

ЗАХИСТ ЕЛЕКТРОННИХ ДОКУМЕНТІВ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Марина Цілина

м. Київ

У сучасних умовах цифрової трансформації суспільства питання захисту електронних документів набуває особливої актуальності. Масове впровадження інформаційно-комунікаційних технологій у діяльність державних органів, наукових установ, бібліотек, архівів і музеїв зумовило появу нових форм зберігання, передавання та використання документів. Проте водночас це спричинило виникнення нових ризиків і загроз інформаційній безпеці, пов'язаних із несанкціонованим доступом, втратою даних, кібератаками та порушенням цілісності цифрового контенту.

Особливо гостро ці питання постали в Україні після початку повномасштабної війни з Російською Федерацією, коли електронні ресурси державних і культурних інституцій стали об'єктами постійних кіберзагроз. Відтак, захист цифрових документів став не тільки технічним завданням, а й складовою національної безпеки, що вимагає правового, організаційного та технологічного забезпечення.

Важливу роль у цьому процесі відіграють установи культури – бібліотеки, архіви, музеї, які акумулюють та оцифровують великі масиви історичних, наукових і мистецьких матеріалів. Саме вони стають центрами формування цифрової культурної спадщини України. Проте ефективне функціонування таких електронних ресурсів можливе лише за умови надійного захисту електронних документів на всіх етапах їхнього життєвого циклу – від створення до довгострокового зберігання. Разом із розвитком цифрових сервісів і активним впровадженням систем електронного документообігу в державному та культурному секторах зростає потреба у створенні комплексної системи інформаційної безпеки, здатної гарантувати цілісність, конфіденційність і доступність даних навіть у кризових умовах.

Однак цей процес супроводжується появою нових викликів у сфері збереження документної інформації, що вимагають своєчасної, скоординованої та ефективної протидії. Саме тому питання захисту електронних документів набуває стратегічного значення для забезпечення безперервності функціонування інформаційних ресурсів держави та установ культури. Показовим прикладом стала масована кібератака 19 грудня 2024 року, під час якої тимчасово припинено роботу ключових державних реєстрів, що підпорядковуються Міністерству юстиції України: Єдиного державного реєстру юридичних осіб, фізичних осіб-

підприємців і громадських організацій, реєстрів спадщини, актів цивільного стану та інших [5]. Роботу електронних адміністративних послуг і реєстраційних процедур було фактично паралізовано. Завдяки наявності резервних копій та заходів захисту даних, відновлення систем тривало понад три тижні. Цей інцидент наочно продемонстрував вразливість цифрової інфраструктури держави та необхідність посилення системного захисту електронних документів як у державному секторі, так і в установах культури, де зберігаються значні обсяги цифрової спадщини.

Для мінімізації шкоди від кібератак застосовуються різноманітні технічні рішення. Зберігання резервних копій у хмарних та фізично віддалених системах дає змогу уникнути втрати даних навіть у разі знищення частини інфраструктури. Під час відновлення нотаріальних реєстрів використовували ізольовані режими роботи, що обмежують поширення шкідливого коду.

Деякі провайдери, зокрема GigaCloud та ADAMANT G-Cloud, забезпечують локальне зберігання даних, резервне копіювання та контроль доступу, підтримуючи безпеку державних і приватних документів [1; 2].

В умовах воєнного стану цифрові архіви, музеї, бібліотеки та інші культурні установи активно впроваджують технології резервного копіювання, хмарного зберігання та шифрування для збереження культурної спадщини. Оцифрування фондів і створення електронних баз даних дають змогу захистити унікальні артефакти від фізичного знищення й забезпечити сталий доступ до них для науковців, здобувачів вищої освіти та міжнародної спільноти.

Масштабне оцифрування архівних фондів відбувається по всій країні. За даними Державної архівної служби, лише у 2023 році створено понад 21 млн цифрових копій документів, що свідчить про зростання темпів цифрової фіксації національної пам'яті та зниження ризиків її фізичної втрати [7].

Важливим напрямом в аспекті порушених проблем є міжнародне партнерство у сфері цифрової безпеки. Так, Державна архівна служба України спільно з Міжнародним альянсом із захисту спадщини в зонах конфліктів (ALIPH) та Державним департаментом США реалізує проєкт із захисту та оцифрування державних архівів, спрямований на створення цифрових копій документів, які перебувають під загрозою знищення внаслідок воєнних дій. У межах цього проєкту, бюджет якого становить близько 645 000 доларів, архівісти проходять навчання із цифрової обробки та захисту даних, а також впроваджують сучасні методи кібербезпеки [6].

У процесі масштабного оцифрування визначається черговість обробки документів із урахуванням їхньої культурної цінності, фізичного стану та формату. Визначення пріоритетів

залишається частково суб'єктивним і залежить від досвіду експертів, залучених до процесу оцінки.

Для підвищення об'єктивності оцінювання цінності та пріоритетності документів для оцифрування, наприклад у Національній бібліотеці України імені Вернадського (далі – НБУВ), діє група експертів, що співпрацює з Міністерством культури та стратегічних комунікацій. Перед оцифруванням здійснюється перевірка фізичного стану унікальних і рідкісних видань. Доцільно не обмежуватися лише особливо цінними документами – оцифровуються також матеріали в задовільному стані, зручні за форматом і розміром, що дає змогу створювати цифрові копії вже на початкових етапах.

Під час війни пріоритетом є створення головних копій – цифрових аналогів, які зберігаються окремо від оригіналів.

Значну роль у забезпеченні якості оцифрування відіграє допомога європейських партнерів. Благодійні організації надали українським бібліотекам професійне обладнання та сховища великої ємності.

Зокрема, НБУВ використовує сканери Zeutschel OS C2 формату A2+, які дозволяють створювати головні копії з роздільною здатністю 600 dpi та автоматизують більшість механічних і програмних процесів.

Із середини 2024 року обсяг цифрових копій зріс до понад 160 000 одиниць, що у понад 13 разів більше, ніж показник попередніх років (12 000 одиниць). Хоча обробка та каталогізація ще тривають, значна частина документів уже доступна користувачам у тестовому режимі [3].

Традиційна модель зберігання передбачала дублювання даних у віддалених сховищах і створення «ізолюваних копій» на локальних носіях. Нова стратегія охоплює три рівні захисту:

1. Використання малогабаритних мережевих сховищ, які не потребують серверних кімнат і можуть бути швидко переміщені.
2. Ізолювані сховища на стійких носіях, розташовані у спеціально укріплених приміщеннях, здатних витримувати вибухи та високі температури.
3. Хмарні сервіси за межами України, які забезпечують резервне копіювання у стабільному середовищі.

У березні 2022 року до нормативно-правових актів щодо технічного захисту інформації було внесено зміни, що дозволили бібліотекам, архівам і музеям зберігати цифрові копії у закордонних хмарних сховищах.

Це відкрило можливість безкоштовного та безпечного зберігання даних у європейських дата-центрах, зокрема в Amazon Web Services (далі – AWS).

Нині в хмарі AWS зберігаються сотні терабайтів українських культурних даних. Безкоштовний період триватиме до шести місяців після завершення воєнного стану.

Важливим кроком стало створення електронного реєстру Музейного фонду України – інтегрованої системи, яка об'єднує всі дані про культурні цінності державної власності. Реєстр розробила українська GovTech-компанія Strimco за замовленням Міжнародного фонду солідарності, що фінансується урядом Польщі, для Міністерства культури та стратегічних комунікацій [8].

Головною метою Реєстру є створення єдиного та повного переліку з 12 млн музейних предметів державної власності із зазначенням їхнього стану та місця зберігання [4]. До цього часу єдина база відсутня, і інформація збиралася лише з різних джерел та статистичних звітів. Консолідований перелік дає можливість систематизувати дані про об'єкти, визначити, які з них були втрачені під час війни, та відстежувати їхнє розташування.

Другим важливим завданням системи є встановлення жорсткішого контролю за переміщенням музейних предметів, особливо під час тимчасових виставок за кордоном. Це має запобігти незаконним спробам привласнення. За допомогою Реєстру можна відслідковувати рух культурних цінностей, а будь-яке переміщення об'єктів обов'язково проходить через систему погодження.

Окремим завданням Реєстру є надання музеям уніфікованого інструменту електронного обліку. До цього часу українські установи користувалися різними підходами – від Excel-таблиць і паперових журналів до російської системи КАМІС. Новий Реєстр забезпечує стандартизований, безпечний та безкоштовний інструмент цифрової інвентаризації, а також можливість інтеграції з наявними базами через API та перенесення даних з різних форматів. Міністерство культури і стратегічних комунікацій проводить навчальні програми для музейних працівників із різним рівнем цифрових навичок, що спрощує перехід на нову систему.

Станом на лютий 2025 року до Реєстру підключено 432 з 652 музеїв, що зберігають предмети державного Музейного фонду, що становить близько 66% від усіх установ [4]. Ці музеї вже тестують функціонал системи, а офіційне підключення всіх установ стане обов'язковим після ухвалення відповідної постанови Кабінету Міністрів. Хоча Реєстр поки що охоплює лише державний фонд, він закладає основу для майбутньої інтеграції приватних колекцій та музейних підрозділів при університетах і наукових інститутах.

Реєстр має важливе міжнародне значення: він дає змогу швидко передавати інформацію про викрадені об'єкти до Інтерполу та наочно підтверджувати право власності України на музейні колекції на міжнародному рівні. Таким чином, система не лише забезпечує повний

облік культурних цінностей країни, а й підвищує здатність держави захищати свої культурні надбання під час війни та на міжнародній арені.

Отже, захист електронних документів у сучасних умовах воєнного стану та глобальної цифровізації набуває стратегічного значення для збереження інформаційних ресурсів України. Кібератаки на державні реєстри, загрози фізичному знищенню архівів і музейних колекцій, а також потреба у швидкому переході до хмарних технологій засвідчили важливість створення цілісної системи кібербезпеки в документній та культурній сферах.

Сьогодні в Україні активно формується інфраструктура цифрового збереження – від впровадження хмарних рішень і систем резервного копіювання до створення електронного реєстру Музейного фонду України. Застосування криптографічних методів, електронного підпису та сучасних протоколів шифрування забезпечує автентичність і цілісність електронних документів, а співпраця з міжнародними партнерами підвищує стійкість українських систем до зовнішніх загроз.

Водночас залишаються актуальними проблеми стандартизації процесів цифрового архівування, правового закріплення статусу електронної копії як офіційного документа, а також необхідність підготовки фахівців з інформаційної безпеки у сфері культури.

Отже, ефективний захист електронних документів має базуватися на поєднанні технічних, правових та організаційних заходів, які включають:

- розвиток державних і відомчих центрів резервного зберігання даних;
- гармонізацію українського законодавства з міжнародними стандартами збереження цифрової спадщини;
- підвищення цифрової грамотності працівників бібліотек, архівів і музеїв;
- розширення партнерства з європейськими та світовими інституціями у сфері кіберзахисту.

У перспективі системний підхід до захисту електронних документів забезпечить неперервність історичної пам'яті, збереження культурної ідентичності та зміцнення інформаційного суверенітету України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ADAMANT G-Cloud. Розміщення ресурсів у G-Cloud ADAMANT – надійний захист інформації, що охороняється державою, 2025. URL: <https://adamant.ua/data-center/g-cloud> (дата звернення: 14.10.2025).

2. GigaCloud. Ваша приватна хмара. URL: <https://gigacloud.ua> (дата звернення: 14.10.2025).

3. Дубровіна Л., Ковтанюк Ю., Лобузін К., Дем'янюк Л. Національна бібліотека України імені Вернадського в часи незалежності та воєнного стану: стратегія розвитку, збереження та міжнародна співпраця. URL: https://www.degruyterbrill.com/document/doi/10.1515/bfp-2024-0062/html?lang=en&srsId=AfmBOorphsNY5qV0vB8X8nL5dxJBxIV4fQkj9aNyF5yxbVmnAxCNnMj_&utm_source (дата звернення: 15.10.2025).

4. Захист культурної спадщини: як працює новий реєстр Музейного фонду. URL: https://digitalstate.gov.ua/uk/news/govtech/zakhyst-kulturnoyi-spadshchyny-iak-pratsiuye-novyy-reyestr-muzeynoho-fondu?utm_source (дата звернення: 14.10.2025).

5. Серов І. Кібератака на державні реєстри України: які дані постраждали і що загрожує мільйонам громадян. URL: <https://tsn.ua/exclusive/kiberataka-na-derzhavni-reyestri-ukrayini-yaki-dani-postrazhdali-i-scho-zagrozhuye-milyonam-gromadyan-2728092.html> (дата звернення: 14.10.2025).

6. США запускають проєкт із захисту українських державних архівів. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-culture/3831195-ssa-zapuskaut-proekt-iz-zahistu-ukrainskih-derzavnih-arhiviv.html?utm_source (дата звернення: 14.10.2025).

7. Україна посіла друге місце в світі за оцифруванням документів. *Укрінформ*. URL: <https://www.ukrinform.ua/rubric-society/3909595-ukraina-posila-druge-misce-v-sviti-za-ocifruvannam-dokumentiv.html> (дата звернення: 14.10.2025).

8. Цифровий захист культурної спадщини у воєнний час. На прикладі музейних та бібліотечних практик. URL: https://nlu.org.ua/storage/files/Infocentr/Tematch_ogliadi/2025/05.06.25.pdf?utm_source (дата звернення: 14.10.2025).