

УДК: 930.25+004

*Ковальський Г. Є., канд. філософ. наук, доцент,  
Державна архівна служба України, м. Київ,  
Вазьянов І. І., магістр, ст. викладач,  
Державний університет інформаційно-комунікаційних технологій, м. Київ*

## **КІБЕРАРХІВІСТИКА: ГОЛОВНІ НАПРЯМИ РЕАЛІЗАЦІЇ**

*Анотація. Цифрове збереження архівних документів НАФ України є важливим завданням, яке вимагає комплексного підходу, включно з технічними, організаційними та фінансовими аспектами. Управління цифровими даними архівного фонду є складним завданням, що вимагає системного підходу та використання сучасних технологій. Метадані відіграють критично важливу роль у забезпеченні ефективного зберігання, пошуку та доступу до цифрових архівів. Використання стандартизованих метаданих, інтеграція з пошуковими системами, контекстуалізація та управління життєвим циклом документів дають змогу створювати інтуїтивно зрозумілі та доступні цифрові архіви, які відповідають потребам різних категорій користувачів. Використання релевантного програмного забезпечення для автоматизації процесів архівування й управління даними є кроком до підвищення ефективності та надійності національних архівних систем. Забезпечення користувачів зручним доступом до цифрових архівів вимагає комплексного підходу, який включає технічні рішення, дизайн інтерфейсу, ефективні системи пошуку та навігації, а також забезпечення доступності для всіх категорій користувачів. Використання передових технологій забезпечить довготривале збереження і допоможе створити зручний та ефективний доступ до архівних ресурсів.*

*Ключові слова: архів, кіберзахист, цифровий архів, цифровізація.*

Прискорення технологічного розвитку у сфері інформаційних технологій зумовило низку світових трендів, з-поміж яких – цифрові реформи архівістики та появи нового явища – кіберархівістики. Цифрова архівістика спрямована у своїй діяльності на зберігання, управління та доступ до цифрових документів і даних. Вона об'єднує традиційні та технологічні методи забезпечення довготривалого збереження цифрової інформації архівних документів. Цифровізація архівних документів Національного архівного фонду є надзвичайно важливим напрямом для забезпечення збереження, доступності і цілісності історичної та культурної спадщини країни. В умовах швидкого розвитку цифрових технологій та збільшення обсягів цифрових даних архіви стикаються з новими викликами та можливостями. Проекти національних цифрових архівів передбачають забезпечення довготривалого збереження цифрової інформації.

Прикладами цифрового доступу до величезного обсягу культурних та історичних документів є National Digital Information Infrastructure and Preservation Program [7] та Digital Public Library of America [3] у США, National Archives of Australia Digital Preservation в Австралії [6], Israel Digital Archives в Ізраїлі [5], Europeana у Євросоюзі [4]. Реалізація основ кіберархівістики є сучасним викликом для національної та світової архівної сфери. Забезпечення реалізації реформ

зберігання архівних документів Національного архівного фонду передбачає послідовне вирішення низки завдань.

Зокрема, проблема *цифрового збереження документів* із забезпеченням постійного і широкого доступу зі збереженням відповідних їм властивостей у часі та просторі. Розглянемо основні аспекти цифрового збереження архівних документів НАФ. Цифровізація НАФ відбувається у двох напрямках: оцифрування архівних документів та утворення цифрового формату документообігу визначеними законодавством фондоутворювачами. Процес оцифрування включає професійне сканування усіх видів паперових архівних документів задля створення цифрових копій, які відправляються на архівне зберігання відповідно до встановлених термінів. Це передбачає використання високоякісної техніки, щоб забезпечити максимальну чіткість та деталізацію документа, а також уніфікацію форматування для забезпечення високої якості зображення, зокрема найпоширеніші формати TIFF та PDF. Функціонування електронних архівів із сучасною документною інформацією передбачає дотримання технологічних умов відповідних офісних програм документообігу за прикладом АСКОД. Утворений масив цифрових даних, створений цифровими методами, з набуттям статусу офіційного документа через накладання кваліфікованого електронного підпису проходить аналогічні етапи передачі на тривале збереження і набуття статусу документа Національного архівного фонду, що передбачено архівним законодавством.

*Зберігання цифрових даних* відбувається у централізованих сховищах із використанням серверів, або хмарних рішень, для накопичення цифрових копій архівних документів, що забезпечує надалі їх централізоване управління та легкий доступ до даних. Відповідним установам необхідно проводити регулярне страхове створення резервних копій для захисту від втрат у випадку збоїв або інших факторів / інцидентів зі зберіганням у географічно розділених локаціях.

Управління цифровими даними архівного фонду є складним та багатограним процесом, що включає в себе організацію, зберігання, захист і забезпечення доступності цифрових архівів. Це важливе завдання, яке дає змогу зберегти історичні, культурні та наукові документи у цифровому форматі для майбутніх поколінь. Утворений масив цифрових даних повинен отримати систему *каталогізації і метаданих*, що дасть змогу реалізувати ефективний пошуковий механізм. Описові, адміністративні та структурні метадані забезпечують контекстуалізацію та зручний пошук цифрових архівних документів. Метадані включають інформацію про авторство, дату, тему, умови доступу та інші важливі атрибути, а організація цифрових архівів у систематизовані каталоги полегшить пошук і доступ до архівних документів. Використання метаданих є ключовим елементом у забезпеченні ефективного зберігання, пошуку та доступу до архів-

них даних. Метадані надають структуровану інформацію про документи, що дає змогу краще розуміти їх зміст, походження та значення. Потрібно брати до уваги й основні аспекти використання метаданих у цифрових архівах.

Варто звернути увагу на використання міжнародних стандартів Dublin Core (містить 15 основних елементів, як-от назва, автор, видавець, дата тощо), Encoded Archival Description (детальні описи архівних документів зі збереженням їх ієрархічної структури) та Metadata Encoding and Transmission Standard (дає змогу зберігати структурні й адміністративні метадані) для забезпечення сумісності та інтеграції з іншими архівами. Europeana використовує Dublin Core для опису мільйонів цифрових об'єктів з архівів, бібліотек і музеїв у всій Європі. Це дає змогу створювати єдину базу даних, доступну для користувачів з усього світу. National Archives and Records Administration використовує EAD для детального опису архівних колекцій, зберігаючи їх ієрархічну структуру та забезпечуючи доступність інформації для дослідників. Налагоджена тісна співпраця між архівами на національному та міжнародному рівнях задля впровадження інтероперабельності через впровадження єдиного стандарту Open Archival Information System [8], що забезпечить уніфікованість, сумісність та інтеграцію систем управління цифровими даними.

До основних компонентів управління цифровими даними відносимо управління життєвим циклом документів, який включає етапи створення, зберігання, використання, архівування та знищення архівних документів. Важливо забезпечити правильне управління на кожному етапі для збереження цілісності та доступності даних. Терміни зберігання різних типів архівних документів повинні спиратися на юридичні вимоги національного законодавства. Протягом «життя» архівний документ може переживати міграцію даних через оновлення форматів файлів та технологій зберігання для забезпечення довготривалої доступності даних. Це потребує постійного моніторингу стану даних для виявлення можливих пошкоджень, або деградації файлів. Це відбувається за підтримки спеціалізованими Програмами контролю стану збереження архівних документів за прикладом Програми здійснення контролю за наявністю, станом і рухом документів НАФ на 2009–2019 роки, яку проводила Державна архівна служба України [2].

Критично важливою є *безпека цифрових архівів* від несанкціонованого доступу, що робить цей аспект основою кіберархівістики. Оскільки цифрові архіви містять важливу інформацію, як-от історичні документи, особисті дані, конфіденційна інформація організацій, їх захист має бути пріоритетним, як того вимагає національне законодавство України [1]. Серед викликів безпеки – кіберзлочинці, інсайдерські загрози від власних працівників, технологічне оновлення стратегій захисту. Забезпечення захисту цифрових архівів від несанкціонованого

доступу є багатограним завданням, що вимагає комплексного підходу, зокрема технічних засобів, організаційних заходів та підвищення обізнаності користувачів. Важливим є інцидент-менеджмент із розробкою планів дій на випадок порушення безпеки.

До важливих методів захисту цифрових архівів відносимо автентифікацію й авторизацію – процес підтвердження особи користувача під час входу у власний акаунт на сайтів архіву використанням паролів тощо. Управління архівними масивами даних передбачає розмежування прав доступу користувачів, працівників та адміністраторів. Шифрування даних архівного фонду є важливим складником стратегії кібербезпеки, яка забезпечує захист конфіденційних та критичних даних від несанкціонованого доступу. Шифрування даних проводиться через перетворення даних у формат, який неможливо прочитати без спеціального ключа. Безпека має забезпечуватися відповідно до законодавчих вимог щодо захисту даних, як-от GDPR (General Data Protection Regulation) у Європі або HIPAA (Health Insurance Portability and Accountability Act) у США.

Шифрування даних архівного фонду є критично важливим для забезпечення конфіденційності, цілісності та доступності архівних документів. В умовах зростаючих кіберзагроз та необхідності захисту від несанкціонованого доступу шифрування стає вагомим елементом у стратегії безпеки цифрових архівів. Серед методів шифрування даних архівного фонду виділимо такі типи: *симетричне шифрування* з використанням одного ключа для шифрування та дешифрування даних за принципом алгоритму AES (Advanced Encryption Standard); *асиметричне шифрування*, за якого використовують пару ключів – публічний для шифрування і приватний для дешифрування – за принципом алгоритму RSA (Rivest-Shamir-Adleman).

Шифрування даних під час передачі на архівне зберігання відбувається через протоколи для захисту даних TLS/SSL, які передаються через інтернет. Вони забезпечують шифрування даних між клієнтом та сервером, запобігаючи їх перехопленню. Віртуальні приватні мережі VPN використовуються для захисту даних, що передаються через загальнодоступні мережі, забезпечуючи безпечний тунель для передачі інформації. Шифрування даних під час архівного зберігання передбачає шифрування всього диска або певних розділів алгоритмами BitLocker (для Windows) та FileVault (для macOS) та шифрування окремих файлів інструментами PGP (Pretty Good Privacy). Впровадження прогресивних методів шифрування, належне управління ключами та дотримання найкращих практик допоможуть забезпечити безпеку та цілісність архівних документів у цифровому форматі.

Використання програмного забезпечення для *автоматизації процесів архівування* та управління даними стає дедалі важливішим у сучасному цифровому середовищі. Це дає змогу значно підвищити ефективність, точність і безпеку архівних процесів. Варто брати до уваги чинники впровадження, переваги, виклики та приклади програмного забезпечення для автоматизації архівування й управління даними. Переваги використання програмного забезпечення полягають у: автоматичному збиранні даних з різних джерел, автоматичному генеруванні метаданих на основі вмісту документів, як-от дати, автори, ключові слова, що спрощує їх каталогізацію та пошук, інтеграцію зі стандартами метаданих для забезпечення сумісності та інтеграції з іншими архівними системами, інтелектуальний пошук методами штучного інтелекту, фільтрацію та сортування результатів пошуку за різними критеріями, збереження різних версій документів з можливістю відстеження змін та відновлення попередніх версій, автоматичне переміщення документів до архівних сховищ на основі їх віку, важливості або інших критеріїв, підвищення ефективності обробки та збереження даних, мінімізації людського фактора, формалізації і стандартизації процесів, шифрування та контролю доступу, моніторингу та аудиту архівних масивів даних.

Забезпечення користувачів зручним *доступом до цифрових архівів* є ключовим завданням для архівних установ. Це включає створення інтуїтивно зрозумілих інтерфейсів, ефективних систем пошуку, а також забезпечення доступності даних для різних категорій користувачів. До основних аспектів забезпечення доступу до цифрових архівів відносимо: інтуїтивно зрозумілий дизайн інтерфейсу, який має бути адаптивним, тобто забезпечувати зручний доступ з різних пристроїв, мати ефективні системи пошуку та навігації, фільтри та сортування, відповідність стандартам доступності WCAG (Web Content Accessibility Guidelines) та мультимовність, створення тематичних цифрових виставок, віртуальні тури, можливість залишати анотації й коментарі до документів, інтерактивні навчальні матеріали та посібники для користувачів.

**Висновки.** Підводячи підсумок, зазначимо, що кіберархівістика є важливою в сучасному світі, де велика кількість інформації зберігається у цифровій формі, і необхідно знайти ефективні способи її збереженості та управління. Кіберархіви є інтеграцією традиційного архівного сховища з сучасними інформаційними технологіями, що забезпечує зберігання, управління та доступ до великого обсягу даних у цифровому форматі. Вони є критично важливими для збереження культурної, історичної та наукової спадщини в умовах зростаючої цифровізації суспільства і викликів війни. Впровадження новітньої моделі кіберархіву є стратегічно важливим для збереження інформації та її доступності у майбутньому. Сучасні технології автоматизації та управління даними дають змогу архівним

установам ефективно виконувати свої завдання, забезпечуючи збереження та доступ до важливих цифрових ресурсів. Це сприятиме не лише збереженню спадщини, але й підтримці наукових досліджень, освіти та культурного розвитку.

### Список використаних джерел

1. Про захист персональних даних: Закон України № 2297-VI від 01.06.2010. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
2. Програми здійснення контролю за наявністю, станом і рухом документів НАФ на 2009–2019 роки. URL: <https://zakon.rada.gov.ua/rada/show/v0190560-09#Text>
3. Digital Public Library of America. URL: <https://dp.la>
4. Europeana. URL: <https://www.europeana.eu>
5. Israel Digital Archives. URL: <https://catalog.archives.gov.il/>
6. National Archives of Australia Digital Preservation. URL: <https://www.naa.gov.au>
7. National Digital Information Infrastructure and Preservation Program. URL: <https://www.digitalpreservation.gov>
8. Open Archival Information System. URL: <https://www.oais.info>

