутня система сертифікації та аудиту архівних систем і послуг LTV, яка б засвідчувала відповідність вимогам стандартів та законодавства. Це знижує загальну довіру до довгострокового збереження електронних документів та унеможливлює побудову складних бізнес-систем, орієнтованих на експлуатацію у період 10 років і більше.

Нижче наведено порівняльну таблицю параметрів нормативного регулювання та практики впровадження довгострокового збереження та довгострокової перевірки за трьома рівнями.

Висновки

Проведений порівняльний аналіз дозволяє зробити певні висновки.

Міжнародна та європейська нормативно-технічна база для довгострокового збереження електронних документів і електронних підписів є достатньо зрілою та комплексною. Глобальний рівень (OAIS/ISO 14721:2024, ISO 16363, IETF RFC 4998/6283, формати AdES) утворює концептуальну та технічну основу, яка в ЄС доповнюється юридичними регуляторними актами (eIDAS, eIDAS 2.0), детальними стандартами і технічними специфікаціями (ETSI EN 319 102/421/422, TS 119 511/512). Впровадження eIDAS 2.0 і відповідних імплементаційних регламентів сформувало цілісну правову архітектуру довгострокової цифрової довіри в ЄС.

Україна має сформоване законодавство, що гармонізоване з eIDAS, та функціонуючу інфраструктуру КНЕДП. Проте основний напрям КНЕДП це надання виключно послуг кваліфікованого електронного підпису і електронної ідентифікації, проте реальне застосування механізмів LTV у державному секторі обмежене, відсутні процедури та сертифікація архівних послуг. Прикладом є

Параметр	Міжнародний рівень	Європейський рівень	Національний рівень
Концептуальна модель архіву	OAIS (ISO 14721:2024) орієнтир для всіх архівів	OAIS + E-ARK	OAIS не імплементовано
Правова база довірчих послуг	Галузеві регуляції (FDA 21 CFR Part 11, ESIGN Act у США) в окремих країнах	Регламент eIDAS (910/2014) + eIDAS 2.0 (2024/1183); єдині правила для всіх 27 держав-членів	Закон «Про електронну ідентифікацію та електронні довірчі послуги» та «Про електронні документи та електронний документообіг»
Послуга довгострокового збереження підписів	Різноманітні підходи: нотаріальне засвідчення, галузеві архіви, приватні хмарні послуги без єдиного стандарту	Кваліфікована послуга збереження визначена в eIDAS 2.0	Послуга збереження підписів законодавчо передбачена, але реальна інфраструктура відсутня
Стандарти технічних форматів підписів	IETF RFC 3161 (TSP), IETF RFC 4998/6283 (ERS)	ETSI EN 319 102 (AdES), PAdES, XAdES, CAdES	CAdES, XAdES, PAdES підтримується
Механізм ланцюга доказів (Evidence Records)	IETF RFC 4998/6283 та реалізовані в окремих системах	TR-ESOR (Німеччина), NF Z42-013 (Франція)	Окремі комерційні рішення (Сайфер Шифр-Arch) реалізують зчеплені геш-ланцюги, але без нормативного підкріплення
Аудит/сертифікація архівів	ISO 16363 (TRAC/RAC), сертифікація CoreTrustSeal, NDSA Levels, DPC RAM	ISO 16363 та національні варіанти (NF 461 у Франції), ETSI TS 119 511	Відсутня система сертифікації архівів, аудит КНЕДП здійснюється Держспецзв'язком
Постквантова криптографія (PQC)	NIST SP 800-208 та FIPS 203–205 стандартизують алгоритми CRYSTALS-Dilithium, FALCON; міграційні рекомендації NIST і ENISA [33]	ENISA Guidelines for Post-Quantum Cryptography Transition, стек стандартів ETSI (базується на стеці NIST), ETSI розробляє PQC-профілі для AdES	Наявність набору квантово-стійких криптографічних алгоритмів на додачу до міжнародних, проте їх використання переважно не регламентоване
Блокчейн/DLT для підтвердження часу	OpenTimestamps, галузеві рішення (EY, Deloitte)	eIDAS 2.0 вводить Electronic Ledgers, Estonian KSI кваліфікований сервіс TSA на базі приватного блокчейну, включений до Trusted List ЄС [34]	Окремі комерційні рішення з елементами блокчейну, без нормативної підтримки

веденні різних національних електронних реєстрів, де використовуються електронні підписи, проте не використовуються механізми притаманні довготривалого збереження підписів і їх перевірки. Для покращення ситуації в цій сфері потрібні скоординовані зусилля Мінцифри, як національного регулятора у сфері електронної ідентифікації і електронних довірчих послуг (у частині технічних вимог до КНЕДП та визначення правового статусу послуги збереження підписів), Мін'юсту, Держархівслужби (у частині архівних вимог та OAIS-відповідності) та Держспецзв'язку (у частині криптографічних стандартів та форматів).

Довгострокова цифрова довіра є безперервним організаційно-технічним процесом, успіх якого забезпечується не лише наявністю стандартів, але й їх послідовним впровадженням у державних і комерційних системах. Саме шлях від наявної законодавчої бази до реального впровадження практик LTV є основним завданням для України на найближчі роки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]. ISO 14721:2025 (CCSDS 650.0-M-3). Space data and information transfer systems – Open archival information system (OAIS) – Reference model. 3rd ed. ISO / CCSDS, 2024.

[2]. ISO 16363:2012. Audit and certification of trustworthy digital repositories. ISO, 2012.

[3]. ISO 14641:2018. Electronic archiving – Design and operation of an information system for the purpose of electronic information preservation. ISO, 2018.

[4]. ISO 15489-1:2016. Information and documentation – Records management. Part 1: Concepts and principles. ISO, 2016.

[5]. IETF RFC 3161 (2001). Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF, 2001.

[6]. 6. IETF RFC 5816 (2010). ESSCertIDv2 Update for RFC 3161. IETF, 2010.

[7]. 7. IETF RFC 4998 (2007). Evidence Record Syntax (ERS). IETF, 2007.

[8]. 8. IETF RFC 6283 (2011). Extensible Markup Language Evidence Record Syntax (XMLERS). IETF, 2011.

[9]. 9. LOC/PREMIS Editorial Committee. PREMIS Data Dictionary for Preservation Metadata. Version 3.0. Library of Congress, 2015.
[10]. Digital Preservation Coalition. Digital Preservation Handbook. 2nd ed. DPC, 2015.
[11]. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. [Електронний ресурс] / NIST. – Режим доступу: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[12]. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). OJ L 257, 28.8.2014.
[13]. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0). OJ L, 30.4.2024.
[14]. ETSI TS 119 511 V1.1.1 (2019-07). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques. ETSI, 2019.
[15]. ETSI TS 119 512 V1.2.1 (2023-05). Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. ETSI, 2023.
[16]. ETSI EN 319 421 V1.3.1 (2025-07). Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. ETSI, 2025.
[17]. ETSI EN 319 422 V1.2.1 (2023-09). Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. ETSI, 2023
[18]. CEN/TS 18170:2025. Functional requirements for the electronic archiving services
[19]. ETSI SR 019 510 V1.1.1 (2017-05) Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures
[20]. BSI TR-03125 (TR-ESOR). Preservation of Evidence of Cryptographically Signed Documents. Version 1.3.1. BSI (Germany), 2022.
[21]. AFNOR NF Z42-013. Archivage électronique – Spécifications fonctionnelles et techniques d'un système informatique à vocation d'archivage électronique. AFNOR, 2020.
[22]. Proctor, N. et al. E-ARK: European Archival Records and Knowledge Preservation – Common Specification for Information Packages. DLM Forum Foundation, 2017.
[23]. ENISA. Security guidelines on the appropriate use of qualified electronic signatures. Ver. 2.0. ENISA, 2016.
[24]. ETSI TS 119 132-3 V1.1.1 (2021-01) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES
[25]. ETSI TS 119 122-3 V1.1.1 (2017-01) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES
[26]. ETSI EN 319 102-1 V1.4.1 (2024-06). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. ETSI, 2024.
[27]. Digital Signature Service. [Електронний ресурс] / European Commission. – Режим доступу: https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html
[28]. Archivable file formats [Електронний ресурс] / Swiss Federal Archives. – Режим доступу: https://www.bar.admin.ch/dam/bar/en/dokumente/konzepte_und_weisungen/archivtaugliche_dateiformate.pdf.download.pdf/archivable_file_formats.pdf
[29]. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017 (зі змінами). URL: https://zakon.rada.gov.ua/go/2155-19
[30]. Наказ Міністерства юстиції України № 1886/5 від 11.11.2014 «Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання». URL: https://zakon.rada.gov.ua/go/z1421-14
[31]. Кваліфіковані надавачі електронних довірчих послуг, а також відомості про самопідписані сертифікати електронної печатки ЦЗО [Електронний ресурс] / Центральний засвідчувальний орган. – Режим доступу: https://czo.gov.ua/ca-registry
[32]. Право-Justice / EU Project. Презентація пілотного проекту електронного архівування, реалізованого за сприяння проекту ЄС «Право-Justice». Kyiv, 2023. URL: https://www.pravojustice.eu/ua/post/vidbula

sya-prezentaciya-pilotnogo-proyektu-elektronnogo-arhivuvannya
[33]. ENISA. Post-Quantum Cryptography: Migration Considerations for Electronic Signatures. ENISA, 2023.
[34]. Guardtime. KSI Blockchain Timestamping Technical Overview. Guardtime, 2023. URL: https://guardtime.com/timestamping

COMPARATIVE ANALYSIS OF STANDARDS AND REGULATORY DOCUMENTS FOR LONG-TERM PRESERVATION AND VALIDATION OF ELECTRONIC DOCUMENTS AND SIGNATURES

The article provides a comparative analysis of international, European and Ukrainian standards and regulatory documents governing long-term preservation of electronic documents and long-term validation of electronic signatures. The regulatory landscape is systematized at three levels: global (OAIS/ISO 14721, ISO 16363, IETF RFC 4998/6283, AdES formats), European (eIDAS 1.0/2.0, ETSI EN 319 series, TR-ESOR, NF Z42-013, E-ARK), and national (Ukrainian Law on Electronic Trust Services, Ministry of Justice Order No. 1886/5 as amended in 2025, e-Archive pilot). Key differences in the depth of legal regulation, maturity of trust service infrastructure, and practical application of LTV mechanisms are identified.

Keywords: long-term digital preservation, long-term validation, electronic signature, OAIS, eIDAS, LTV, PAdES, XAdES, CAdES, ETSI, Evidence Record, electronic trust services.

Охріменко Андрій Олександрович, кандидат технічних наук, старший викладач кафедри системного аналізу та інформаційних технологій Маріупольського державного університету.
E-mail: a.okhrimenko@mu.edu.ua
Orcid ID: 0000-0001-8270-2863.
Okhrimenko Andrew, PhD in Eng., Senior Lecture of Academic Department of Systems Analysis & IT, Mariupol State University.

Стокіпний Олександр Леонідович, кандидат технічних наук, доцент кафедри інтелектуальних кібернетичних систем, Державний університет «Київський авіаційний інститут»
E-mail: oleksandr.stokipnyi@kai.edu.ua
ORCID: 0009-0007-4346-9684
Stokipnnyi Oleksandr, PhD in Eng., Associate Professor of Academic Department of intelligent cybernetic systems, State University «Kyiv aviation institute»

Ковтун Владислав Юрійович, кандидат технічних наук, доцент кафедри програмної інженерії та інтелектуальних технологій управління, Національний технічний університет «Харківський політехнічний інститут»
E-mail: vladislav.kovtun@gmail.com
ORCID: 0000-0002-4303-3510

Kovtun Vladislav, PhD in Eng., Associate Professor of Academic Department, Associate Professor, Department of Software Engineering and Intelligent Management Technologies, National Technical University «Kharkiv Polytechnic Institute»