

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ЦИФРОВОЇ ПАМ'ЯТІ ДЕРЖАВНИХ І РЕГІОНАЛЬНИХ ДОКУМЕНТАЛЬНИХ РЕСУРСІВ

Квач Альона

м. Київ

Цифрове суспільство актуалізує питання безпечного функціонування документно-інформаційних систем, що забезпечують збереження пам'яті держави, її інституцій і громад. Інформаційна безпека виступає не лише технічним, а й культурно-комунікаційним чинником, оскільки від рівня захисту цифрових ресурсів залежить цілісність національної інформаційної пам'яті, довіра до офіційних джерел і доступ громадян до достовірної інформації. У системі документаційного забезпечення діяльності органів державної влади інформаційна безпека передбачає створення комплексних механізмів захисту електронних документів, метаданих і комунікаційних каналів. Важливим є забезпечення автентичності, цілісності та довготривалого збереження цифрових даних, особливо тих, що мають правовий, управлінський або культурно-історичний характер.

Особливого значення у цьому контексті набуває краєзнавча діяльність бібліотек, які протягом багатьох років збирають, зберігають і систематизують локальні історичні джерела, документи та публікації. Цифровізація таких ресурсів дозволяє створювати електронні колекції, репозитарії та бази даних, що відтворюють локальну історію та культурну спадщину регіонів. Безпечне функціонування означених систем забезпечує доступ науковців, освітніх установ і громадськості до достовірної інформації, зберігаючи цілісність цифрової пам'яті краю. Разом із цим, взаємодія державних структур із бібліотеками сприяє інтеграції локальної інформації у національний і міжнародний інформаційний простір, підсилюючи роль бібліотек як важливих суб'єктів управління знаннями та культурною пам'яттю.

Ефективність таких процесів визначається не лише технологічними засобами захисту, а й організаційними стратегіями управління ризиками, нормативним регулюванням та формуванням культури інформаційної відповідальності серед фахівців, що працюють із цифровими документами. Цифрова етика, дотримання принципів прозорості, конфіденційності та автентичності стають базовими умовами сталого розвитку локальної та національної інформаційної пам'яті. Відтак інформаційна безпека стає ключовим елементом функціонування системи документаційного забезпечення діяльності органів державної влади, оскільки від її стану залежить стабільність управлінських процесів, довіра громадян до

державних інституцій та збереження національної інформаційної спадщини. Надійність електронних систем управління вимагає комплексного підходу, який включає технічні засоби захисту, організаційні механізми контролю доступу та постійний аудит інформаційних потоків. Критичною складовою є забезпечення цілісності та автентичності електронних документів, що дозволяє гарантувати достовірність прийнятих управлінських рішень. Важливим аспектом є інтеграція міжнародних стандартів управління інформаційною безпекою та документами, що забезпечує відповідність сучасним нормативним вимогам і кращим практикам. Окрім цього, розвиток цифрової інфраструктури органів влади потребує систематичного підвищення кваліфікації персоналу, відповідального за збереження та захист інформації, з урахуванням новітніх технологічних і правових викликів.

Зростання обсягів електронної документації, а також використання хмарних технологій, віддалених сервісів і систем електронного документообігу створюють нові ризики втрати, викривлення або несанкціонованого доступу до офіційної інформації. Тому питання кіберзахисту, автентифікації, резервного збереження й контролю доступу до документних ресурсів набувають особливої актуальності. А у контексті державного управління інформаційна безпека виконує подвійну функцію: з одного боку, гарантує безперервність управлінської діяльності, а з іншого – забезпечує збереження цифрової пам'яті суспільства як складової національної ідентичності.

Саме тому проблема захисту електронних документів і метаданих виходить за межі суто технічної площини, набуваючи гуманітарного виміру, пов'язаного з охороною історичної, правової та культурної інформації. Особливо важливою є роль бібліотек та архівів у створенні цифрових репозитаріїв локальної історії, які не лише фіксують культурну спадщину регіонів, а й забезпечують її безпечне зберігання та доступність для науковців, освітніх установ і громадськості. Тож, інтеграція державних стандартів інформаційної безпеки з краснзнавчими практиками сприяє формуванню цілісної цифрової пам'яті країни, зберігаючи зв'язок між національною і локальною історико-культурною спадщиною.

Актуальність дослідження також зумовлена необхідністю узгодження національної системи інформаційної безпеки з міжнародними стандартами управління електронними документами (ISO 15489, ISO/IEC 27001 тощо), що визначають вимоги до довготривалого збереження, цілісності та конфіденційності цифрових ресурсів. В умовах воєнних загроз і гібридних впливів питання інформаційної безпеки державних і регіональних документальних систем стає не лише адміністративним, а й стратегічним пріоритетом держави. Впровадження таких стандартів дозволяє забезпечити єдині підходи до управління електронними документами, підвищити рівень контролю за доступом та захистом інформації. Окрім того, системне дотримання міжнародних норм сприяє інтеграції української практики

управління документами у глобальний інформаційний простір, підвищуючи довіру до державних електронних сервісів на міжнародному рівні.

Мета наукової роботи – окреслити роль і значення інформаційної безпеки у забезпеченні надійного функціонування систем документаційного забезпечення органів державної влади та збереженні цифрової пам'яті державних і регіональних документальних ресурсів; показати важливість краєзнавчої діяльності бібліотек у формуванні електронних колекцій і цифрових репозитаріїв локальної історії; означити основні напрями підвищення рівня захищеності електронних документів, метаданих і комунікаційних каналів; а також продемонструвати взаємозв'язок між технологічними, організаційними й гуманітарними аспектами безпечного управління інформацією в умовах цифрової трансформації та інтеграції локальної та національної цифрової спадщини.

Проблематика інформаційної безпеки та управління цифровими документальними ресурсами є предметом численних наукових досліджень, що охоплюють як теоретичні, так і прикладні аспекти. Вивчення міжнародних стандартів, зокрема ISO/IEC 27001 та ISO 15489-1, дозволяє окреслити сучасні підходи до організації безпечного електронного документообігу та управління записами, а також визначити ключові принципи їх імплементації в державних і регіональних структурах. Так, сертифікація за стандартом ISO/IEC 27001 надає організаціям численні переваги, серед яких підвищення довіри клієнтів і партнерів, зниження ризиків витоку даних, оптимізація внутрішніх процесів управління інформаційною безпекою та формування конкурентних переваг на ринку [1]. Впровадження цього стандарту сприяє усвідомленню ризиків, створенню комплексних стратегій управління інформацією та підвищенню стійкості організацій до сучасних кіберзагроз [2]. Стандарт ISO 15489-1:2018 визначає поняття та принципи керування записами, включаючи організаційні політики, метадані, моніторинг і навчання персоналу, що забезпечує достовірність, цілісність та доступність документальних ресурсів [3]. У контексті державного управління це створює основу для ефективного електронного документообігу та довготривалого збереження цифрової пам'яті державних і регіональних структур.

Дослідження вітчизняних авторів, зокрема Тверитникової О.Є. та Салати Г.В., висвітлюють практичні аспекти впровадження міжнародних стандартів у сфері архівної та бібліотечної справи. Автори підкреслюють, що інтеграція системи менеджменту якості сприяє підвищенню ефективності управлінських процесів і забезпеченню надійності збереження документальної інформації [4]. Таким чином, сучасна історіографія підкреслює комплексність підходів до інформаційної безпеки та управління записами, поєднуючи технологічні, організаційні та нормативні аспекти для забезпечення надійного функціонування документально-інформаційних систем органів державної влади.

Інформаційна безпека у системі документаційного забезпечення діяльності органів державної влади є комплексною категорією, що поєднує технічні, правові, організаційні та комунікаційні аспекти управління інформацією та спрямована на захист документних ресурсів від несанкціонованого доступу, модифікації, знищення чи втрати, а також на забезпечення достовірності й цілісності даних, що циркулюють в управлінських процесах. У сучасних умовах цифрової трансформації державного сектору безпека інформаційних потоків набуває статусу стратегічного ресурсу, від якого залежить ефективність прийняття управлінських рішень та збереження історико-правової пам'яті інституцій. Вагомим компонентом такої безпеки є інтеграція державних електронних систем із цифровими колекціями бібліотек та архівів, що фіксують локальні історико-культурні джерела, що дозволяє формувати надійні електронні репозитарії регіональної інформації, зберігати її цілісність і забезпечувати доступність для наукових досліджень та освітніх програм. Таким чином, взаємодія органів влади з бібліотеками і архівами не лише підвищує якість управлінських рішень, а й сприяє збереженню та популяризації цифрової пам'яті регіонів, що є важливою складовою національної інформаційної спадщини.

З огляду на зростання ролі електронного документообігу, ключовими складовими інформаційної безпеки виступають системи аутентифікації користувачів, криптографічний захист даних, багаторівневий контроль доступу, резервне копіювання інформації та аудит подій. Представлені інструменти забезпечують надійність цифрової інфраструктури, сприяють запобіганню інформаційним витокам і формують довіру до електронних адміністративних сервісів. Особливу увагу варто приділяти розробці політик доступу, які визначають рівні відповідальності та обов'язки користувачів при роботі з електронними документами. Важливим є впровадження систем моніторингу та раннього виявлення інцидентів, що дозволяє своєчасно реагувати на спроби несанкціонованого доступу. Використання сучасних криптографічних алгоритмів забезпечує захист конфіденційної інформації навіть у разі втрати фізичних носіїв даних. Резервне копіювання та дублювання інформаційних масивів гарантують безперервність доступу до критично важливих ресурсів у разі технічних збоїв. Регулярний аудит подій і перевірка журналів активності дозволяють оцінювати ефективність заходів безпеки та виявляти потенційні ризики. Окрім того, інтеграція цих інструментів у єдину систему управління інформаційною безпекою створює комплексний захист, що охоплює технологічні, організаційні та нормативні аспекти функціонування державних електронних сервісів.

Особливого значення набуває формування політики безпеки документних ресурсів, яка повинна ґрунтуватися на поєднанні національних нормативно-правових актів (зокрема Закону України «Про інформацію», «Про захист інформації в інформаційно-

телекомунікаційних системах», «Про електронні документи та електронний документообіг») із міжнародними стандартами (ISO/IEC 27001, ISO 15489, ISO 30300 тощо), що у свою чергу забезпечує інтеграцію українських практик у світовий контекст управління інформаційною безпекою. У цьому процесі особливу роль відіграють бібліотеки, які не лише накопичують і систематизують локальні історичні та культурні документи, а й сприяють формуванню електронних репозитаріїв, що зберігають цифрову пам'ять регіонів. Забезпечення безпеки таких електронних ресурсів дозволяє гарантувати достовірність, цілісність і довготривале збереження інформації, що має історичну, культурну чи управлінську цінність. Інтеграція державних стандартів і бібліотечних практик створює основу для надійного управління локальною та національною інформаційною спадщиною, водночас забезпечуючи її доступність для науковців, освітніх установ і громадськості, що підсилює роль бібліотек як стратегічних суб'єктів у формуванні цифрового інформаційного простору та підтримці краєзнавчої пам'яті краю.

Важливо, що захист документних ресурсів розглядається не лише як технологічний процес, а як складова цифрової пам'яті держави. Адже кожен електронний документ, створений органами влади, має потенційну історичну, культурну чи суспільну цінність. Тому питання довготривалого збереження електронних архівів, метаданих, реєстрів і управлінської документації безпосередньо пов'язане із забезпеченням тяглості національної інформаційної спадщини. Сучасна ж концепція «цифрової пам'яті» розглядає державні та регіональні документальні ресурси як інтегральну частину інформаційно-культурного простору. Їх безпечне функціонування можливе лише за умови дотримання принципів кіберстійкості, використання національних стандартів захисту інформації, резервного копіювання, контролю доступу та етичного управління даними. Особливої уваги набуває взаємодія державних структур із бібліотеками, архівами, музеями у створенні спільних цифрових репозитаріїв і баз даних. Представлені ресурси формують не лише управлінську, а й краєзнавчу складову пам'яті регіонів, забезпечуючи сталий зв'язок між інформаційною інфраструктурою влади й локальними історико-культурними спільнотами.

Ефективна реалізація політики інформаційної безпеки у сфері документаційного забезпечення діяльності органів державної влади потребує чіткої координації між центральними та регіональними структурами, а також формування єдиної методології управління цифровими документами. Значну роль у цьому процесі відіграють фахівці інформаційно-бібліотечної та архівної справи, які забезпечують експертизу документних потоків, розробляють стандарти метаданих, контролюють автентичність джерел та здійснюють науково-методичний супровід цифрових колекцій. Вони беруть активну участь у створенні електронних архівів локальної історії та цифрових репозитаріїв краєзнавчих

матеріалів, що дозволяє зберігати культурно-історичну спадщину регіонів у доступній та захищеній формі. Їхня участь у формуванні безпечних електронних архівів сприяє підвищенню якості управлінських рішень і гарантує достовірність документальної інформації, що циркулює в системі державного управління, водночас зміцнюючи локальну та національну цифрову пам'ять.

Таким чином, інформаційна безпека у контексті цифрової пам'яті державних і регіональних документальних ресурсів постає як багаторівнева система, що інтегрує технологічні, правові, етичні та культурні виміри. Вона покликана не лише запобігати загрозам і забезпечувати захист інформації, а й підтримувати сталий розвиток суспільства через збереження історичної тяглості, відкритість знань і довіру до офіційних джерел. Особливого значення набуває взаємодія державних структур із бібліотеками, які формують електронні колекції та цифрові репозитарії локальної історії, забезпечуючи відтворення культурно-історичної спадщини регіонів. Формування безпечного інформаційного середовища, заснованого на принципах прозорості, відповідальності та професійної компетентності, є запорукою зміцнення державних інституцій і розвитку національної цифрової спадщини в умовах глобальних викликів. Отже, інформаційна безпека є системоутворювальним елементом цифрової пам'яті держави, що поєднує технологічні, правові та гуманітарні виміри. Її інтеграція у систему документаційного забезпечення органів державної влади та взаємодія з бібліотеками й архівами сприяє збереженню локальної та національної ідентичності, забезпеченню доступу до достовірної інформації та підтримці сталого розвитку цифрового культурного простору країни.

Література:

1. Основні переваги сертифікації ISO/IEC 27001. URL: <https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001> (дата звернення: 15.10.2025.)
2. Як стандарт ISO/IEC 27001 допомагає розвиватися сучасному бізнесу. URL: <https://my-itspecialist.com/standard-iso/iec-27001-for-business> (дата звернення: 15.10.2025.)
3. ДСТУ ISO 15489-1:2018 Інформація та документація. Керування записами. Частина 1. Поняття та принципи (ISO 15489-1:2016, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80384 (дата звернення: 15.10.2025.).
4. Тверитникова О.Є., Салата Г.В. Менеджмент якості архівної та бібліотечної справи: до проблеми імплементації міжнародних стандартів. *Бібліотекознавство. Документознавство. Інформологія*. 2023. № 2. С. 48 – 53. URI: <http://elib.nakkkim.edu.ua/handle/123456789/4944> (дата звернення: 15.10.2025.).