ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: **«СУЧАСНІ УКРАЇНСЬКІ ВИКЛИКИ БЕЗПЕКИ АРХІВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ»**

на здобуття освітнього ступеня магістра
зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
(код, найменування спеціальності)
освітньо-професійної програми Управління інформаційно-комунікаційною діяльністю *(назва)*

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Анна ДУДОВА

Виконала: здобувачка вищої освіти
гр. ДЗДМ-61
Анна ДУДОВА

Керівник: Леся КОВАЛЬСЬКА
д. і. н., професор

Рецензент: Ірина П’ЯТНИЦЬКОВА
к. і. н., доцент

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності
Ступінь вищої освіти Магістр
Спеціальність 029 Інформаційна, бібліотечна та архівна справа
Освітньо-професійна програма Управління інформаційно-комунікаційною діяльністю

ЗАТВЕРДЖУЮ
Завідувач кафедри документознавства та інформаційної діяльності
_____ Тетяна СИДОРЕНКО
«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дудової Анни Романівни

1. Тема кваліфікаційної роботи: Сучасні українські виклики безпеки архівних інформаційних ресурсів
керівник кваліфікаційної роботи Леся КОВАЛЬСЬКА доктор істор. наук, професор, професор кафедри документознавства та інформаційної діяльності,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 р. № 320
2. Строк подання кваліфікаційної роботи «16» грудня 2024 р.
3. Вихідні дані до кваліфікаційної роботи:
Мета роботи полягає у виявленні головних загроз ефективного функціонування архівних інформаційних ресурсів та формулюванні безпекових заходів в умовах сучасних українських викликів російської агресії.
Об’єктом роботи виступають архівні інформаційні ресурси, які функціонують в умовах інформаційної та військової агресії.
Предмет дослідження становлять заходи безпеки функціонування архівних інформаційних ресурсів, забезпечення цілісності та збереження інформації.
4. Перелік питань, які потрібно розробити:
   1. Теоретична основа вивчення безпеки архівних інформаційних ресурсів.
   2. Диджиталізація архівного інформаційного простору України та потреба його захисту в умовах війни.
   3. Вдосконалення захисту архівних інформаційних ресурсів в умовах військової агресії.
5. Перелік ілюстративного матеріалу: презентація, 23 рисунки, 1 таблиця.
6. Дата видачі завдання «09» вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної магістерської роботи	Строк виконання етапів роботи	Примітки
1	Визначення тематики, вибір наукового керівника, уточнення теми	09.09.2024	
2	Розробка та складання плану кваліфікаційної магістерської роботи	14.09.2024	
3	Підготовка 1 розділу	05.10.2024	
4	Підготовка 2 розділу	26.10.2024	
5	Підготовка 3 розділу	22.11.2024	
6	Висновки	30.11.2024	
7	Підготовка остаточного варіанту роботи	12.12.2024	
8	Написання відгуку науковим керівником	13.12.2024	
9	Оформлення та представлення роботи на кафедру та перевірка на плагіат	16.12.2024	
10	Підготовка доповіді, презентації та ілюстративного матеріалу, зовнішня рецензія	19.12.2024	
11	Попередній захист	20.12.2024	
12	Основний захист кваліфікаційної магістерської роботи	21.01.2025	

Здобувач вищої освіти Анна ДУДОВА

Керівник
кваліфікаційної роботи Леся КОВАЛЬСЬКА

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 88 стор., 23 рис., 1 табл., 81 джерело.

Мета роботи: виявлення головних загроз ефективного функціонування архівних інформаційних ресурсів та формулювання безпекових заходів в умовах сучасних українських викликів російської агресії.

Об'єктом роботи виступають архівні інформаційні ресурси, які функціонують в умовах інформаційної та військової агресії.

Предмет дослідження становлять заходи безпеки функціонування архівних інформаційних ресурсів, забезпечення цілісності та збереження інформації.

Короткий зміст роботи: розкрито теоретико-методологічні підходи вивчення безпеки інформаційних ресурсів; досліджено особливості диджиталізації архівного інформаційного простору України та потреба його захисту в умовах війни розглянуто систему захисту інформації та комунікації з врахуванням потреби захисту інформації та комунікації; проаналізовано автоматизовані систем захисту інформації та комунікації; встановлено необхідність впровадження і вдосконалення захисту архівних інформаційних ресурсів в умовах військової агресії.

Ключові слова: архів, архівний інформаційний ресурс, інформаційна безпека, суспільство, захист інформації, війна.

ABSTRACT

The textual part of the qualifying work for obtaining a master's degree: 88 pages, 23 figures, 1 tables, 81 sources.

The purpose of the work: to identify the main threats to the effective functioning of archival information resources and to formulate security measures in the conditions of modern Ukrainian challenges of Russian aggression.

The object of the work is archival information resources that function in the conditions of informational and military aggression.

The subject of the study is security measures for the functioning of archival information resources, ensuring the integrity and preservation of information.

Brief content of the work: theoretical and methodological approaches to the study of the security of information resources are disclosed; the peculiarities of digitization of the archival information space of Ukraine and the need for its protection in war conditions were investigated; the information and communication protection system was considered, taking into account the need for information and communication protection; automated information and communication protection systems were analyzed; the need to implement the improvement of protection of archival information resources in conditions of military aggression has been established.

Keywords: archive, archival information resource, information security, society, information protection, war.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувачка Дудова А.Р. до захисту кваліфікаційної роботи за спеціальністю 029 Інформаційна, бібліотечна та архівна справа
(код, найменування спеціальності)
освітньо-професійної програми Управління інформаційно-комунікаційною діяльністю *(назва)*
на тему: «Сучасні українські виклики безпеки архівних інформаційних ресурсів».

Кваліфікаційна робота і рецензія додаються.

Директор ННІМП _____ Світлана ПЕТРОВСЬКА

Висновок керівника кваліфікаційної роботи

Здобувачка Анна ДУДОВА самостійно та відповідально підійшла до виконання кваліфікаційної роботи. Тема роботи своєчасно сформульована та затверджена на засіданні кафедри. Проблема кваліфікаційної роботи «Сучасні українські виклики безпеки архівних інформаційних ресурсів» відображає стан архівної галузі сьогодні та актуалізує проблему убезпечення архівних ресурсів в умовах війни. Саме ці аспекти стали вагомими у розкритті проблеми, дозволили запропонувати заходи убезпечення інформаційної архівної діяльності та вдосконалення безпекових заходів. Календарний план підготовки кваліфікаційної роботи витримано, робота вчасно пройшла перевірку на плагіат. Магістерська робота відповідає вимогам, які висуваються до кваліфікаційних робіт та може бути рекомендована до захисту.

Керівник кваліфікаційної роботи _____ Леся КОВАЛЬСЬКА

«____» _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута на засідання кафедри документознавства та інформаційної діяльності. Здобувачка Дудова А.Р. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою документознавства
та інформаційної діяльності Тетяна СИДОРЕНКО

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Прогрес у сфері інформаційних технологій характеризується впровадженням інформаційно-комунікаційних технологій в усі сфери буття українського суспільства. Це спричиняє необхідність адаптації вітчизняного законодавства задля регулювання та формування нових вимог захисту інформації, зокрема архівних інформаційних ресурсів. Військова агресія рф поставила питання збереженості Національного архівного фонду України, як важливого документно-культурного надбання українського народу та людства загалом.

Питання збереження архівних фондів набуває актуальності й через технічний прогрес, що робить диджиталізацію безальтернативним варіантом у пролонгації життєвого циклу архівного документу. Широке використання персональних технічних засобів вимагає постійного доступу до інформації, що зміщує акценти роботи архівіста зі збереження інформації на сервісне обслуговування користувачів інформації архівних документів. Тому забезпечення доступу та реалізація механізмів захисту інформації є необхідними складовими, щоб діяльність організацій у сфері архівної інформаційної комунікації була ефективною.

Сучасні персональні гаджети виконують функції зв’язку, зберігання особистих даних, цифрового інструмента для роботи, навчання, проведення банківських операцій, медичного обслуговування, участі в громадському житті та ідентифікації особи. Масове використання персональних пристроїв та безупинний розвиток їх інформаційно-комунікаційних можливостей порушує питання трансформації архівних установ в сервісні організації з адміністрування безпечного доступу до даних архівних інформаційних ресурсів. Все це в свою чергу підвищує ризики несанкціонованого доступу, загрозу втрати / пошкодження даних та суттєво актуалізує питання захисту інформації.

Захист архівних інформаційних ресурсів є складною та тривалою у часі роботою. Він вимагає поєднання технічних заходів, створення нормативно-

правового підґрунтя, соціально-психологічного сприйняття суспільства, впливу на формування соціального запиту на інформацію про минуле. Правильно організована система безпеки Національного архівного фонду України не тільки допоможе зберегти соціально-історичну інформацію архівних документів, але й забезпечить їх доступність для майбутніх поколінь українців.

Сьогодні Україна перебуває в умовах значних ризиків стабільного функціонування архівної системи – архівні інформаційні ресурси Донецької і Луганської областей та Автономної республіки Крим фактично втрачено, державні архіви прифронтових областей знаходяться у зоні ризику через постійні обстріли та бомбардування ворога.

Проте, українське суспільство демонструє вагомий потенціал для переходу на наступний технічний рівень, за умови запровадження державного єдиного комплексного підходу диджиталізації соціального простору. Законодавство має відповідати запиту суспільства на цифрові трансформації, а технології повинні підтримувати демократичні принципи та формувати громадянську позицію.

Широкий доступ до інформаційних ресурсів держави засобами цифрових технологій створить умови переходу до нової форми демократії – е-демократія. Саме тому державні установи України покликані очолити процес диджиталізації, створення умов безпеки інформації, систем контролю віртуального простору. Забезпечення захисту інформаційно-комунікаційної діяльності потребує постійного вдосконалення та участі в становленні цифрового середовища.

Швидкий розвиток цифрових технологій та зростання ролі громадянського суспільства висувають на перший план необхідність ефективної взаємодії влади та населення. Однак, паралельно з цим зростає ризик витоку конфіденційних даних, які є власністю держави та / або захищені законом. Забезпечення безпеки інформації та створення надійного комунікаційного середовища є ключовим завданням для успішного управління країною та її сталого розвитку. Це стосується як конфіденційних, так і відкритих державних даних, які використовуються для прийняття управлінських рішень.

У сучасному інформаційному суспільстві ефективна комунікація між владою та громадянами є необхідною умовою сталого розвитку держави. Однак, для забезпечення відкритості та прозорості влади, важливо захищати конфіденційні дані та створювати безпечне середовище для обміну інформацією. Це дозволить підвищити довіру громадян до державних органів та сприяти активній участі населення в управлінні державними справами.

Згідно із Законом України «Про інформацію», захист інформації, що є державною власністю, є одним з пріоритетних завдань. Створення ефективної системи захисту даних та безпечного комунікаційного середовища є необхідною умовою для забезпечення національної безпеки та сталого розвитку країни. Сьогодні архівна справа активно інтегрується в загальну концепцію цифрової трансформації економіки України. Диджиталізація архівів має здійснюватися на основі єдиних галузевих стандартів і правил, які регулюють створення, зберігання, облік, опис та використання цифрових копій. Це необхідно для забезпечення узгодженого механізму взаємодії органів влади на всіх рівнях.

Застосування сучасних технологій захисту інформації та заходи кібербезпеки в архівній сфері є необхідним для захисту архівних інформаційних ресурсів та захисту прав громадян у цифровому середовищі. Україна, як і інші країни світу, стикається з викликами, пов’язаними із захистом інформації в умовах глобалізації. Вивчення міжнародного досвіду організації захисту архівних інформаційних ресурсів та впровадження сучасних стандартів кібербезпеки є важливим завданням національної інформаційної безпеки.

Мета дослідження полягає у виявленні головних загроз ефективного функціонування архівних інформаційних ресурсів та формулюванні безпекових заходів в умовах сучасних українських викликів російської агресії.

Реалізація мети передбачає послідовне вирішення **завдань:**

- розкрити особливості науково-методологічного обґрунтування інформаційної комунікації та безпеки архіву;

- охарактеризувати концептуальні основи функціонування архівних інформаційних ресурсів та інформаційної безпеки суспільства;

- визначити особливості нормативно-правового регулювання захисту культурної спадщини на національному і міжнародному рівні;

- проаналізувати рівень відкритості доступу до архівної інформації на вебпорталі Укрдежархіву;

- розглянути можливості доступу до архівної інформації через міжархівний пошуковий портал;

- дослідити напрями реалізації Програми оцифрування Національного архівного фонду та перспективи удоступнення інформації для користувача архівної інформації;

- визначити напрями реалізації заходів безпеки інформації архівних документів з різним рівнем доступу;

- розкрити інноваційні заходи в організації кібербезпеки електронних масивів українських державних архівів;

- показати заходи фізичного збереження архівних документів на матеріальних носіях.

Об'єктом роботи виступають архівні інформаційні ресурси, які функціонують в умовах інформаційної та військової агресії.

Предмет дослідження становлять заходи безпеки функціонування архівних інформаційних ресурсів, забезпечення цілісності та збереження інформації.

Стан наукової розробки теми. У сферах наукових галузей, які досліджують різі аспекти архівних інформаційних ресурсів – історичного документознавства, архівознавства та джерелознавства, нині активно впроваджуються нові методологічні підходи. Сьогодні архівознавці особливу увагу приділяють вивченню аудіовізуальних архівних ресурсів, що відбувається через стрімкий розвиток технологій і методів їх впровадження до архівознавчого наукового обігу. Синергія різних теоретико-методологічних парадигм дозволяє дослідити архівні інформаційні ресурси, що ґрунтуються на розробках В. Бездрабко, Г. Боряка, М. Варшавчика [43; 4; 7], Я. Калакури, С. Кулешова [39; 40; 69], Л. Ковальської [32; 33; 34], Г. Швецової-Водки та інших вітчизняних вчених. А також вивчення окремих аспектів проблематики інформаційного

суспільства, які представлено у працях закордонних дослідників (К. Аннана, Д. Бел, М. Кастельса, М. Макклюена, Й. Масуда, Є. Роговського, Е. Тофлера, Ф. Уебстера та інші).

Джерельна база дослідження. Положення магістерського дослідження ґрунтуються на законодавстві та нормативно-правових актах, що регулюють функціонування архівної справи: ЗУ «Про Національний архівний фонд та архівні установи» № 3814-XII 24.12.1993 [21], ЗУ «Про Національну програму інформатизації» № 2807-IX 01.12.2022 [23], ЗУ «Про інформацію» № 2657-XII 02.10.1992 [20], «Правила роботи архівних установ України» затверджені наказом Міністерства юстиції України № 656/5 08.04.2013 [58], зареєстрованим в Міністерстві юстиції України № 584/23116 10.04.2013, «Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» затверджені наказом Міністерства юстиції України № 1000/5 18.06.2015, зареєстровані у Міністерстві юстиції України № 736/27181 22.06.2015 [57].

Методи дослідження. У процесі дослідження сформульованої мети та вирішення завдань запропонованих у роботі, використано комплекс методів. На різних етапах дослідження під час вирішення поставлених завдань використано аналітичний метод роботи з джерелами інформації та проведення всебічного аналізу проблеми. Методи пошуку і систематизації наукової інформації використано у процесі визначення стану розробленості наукової проблеми, а документальний метод дозволив осмислити залучені документи як підтвердження подій і явищ. Порівняльний метод дозволив простежити категоріальний апарат в історичній ретроспективі та сучасних його проявах, виявляючи тенденції та особливості розвитку. Системний метод застосовано у вивченні специфіки функціонування та протидії об’єкта дослідження, що дозволило сформулювати цілісне бачення проблеми та системність в узагальненні проблем і шляхів їх вирішення. Запропонований методологічний комплекс дозволив розглянути об’єктно-предметну складову більш детально, дослідити її інструментарій та особливості використовування на практиці,

ознайомитись із ситуацією в інформаційно-комунікаційному просторі України та запропонувати перспективні напрями дослідження у інформаційній сфері.

Наукова новизна полягає у розкритті стратегій побудови ефективних безпекових систем захисту архівних інформаційних ресурсів в умовах інформаційно-кібернетичного впливу російського агресора як гібридного засобу ведення війни; спробі комплексно дослідити процеси диджиталізації архівної сфери і проаналізувати вибудовування концепції захисту інформаційних ресурсів; проведенні аналізу теоретико-методичного інструментарію для вирішення проблем безпеки архівних інформаційних ресурсів.

Практичне значення полягає у створенні наукового підґрунтя аналізу новітніх викликів у сфері диджиталізації архівного простору, щодо технологічних можливостей захисту архівних інформаційних ресурсів; практичній спрямованості теоретичних досліджень з питань диджиталізації архівного інформаційного простору, політики відкритості архівної інформації шляхом використання ресурсів вебпорталу Укрдержархіву та міжархівного пошукового порталу, реалізації програми оцифрування Національного архівного фонду; вдосконаленні архівних інформаційних ресурсів в умовах військової агресії від фізичного збереження до кіберзахисту архівних масивів даних.

Апробація результатів дослідження. Окремі результати кваліфікаційної магістерської роботи були оприлюднені під час роботи Другої Всеукраїнської науково-практичної інтернет-конференції «Соціальні комунікації в умовах глобалізації суспільства: виклики та перспективи» Державного університету інформаційно-комунікаційних технологій (07 листопада 2024 року, м. Київ, 2024) та опубліковані у збірнику матеріалів.

Структура кваліфікаційної роботи визначена метою і завданнями та складається із вступу, трьох розділів дев’яти підрозділів, висновків, списку використаних посилань. Перелік посилань налічує 81 найменування. Перелік ілюстративного матеріалу включає 23 рисунки та 1 таблицю. Робота викладена на 88 сторінках друкованого тексту, основна частина якої становить 70 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНЕ ПІДГРУНТЯ БЕЗПЕКИ АРХІВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1. Наукові та методологічні основи проблеми інформаційної безпеки

Сьогодні інформація швидко перетворюється на багатофакторний складний феномен. Інформаційно-комунікаційні технології не тільки змінюють способи передачі та використання інформації, але й впливають на соціальні аспекти психіки і розвиток людської думки. Все це позначається на трендах розвитку технологій, науки, медицини та суспільства в цілому. Ці впливи змінюють процес формування особистості, стимулюючи бажання більш глибокого розуміння світу. З розвитком інформаційних технологій реальність дедалі більше віртуалізується, що створює нове кібернетичне середовище з власними правилами інформаційної взаємодії, соціально-етичними нормами, викликами і загрозами. Нині важливо знайти способи вирішення основних розбіжностей, які виникають у процесі розвитку суспільства та соціалізації людини в питаннях використання та захисту інформації.

Швидкий розвиток технологій та поява нових форм спілкування в сучасному суспільстві вимагають від влади ефективної комунікації з громадянами. Це не лише покращить систему управління в суспільстві, а й сприятиме стабільному розвитку усіх її галузей, зокрема й архівної. Важливою складовою такого діалогу є забезпечення безпеки інформації та створення надійного середовища для спілкування.

У світі, де інформація стає все більш доступною, виникає необхідність захищати її та забезпечувати захист онлайн-спілкування. Особливо гостро це питання стоїть у контексті взаємодії влади та суспільства. Ефективна комунікація між ними неможлива без гарантування конфіденційності та захисту даних. Активна участь громадян у суспільному житті та розвиток самоорганізації вимагають від влади нових підходів до комунікації. Створення ефективної системи взаємодії влади та суспільства є ключовим завданням для забезпечення

сталого розвитку країни. При цьому важливо не забувати про необхідність захисту інформації та створення безпечного цифрового середовища.

Швидкі зміни в суспільстві вимагають від архівістів ефективної комунікації з користувачами. Для цього необхідно створити безпечне комунікативне середовище для обміну інформацією та забезпечити захист персональних даних. Метою держави в цифрових трендах архівної справи має бути створення такої управлінської моделі де є забезпечення єдності принципів розробки та впровадження засад багаторівневої системи захисту архівних інформаційних ресурсів, працівників архівних установ і користувачів архівної інформації. Державна архівна служба України має сформулювати вимоги, створити систему контролю центральних державних архівів, яка буде виступати програмними орієнтирами для регіональних програм безпеки в архівній галузі.

Тема безпеки архівних інформаційних ресурсів в Україні набуває все більшої актуальності у зв’язку з наступними факторами. Зокрема, невідворотній процес переходу до цифрових архівів. Зростання кількості електронних документів та перехід на цифрові архіви збільшує ризики кібератак, втрати даних та несанкціонованого доступу. Зростання кіберзагроз, рівень їх складності та цілеспрямованість потребують постійного оновлення засобів захисту. Найголовнішим фактором є важливість історичної пам’яті для буття українського соціуму. Архівні дані є важливим джерелом для досліджень, освіти та культурної спадщини. Їхня втрата може призвести до незворотних наслідків.

Архівні дані є носіями історичної пам’яті народу, а архівні документи елементом національної культурної спадщини. Тому їх збереження є національним завданням. Безпечні умови і стабільність роботи архівів забезпечують право на доступ до інформації для дослідників, державних органів та громадськості. Надійний захист даних підвищує довіру до архівів як надійних зберігачів інформації.

В Україні проводяться активні дослідження в галузі безпеки архівних інформаційних ресурсів. Науковці та фахівці розробляють нові методи захисту даних, проводять тренінги для персоналу архівів, беруть участь у міжнародних

проектах. Інформація стає фактором, який може спричинити технологічні аварії, військові та політичні конфлікти, а також порушити роботу фінансових систем і державного управління.

Оскільки інтереси людей і держав все частіше реалізуються через інформаційні технології, зростає потреба в міцній інформаційній безпеці. Інформаційні атаки можуть цілеспрямовано змінювати світогляд і моральні цінності як окремих осіб, так і суспільства загалом, нав'язуючи чужі інтереси, мотиви поведінки та спосіб життя. З цієї причини важливо розглянути сутність і форми сучасних методів прихованого агресивного впливу та особливостей поняття інформаційна безпека (табл.1.1). Це включає виявлення агресивних дій, які загрожують національній безпеці, і створення способів протидії цим діям у різних сферах буття соціуму.

Таблиця 1.1 – Зміст поняття інформаційна безпека у наукових працях

Хоффман Л.Дж.	це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації
Литвиненко О.	одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами
Горбатюк О.М.	стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
Богуш В.	стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави
Сороківська О.	суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності
Бурячок В.Л.	стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам

Система інформаційної безпеки формується з використанням широкого набору критеріїв, що призводить до різноманітних підходів до розуміння цього

поняття. Зарубіжна дослідники під такою системою розуміють захист інформації структурований такими компонентами, як цілісність, доступність та конфіденційність даних. Під цілісністю інформації мається на увазі незмінність системи сторонніми особами або процесами, тобто її збереження в авторському вигляді (див. табл. 1.1). Це також включає достовірність інформації, що відображає її відповідність реальності та точність передачі змісту. Конфіденційність передбачає обмеження доступу до інформації для осіб, які не мають на це дозволу, і пов'язана з регулюванням доступу до даних. Доступність інформації означає, що компетентний користувач може скористатися інформацією у потрібний час та відповідно до політики безпеки, не чекаючи понад встановлений час. Тобто інформація має бути доступною у необхідному форматі та місці, коли це потрібно користувачу [11, с. 190].

Аналіз наведених ризиків актуалізує нове розуміння проблеми дослідження, зокрема поняття інформаційної безпеки. Інформаційна безпеку, за словами Б. Кормич, означає збереження законних правил і параметрів інформаційних процесів і відносин, які створюють умови, необхідні для існування держави, людини та суспільства як учасників цих процесів і відносин [31, С. 125].

Інші науковці стверджують, що інформаційна безпеку означає, що важливі інтереси людини, суспільства та держави захищаються від будь-яких небезпек, пов’язаних із неповнотою, затримками, недостовірністю або негативними впливами, а також негативні наслідки від роботи інформаційних технологій і несанкціонованого поширення інформації (див. табл 1.1). Крім того, інформаційна безпека суспільства означає, що його духовні та культурні цінності, соціальні норми поведінки, інформаційна інфраструктура та повідомлення, що передаються, не можуть бути пошкоджені [31, С. 126].

Отже, інформаційна безпека є станом і умовами існування суспільства, які забезпечують сприятливе середовище для розвитку особистості, суспільства та держави, а також інших об'єктів. При цьому інформаційна безпека кожного з цих об'єктів розглядається не як частина загальної безпеки, а як її ціль і результат. Абсолютної безпеки не існує, адже загрози є невід’ємною частиною існування

будь-якого об’єкта. Модель системи інформаційної безпеки має бачити джерела та адресата загроз, які джерела цих загроз, а також механізми їх нейтралізації.

Для повноцінного та адекватного дослідження проблеми безпеки архівних інформаційних ресурсів необхідно звернутися до розкриття дефініцій понятійного апарату теми подані за Законами України та іншими нормативно-правовими актами (Додаток Б-В). З’ясування сукупності термінів, понять і визначень, які використовуються в певній науковій чи професійній сфері для опису, аналізу та пояснення явищ або процесів стає можливим при зверненні до наукових розвідок фахівців та законодавства України. Це допоможе створити основу для спільного розуміння предмету дослідження, забезпечуючи точність та однозначність у комунікації. У наукових дослідженнях понятійний апарат має велике значення, оскільки від його чіткості залежить коректність викладення думок, аналізу даних та інтерпретації результатів.

Архівний документ – документ незалежно від його виду, виду матеріального носія інформації, місця, часу створення і місця зберігання та форми власності на нього, що припинив виконувати функції, для яких був створений, але зберігається або підлягає зберіганню з огляду на значущість для особи, суспільства чи держави або цінність для власника також як об’єкт рухомого майна [21].

Архівна справа – галузь життєдіяльності суспільства, що охоплює наукові, організаційні, правові, технологічні, економічні та інші питання діяльності юридичних і фізичних осіб, пов’язані із нагромадженням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться [21].

Архівна установа, архів, архівний підрозділ, архівний відділ – це відповідно установа чи структурний підрозділ, що забезпечує облік і зберігання архівних документів, використання відомостей, що в них містяться, та формування Національного архівного фонду і/або здійснює управління, науково-дослідну та інформаційну діяльність у сфері архівної справи і діловодства [21].

База даних – іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області [23].

Захист інформації – сукупність заходів, спрямованих на запобігання порушенню конфіденційності, цілісності, доступності інформації, здійсненню її несанкціонованої модифікації. Захисту підлягає інформація у будь-якій формі чи відображенні, дані і програми автоматизованих систем, неправомірні дії з якими можуть зашкодити власникові, користувачеві чи іншим учаснику інформаційної діяльності, призвівши до серйозних втрат у галузях науково-технічної, адміністративно-господарської та комерційної. діяльності організацій, підприємств і держави [26].

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення [31, с.123]

Інформаційно-комунікаційна діяльність – це трансляція інформації між населенням, організаціями різних форм власності шляхом використання спеціальної системи символів, кодів, засобів та організаційних форм; соціальна взаємодія, що має низку специфічних властивостей і ознак, спрямована на регулювання поведінки людей, роботи інститутів державної влади заради досягнення певної мети [12, с.163].

Інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) [23].

Концептуальна модель – це багаторівневе представлення системи, що поєднує алгоритми, припущення, перелік взаємопов'язаних понять для опису, разом з властивостями й характеристиками, класифікацією, за типами ситуацій, ознаками в даній області і законів протікання процесів в ній. Концептуальна модель може бути зображена за допомогою графічних нотацій (діаграм причинно-наслідкових циклів, діяльності тощо) [European Journal of Operational Research].

Користувач архівними документами – фізична або юридична особа, яка відповідно до законодавства ознайомлюється з архівними документами [21].

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем (Додаток В) [15].

Національний архівний фонд – сукупність архівних документів, що відображають історію духовного і матеріального життя Українського народу та інших народів, мають культурну цінність і є надбанням української нації [21].

Отже, з розвитком цифрових технологій інформаційна безпека стає екзистенційним питанням для незалежності держав, оскільки вона передбачає контроль за джерелами інформації та використанням комунікаційних ресурсів у межах технологічних блоків та економічних об’єднань. Перелік використаних в дослідженні дефініцій не є вичерпним, проте цілком достатнім для синхронізації розуміння теми їх застосування. Наведені поняття в повній мірі розкривають сутність процесу організації захисту архівних інформаційних ресурсів.

1.2. Тенденції розвитку архівних ресурсів та їх убезпечення від стороннього впливу

Прогресивний розвиток інформаційного суспільства є однією з головних характеристик сучасності. Швидкий розвиток інформаційних технологій та комунікаційних мереж перетворює сучасне суспільство на динамічний інформаційний простір. Цей простір є результатом колективної інтелектуальної діяльності людей, де створюються, обмінюються та зберігаються знання. Постійне зростання обсягів інформації та її доступності призводить до нових можливостей для розвитку науки, економіки та демократії, але водночас створює нові виклики.

В умовах диджиталізації активно розвиваються новітні форми інформаційно-комунікаційних технологій, створюючи сприятливі умови для

ефективного використання знань в сфері економічного зростання українського суспільства, у вирішенні ключових завдань управління соціальними процесами та демократизації суспільного життя. Ці процеси сприяють формуванню інформаційного простору, де інформація створюється, поширюється, використовується та зберігається (Додаток А).

Інформаційний простір являє собою історично сформовану структуру, забезпечену правовими гарантіями та засобами зв'язку, що об'єднує інформаційні ресурси, які виникають у результаті комунікаційної діяльності людей, забезпечуючи максимальну доступність для користувачів. Знання та інформація породжують нові знання, а їхній вплив та роль у розвитку суспільства зростають у геометричній прогресії.

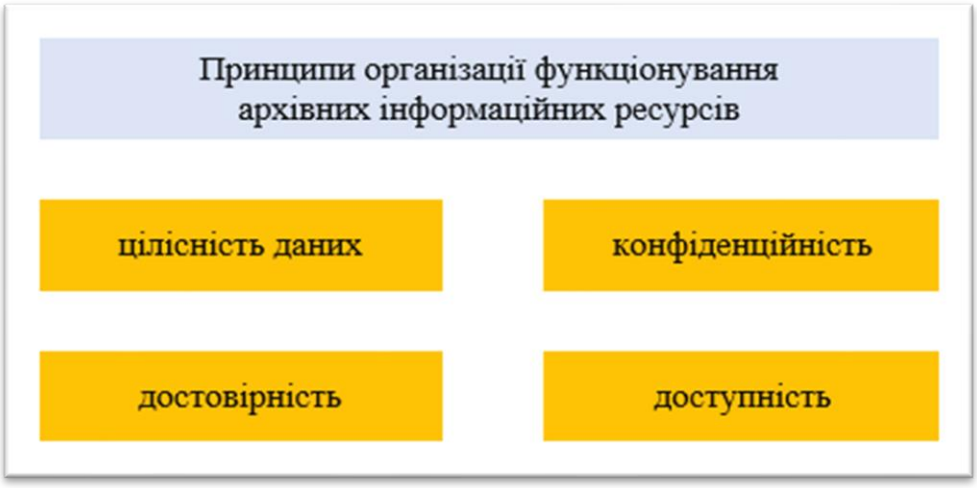


Рисунок 1.1 – Принципи організації функціонування архівних інформаційних ресурсів (Додаток А)

У цьому контексті головна мета інформаційно-комунікативної діяльності полягає в запобіганні будь-яким можливим зловживанням при визначенні прав і свобод людини в інформаційній сфері. Інформаційна безпека є одним із ключових аспектів захисту надзвичайно важливих інтересів будь-якої країни світу. Вона передбачає створення умов для обмеженого доступу до інформації через розподіл прав доступу, захист від несанкціонованого доступу та ознайомлення з інформацією, а також забезпечення конфіденційності та цілісності даних (див. рис. 1.1).

Інформація стала одним з найважливіших ресурсів сучасного суспільства. Вона не лише сприяє розвитку науки і технологій, але й впливає на формування громадянської свідомості. Інформаційний простір, як складна система, об'єднує різноманітні інформаційні ресурси, забезпечуючи доступ до знань для широкого кола користувачів. Зокрема, архівні інформаційні ресурси є сукупністю інформації, що зберігається в архівних документів, і має історичну, наукову, культурну або юридичну цінність. Ці ресурси містять дані, які зберігаються для використання у дослідженнях, забезпечення прав громадян, організацій та держави, а також для збереження національної пам’яті та культурної спадщини.

До архівних інформаційних ресурсів належать різноманітні види документів: паперові, електронні, аудіовізуальні, фото-, кіно-, відеодокументи тощо. Вони можуть бути створені як державними, так і приватними установами, організаціями або фізичними особами, та зберігаються в архівах для подальшого їхнього руху в часі і просторі. Ці ресурси структуруються, обліковуються і каталогізуються, що забезпечує їхню збереженість та доступність для користувачів, як науковців, так і громадськості.

Інформаційний простір архівної сфери, як складна система, потребує чіткого правового регулювання та захисту. Закони України у сфері обігу інформації забезпечують захист архівних інформаційних ресурсів, авторських прав та свободи слова. Водночас, правові норми повинні сприяти розвитку інформаційної комунікації між архівістами і користувачами та забезпечувати рівний доступ до інформації для всіх громадян. Сучасне світове суспільство характеризується стрімкою глобалізацією інформаційних технологій, що формує глобальний архівний інформаційний простір. Цей простір є джерелом знань про минуле, сприяє розвитку громадянського суспільства та створює нові виклики для правового регулювання.

Архівні інформаційні ресурси характеризуються соціально-історичними особливостями і виражені через знаково-символічну систему. Користувачу інформації архівного документного ресурсу важливо зрозуміти сутність інформації, закладеної в документі, як етап пізнання різних явищ об'єктивної

реальності. Адже зміст інформації має об'єктивний характер, це відображається в текстових даних історичних джерел, які передають соціально-історичну дійсність. Двоїстий характер документальних ресурсів визначає суб'єктивність соціальної інформації, що виникає внаслідок взаємодії соціального суб'єкта з реальністю та виражає його цілі, завдання й ціннісні орієнтири. Знаково-семантичний аспект архівного інформаційного ресурсу має прагматичне значення для суб'єкта. Ідеальна за своєю сутністю інформація закріплюється на матеріальних носіях у конкретній формі. Змістово-семантична частина передає поняття, образи та ідеї, закладені в інформаційному повідомленні. Знаковий компонент є матеріальним, сприйманим через відчуття і зафіксованим для передачі в просторі та часі у вигляді символів, які класифікуються за зовнішньою подібністю [34, с. 47].

Існують різні методологічні підходи до розуміння поняття «архівний інформаційний ресурс». Проте, найбільш вдалим для застосування у цьому кваліфікаційному дослідженні, широким у змістовому та методологійному розумінні є визначення неведене науковцем Л. Ковальською (див. рис. 1.1). Під документально-інформаційними ресурсами вчена розуміє такі види писемних та аудіовізуальних джерел інформації, з властивими формальними ознаками документа як інформаційного об’єкта, де інформація зафіксована на матеріальному носієві за допомогою фізико-хімічних засобів задля трансляції у просторі і часі, а закодовані знання та інформаційні повідомлення відображають ієрархічні, документаційні й комунікаційні зв’язки суспільства» [34].

У різні часи у науковців збільшується увага до дослідження інформаційного аспекту різноманітних видів і типів документів. Сучасні інформаційні ресурси архівів і бібліотек, працюють переважно з «інформацією як річчю». Ці ресурси обробляють інформацію лише у формалізованій формі, що дозволяє її оцифровувати та створювати стандарти використання. Кожен вид документів має специфічні методи обробки та формалізовані способи опису інформації. Тому системи зберігання та пошуку працюють з «інформацією як річ», яка

матеріально виражена у документах. Водночас така інформація може зберігатися як у фізичних, так і в цифрових колекціях музеїв та архівів [34, с.72].

Рисунок 1.2 – Види документів інформаційних архівних ресурсів.

Вивчаючи історичні аспекти минулого з допомогою архівних інформаційних ресурсів, необхідно враховувати вплив на процес їхнього утворення конкретних соціальних інститутів, визначення суб'єктів та об'єктів впливу. Це підкреслює важливість фіксації інформації у документованій формі як інструменту владного впливу на суспільство. Ці аспекти соціальної динаміки інформації визначають технології документування як окремі соціальні процеси. Поява демократичних теорій та зростання рівня індивідуальної свободи є закономірним результатом розвитку інформаційних технологій, інституціалізації інформаційних комунікацій та формування відповідного соціального середовища. Прихильники теорій М. Вебера та М. Фуко пов'язують інформаційно-документознавчі технології з посиленням соціального контролю, інституційним зростанням значимості влади в соціумі [34, с. 54].

Коли користувач архівної інформації об'єктивує соціальну інформацію, вона набуває об'єктно-суб'єктної природи та особливостей документального носія інформаційних даних. Документальні носії історичних даних містять шари прямої та непрямої інформації, зафіксовані на різних етапах її розвитку.

Соціальна інформація архівного документа є сукупністю знань, необхідних для того, щоб суспільство могло існувати. М. Варшавчик розуміє джерельну

інформацію як сукупність різноманітних типів інформації, які містяться в джерелі, а також зв'язків, які існують між ними, що гарантує, що джерело є незмінним і може служити основою для наукового знання [7]. Оскільки вони були частиною інформаційно-комунікаційних процесів суспільства, кожне документальне джерело містить значну кількість соціальної інформації. На наступному етапі джерело стає об'єктом дослідження та носієм історичної інформації. Це дає уявлення про зміст і особливості соціально-інформаційних процесів, які відбувалися в минулому.

Отже, архівний інформаційний ресурс складається з різних видів документів, які необхідні для досягнення мети та цілей соціально-історичного вивчення користувачем. Виділяються основні документальні ресурси інформації, які містять необхідні дані для дослідників. У наш час архівний інформаційний ресурс демонструє наукову соціально-історичну цінність, показуючи, наскільки він був залучений до соціального інформаційного процесу. Усвідомлення того, наскільки автори документу і їхні здібності до створення та використання інформації, дає можливість дослідникам з'ясувати причини та мотиви поведінки людей, їхніх дій, рішень тощо.

Нині світ знаходиться на цивілізаційному зламі – відбувається перехід від індустріального суспільства до інформаційного, що супроводжується стрімким піднесенням значення інформаційних технологій. Все це суттєво трансформує суспільне життя, вже існує низка концепцій реалізованих у комплексі організаційних, технічних і програмних засобів, а також методів і заходів, спрямованих на регулювання та захист інформації. Це підкреслює важливість усвідомлення та впровадження ефективних заходів безпеки в інформаційному просторі.

У сучасному цифровізованому світі, де існують конфлікти, протиріччя, глобальні проблеми та складні військові ситуації, а також реальні загрози інформаційної війни, виникає нагальна потреба в їхньому розв'язанні з врахуванням інформаційного пріоритету. В першу чергу це стосується активного використання інформаційно-комунікаційних технологій у суспільстві, що

збільшує ризики втрати важливих, викрадення, спотворення або пошкодження даних від яких залежить життєдіяльність усіх сфер соціуму.

Володіння та обмін даними як інформаційним ресурсом розвитку завжди визначали ключові вимоги до якості інформаційно-комунікаційного простору будь-якої країни. З появою цифрової техніки та інформаційно-комунікаційних технологій виникли численні проблеми, пов’язані з безпекою. Зросла потреба в обміні досвідом та використанні напрацювань, особливо під час створення власних баз даних та віртуальних інформаційних продуктів. Це питання є набуває надзвичайної ваги у контексті впровадження новітніх інформаційно-комунікаційних технологій в економічну, військову та науково-освітню діяльність держави.

Концептуально проблему безпеки архівних інформаційних ресурсів поділяють на два основних аспекті: інформаційно-технічні прояви та інформаційно-гуманітарні прояви, які наведені на Рисунку. Технічні аспекти захисту інформації охоплюють загрози, зокрема кібератаки, що можуть порушувати цілісність, конфіденційність або доступність даних. До таких атак належать віруси, хакерські втручання, атаки на мережеві системи та інші технічні загрози.

Наведені концептуальні підходи взаємно інтегровані та доповнюють один одного, а їхня спрямованість залежить від завдань і мети впливу на суспільство (див. рис. 1.3). Врахування у соціальному розвитку суспільства технічних і гуманітарних площин безпеки архівних інформаційних ресурсів спричиняє потребу в постійної актуалізації технічних наукових знань, підвищення рівня спеціалізованої і загально-суспільної освіти. Складні прогресивні процеси в епоху цифрової техніки зумовлюють появу нових принципів захисту інформації від сучасних загроз, як в сфері цифрових технологій, так і сфері соціально-гуманітарного впливу.

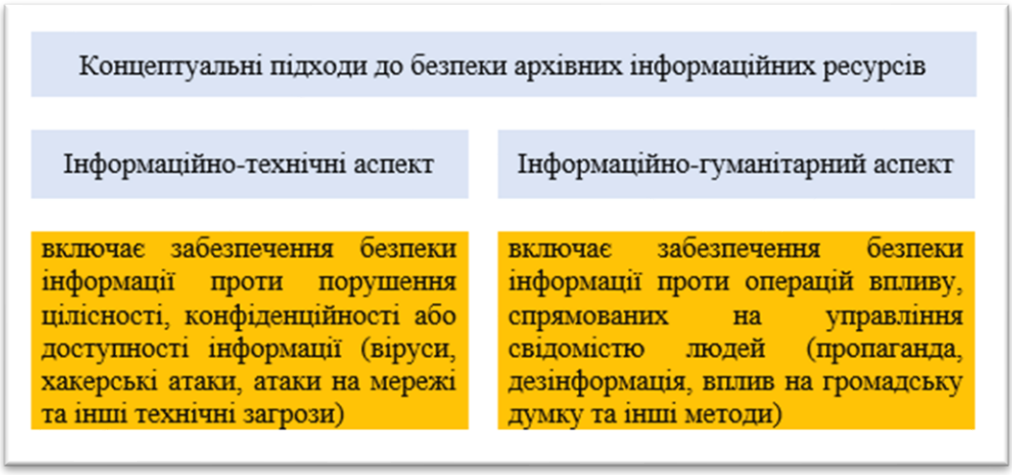


Рисунок 1.3 – Концептуальні підходи до розуміння безпеки архівних інформаційних ресурсів

Через соціальні аспекти інфомаційного впливу або змінення конотації конкретних інформаційних ресурсів виникає напрям гуманітаристики з власною понятійною базою. Зокрема, терміни «інформаційна війна» та «інформаційна зброя» набувають актуальності для опису різноманітних операцій інформаційної агресії рф проти України. Такі операції ворога мають на меті вплинути на свідомість окремих осіб та масову аудиторію, а також обмежувати право на доступ до інформаційних ресурсів. Визначальне місце тут мають архівні інформаційні ресурси, оскільки з архівними процесами декомунізації та деколонізації документна інформація архівів набуває ідеологічного характеру. З її допомогою агресором формуються усталені ідеологічні конструкції та змістові посили для зміни масової свідомості.

Враховуючи наведені соціально-історичні аспекти, з’являється потреба включення до процесу захисту фахівців технологічного рівня. Їх завдання полягає у в убезпеченні архівних інформаційних ресурсів від несанкціонованого стороннього доступу, модифікації або знищення. Будь-яка інформаційна система, зокрема й архівна, концентрує величезну кількість інформаційних ресурсів з усіх сфер життєдіяльності соціуму. Тому вибудовування ефективного захисту в інформаційно-технологічній та інформаційно-гуманітарній площинах нині набуває вирішального екзистенційного значення для національної безпеки України.

Отже, неефективно організований захист може призвести до несанкціонованого доступу. Це може спричинити втрату конфіденційної інформації, загрозу цілісності та викривленості баз даних, і поширення особистої інформації. Такі заходи захисту технологічного рівня, як шифрування, автентифікація та контроль доступу, покликані запобігти таким загрозам. Також, постійно вдосконалення вимагає програмне та апаратне забезпечення, що убезпечить архівні інформаційні ресурси від несанкціонованому доступу. Гуманітарний рівень безпеки архівних інформаційних ресурсів передбачає низку організаційних заходів щодо правового захисту інформації, підвищення освітнього рівня громадян в сфері цифрової інформаційної гігієни тощо.

1.3. Нормативне регулювання захисту документної спадщини в Україні та країнах ЄС

Функціонування архівних інформаційних ресурсів українських архівів регулюється національним законодавством та нормами міжнародного права. Згідно Закону України «Про Національний архівний фонд та архівні установи» документи «Національного архівного фонду України є складовою частиною вітчизняної і світової культурної спадщини та інформаційних ресурсів суспільства, перебуває під охороною держави і призначений для задоволення інформаційних потреб суспільства і держави, реалізації прав та законних інтересів кожної людини. Документи Національного архівного фонду є культурними цінностями, що постійно зберігаються на території України або згідно з міжнародними договорами, згода на обов’язковість яких надана Верховною Радою України, підлягають поверненню в Україну» [21].

Положення кваліфікаційної роботи ґрунтуються на законодавстві та нормативно-правових актах, що регулюють функціонування архівної справи: Закон України «Про Національний архівний фонд та архівні установи» № 3814-XII 24.12.1993 [21], Закон України «Про Національну програму інформатизації» № 2807-IX 01.12.2022 [23], Закон України «Про інформацію» № 2657-XII 02.10.1992 [20], «Правила роботи архівних установ України…» затверджені

наказом Міністерства юстиції України № 656/5 08.04.2013 [58], зареєстрованим в Міністерстві юстиції України № 584/23116 10.04.2013, «Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» затверджені наказом Міністерства юстиції України № 1000/5 18.06.2015 [57], зареєстровані у Міністерстві юстиції України № 736/27181 22.06.2015 (Додаток Б-В).

Національне законодавство України регулює питання фізичного збереження архівних інформаційних ресурсів та, з активним розвитком цифрових технологій, електронних архівних інформаційних ресурсів. В Україні розроблені законодавчі та нормативні акти, які забезпечують безпечні умови розвитку інформаційного суспільства, регулюють захист інформації та визначають межі встановлення, розвитку й регулювання інформаційних відносин. Норми законодавства, що стосуються інформаційних відносин, здебільшого спрямовані на захист інформації. Водночас менше уваги приділено положенням із захисту людини, суспільства й держави від впливу шкідливої інформації.

Крім суто архівних існує низка законів і нормативно-правових актів з питань регулювання інформаційної сфери та проблем цифровізації суспільних процесів. Зокрема, Закони України «Про Національну програму інформатизації» [23], «Про охорону культурної спадщини» [25], розпорядження Кабінету міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні», «Про схвалення Концепції розвитку системи електронних послуг в Україні» [67], «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації», «Про схвалення Стратегії розвитку інформаційного суспільства в Україні».

В українському законодавстві представлено регуляторні акти з питань безпеки в сфері інформаційної діяльності. В 2017 р. Указом Президента України

схвалено «Доктрину інформаційної безпеки України». У документі низку загроз національній безпеці в інформаційній сфері наведені нижче (Додаток В).

У 2020 р. було підготовлено проєкт «Стратегії розвитку архівної справи на період до 2025 року» [74]. Документ визначає цілісну систему стратегічних і операційних цілей для реалізації державної політики у сфері архівної справи. Стратегія включає: гарантування того, що всі архіви мають рівний доступ до інформації, знань і послуг; зміцнення інституційної спроможності архівів; оновлення нормативно-правової бази галузі архівної сфери; і формування та розвиток комунікативної політики.

Першочерговими цілями стратегії є реформа системи управління архівною справою, розробка нових архівних законів, покращення якості та доступності архівних послуг, активізація оцифрування документів, і формування позитивного іміджу архівних установ у суспільстві.

З прогресивним рухом інформаційних технологій і, відповідно, появою нових видів безпекових викликів та загроз інформаційним ресурсам в України виникає потреба у нормативному регулюванні та створенні держаного контролю у захисті інформаційної комунікації. Наразі в Україні існує низка законів захисту національних інформаційних ресурсів: «Про захист інформації в інформаційно-телекомунікаційних системах» [19], «Про Державну службу спеціального зв'язку та захисту інформації України», «Про Національну програму інформатизації» [23] (Додаток Б-В).

Згідно них захист держаних інформаційних ресурсів покладено на Державну службу спеціального зв'язку та захисту інформації. Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є формування і реалізація державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також захисту державних інформаційних ресурсів і інформації, захист якої встановлено законом; участь у формуванні політики електронного документообігу для державних органів у

частині захисту інформації, розробка і впровадження електронного цифрового підпису; забезпечення діяльності суб'єктів, які займаються боротьбою з тероризмом [44].

Ефективне управління національними ресурсами є ключовою умовою для забезпечення інформаційної безпеки держави та реалізації державної політики в сфері інформатизації. Створення системи національних ресурсів закладено у Національної програми інформатизації. Спеціально уповноважений центральний орган виконавчої влади в галузі зв'язку та інформатизації відповідає за управління та координацію заходів з формування, використання та захисту національних ресурсів, ведення Національного реєстру електронних ресурсів та підготовку щорічних звітів. Наразі, на базі вебпорталу «Дія» функціонує Національний реєстр електронних інформаційних ресурсів, який є інтегральною системою що поєднує значну частину державних реєстрів із різних сфер життєдіяльності держави [46].

Стратегія створення системи державних ресурсів спрямована на їхню систематизацію, інтеграцію, прозорість і забезпечення відкритого доступу для громадян, що підвищує ефективність роботи державних органів. Реалізація політики у сфері державних інформаційних ресурсів передбачає: ведення Національного реєстру, систематизацію й актуалізацію державних ресурсів, формування умов їх ефективного використання, удосконалення правової бази та координацію державних і недержавних структур у цій сфері [8].

Національне законодавство будується на принципах закладених у міжнародному праві. Принциповим було врахування Хартії про збереження цифрової спадщини (Charter on the Preservation of Digital Heritage), Принципів доступу до архівів, схвалених Міжнародною радою архівів, Рекомендації Комітету Міністрів Ради Європи державам-членам стосовно європейської політики доступу до архівів № R 13, Конвенції Ради Європи про доступ до офіційних документів, Ванкуверської декларація «Пам'ять світу в цифрову епоху: оцифрування і збереження» («Memory of the World in the Digital Age: Digitization and Preservation»), Програми ЮНЕСКО «Інформація для всіх»

(Information for All Programme), Стратегії ЮНЕСКО щодо розвитку архівної справи та діловодства. Програми RAMP, а також документів Європейського Союзу: Цифрового порядку денного для Європи (Digital Agenda for Europe); Програми ЄС «Горизонт 2020 – Рамкова програма з досліджень та інновацій».

Отже, швидкий технологічний прогрес, поширення цифрових технологій та технологій інформаційного суспільства зумовлюють зростаючі потреби в систематичному перегляді нормативної бази та науково-теоретичному обґрунтуванні вектору інформатизації України. Це необхідно для забезпечення захисту архівних інформаційних ресурсів з урахуванням сучасних зовнішніх впливів інформаційних технологій, захисту особистих даних, безпеки діяльності у віртуальному просторі, веденні агресивних інформаційних війн тощо. Документна комунікація виконує функцію поєднання людей через засоби архівних інформаційних ресурсів. Тому важливо створити надійні правові інструменти інформаційної безпеки, враховуючи інформаційну (а також збройну) агресивну війну рф проти України. Інформаційна незахищеність впливає на політичну ситуацію в Україні та геополітичну в світі. Наслідком неконтрольованого інформаційного простору буде маніпулювання змістом інформаційного поля та зміна конотацій інформації архівних інформаційних ресурсів. Імплементація міжнародного права та створення юридичних запобіжників стане надійним бар’єром на захисті архівних інформаційних ресурсів.

РОЗДІЛ 2
ДИДЖИТАЛІЗАЦІЯ АРХІВНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ТА ПОТРЕБА ЙОГО ЗАХИСТУ В УМОВАХ ВІЙНИ

2.1. Відкритий доступ до архівної інформації та електронні архівні ресурси на вебпорталі Укрдежархіву

Вебпортали є прогресивною формою комунікації у соціумі та виявом розвитку громадянського суспільства. Зокрема, обмін інформацією державних органів і організацій з громадянами поступово зміщується в цифрову площину. Архівні установи активно працюють над створенням каналів комунікації з використання диджитал технологій з виключенням людського фактору в цьому процесі. Веб-сайти цінуються через рух у просторі і часі складних електронних документів, який не можливо досягти традиційними методами комунікації.

Вебпортали пропонують користувачам широкий спектр різноманітного контенту, широкий спектр інтерактивних послуг і покликання на інші веб-сторінки. Надання загальної інформації про архіви та архівні документи, сприяння пошуку архівних документів, інформування про діяльність архівів, надання послуг, популяризація архівної справи та формування позитивного іміджу архівів є основними цілями створення архівних вебпорталів.

У виконанні інформаційно-комунікаційної функції архіву електронні ресурси відіграють важливу роль, і вони мають деякі переваги порівняно з традиційними засобами комунікації. Так, офіційні вебпортали мають завдання формування позитивного образу установи, подання інформації про її історію, сучасний стан, організаційно-функціональні можливості, науково-технічні потенціали тощо.

У рамках розробки «Програми інформатизації архівної справи» 20 вересня 2000 р. Державний комітет архівів України видав наказ «Про створення веб-сайту Державного комітету архівів України» [наказ], який офіційно відкрився 24 грудня 2000 р. У той самий день, що й десять років тому, було представлено оновлену версію карти та структури веб-порталу.

Зважаючи на те, що веб-сайт ДКА України у 2002 р. було внесено до реєстру ЮНЕСКО, а в 2004 р. він отримав статус вебпорталу, можна припустити, що його розробники мали стратегічну мету не лише інформувати громадськість про події та події, пов’язані з архівним сектором, а й забезпечити інтелектуальний доступ до архівних документів НАФ [66].

Вже 9 грудня 2010 р. було засновано вебпортал «Архіви України» Державної архівної служби України, що виступає правонаступником ДКАУ (див. рисунок 2.1) (Додаток Г). На думку Г. Боряка, створення оновленого вебпорталу відбулося в результаті різноманітних організаційно-правових заходів, спрямованих на інформатизацію архівної галузі, і сьогодні він є потужним інформаційним ресурсом, який містить широкий спектр різноманітних відомостей про документальну культурну спадщину України [4].

Рисунок 2.1 – Версія вебпорталу Державної архівної служби України до 2020 р. (Додаток Г)

З 2020 р. вебпортал Державної архівної служби України отримав універсальний для усіх вищих органів виконавчої влади дизайн і функціонал, що відповідає цифровим вимогам новітньої доби. На вебпорталі з’явився важливий канал зв’язку між розпорядниками архівних інформаційних ресурсів та користувачами архівної інформації.

Наразі вебпортал виступає цифровим архівних інформаційним ресурсом і є корисним інструментом для громадян і організацій, щоб отримати інформацію, яка стосується соціально-історичних зацікавлень користувачів архівної інформації (див. рисунок 2.2). Він також може задовольнити їхні потреби в знаннях про склад і зміст документів НАФ. Це допомогло встановити зв'язок між користувачами таких даних і архівними установами.

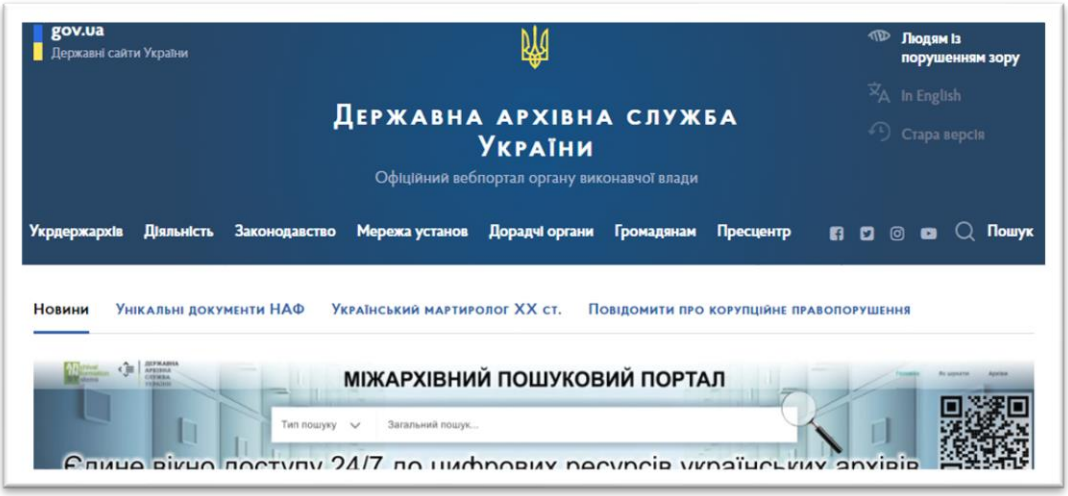


Рисунок 2.2 – Оновлений вебпортал Державної архівної служби України (Додаток Г)

Публікація путівників по архівним фондам центральних, галузевих і регіональних архівних установ, а також інших довідників демонструє розуміння цінності цього інформаційного ресурсу. Змістовне наповнення розділів, що стосуються архівів України та, якщо потрібно, світу, дозволяє користувачам знайти необхідні дані про місцезнаходження документів без відвідування архівної установи в режимі 24/7. Це значно заощаджує час користувача та зменшує робоче навантаження на працівників архівів. Найважливішим завданням для подальшого вдосконалення інформаційного ресурсу «Архіви України» є покращення комунікації з користувачами вебпорталу (Додаток Г).

Державна архівна служба України сьогодні має офіційний вебпортал, який включає архівно-пошуковий проєкт «Український мартиролог XX століття» з розширеними можливостями бази даних. У цій базі зібрано інформацію про близько 127 тисяч репресованих осіб, якою скористалися понад 50 тисяч відвідувачів. Також доступна база даних «Унікальні документи Національного

архівного фонду», що дозволяє переглядати цифрові копії документів, віднесених до культурної спадщини. На даний момент до унікальних документів віднесено 436 архівних матеріалів, які мають важливе значення для національної самосвідомості та культурної спадщини України [58].

Крім того, вебпортал містить електронний ресурс «Архіви Криму», що надає онлайн доступ до цифрових копій метричних книг з Державного архіву Автономної Республіки Крим та Севастополя, а також документів Галузевого державного архіву Служби безпеки України. Проєкт «Архів архівного законодавства» дозволяє користувачам шукати документи за шістнадцятьма умовно визначеними категоріями, а також критично аналізувати їхні положення та висновки. Це забезпечує можливість порівняти дані документи з сучасною нормативно-правовою базою архівної галузі. Так, вебпортал став важливим інструментом для дослідження архівних матеріалів та підвищення обізнаності громадськості про українську історію та культуру [58].

За аналогією інформаційного архівного ресурсу вебпорталу «Архіви України» побудовано вебсайти центральних державних архівних установ, галузевих державних архівів, обласних державних архівів та архівних установ місцевих органів влади. Проте, вебпортал «Архіви України» Державної архівної служби України, який містить доступ до вебсайтів усіх державних архівних установ України, наразі є найважливішим джерелом офіційної інформації в архівній сфері для нашої держави [58].

Державна архівна служба України в тестовому режимі запустила новий інформаційний ресурс, що спрощує пошук інформації в сфері архівної справи, діловодства та функціонування системи страхового фонду документації. Цей ресурс надає можливість отримувати офіційну інформацію та відповіді на актуальні запитання в режимі 24/7. В даний час база знань включає п’ять розділів, серед яких архівні документи на ресурсах партнерів, архівні інформаційні ресурси, методичні та наукові розробки, страховий фонд документації та робота архівів в умовах воєнного стану [58].

В рамках пріоритетного напряму цифрової трансформації архівів та установ страхового фонду документації в умовах війни, Державною архівною службою України у 2023 році було організовано оновлення відомчої системи електронного документообігу. Це оновлення сприяє поліпшенню процесів обробки документів і управління ними. Також було підготовлено та направлено пропозицію до Міністерства цифрової трансформації України щодо включення створення єдиного державного електронного реєстру Національних архівних інформаційних ресурсів до завдань Національної програми інформатизації на 2024-2026 роки [23].

Запровадження єдиного державного електронного реєстру дозволить автоматизувати облік, зберігання та використання архівних інформаційних ресурсів, що значно покращить їх доступність. Це стане важливим кроком у забезпеченні ефективності роботи архівних установ в Україні. Завдяки цим ініціативам, архіви зможуть краще реагувати на виклики сучасності, що, безсумнівно, підвищить якість надання архівних послуг [58].

Усі вебпортали архівних установ України, як цифрові архівні інформаційні ресурси, мають завдання створити ефективні канали комунікації архіву з користувачем архівної інформації. Людський капітал створюється завдяки сучасним інформаційно-комунікаційним технологіям, які закладають основу для створення «інформаційного суспільства». Інформаційні дані є необробленою цифровою масою та фактажем, що відображають конкретну частину реальності. А сама інформація виступає даними, що отримали смислове навантаження.

Обидві наведені інформаційні категорії є важливими елементами архівного інформаційного ресурсу та надзвичайно вагомі для ефективної комунікації. Коли інформація є достовірною, своєчасною, повною та актуальною – вона особливо цінна. Коли інформація обмінюється між двома або більше суб’єктами процесу, це називається комунікативним процесом.

Метою встановлення комунікативного процесу полягає в тому, щоб люди знали інформацію, яка є предметом обміну, тобто повідомлення. Тим не менш, сам факт обміну інформацією не гарантує, що вона буде передана ефективно й

без викривлення. Таким чином, для забезпечення безпеки інформаційних систем і комунікацій важливо знати про етапи комунікаційного процесу, а також знайти способи їх убезпечення від зловмисного впливу і використання.

Захист архівної інформації, даних, комунікаційних послуг і послуг з обробки та передачі даних, а також обладнання та засоби є вельми необхідним. Сучасні тенденції показують, що безпечна інформаційна комунікація дозволяє навіть найменш розвиненим країнам перетворити свою економіку на інформаційну та високотехнологічну. Такі економіки можуть спеціалізуватися на виробництві цифрових товарів із високою доданою вартістю та конкурувати на глобальному ринку з передовими економіками. Технологічні досягнення в інформаційній сфері сприяють глобалізації, створюючи інфраструктуру, яка полегшує глобальні зв'язки. Рушійною силою глобалізації в сучасному світі залишається революція в інформаційних і комунікаційних технологіях.

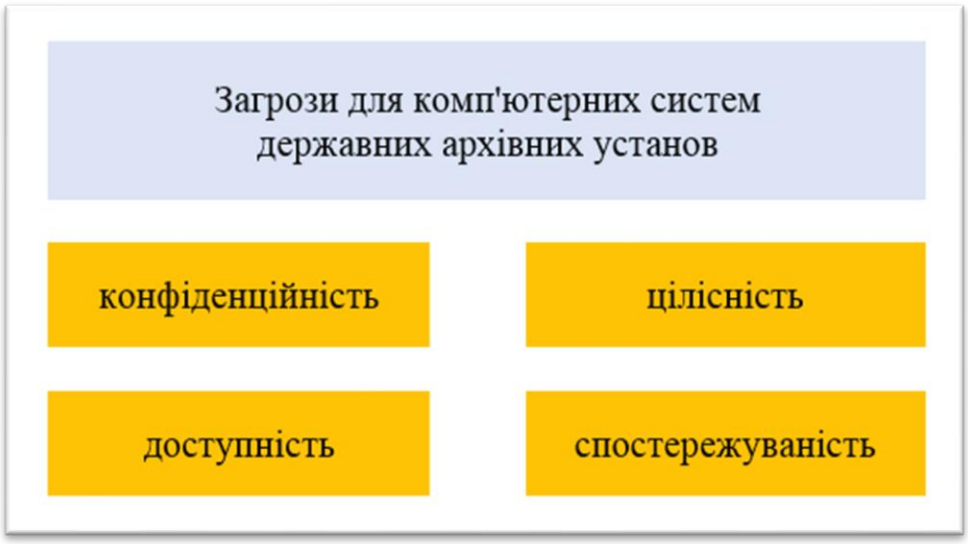


Рисунок 2.3 – Загрози для комп'ютерних систем державних архівних установ

Інформаційна безпека інформації на вебпорталі визначається не лише рівнем захищеності інформації, а й стійкістю основних сфер життєдіяльності алгоритмів та цифрових моделей сайту. Автоматизація систем захисту охоплює не лише технічні аспекти інформаційних систем або безпеку електронних даних, а й всі елементи захисту даних незалежно від їхньої форми. Це включає заходи, спрямовані на забезпечення конфіденційності, цілісності, доступності інформації (див. рисунок 2.3).

Інформаційні технології поєднують технічні засоби обробки та передачі даних із аспектами організаційного управління та соціально-економічного впливу. Автоматизовані алгоритми захисту інформації мають функціонувати системно, гарантуючи заходи безпеки в усіх аспектах використання інформації. Потенційні загрози для комп'ютерних систем можна побачити на рисунку 2.3. Кожен з цих аспектів має свої потенційні загрози, що можуть виникнути на окремих комп'ютерах.

Отже, вебпортал Укрдержархіву, який є потужним джерелом інформації, допомагає краще зрозуміти документальну спадщину України та наблизити архіви до потреб сучасних користувачів і суспільства в цілому. Вебсайт «Архіви України» має два аспекти. З одного боку, він дає людям можливість більше дізнатися про документи Національного архівного фонду, які містять унікальну інформацію про історію нашого народу та культурні надбання світу. А також, забезпечує іміджеву складову функціонування та актуалізацію популярності такої роботи, як почесну професію архівіста.

2.2. Можливості «Міжархівного пошукового порталу» у наданні доступу до архівної інформації

Перша половина 2022 р. позначилася не тільки активізацією воєнної агресії рф проти України, а й розумінням необхідності масштабного оцифрування архівних фондів задля порятунку від невибіркових бомбардувань у містах України. Вже у травні 2022 р. Голова Укрдержархіву Анатолій Хромов презентував електронний архівний інформаційний ресурс «Міжархівний пошуковий портал» (див. рисунок 2.4). Пошукову систему створено за принципами європейських країн, що мають відповідні інтегральні електронні архівні ресурси побудовані за уніфікованими вимогами пошуку архівних документів і надання громадянам єдиний доступ до оцифрованого культурного надбання.

Головною задачею ресурсу ставилося забезпечення цілодобового доступу до цифрових архівних інформаційних ресурсів за принципом електронного

єдиного вікна, яке працює за принципом 24/7 без оператора з автоматичною обробкою запиту користувача. За очікуваннями архівістів відкриття порталу має змінити вектор роботи архівів. Зокрема, принцип надання сервісних архівних послуг та полегшити роботу працівників державних архівів.

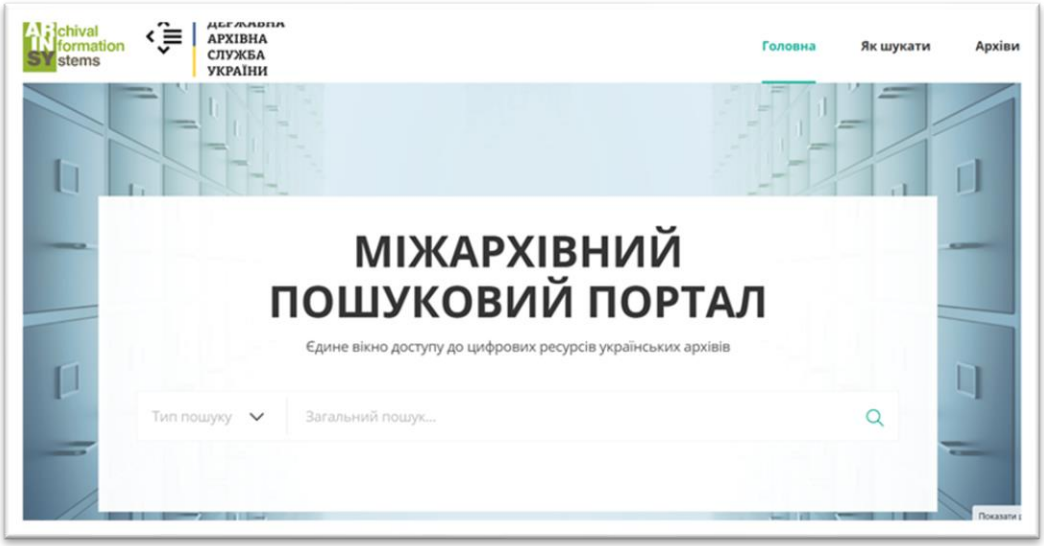


Рисунок 2.4 – Вебпортал Державної архівної служби України з електронним банером для переходу до «Міжархівного пошукового порталу» (Додаток Д)

Державні архіви працюють можливістю розширення роботи архівного інформаційного ресурсу. Портал має полегшити життя, як архівістів, так і користувачів, що є особливо актуальним в соціальних обмеження ковідного періоду життя та умовах складного доступу до архівної інформації в період війни. На момент появи «Міжархівного пошукового порталу» для півтора мільйона повнотекстових електронних копій архівних документів було створено повноцінний пошуковий апарат для представлення на пошуковому ресурсі центральними архівами ЦДАВО, ЦДАГО та ЦДАМЛМ (Додаток Д).

З появою «Міжархівного пошукового порталу» динаміка оцифрування архівних документів пришвидшилася і на 2022 р. приріст електронних документів становив 500 %. Оцифровані раніше документи для оприлюднення розміщувалися на різних електронних ресурсах і платформах, що в свою чергу робило неможливим організований пошук потрібного документа або тематичної колекції електронних документів.

Насьогодні «Міжархівний пошуковий портал» надає користувачам архівної інформації понад десять мільйонів електронних копій архівних інформаційних ресурсів. Ці документи охоплюють дев’ять тематичних комплексів з фондів ЦДАВО України, ЦДІАК, ЦДІАЛ, ЦДАГОУ, ЦДАМЛМ, державних архівів Кіровоградської, Львівської, Полтавської областей та інших. А також, у 2024 році до пошукового порталу доєднається Державний архів Київської області. В перспективі доступ до електронно фонду архівних документів залучать усі центральні та обласні державні архіви [5].

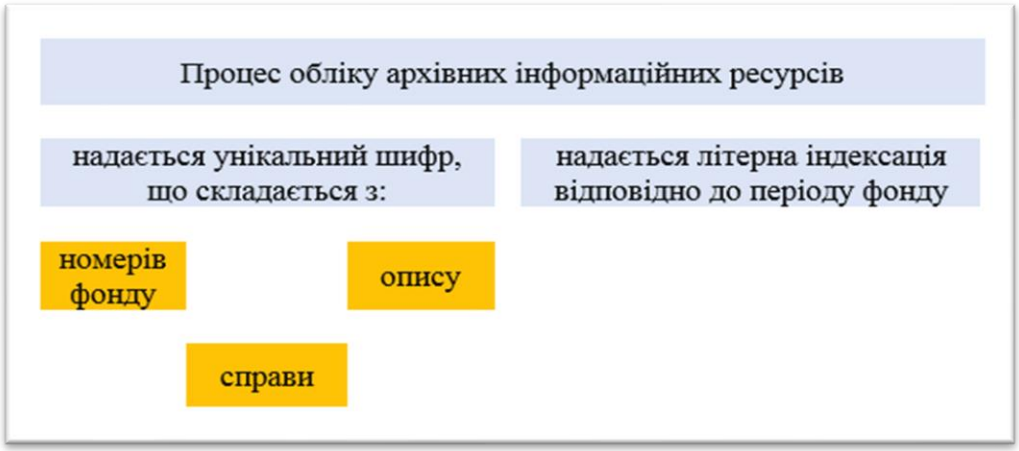


Рисунок 2.5 – Процес облікування справ, описів, фондів та надання відповідної нумерації та індексації

Організація колекцій оцифрованих архівних документів відбувається за принципами архівознавства. Документи в архівах упорядковані у фонди та колекції за принципом логіки. Фонд містить систематизовану документацію, створену в процесі діяльності фондоутворювача – установи, організації, підприємства або особи. Колекції складаються з тематичних документів. У межах фондів / колекцій архівні документи розділені на описи. Вони поєднують групи справ, організовані за тематичним, хронологічним чи іншими критеріями. Одиницею зберігання є справа, яка містить як один документ, так і сукупність створену в процесі діловодства або об’єднану спільною темою.

Для ефективності пошуку в архіві справі надається унікальний шифр, що складається з номерів фонду, опису та справи. У центральних та державних

архівах областей номерам фондів надається літерація, що вказує тематичну або хронологічну приналежність фонду (див. рисунок 2.5).

«Міжархівний пошуковий портал» було реалізовано за допомогою компанії «Архівні інформаційні системи» та державними архівами (див. рисунок 2.6). Ресурс поєднує електронні документи державних архівів та тематичні колекції документів, розміщені на платформі «Archium». Пошук на порталі побудовано за морфологічним принципом, він має гнучкі та інтуїтивні налаштування. Пошукова система порталу охоплює повні тексти довідкового апарату з окремих архівних інформаційних ресурсів. В першу чергу це назви фондів, історичні довідки, анотації до фондів та описів, заголовки справ і документів, а також покажчики, що є аналогами традиційних архівних каталогів.

Рисунок 2.6 – Потенційні можливості адміністрування «Міжархівного пошукового порталу»

Портал об'єднує електронні архівні інформаційні ресурси і тематичні цифрові колекції документів на платформі «Archium» в єдиний пошуковий простір архівів (див. рисунок 2.6). Пошукова система має гнучкі налаштування, підтримує морфологічний аналіз і дозволяє шукати за повними текстами довідкової інформації з локальних архівних ресурсів. Зокрема, можна здійснювати пошук за назвами фондів, історичними довідками, анотаціями фондів та описів, заголовками справ і документів, позиціями покажчиків, які виконують функцію традиційних архівних каталогів.

Цифрова платформа «Archium» призначена для реалізації проєктів електронного архіву. Цей програмний комплекс дає змогу створювати та оприлюднювати документальні онлайн-колекції, формувати масштабні електронні архівні інформаційні ресурси для державних архівів (див. рис. 2.6).

«Archium» має п’ятиступеневу ієрархічну структуру контенту з гнучкими налаштуваннями, підтримує введення та представлення описових і структурних метаданих, а також оснащена багатофункціональним інтерфейсом для перегляду цифрових зображень. Вона пропонує широкі можливості для тегування, повнотекстовий пошук із розділенням результатів за типами метаданих і тегів, а також зручний, інтуїтивний адміністративний інтерфейс для управління контентом, автоматизації введення даних, управління користувачами та доступом (Додаток Г).

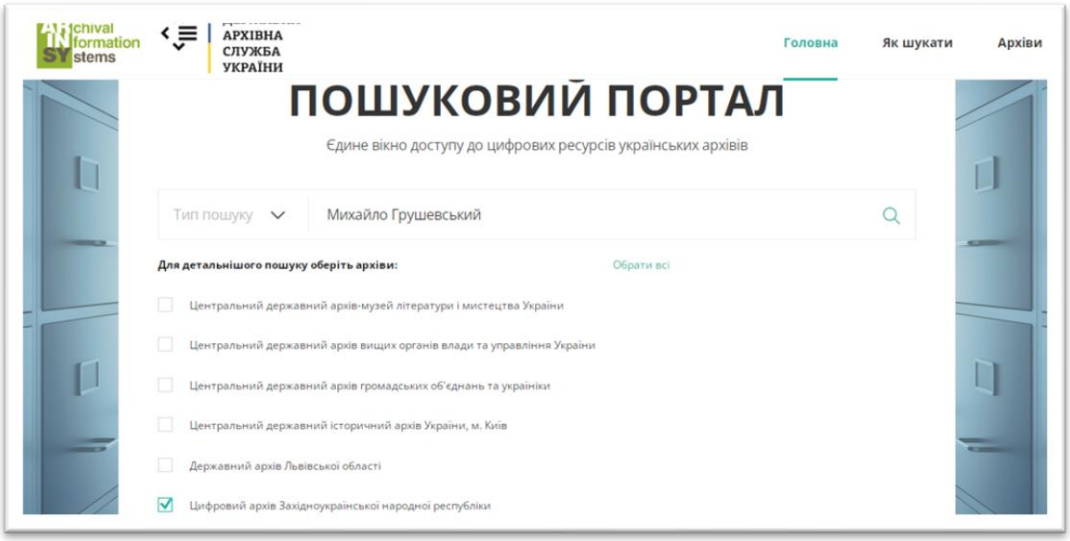


Рисунок 2.7 – Робота в меню пошукової системи «Міжархівного пошукового порталу» (Додаток Д)

Для здійснення пошуку необхідно обрати на головній сторінці архівний інформаційний ресурс із запропонованого переліку (див. рисунок 2.7). Пошук можна здійснювати по доступному повнотекстовому контенту і по заголовках оцифрованих справ на локальних архівних інформаційних ресурсах (Додаток Г).

Після вибору параметрів за допомогою ключових слів здійснюється пошук, а результати відображаються окремими вкладками фондів, описів, справ,

документів та покажчиків. Результати пошуку можливо відфільтрувати за архівом / колекцією або за оцифрованою справою (див. рисунок 2.8).

Окрім загальної пошукової системи «Міжархівного пошукового порталу», пошук можна здійснити на локальному архівному інформаційному ресурсі на який можна перейти за покликанням з наданого результату пошуку або безпосередньо зі сторінки «Архіви» скориставшись покликанням e-resource.

Рисунок 2.8 – Результати видачі пошукової системи «Міжархівного пошукового порталу» (Додаток Д)

За два роки роботи до центральних державних архівів – перших учасників проєкту, долучились три державних архіви – Кіровоградської, Львівської, Полтавської областей. Так, у 2023 р. працівники обласного Державного архіву Полтавської області оцифрували 4 млн 200 аркушів паперових документів, які успішно було оприлюднено за допомогою пошукової системи. Цей державний архів став лідером серед учасників проєкту «Міжархівного пошукового порталу» серед обласних державних архівів [51].

У 2024 р. Державний архів Кіровоградської обласні став третім архівом серед обласних архівів України та приєднався до проєкту архівної пошукової системи як восьмий учасник. Завдяки співпраці з американською корпорацією FamilySearch International з 2022 р. було оцифровано понад ста тисяч справ і близько шість з половиною мільйонів сторінок генеалогічних документів. Це

дало змогу значно наповнити електронний ресурс архіву, додавши майже триста тисяч цифрових документів [30].

Навколо «Міжархівний пошуковий портал» відбувається методологійний дискурс, обговорюється інтеграція державних архівів на публічному рівні, що передбачає представлення оцифрованих документів та впровадження потужного інструменту для повнотекстового пошуку. Другою складовою цієї інтеграційної платформи стане адміністративний інтерфейс для управління порталом, який дозволить вирішувати управлінські завдання для Укрдержархіву та державних архівів. Це включає інтеграцію облікових даних та статистики, що дасть змогу ефективно планувати на основі звітності, в результаті чого паперові звіти стануть минулим. «Наша наступна мета – реалізувати цю частину проекту, що суттєво підвищить ефективність внутрішньої роботи архівів та архівної служби», – говорить А. Хромов в інтерв'ю Ukrainer [65].

Отже, онлайн-сервіс «Міжархівний пошуковий портал» має амбітні цілі поєднати електронні архівні інформаційні ресурси усіх державних архівів у єдину пошукову мережу, щоби мільйони оцифрованих справ, мільярди електронних копій архівних документів стали доступними будь-якому користувачеві архівної інформації. Окрім документних інформаційних ресурсів архівістами планується залучення до пошукової системи «Міжархівного пошукового порталу» приватні колекції документів та музейні колекції. Прикладом є тематичні колекції документів штабу райхсляйтера Розенберга або архів Західноукраїнської Народної Республіки.

2.3. Розширення доступу до архівної інформації

Цифровий фонд документів Національного архівного фонду формується шляхом оцифрування аналогових архівних інформаційних ресурсів з різних носіїв і є ключовим аспектом цифровізації архівної справи в Україні. На сьогодні в державних архівних установах, які підпорядковані Державній архівній службі України, активно проводиться робота з уніфікації та оптимізації всіх процесів, пов'язаних із функціонуванням цього фонду. Якщо архівні інформаційні ресурси

на паперовому носії мають цілком зрозумілі інструментальні та методичні алгоритми дії, то оцифрування аудіовізуальних архівних документів вимагає залучення більш складних видів цифрових інструментів і методологічних моделей.

Процес роботи з аудіовізуальними документами Національного архівного фонду має враховувати специфіку архівної діяльності з різними аналоговими документними носіями. Науково-методичне забезпечення оцифрування здійснюється через методичні рекомендації, розроблені науковими працівниками Українського науково-дослідного інституту архівної справи та документознавства [78]. Це є основним результатом спеціальної прикладної науково-дослідної роботи, яка продовжує галузеві дослідження у сфері організації цифрового фонду документів НАФ [10].

Для прискорення діджиталізації архівних установ та введення у соціальний електронний обіг архівні інформаційні ресурси Державна архівна служба України затвердила наказом № 165 від 29.12.2021 р. «Програму оцифрування архівних інформаційних ресурсів на 2022-2025 роки» (далі – Програма цифрування) [64]. До Програми оцифрування залучені усі центральні державні архіви, державні архіви областей, архів місті Києва, а також низка галузевих державних архівів.

На сьогодні на зберіганні в центральних та обласних державних архівах перебуває більше восьмидесяти шести мільйонів архівних справ збережених на паперовому носії. За видами це інформаційні ресурси з паперовим носієм, кінодокументи, фотоокументи та фонодокументи, що залучені до Національного архівного фонду і за хронологією охоплюють період від XIII до XXI століть.

Головною метою Програми оцифрування є забезпечення вільного доступу до архівних інформаційних ресурсів і покращення якості архівних послуг. Програма визначала графік кількісних показників для оцифрування архівних ресурсів (од.зб./од.обл., файли, описи) за видами оцифрування увійшли архівні документи на паперових носіях – науково-технічна документація, документи особового походження, а також аудіовізуальні документи.

Програма була розроблена на основі аналізу досягнень і практик державних архівів за останні роки, а також врахування людських, технічних і фінансових ресурсів (Додаток Е). У той же час було виявлено, що оцифрування архівних документів має як значні переваги, так і певні недоліки. Переваги включають зручність і швидкість копіювання без втрати якості; можливість необмеженого тиражування копій; простота організації доступу до інформації та створення ієрархічних структур; оцифрування в кольорі з достатньою роздільною здатністю зберігає оригінальний вигляд; тривале зберігання цифрових копій при перенесенні на нові носії; і використання алгоритмів стиснення для збереження в актуальних графічних форматах [2].

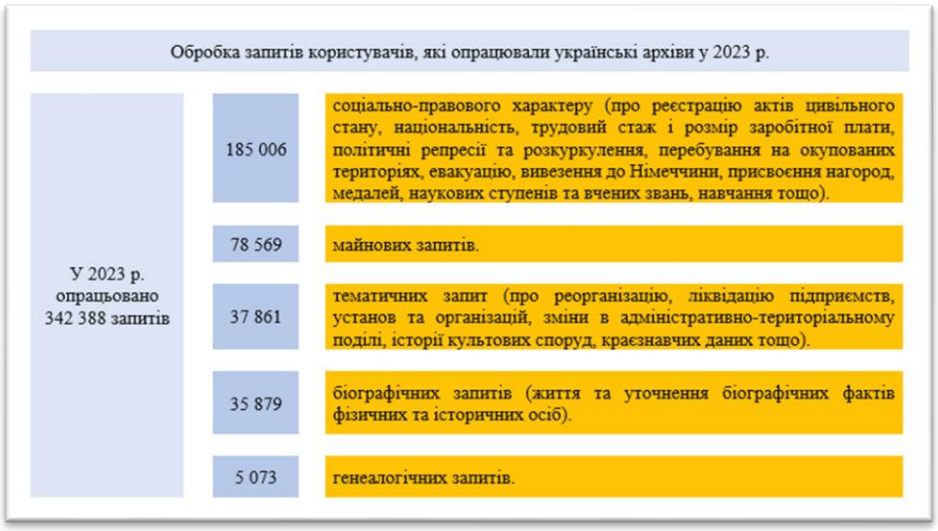


Рисунок 2.9 – Активність громадян із поданням запитів на соціально-історичну інформацію за минулий 2023 р.

Реалізація Програми є життєвоважливою для збереження соціально-історичної інформації та налагодження соціальної комунікації у суспільстві. Так, за 2023 р. українська архівна система отримала 342 388 запитів від користувачів архівної інформації (див. рисунок 2.9). Тільки розширення цифрового фонду користування зможе зробити архівну комунікацію автономізованою. Це зменшить завантаженість архівів соціальною роботою і дасть можливість переорієнтувати архівістів на виконання їх безпосередньої функції збереження культурної документної спадщини.

Розробка ефективної та надійної системи для зберігання, управління та доступу до цифрових копій документів є основною метою будь-якої стратегії оцифрування. Регулярне оновлення стратегії відповідно до технологічних новин і потреб організації є важливим (див. рисунок 2.10).

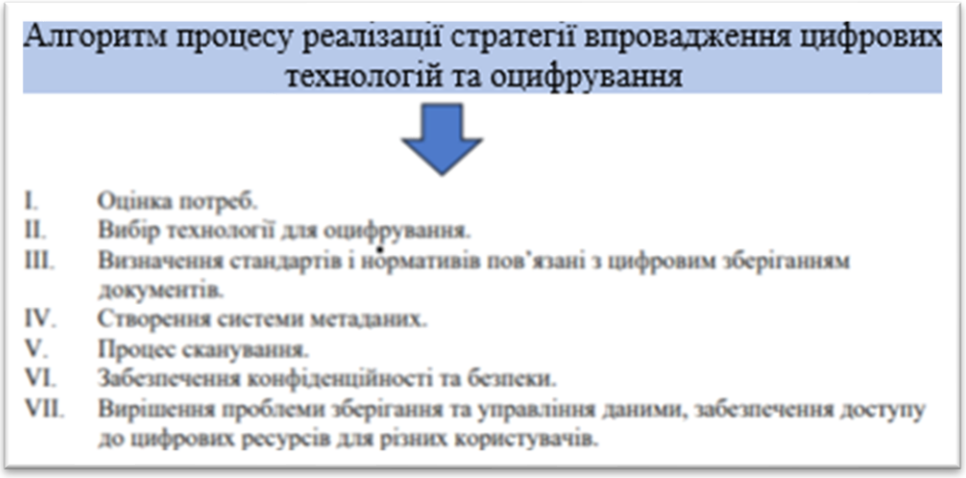


Рисунок 2.10 – Стратегія впровадження цифрових технологій та оцифрування документів

Нині оцифруванням архівних документів займаються не лише державні архіви. До них долучено Державний центр збереження документів Національного архівного фонду, Благодійний фонд «Меморіал Голокосту «Бабин Яр», Мукачівська греко-католицька єпархія та інші установи. Для прискорення цього процесу в червні 2020 р. Укрдержархів уклала меморандум про співпрацю з американською корпорацією FamilySearch International. Станом на кінець 2023 р. двадцять два державні архіви підписали угоди з FamilySearch International, що значно пришвидшило процес оцифрування архівів.

Виконання Програми оцифрування архівних інформаційних ресурсів супроводжується й процесом оприлюднення оцифрованих архівних документів . Оцифрування документів здійснюється за допомогою різних типів сканерів або цифрових фотокамер. До 2019 р. процес оцифрування архівних інформаційних ресурсів просувався повільно – державні архіви оцифрували лише 207 221 документів та 58 537 описів справ. Ковідні соціальні обмеження на комунікацію, пересування і активне соціальне життя поставило питання удоступнення архівної інформації. З поширенням масштабів російсько-української війни у

2022 р. темпи оцифрування державних архівів починають значно зростати. Для архівістів стає зрозуміли, зберегти паперові документи від вогню війни можна тільки оцифрувавши їх і забезпечивши цифровий доступ до електронних архівних ресурсів.

У період 2022-2023 темпи оцифрування архівних інформаційних ресурсів зросли – 843 667 архівних документів, а також 60 953 описи справ (див. рисунок 2.11). Так, у 2023 р. архіви оцифрували 586 762 документів, а це в 15 разів більше 2018 року, коли в електронний формат було переведено лише 904 одиниць зберігання. Загалом на початок 2024 р. оцифровано 1 414 000 документів і 167 000 описів [76].

Рисунок 2.11 – Динаміка оцифрованих архівних документів НАФ

Станом на 1 січня 2024 р. держархіви оцифрували 3,5 % архівних документів і 47 % описів справ Національного архівного фонду, що зберігаються в семи центральних державних архівах України та 25 обласних державних архівах, включно з Києвом (див. рисунок 2.11). Центральні державні архіви, які на відміну від обласних знаходяться під прямими адмініструванням Державної архівної служби України, оцифрували 8,8 % документів Національного архівного фонду та майже 80 % описів справ.

На жовтень 2024 р. для відвідувачів офіційного вебпорталу Державної архівної служби України доступно в Міжархівному пошуковому порталі 10 млн. електронних копій архівних інформаційних ресурсів, які охоплюють дев’ять

тематичних документальних комплексів (рис. 2.12). Зокрема, це фонди Центрального державного архіву вищих органів влади та управління України, Центрального державного історичного архіву України в Києві та Центрального державного історичного архіву України у Львові, Центрального державного архіву громадських об'єднань та україніки, Центрального державного архіву-музею літератури і мистецтва України, а також державних архівів Кіровоградської, Львівської та Полтавської областей, архіву ЗУНР та інших [45].

Рисунок 2.12 – Архіви з найбільшою кількістю оцифрованих документів НАФ станом на 01.10.2024 р.

В оцифруванні архівних інформаційних ресурсів надскладним є диджитадізація аудіовізуальних документів, що вимагає специфічного підходу та інструментарію. Методика створення цифрових копій аудіовізуальних документів передбачає точне і повне відтворення оригіналу і детально опрацьована у методичних рекомендаціях УНДІАСД [78]. Результатом процесу оцифрування аудіовізуального документа аналогового формату є оригінальна цифрова копія, яка виготовляється безпосередньо з оригіналу в найвищій доступній якості. Ця копія слугує вихідним матеріалом для створення майстер-копії документа. Відповідно, якісні технічні характеристики отриманої оригінал-копії не можуть бути нижчими за ті, що встановлені для створення майстер-копії [10].

Цифровізація аналогових архівних інформаційних ресурсів аудіовізуального характеру, незалежно від носіїв (паперових, аудіовізуальних, електронних), в результаті має електронний файл у визначеному форматі. Цей файл може містити інформацію у вигляді зображення, звуку або відео. Копії оцифрованих аналогових документів стають аудіовізуальними документами в цифровій формі, що дозволяє державним архівам працювати з ними за моделлю, призначеною для цифрових аудіовізуальних матеріалів [10].

У рамках пілотного проєкту впровадження системи «Еларсис» було реалізовано стандартні технологічні процедури для приймання та передачі архівних електронних справ та документів Національного архівного фонду. Ці процедури охоплюють архівні підрозділи вищих органів державної влади, міністерств, інших центральних органів виконавчої влади, а також державних установ, зокрема на прикладі архіву Міністерства юстиції України. Також було розроблено програмні засоби для опрацювання уніфікованих форматів інформаційних об’єктів, на підставі яких здійснюється приймання електронних документів на постійне зберігання. Ці дії сприяють формуванню єдиної системи архівного документообігу в Україні [66].

Крім того, в проєкті впроваджено технологічні рішення для зберігання та захисту інформації архівних електронних документів у системі архівного документообігу. Розроблено також інтеграційні, програмні та інтерфейсні рішення, що забезпечують авторизований доступ до архівних електронних документів і метаданих для працівників архівних установ України. Ці рішення реалізуються відповідно до принципу походження документів і вимог щодо їх обліку, зокрема в Центральному державному архіві вищих органів влади та управління України. Завдяки цьому, фахівці отримують можливість більш ефективно взаємодіяти з архівними даними [66].

Останнім етапом стало впровадження інтеграційного рішення для обміну документами між архівними підрозділами державних органів, органів місцевого самоврядування та підприємств. На прикладі архіву Міністерства юстиції України та Центрального державного архіву вищих органів влади, було

налагоджено співпрацю з Системою архівного електронного документообігу (САЕД). Цей підхід не лише покращує обробку документів, але й забезпечує їх надійне зберігання та захист. В результаті реалізації проєкту вдалося досягти значних покращень у сфері архівного документообігу в Україні [66].

У межах пілотного проєкту було підтверджено, що система «Еларсис» ефективно виконує всі нормативно визначені технологічні процедури для приймання та передачі архівних електронних справ і документів. На основі отриманих результатів проєкту були підготовлені пропозиції щодо внесення змін до нормативно-правових документів, які регулюють роботу з електронними документами та їх подальшу передачу на постійне архівне зберігання [66].

Для покращення процесів приймання та передачі електронних архівних документів було оновлено систему електронного документообігу Укрдержархіву до актуальної версії. Це оновлення має на меті оптимізувати бізнес-процеси, що сприятиме внесенню коректних змін до нормативних документів, які регламентують приймання та передачу архівних електронних документів на постійне зберігання [66].

Отже, затверджена Державною архівною службою України «Програма оцифрування архівних інформаційних ресурсів на 2022-2025 роки» регулює процес оцифрування архівних інформаційних ресурсів та їх подальше оприлюднення в Україні. Незважаючи на складні умови війни, ця програма продовжує працювати. На сьогодні можна констатувати, що план заходів Програми з оцифрування виконується і навіть перевиконується за рахунок залучення донорських і партнерських послуг закордонних і вітчизняних громадських організацій в архівної сфери. Програма має на меті забезпечити безперешкодний доступ до архівних ресурсів і підвищити якість архівних послуг для потреб користувачів.

РОЗДІЛ 3
ВДОСКОНАЛЕННЯ ЗАХИСТУ АРХІВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ

3.1. Реалізація систем захисту архівних інформаційних ресурсів

Основними компонентами інформаційної безпеки держави є: обсяг інформаційних продуктів, вироблених у країні та державі; здатність мереж витримати зростаюче навантаження на інформацію; здатність держави контролювати розвиток виробництва та розповсюдження інформації; і відкритість для громадян усі можливих інформаційні ресурси. Саме тому важливо забезпечити правильне адміністрування доступу до критично-важливої інформації без негативного впливу на буття держави.

Згідно зі ст. 9 Закону України «Про доступ до публічної інформації», інформація в документах органів державної влади, що стосується внутрішньовідомчої службової кореспонденції, може бути класифікована як службова [18]. До таких документів належать доповідні записки та рекомендації, якщо вони стосуються розробки напрямів діяльності установи або реалізації контрольних та наглядових функцій органами державної влади, а також процесів ухвалення рішень.

Порядок діловодства з документами, що містять інформацію з обмеженим доступом, регулюється підзаконним нормативно-правовим актом — постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736. Цією постановою затверджено Типову інструкцію про порядок обліку, зберігання, використання та знищення документів та інших матеріальних носіїв, що містять службову інформацію [45].

У нинішніх умовах воєнного стану, запровадженого через агресію рф проти України та повну воєнну мобілізацію економіки, питання роботи з інформацією службового характеру та її захисту набувають особливої важливості для органів місцевого самоврядування та військових адміністрацій. Зазвичай військові адміністрації створюються в громадах, що знаходяться в зоні бойових дій або під

окупацією. Головним завданням військових адміністрацій є захист прав та інтересів громадян у найбільш уражених збройною агресією районах, що вимагає тісної співпраці з військовим командуванням.

Згідно Інструкції № 736, в адміністрації повинна бути створена постійно діюча комісія з питань роботи із службовою інформацією, положення та склад якої слід затвердити розпорядженням керівника адміністрації [45]. З огляду на особливості діяльності військової адміністрації, можна розглянути можливість створення кількох комісій за напрямками діяльності установи.

Якщо у військовій адміністрації відсутній структурний підрозділ з діловодства або документаційного забезпечення, відповідальність за роботу з документами, що містять службову інформацію, покладається на визначену керівництвом посадову особу. Під час затвердження інструкції з діловодства, положення про структурні підрозділи та посадові інструкції в рамках тимчасової структури виконавчих органів місцевої ради мають визначати, що відповідні обов'язки закріплюються за відповідними структурними підрозділами або посадовими особами.

Внутрішньовідомча службова кореспонденція включає будь-який документ, незалежно від його назви чи реквізитів, підготовлений працівником суб’єкта владних повноважень і адресований працівнику або підрозділу цього ж суб’єкта. Обмін документами з іншим суб’єктом владних повноважень або з фізичними чи юридичними особами не є «внутрішньовідомчою» кореспонденцією. Важливо, щоб цей документ мав службовий характер, тобто був пов’язаний із виконанням функцій суб’єкта владних повноважень.

Під «відомством» слід розуміти центральний апарат органу влади та його територіальні відгалуження (див. рисунок 3.1). Документи, що можуть містити службову інформацію, зазвичай створюються перед публічним обговоренням або прийняттям рішення, і після цього втрачають статус службової інформації. Наприклад, підготовка проєкту нормативно-правового акту може включати розробку концепції, збір пропозицій від структурних підрозділів, складання

першого тексту, обмін службовими записками та надання доручень керівництва щодо змісту і строків підготовки.

Документи втрачають статус «для службового користування» після публічного обговорення або прийняття нормативно-правового акту. Ст. 9 Закону України «Про доступ до публічної інформації» також дозволяє віднести до службової інформацію, отриману в ході оперативно-розшукової, контррозвідувальної діяльності чи у сфері оборони, якщо вона не є державною таємницею [18]. Однак відповідність цим критеріям не гарантує автоматичного надання статусу «службової» — така інформація може вважатися службовою лише після проведення «трискладового тесту», що підтверджує підстави для обмеження доступу.

Рисунок .3.1 – Характеристики службової інформації

Будь-яка інформаційна технологія включає наступне: створення даних, оброблення, зберігання та передачу. Для забезпечення безпеки необхідно забезпечити надійну роботу всіх компонентів системи. З цієї точки зору головною метою діяльності в галузі інформації є створення повністю відкритої інформаційної бази.

Допуск посадових осіб до електронних документів з грифом «для службового користування» є важливою складовою управлінської діяльності та

забезпечення інформаційної безпеки в органах державної влади (див. рисунок 3.2). Ці документи містять інформацію, яка може бути чутливою або важливою для виконання службових обов’язків, тому їх доступність регулюється спеціальними нормами.

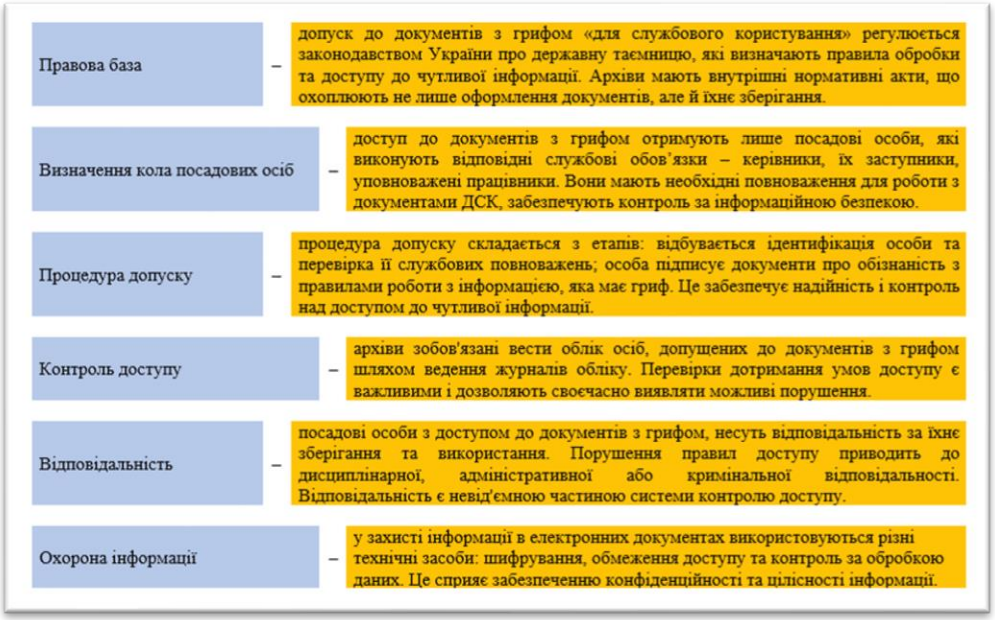


Рисунок 3.2 – Основні аспекти допуску посадових осіб до документів з грифом ДСК

В цілому, допуск посадових осіб до електронних документів з грифом «для службового користування» є складовою системи управлінської безпеки, що забезпечує ефективне виконання службових функцій та захист архівних інформаційних ресурсів від несанкціонованого доступу (Додаток Ж).

Економічний потенціал країни є одним із ключових чинників національної безпеки, що включає як матеріальні, так і духовні сили суспільства, а також здатність держави мобілізувати ці сили для захисту своїх інтересів. Інформація архівних ресурсів відіграє важливу роль у всіх сферах людської діяльності, сприяючи підвищенню цього потенціалу шляхом зростання матеріальних і духовних сил суспільства. Вона також створює умови для координації і мобілізації архівних інформаційних ресурсів, необхідних для ефективної діяльності країни.

Крім того, архівна інформація формує як матеріальні, так і інтелектуальні ресурси, що є критично важливими для надійного захисту від агресивних дій

інших держав у інформаційному просторі. Завдяки організованому захисту архівних інформаційних ресурсів країна може краще протистояти зовнішнім загрозам і забезпечувати свою безпеку. Отже, збереження та розвиток інформаційного потенціалу української архівної системи є важливими для підтримки національної стабільності.

Отже, головним завданням заходів із забезпечення безпеки архівних інформаційних ресурсів з грифом ДСК є мінімізація можливої шкоди, що може виникнути через неповноту, несвоєчасність або недостовірність інформації. Це також включає захист від негативного інформаційного впливу та наслідків, пов’язаних із функціонуванням інформаційних технологій. Надійні заходи безпеки допомагають попередити несанкціоноване розповсюдження службових даних, що може призвести до витоків конфіденційної інформації. У сучасному світі, де інформація є одним із найважливіших ресурсів, захист її достовірності та доступності стає пріоритетом, а інформаційна безпека сприяє стабільності та надійності всіх аспектів роботи з службовими даними.

3.2. Організаційно-нормативні заходи кібербезпеки архівних інформаційних ресурсів

Інформаційні технології мають важливі складові: генерацію інформації, її обробку, зберігання та використання. У контексті безпеки важливо гарантувати стабільну роботу всіх елементів цієї системи. Якщо розглядати проблему з цієї точки зору, основна мета інформаційної діяльності полягає в створенні якісного відкритого інформаційного простору.

Важливим фактором впровадження державної інформаційної політики є розвиток розгалуженої і захищеної інформаційної інфраструктури. Невід'ємною її складовою є стратегічні архівні інформаційні ресурси, що мають велике значення в умовах інформаційної війни та розвитку інформаційного ринку. Згідно з Законом України «Про Концепцію національної програми інформатизації», до інформаційної інфраструктури відносяться: міжнародні та міжміські телекомунікаційні та комп'ютерні мережі, системи інформаційно-

аналітичних центрів, інформаційні ресурси, інформаційні технології, науково-дослідні установи, що займаються проблемами інформатизації, а також виробництво і обслуговування технічних засобів інформації та система підготовки кваліфікованих кадрів у сфері інформатизації [23].

Інформаційна інфраструктура складається з низки елементів до яких відносяться системи виробництва інформаційних продуктів, доставки їх до споживачів, виробництва засобів виготовлення інформаційних продуктів, створення інформаційних технологій, накопичення та зберігання інформаційних ресурсів [72].

Загрози для безпеки інформаційно-телекомунікаційних систем можуть надходити як від урядових структур, так і від інших організацій. Це включає незаконне збирання та використання даних, вразливість технологій обробки інформації, додавання компонентів з несанкціонованими функціями в апаратне або програмне забезпечення. До того ж, створення шкідливих програм може порушувати роботу систем захисту, а також призводити до пошкодження або знищення пристроїв для обробки даних, телекомунікаційного обладнання та каналів зв’язку.

Додатково, існують ризики, пов'язані з втручанням у парольно-ключові системи, компрометацією засобів криптографічного захисту, витоками даних через технічні канали, перехопленням інформації, особливо у приміщеннях державних установ. Також для бізнесу це можуть бути проблеми крадіжки або руйнування інформаційних носіїв, перехоплення та підробки даних у мережах, несанкціонований доступ до баз даних та використання сумнівних іноземних технологій в інфраструктурі.

Важливим кроком у вирішенні проблем інформаційної безпеки є ідентифікація загроз і аналіз заходів захисту від них. Загрози інформаційній безпеці можуть проявлятися у вигляді дій чи впливу негативних факторів, через які соціальні об'єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері. Такі загрози також

можуть порушувати нормальне функціонування, спричиняти руйнування або стримувати розвиток технічних об’єктів інформаційної безпеки.

Загрози для інформаційно-телекомунікаційних систем в Україні можуть включати протиправне збирання та використання даних, порушення технологій обробки інформації, впровадження в апаратне та програмне забезпечення несанкціонованих компонентів, які виконують непередбачені функції. До цього також належать розробка і поширення шкідливих програм, які порушують роботу систем, особливо засобів захисту інформації, а також знищення, пошкодження чи радіоелектронне пригнічення засобів обробки інформації, телекомунікацій та зв'язку. Загрози можуть впливати на парольно-ключові системи, призводити до компрометації ключів і засобів криптографічного захисту, витоку інформації через технічні канали, перехоплення даних за допомогою електронних пристроїв, зокрема у службових приміщеннях органів влади та підприємств [72].

Крім того, ризики включають крадіжку або руйнування носіїв інформації, перехоплення та дешифрування інформації у мережах передачі даних, а також нав'язування помилкової інформації. Використання несертифікованих технологій, засобів захисту та телекомунікації також становить загрозу, як і несанкціонований доступ до банків даних та порушення законодавчих обмежень щодо поширення інформації.У сучасному інформаційному суспільстві розвиток систем захисту даних і технологічної безпеки комунікацій має вирішальне значення. Надійний захист інформації запобігає незаконному доступу та втраті даних. Ефективні технології безпеки сприяють стабільній роботі інформаційних систем і забезпечують довіру до комунікаційних процесів [72].

Процес посилення заходів захисту та вдосконалення технологічної безпеки у сфері комунікацій ґрунтується на декількох ключових напрямках та тенденціях (див. рисунок 3.3). Перш за все, кібербезпека стає пріоритетом у зв’язку з постійно зростаючими загрозами, які вимагають ефективних заходів для захисту від кібератак, зловживань та несанкціонованого доступу до інформації.

Відповідні ініціативи спрямовані на створення більш надійних механізмів захисту даних.

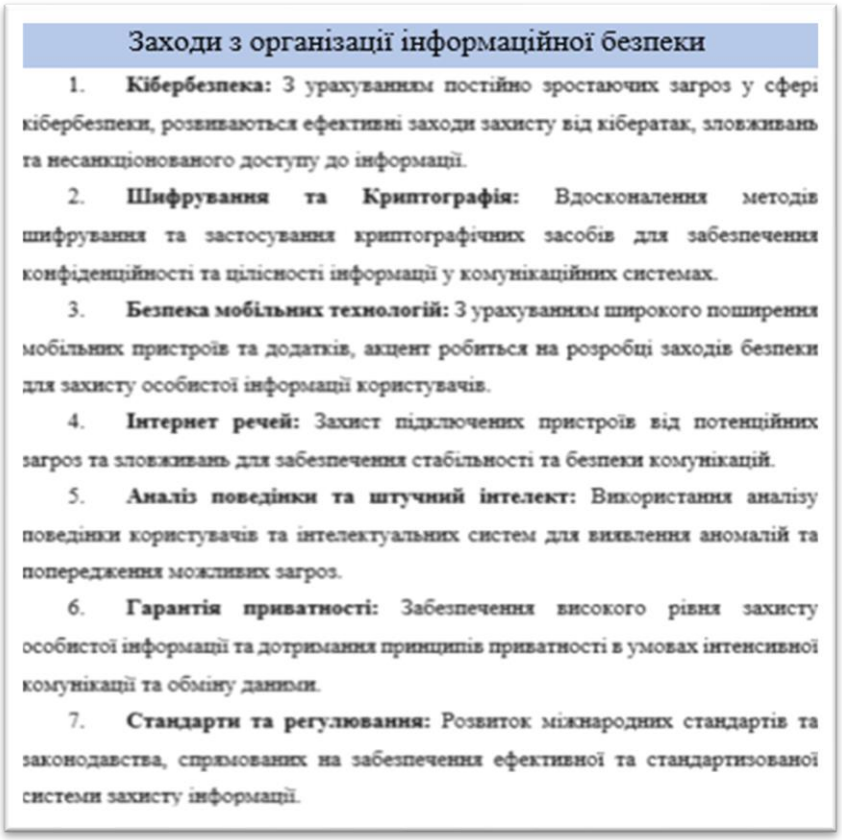


Рисунок 3.3 – Заходи з організації інформаційної безпеки в державних архівних установах

Наступним важливим аспектом є шифрування та криптографія, які вдосконалюються для забезпечення конфіденційності та цілісності інформації в комунікаційних системах. Використання сучасних методів шифрування допомагає запобігти витоку даних та гарантує безпеку передачі інформації. Розробка нових криптографічних протоколів також сприяє підвищенню рівня захисту (Додаток К).

Безпека мобільних технологій набуває все більшого значення через широке поширення мобільних пристроїв та додатків. Особливу увагу приділяють розробці заходів безпеки, які захищають особисту інформацію користувачів на цих платформах. Це включає в себе як апаратні, так і програмні рішення для запобігання несанкціонованому доступу.

Захист Інтернету речей є ще одним критично важливим напрямком, оскільки кількість підключених пристроїв зростає. Забезпечення безпеки цих пристроїв від потенційних загроз та зловживань допомагає підтримувати стабільність комунікацій. Створення ефективних механізмів контролю та захисту даних у цій сфері є необхідним кроком до зниження ризиків.

Аналіз поведінки користувачів та впровадження штучного інтелекту використовуються для виявлення аномалій і запобігання можливих загроз. Ці технології дозволяють системам швидко реагувати на незвичайну активність та вчасно вживати заходів безпеки. Застосування таких інновацій допомагає підвищити загальний рівень захисту інформаційних систем.

Гарантія приватності також залишається важливим аспектом у сучасних комунікаціях. Забезпечення високого рівня захисту особистої інформації користувачів, а також дотримання принципів приватності є критично важливими у контексті інтенсивного обміну даними. Установлення відповідних стандартів і протоколів допоможе зберегти довіру користувачів.

Нарешті, розвиток міжнародних стандартів та регулювання у сфері інформаційної безпеки забезпечує ефективну та стандартизовану систему захисту. Важливо, щоб ці стандарти відповідали сучасним викликам і вимогам, які постають перед організаціями. Згуртовані зусилля на міжнародному рівні сприятимуть зміцненню захисту даних у всьому світі.

Застосування міжнародних стандартів, як-от ISO/IEC 27001, допомагає слідувати найефективнішим практикам захисту інформації. Ліцензування та сертифікація спеціалістів із кібербезпеки підвищують їхню кваліфікацію та відповідальність в межах організації. Важливо також мати нормативні документи, що регламентують порядок дій у разі виникнення інцидентів чи загроз.

ISO/IEC 27001 — це міжнародний стандарт, що визначає вимоги до створення, впровадження, підтримки та вдосконалення системи управління інформаційною безпекою (далі – СУІБ). Він був розроблений Міжнародною організацією зі стандартизації (далі – ISO) та Міжнародною електротехнічною

комісією (далі – IEC) з метою захисту конфіденційності, цілісності та доступності інформаційних ресурсів організацій (див. рисунок 3.4). Цей стандарт надає універсальний підхід до управління ризиками інформаційної безпеки, адаптований для організацій різного масштабу та галузей.

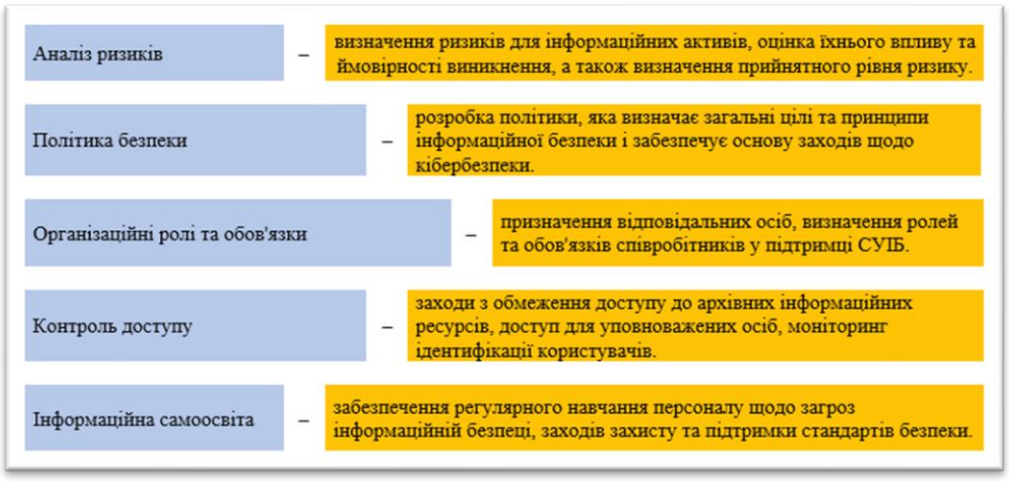


Рисунок 3.4 – Основні положення стандарту ISO/IEC 27001 в системі кіберзахисту архівної установи

Процес впровадження СУІБ за стандартом ISO/IEC 27001 складається з планування, виконання, перевірки та вдосконалення системи, відомого як цикл PDCA (Plan-Do-Check-Act). Організації, які відповідають вимогам цього стандарту, можуть пройти сертифікацію, яка підтверджує їх відповідність найвищим вимогам інформаційної безпеки. ISO/IEC 27001 забезпечує структурований підхід до управління інформаційними ризиками, що дозволяє організації зменшити ймовірність кіберзагроз, захистити конфіденційні дані й підвищити довіру до своїх інформаційних процесів.

Наведене дозволяє утворення стійких систем кіберзахисту, які здатні ефективно працювати в умовах високого ризику. Проте, незважаючи на переваги інформаційно-комунікаційних технологій, ефективне використання стикається із перешкодами які блокують потенціал цих технологій. На заваді стають проблеми слабкої телекомунікаційної інфраструктури, низького рівня цифрової грамотності та обмеженої обізнаності про Інтернет.

Якщо в архівних установах є дозвіл на здійснення діяльності з технічного захисту інформації, то вони за згодою Державної служби спеціального зв’язку та

захисту інформації України можуть організовувати проведення державної експертизи комплексних систем захисту інформації. Ця експертиза охоплює інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи підприємств, установ і організацій, які підпорядковані відповідним органам. Для створення комплексної системи захисту державної інформації або інформації з обмеженим доступом використовуються засоби, які мають сертифікати відповідності або позитивні експертні висновки після державної експертизи. Проведення державної експертизи цих засобів і підтвердження їх відповідності проводяться відповідно до вимог законодавства.

Для мережевого захисту архівних інформаційних ресурсів варто використовувати міжмережеві екрани, що блокують зовнішні атаки та несанкціонований доступ до мережі. Важливо враховувати можливість впровадження неправдивої інформації в системи супротивника, що може спотворити дані для прийняття рішень. Це є формою інформаційної атаки, де інформація стає як метою, так і засобом нападу. Такі заходи є частиною загальної стратегії інформаційної безпеки для збереження конфіденційності, цілісності та доступності даних.

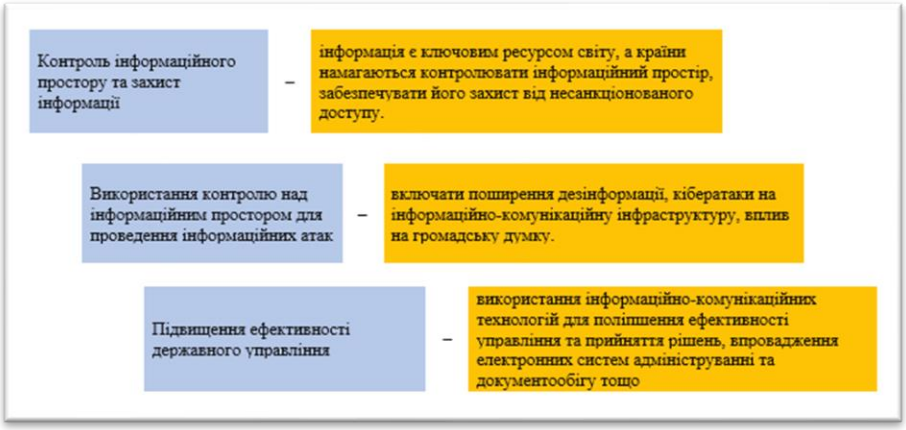


Рисунок 3.5 – Головні цілі інформаційної війни рф проти України

В умовах воєнних дій агресор використовує засоби інформаційної війни і ставить перед собою різноманітні цілі впливу, зокрема контроль інформаційного простору та захист власної інформації. Інформація є одним із ключових ресурсів, і країни прагнуть контролювати її, щоб запобігти несанкціонованому доступу.

Захист своєї інформації дозволяє зберегти безпеку, стабільність та конкурентну перевагу на міжнародній арені.

Контроль над інформаційним простором також дає можливість проводити інформаційні атаки (див. рисунок 3.5). Це може виражатися через поширення дезінформації, здійснення кібератак на критичну інфраструктуру інших держав та маніпулювання громадською думкою. Такі дії спрямовані на ослаблення противника та досягнення стратегічних переваг без прямого військового втручання.

Інформаційно-комунікаційні технології також використовуються для підвищення ефективності державного управління. Завдяки електронному урядуванню та іншим сучасним рішенням держави можуть покращити процеси управління і прийняття рішень. Ці інновації не лише сприяють прозорості та доступності, а й зміцнюють зв'язок між урядом та громадянами.

У контексті зростання випадків несанкціонованих дій з комп'ютерною інформацією в Україні стає важливим створення чіткої та ефективної системи захисту. Освіта та підвищення обізнаності користувачів щодо потенційних ризиків та способів захисту є ключовими аспектами. Кібербезпека стала невід'ємною частиною повсякденного життя, тому забезпечення безпечного використання технологій є спільною відповідальністю як окремих осіб, так і організацій. Цей процес включає не лише формальні заходи безпеки, але й активну участь фахівців у розробці та впровадженні стратегій захисту.

Дотримання основних правил безпеки, таких як уникнення відкриття підозрілих посилань і завантаження ненадійних файлів, є критично важливим для захисту інформації. Ефективні антивірусні рішення здатні запобігти небажаним вторгненням і зберегти конфіденційність даних. Для забезпечення надійного захисту організаціям слід провести детальний аналіз програмного забезпечення, щоб знайти найкращі рішення, які відповідають їхнім потребам. Це дозволить оптимізувати захист системи від вірусів та інших кіберзагроз.

Оцінка працездатності та ефективності різних продуктів безпеки включає тестування їх можливостей у реальних умовах використання. Також важливо

перевірити, як програмне забезпечення сумісне з іншими застосунками та обладнанням, яке вже використовується. Тільки за таких умов організації можуть бути впевнені в адекватності обраних рішень для захисту своїх інформаційних ресурсів. Таким чином, комплексний підхід до кібербезпеки забезпечить надійний захист від можливих загроз.

Отже, організаційні і нормативно-правові заходи кібербезпеки архівних інформаційних ресурсів спрямовані на створення умов для надійного захисту інформації в архівах. Організаційні заходи включають розробку політик доступу, що регламентують права і обов'язки співробітників у роботі з інформаційними ресурсами. Важливим аспектом є навчання персоналу правилам кібербезпеки, що допомагає мінімізувати людський фактор як можливий ризик для інформації. Регулярний аудит і контроль архівних систем дозволяють виявляти слабкі місця в системі безпеки та вчасно усувати їх. Крім того, створення команд для реагування на інциденти кібербезпеки забезпечує оперативну протидію загрозам.

3.3. Програмно-технічні заходи кібербезпеки архівних інформаційних ресурсів

Для захисту комп'ютерної інформації необхідно використовувати комплекс заходів, зокрема регулярно оновлювати операційну систему, встановлювати складні паролі та налаштовувати багатофакторну аутентифікацію. Важливими є також застосування антивірусного програмного забезпечення і ретельний підхід до вибору програм та застосунків. Такий підхід допомагає знизити ризик несанкціонованого доступу та забезпечити безпеку даних.

Комплекс організаційних засобів захисту інформації поділяється на фізичні та апаратно-програмні, що включають електричні, механічні, електромеханічні та електронні пристрої. Фізичні засоби зазвичай представлені у вигляді автономних систем, які забезпечують загальний захист об'єктів з обробки інформації. Апаратні засоби розміщуються безпосередньо у складі обчислювальної техніки, телекомунікаційних пристроїв чи інших апаратів із

стандартним інтерфейсом зв’язку. Програмні засоби охоплюють програмне забезпечення, що виконує функції захисту даних.

У процесі роботи з інформацією в органах влади було запропоновано кілька ключових напрямків для забезпечення її захисту (див. рисунок 3.6). Перш за все, необхідно впровадити технічні засоби безпеки, які забезпечать належний рівень захисту даних у організації. Це включає використання сучасних технологій для запобігання несанкціонованому доступу і витоку інформації.

Додатковим етапом є впровадження паролів для доступу до технічних і програмних засобів, що суттєво підвищить рівень безпеки. Паролі повинні бути достатньо складними, щоб ускладнити їхнє злому, а також періодично змінюватися для зменшення ризиків.

Окрім цього, варто запровадити використання кваліфікованих електронних підписів (КЕП) для всіх структурних одиниць організації. Це дозволить не лише захистити інформацію, але й підтвердити її цілісність і автентичність, забезпечуючи таким чином більш високий рівень довіри до документів та даних, що обробляються.

Процес шифрування інформації здійснюється за допомогою регулярно змінюваного коду ключа, що забезпечує унікальність представлення даних навіть при використанні одного й того ж алгоритму чи пристрою. Знання ключа дозволяє швидко та надійно розкодувати дані, що робить доступ до них простішим для авторизованих користувачів. Проте без ключа ця процедура може стати практично неможливою, навіть при використанні комп'ютерних систем.

Для покращення безпеки інформації була запроваджена система резервного копіювання, що значно знизила ризик втрати важливих даних. Це дозволяє підприємству зберігати критично важливу інформацію в надійному місці та швидко відновлювати її у разі необхідності. Також було проведено детальний аналіз антивірусного програмного забезпечення, щоб вибрати найбільш ефективні рішення для кожного персонального комп'ютера.

Впровадження системи криптографічного кодування інформації дозволило підприємству підвищити рівень захисту даних під час їх передачі. Ця технологія

забезпечує надійний захист від несанкціонованого доступу і зловживань, створюючи додаткові бар'єри для потенційних загроз. Криптографічні рішення стають дедалі важливішими у сучасному інформаційному середовищі.

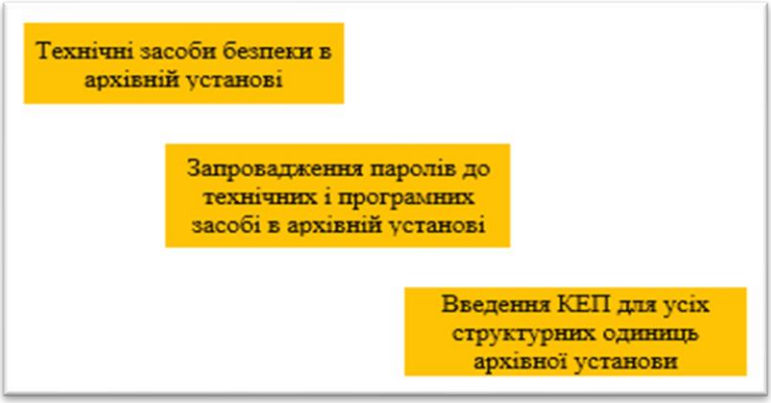


Рисунок 3.6 – Організація захисту архівних інформаційних ресурсів за основними напрямами

В результаті реалізації цих заходів підприємство забезпечило більш високий рівень захисту своїх інформаційних ресурсів. Це не лише підвищило довіру до системи, але й створило сприятливі умови для ефективної роботи з даними. Безперечно, регулярне оновлення та вдосконалення цих систем є необхідною умовою для підтримки безпеки інформації в умовах зростаючих загроз.

Технічне та програмне забезпечення для стійкої роботи державної архівної установи складається з системного інструментарію, що забезпечують ефективну обробку та функціонування інформації (див. рисунок 3.7). Комп’ютерне обладнання є важливим елементом для роботи членів ради та службовців. Забезпечення їх робочих місць якісними комп'ютерами, ноутбуками, моніторами та іншим необхідним обладнанням сприяє підвищенню продуктивності праці. Це дозволяє ефективніше виконувати завдання та обробляти інформацію.

Локальні мережі та інтернет-з'єднання грають важливу роль у забезпеченні стабільного доступу до інформаційних ресурсів (див. рисунок 3.7). Важливою складовою є забезпечення надійного підключення до Інтернету та внутрішніх локальних мереж архіву. Це дозволяє забезпечити безперебійну комунікацію та обмін інформацією між архівістами та користувачами архівної інформації.

Рисунок 3.7 – Технічне та програмне забезпечення роботи державної архівної установи

Офісні програми є важливим інструментом для обробки текстової інформації, створення електронних таблиць та презентацій. Вони також забезпечують організацію електронної пошти та планування календарних подій. Використання таких пакетів значно підвищує ефективність роботи в архівної установи. Завдяки їм архівісти можуть швидко і зручно виконувати різноманітні завдання.

Електронна система документообігу забезпечує зручність у обробці, зберіганні та обміні між працівниками Укрдержархіву та іншими архівними установами управлінськими документів. Використання таких систем значно спрощує адміністративні процеси, дозволяючи швидше реагувати на запити та потреби. Вони також підвищують ефективність управління документами, зменшуючи ризик їх втрати чи несанкціонованого доступу. Завдяки електронному документообігу, архівісти можуть легше співпрацювати та обмінюватися важливою інформацією [9].

Інформаційні системи для управління забезпечують ефективний облік і моніторинг різних аспектів діяльності державних архівних установ. Використання спеціалізованих програм дозволяє здійснювати бюджетування, планування розвитку та інші адміністративно-управлінські функції. Це значно спрощує процес прийняття рішень і підвищує прозорість в управлінні. Завдяки таким системам, архіви можуть більш ефективно організовувати свою роботу та досягати поставлених цілей.

Системи безпеки та захисту інформації забезпечують конфіденційність і цілісність даних через застосування антивірусного програмного забезпечення, фаєрволів та інших засобів захисту. Ці інструменти допомагають запобігти несанкціонованому доступу та атакам на архівні інформаційні ресурси. Впровадження таких заходів є критично важливим для підтримки безпеки даних архівів. Завдяки цим системам, інформація залишається захищеною від можливих загроз та втрат.

Технічна підтримка полягає в забезпеченні якісного обслуговування, яке включає оперативне вирішення проблем та регулярне оновлення програмного і апаратного забезпечення. Це дозволяє швидко реагувати на можливі неполадки та підтримувати стабільну роботу систем. Забезпечення технічної підтримки є важливим аспектом для ефективного функціонування архівних установ. Таким чином, організація може зосередитися на своїх основних завданнях, знаючи, що її технологічні рішення знаходяться в надійних руках.

Основна мета цього технічного та програмного забезпечення полягає в забезпеченні ефективної та безперебійної діяльності мережі державних архівних установ. Воно сприяє комфортній роботі та обміну інформацією між усіма учасниками інформаційно-комунікаційного процесу. Таке забезпечення дозволяє оптимізувати робочі процеси і підвищити продуктивність. Завдяки цьому, будь-яка державна архівна установа може краще виконувати свої функції та відповідати потребам громадян [9].

Вибір антивірусного програмного забезпечення для безпечної роботи комп'ютерів є ключовим елементом інформаційної безпеки державної архівної установи. Серед найбільш поширених і надійних антивірусних програм є Avast, AVIRA, NOD32 та інші (Додаток Л). Антивірусні програми виконують кілька ключових функцій для забезпечення безпеки (див. рисунок 3.8). Вони здійснюють планове сканування пам’яті та вмісту дисків, що дозволяє вчасно виявляти потенційні загрози. Крім того, ці програми сканують пам’ять комп’ютера, а також файли, що обробляються під час виконання різних операцій.

Автоматичне оновлення антивірусних баз через Інтернет гарантує, що система завжди захищена від нових вірусів і шкідливих програм.

Рисунок 3.8 – Відображення принципу функціонування антивірусного захисту

Впровадження антивірусної програми з криптографічним захистом інформації складається з кількох важливих етапів. Першим кроком є вибір відповідного антивірусного рішення, яке повинно відповідати вимогам користувача та характеристикам комп'ютерної системи. Це дозволяє забезпечити максимально ефективний захист від шкідливих програм і загроз. Успішний вибір програми є основою для подальшої реалізації заходів з кібербезпеки [24].

Наступним етапом є встановлення та налаштування обраної антивірусної програми на комп'ютер. Процес встановлення повинен включати налаштування параметрів, щоб забезпечити оптимальний рівень захисту. Правильна конфігурація програми допомагає запобігти можливим атакам і загрозам безпеці. На цьому етапі важливо враховувати специфіку системи та потреби організації.

Налаштування регулярного оновлення вірусних баз є критично важливим для ефективної роботи антивірусного захисту. Забезпечення постійного оновлення дозволяє програмі виявляти нові загрози та реагувати на них вчасно. Цей етап є невід’ємною частиною безпеки інформаційних систем, оскільки нові види вірусів з'являються постійно. Тому систематичне оновлення бази даних є ключовим моментом для підтримки захисту [24].

Використання криптографічних засобів забезпечує додатковий рівень захисту конфіденційної інформації. Шифрування даних і застосування

безпекових протоколів дозволяють захистити важливу інформацію від несанкціонованого доступу. Цей етап сприяє надійному збереженню даних, що особливо важливо в умовах зростаючих кіберзагроз (Додаток В). Включення криптографічного захисту робить систему більш стійкою до атак.

Останнім етапом є постійний моніторинг роботи антивірусної програми та криптографічних заходів. Систематичний контроль дозволяє швидко виявляти та вирішувати потенційні проблеми, що можуть виникнути в процесі роботи. Цей етап є важливим для підтримки високого рівня безпеки та забезпечення надійної роботи інформаційних систем.

Безпека інформації є безперервним процесом, тому регулярне оновлення та вдосконалення заходів захисту є критично важливими для забезпечення інформаційної безпеки. Постійний моніторинг і аналіз можливих загроз допомагають ідентифікувати вразливі місця системи. Для ефективного захисту необхідно адаптуватися до нових викликів у світі кібербезпеки. Це дозволяє не зберегти дані та підтримувати довіру користувачів до інформаційних систем [24].

Необхідно відзначити, що існує безліч засобів, які можуть бути використані для несанкціонованого доступу до інформації. Захист інформації від такого доступу охоплює діяльність, спрямовану на запобігання отриманню захищеної інформації особами, які діють в порушення установлених правовими документами або без дозволу власника інформації. Під системою захисту інформації розуміють комплекс органів і виконавців, технічних засобів, а також об'єктів, що підлягають захисту, які організовані і функціонують відповідно до правил, визначених правовими, організаційно-розпорядницькими та нормативними документами. Система захисту інформації є інтегрованою структурою, що поєднує різні елементи для забезпечення безпеки даних. Цей захист є критично важливим для підтримання конфіденційності і цілісності інформації. Зрештою, ефективна система захисту допомагає мінімізувати ризики несанкціонованого доступу та його негативні наслідки.

ВИСНОВКИ

Інформаційно-комунікаційна діяльність, яка сьогодні заполонила всі сфери суспільства, забезпечує швидку обробку та доступ до різних джерел інформації, відзначається відкритістю та доступністю будь-якої інформації, але в той же час її незахищеністю. Тема безпеки архівних інформаційних ресурсів в Україні є надзвичайно актуальною. Необхідно продовжувати дослідження в цій галузі, впроваджувати нові технології та підвищувати технічну обізнаність архівістів та користувачів. Лише спільними зусиллями можна забезпечити збереження національної культурної спадщини для майбутніх поколінь.

1. Інформація дедалі більше впливає на суспільні процеси, що підвищує їхню вразливість до інформаційного впливу. Вона може стати чинником, здатним спричинити масштабні аварії, військові конфлікти чи дезорганізувати державне управління. Аналіз питань інформаційної безпеки виявляє методологічні прогалини для аналізу інформаційно-технологічних загроз, пов’язаних з науково-технічним прогресом. Перелік залучених дефініцій, хоча й не є вичерпним, проте цілком задовольняє потребу в синхронізації розуміння проблеми їх застосування та повністю розкриває сутність процесу організації захисту архівних інформаційних ресурсів. Все це підкреслює важливість залучення досягнень науки та техніки до управління інформаційними ризиками задля стабільності та безпеки.

2. Основні напрями діяльності задля забезпечення інформаційної безпеки держави включають широкий спектр заходів. До них належать розвиток науково-практичних засад і створення законодавчої та нормативно-правової бази для захисту інформації. Крім того, це розробка концепції інформаційної безпеки, а також правових та організаційних документів, які підтримують збереження й розвиток інформаційних ресурсів. Формування правового статусу суб’єктів системи інформаційної безпеки та регулювання процесу ліквідації наслідків загроз є окремими важливими аспектами. У разі порушення інформаційної безпеки проводять заходи з відновлення прав і ресурсів та реалізуються

компенсаторні заходи. Також постійно вдосконалюються форми й методи для запобігання й нейтралізації загроз інформаційній безпеці, зокрема шляхом розвитку сучасних технологій захисту.

3. Нові види технологічних та інформаційних загроз, разом із складністю та різноманітністю сучасних інформаційно-телекомунікаційних систем вимагають науково-правового вирішення. Для ефективного захисту архівних інформаційних ресурсів необхідно розробити системний підхід, що базується на комплексному аналізі загроз. Це передбачає правове унормування розвитку методологічних, технологічних та організаційних основ для створення відповідних систем безпеки інформаційних технологій. Тоді можна врахувати аспекти, пов’язані із захистом даних, та в правовому полі ефективно протистояти новим викликам. Поглиблене дослідження у цій сфері допоможе розробити стратегії, що відповідатимуть сучасним вимогам безпеки. Це сприятиме збереженню цілісності та конфіденційності архівних інформаційних ресурсів.

4. Відкритий онлайн доступ до електронних архівних інформаційних ресурсів є важливим кроком у забезпеченні прозорості та підзвітності державних установ, сприяючи розвитку громадянського суспільства і демократичних принципів. Вебпортал Укрдержархіву, що містить електронні архівні інформаційні ресурси, дозволяє користувачам швидко отримувати доступ до важливих документів та даних, що підвищує ефективність їх використання. Завдяки інтеграції різних архівних онлайн проєктів, пошукових систем та баз даних, користувачі можуть знайти потрібну інформацію, що має соціокультурну та соціально-історичну значимість. Окрім цього, відкриті архівні ресурси сприяють науковим дослідженням та самоосвіті, дозволяючи дослідникам та здобувачам вивчати матеріали без зайвих перешкод. Реалізація політики відкритого доступу є ключовим чинником у розвитку архівної справи, збереженні й удоступненні культурної спадщини України.

5. На виконання завдання відкритого доступу запропоновано нову пошукову систему «Міжархівний пошуковий портал», створений для інтеграції державних архівів в єдину інформаційну систему архівної галузі. Цей ресурс

сприяє інформатизації та автоматизації архівної справи, забезпечуючи єдиний інформаційний простір для центральних та обласних архівів. Пошуковий портал дозволяє переглядати оцифровані документи онлайн, виконувати повнотекстовий пошук документів та замовляти документи до читального залу архіву через мережу інтернет. Основними завданнями архівів є розвиток цифрового контенту, створення електронних публічних сервісів та забезпечення доступу до архівних ресурсів для широкого кола користувачів.

6. Враховуючи умови воєнної агресії рф проти України та знищення українських архівів в окупації, оцифрування архівних документів за планом заходів Програма оцифрування стає необхідним кроком у збереженні архівної спадщини та забезпеченні доступу до архівних документів. Програма електронного архівного документообігу «Еларсис» дозволяє спростити та убезпечити процеси приймання, обробки та зберігання електронних документів. Система забезпечує інтеграцію з різними архівними підрозділами, що сприяє зручному обміну даними та документами між державними установами. Оцифрування покращує доступ до архівних ресурсів, допомагає зберігати фізичні документи від зношення та ушкоджень. Реалізація електронного документообігу підвищує ефективність сучасної архівної інфраструктури.

7. Забезпечення безпеки архівних інформаційних ресурсів, що мають гриф «для службового користування», є критично важливим аспектом управління даними в державних архівних установах, що забезпечує національну безпеку. Необхідно впроваджувати надійні нормативно-правові системи контролю доступу, які обмежують доступ до конфіденційної інформації лише для уповноважених осіб. Регулярне проведення аудитів та оцінок ризиків контролюючими органами допоможе виявити вразливості в існуючих системах та запобігти можливим витокам інформації. Важливим є також навчання співробітників щодо принципів кібербезпеки інформації та актуальних загроз, що дозволить знизити ризики людського фактору. Загалом, комплексний підхід до безпеки архівних інформаційних ресурсів забезпечить їх цілісність, конфіденційність та доступність в умовах сучасних викликів.

8. Організаційні заходи безпеки поділяються на організаційно-технічні та організаційно-правові, які впроваджуються під час створення та функціонування структур. Безпекові заходи регулюються законодавством і стандартами, які визначають вимоги до зберігання, обробки та захисту архівних даних. Використання міжнародних стандартів, таких як ISO/IEC 27001, сприяє дотриманню найкращих практик у сфері захисту інформації. Ліцензування та сертифікація співробітників з кібербезпеки підвищує рівень компетентності та відповідальності в організації. Обов'язковим є створення нормативних документів, що описують порядок дій у випадку виявлення інцидентів або загроз. Поєднання організаційних і нормативно-правових заходів дозволяє забезпечити комплексний захист архівних інформаційних ресурсів та підтримувати їхню цілісність і доступність у довготривалій перспективі.

9. Програмно-технічні заходи кібербезпеки архівних інформаційних ресурсів спрямовані на забезпечення захисту конфіденційної та соціально-історичної інформації архівів від несанкціонованого доступу та кібератак. Одним із ключових елементів є застосування антивірусного захисту та брандмауерів для запобігання зловмисному проникненню. Системи резервного копіювання і шифрування даних гарантують безпеку інформації навіть у випадку втрати або викрадення даних. Аутентифікація користувачів і регулярний моніторинг активності допомагають мінімізувати ризик внутрішніх загроз та випадкового доступу. Такі заходи є необхідними для підтримки безперервності роботи архівних систем і захисту інформаційних ресурсів від кіберризиків.

Враховуючи результати проведеного дослідження видається можливим формулювання напрямів подальших наукових рефлексії. Зокрема, цікавою темою прикладного характеру буде порівняльний аналіз систем захисту архівних даних в різних країнах. Практичністю відрізняється проблема вивчення впливу штучного інтелекту на безпеку архівних інформаційних ресурсів. Важливим механізмом теоретичного обґрунтування наукових досліджень є розробка методології оцінки рівня захищеності архівів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014, № 1. URL: http://surl.li/cisvcl

2. Бождаган'ян М. Організація оцифрування документів в архівних установах України. Збірник праць молодих науковців ЦНТУ, Вип.14, 2024 С. 50-55.

3. Бойко В.О. Європейське приватно-державне співробітництво у сфері кібербезпеки: підходи до формування та нормативно-правові засади. Аналітична записка. URL: https://niss.gov.ua/sites/default/files/2017-10/Boiko_kiber-3afb5.pdf

4. Боряк Г.В. Архіви України: В серці суспільства чи на маргінезі суспільних потреб? *Архіви України*. 2004. № 1-2(253). С. 5-28.

5. В інформаційному ресурсі «Міжархівний пошуковий портал» доступні понад 10 млн сканкопій документів. URL: http://surl.li/hzbvip

6. Ванкуверська декларація «Пам'ять світу в цифрову епоху: оцифрування і збереження» («Memory of the World in the Digital Age: Digitization and Preservation», 2012 р. URL: http://surl.li/blsgww

7. Варшавчик М. Джерелознавство історичне. *Українська архівна енциклопедія* [Д-М. Робочий зошит]. Київ: Держкомархів України, 2006. С. 106-107.

8. Гловацький В.В. Безпека державних інформаційних ресурсів. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. № 3(43) С.79-82. URL: https://journals.dut.edu.ua/index.php/sciencenotes/article/view/775/719

9. Гнатюк С.Л. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки України. Аналітична записка. URL: http://surl.li/bubixi

10. Дідух Л.В. Дослідження методики оцифрування аудіовізуальних документів національного архівного фонду. Міжнародна наукова конференція «*Бібліотека. Наука. Комунікація. Інноваційні трансформації ресурсів і послуг*» (2022). URL: http://conference.nbuv.gov.ua/report/view/id/1447

11. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. № 1(24)/2018. С.87-103.

12. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. *Наука і оборона*. 2020. № 16. С. 356-358.

13. Доступ до архівних документів: законодавство і практика. Харківська правозах. група. Харків: Права людини, 2010. 416 с. ISBN 978-617-587-018-1.

14. ДСТУ 2732:2023 Діловодство й архівна справа. Терміни та визначення понять. Наказ від 25.05.2023 № 121 Про прийняття національного стандарту та скасування національного стандарту. К.: Держстандарт України, 2024. ст. 33. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=103322

15. ДСТУ 2395-2000. Інформація та документація. Обстеження документа, встановлення його предмета та відбір термінів індексування. Загальна методика (ГОСТ 30671-99) (ISO 5963:1985, IDT). На заміну ДСТУ 2395-94; чинний від 2001-07-01.

16. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. К.: ДСТСЗІ СБ України, 1999. 216 с.

17. Закон України Про державну таємницю. № 3855-XII. 21 січня 1994 р. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

18. Закон України Про доступ до публічної інформації. № 2939-VI. 13 січня 2011 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

19. Закон України Про захист інформації в інформаційно-телекомунікаційних системах. *Відомості Верховної Ради України* (ВВР). 1994. № 31. ст.286. URL: http://surl.li/ayraqb

20. Закон України Про інформацію. *Відомості Верховної Ради України* (ВВР). 1992. № 48. ст. 650 02 жовтня 1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

21. Закон України Про Національний архівний фонд та архівні установи № 3814-XII 24.12.1993. URL: https://zakon.rada.gov.ua/laws/show/3814-12#Text

22. Закон України Про національну безпеку України. *Відомості Верховної Ради* (ВВР). 2018. № 31. ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

23. Закон України Про Національну програму інформатизації № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text

24. Закон України Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

25. Закон України Про охорону культурної спадщини. URL: https://zakon.rada.gov.ua/laws/show/1805-14#Text

26. Захист інформації. Енциклопедія сучасної України. URL: https://esu.com.ua/article-15872

27. Зибін С.В. Захист інформації від несанкціонованого доступу в системах обробки інформації. *Інформаційна безпека*. 2017. № 21. 440 с.

28. Зіма І.І. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спец.). *Наука і оборона*. 1998. № 1. С. 56-58.

29. Ініціативне документування подій широкомасштабної збройної агресії Російської Федерації проти України: метод. рекомендації / Держ. арх. служба України, УНДІАСД; уклад.: Л.В. Дідух, Т.М. Ковтанюк, В.В. Скальський. Київ, 2023. 100 с.

30. Кіровоградська обласна військова адміністрація. URL: https://dakiro.kr-admin.gov.ua/news/2024/03-29/new.php

31. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*. 2010. № 3. с. 123-129.

32. Ковальська Л. Документна комунікація користувачів архівної інформації. Intercultural Communication. 2019, 1 (6), 231-248.

33. Ковальська Л., Дідур І. Потреби користувачів архіву та новітні форми використання архівної інформації. Вісник студентського наукового товариства ДонНУ імені Василя Стуса. 2018, 1 (10)., 131-136.

34. Ковальська Л.А. Джерелознавчий дискурс історії радянського Руху Опору (1941-1945 рр.). Донецьк-Вінниця: ТОВ «Нілан-ЛТД», 2015. 462 с.

35. Конвенція Ради Європи Про доступ до офіційних документів, схвалена в Тромсо 18.06.2009. URL: https://zakon.rada.gov.ua/laws/show/994_001-09#Text

36. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 8 жовтня 1997 р. N 1126. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text

37. Крупський С.Н. Захист інформації від несанкціонованого доступу в системах обробки інформації. К.: Наука, 2018. 256 с.

38. Кузьменко Б.В. Організаційно-правові та програмно-технічні засоби забезпечення інформаційної безпеки: навч. посібник. К.: НАУ, 2018. 364 с.

39. Кулешов С.Г. Документознавство: Історія. Теоретичні основи. К., 2000. 161 с.

40. Кулешов С.Г. Загальне документознавство: навч. посіб. / Укрдержархів; УНДІАСД. Київ: «Києво-Могилянська академія», 2012. 122 с.

41. Мазуркевич Т.Л. Виклики інформаційно-комунікаційної безпеки в суспільстві. Збірник матеріалів VI Всеукраїнської наукової конференції «*Інформаційні технології і системи в документознавчій сфері*». Вінниця: ДонНУ імені Василя Стуса, 2021. С. 56-59.

42. Марчук О.В., Нагорна М.В., Недюха О.А., Пасічник В.М., Захист інформації. Енциклопедія державного управління: у 8 т. К.: НАДУ, 2018. Т.2. Методологія державного управління. с. 170-172.

43. Методика оцінювання якості надання архівних послуг (сервісів) / Держ. арх. служба України, УНДІАСД; уклад.: В.Ф. Бойко, В.В. Бездрабко, Р.В. Романовський. Київ, 2023. 43 с.

44. Наказ Адміністрації Держспецзв'язку від 16 січня 2023 року № 01т, зареєстрований в Міністерстві юстиції України 23 січня 2023 року за № 147/39203. URL: https://zakon.rada.gov.ua/rada/show/v0633519-23#Text

45. Наказ МЮ України від 18.06.2015 № 1000/5 «Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і

організаціях», зареєстрований в Міністерстві юстиції України 22.06.2015 № 736/27181. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text

46. Національний реєстр електронних інформаційних ресурсів. Вебпортал «Дія». URL: https://e-resources.gov.ua/#/

47. Національний стандарт ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення». URL: http://surl.li/egekns

48. Національний стандарт ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». URL: http://surl.li/bbhexn

49. Національний стандарт ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення». URL: https://tzi.com.ua/478.html

50. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

51. Обласний держархів приєднався до онлайн-проєкту, завдяки якому полтавці зможуть дослідити свій родовід. Інтеренет-видання «*Полтавщина*». URL: https://poltava.to/news/74492/

52. Перелік відомостей, що становлять службову інформацію і яким надається гриф обмеження доступу «Для службового користування» в Національній комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг. Наказ НКРЕКП від 15.09.2023 № 65-од. URL: http://surl.li/eewgfc

53. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМУ від 8 лютого 2021 р. № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text

54. Постанова Кабінету Міністрів України від 13 березня 2002 року № 281 «Про деякі питання захисту інформації, охорона якої забезпечується державою». URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF#Text

55. Постанова Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження «Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

56. Постанова КМУ від 19.10.2016 р. № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію». URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text

57. Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» затверджені наказом Міністерства юстиції України № 1000/5 18.06.2015, зареєстровані у Міністерстві юстиції України № 736/27181 22.06.2015. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text

58. Правила роботи архівних установ України» затверджені наказом Міністерства юстиції України № 656/5 08.04.2013, зареєстрованим в Міністерстві юстиції України № 584/23116 10.04.2013. URL: https://zakon.rada.gov.ua/laws/show/z0584-13#Text

59. Про Доктрину інформаційної безпеки України. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

60. Про Доктрину інформаційної безпеки України. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29.12.2016. URL: https://www.president.gov.ua/documents/472017-21374

61. Про затвердження Зводу відомостей, що становлять державну таємницю. Міністерство юстиції України 14 січня 2021 р. за № 52/35674. Наказ ЦУ СБУ від 23.12.2020 № 383. URL: http://surl.li/ecnzkx

62. Про затвердження Порядку використання комп’ютерних програм в органах виконавчої влади. Постанова Кабінету Міністрів від 10 вересня 2003 р. № 1433. URL: https://zakon.rada.gov.ua/laws/show/1433-2003-%D0%BF#Text

63. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова Кабінету Міністрів України від 29 березня 2006 р.№ 373: URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

64. Про затвердження Програми оцифрування архівних інформаційних ресурсів на 2022-2025 роки: Наказ Державної архівної служби України №165 від 29.12.2021р. URL: http://surl.li/iisflo

65. Про оцифрування, збереження й відкритість архівів. Інтерв'ю Анатолія Хромова проєкту Ukrainer. URL: https://www.ukrainer.net/anatoliy-khromov/

66. Про роботу Укрдержархіву, архівних установ і спеціальних установ страхового фонду документації у 2023 році та пріоритети на 2024 рік. КМУ. URL: http://surl.li/ojhneu

67. Про схвалення Концепції розвитку системи електронних послуг в Україні. розпорядження Кабінету міністрів України від 16 листопада 2016 р. № 918-р. Київ. URL: https://zakon.rada.gov.ua/laws/show/918-2016-%D1%80#Text

68. Програми ЮНЕСКО «Інформація для всіх» (Information for All Programme, 2010 р.). URL: https://www.unesco.org/en/newsroom

69. Робота архівних установ в умовах дії особливих правових режимів: метод. рекомендації / Держ. арх. служба України, Укр. наук.-дослід. ін-т архів. справи та документознавства; уклад.: В. Ф. Бойко, С. Г. Кулешов. Київ, 2023. 50 с.

70. Рекомендація № R (2000) 13 Комітету Міністрів країнам-членам стосовно європейської політики доступу до архівів. Рада Європи. Комітет міністрів. URL: http://surl.li/zlqdox

71. Стан, тенденції і перспективи інтеграції Україна – ЄС в архівному секторі: аналіт. огляд / Держ. арх. служба України, УНДІАСД; уклад.: Н. В. Залєток, Є. М. Чорноморець. Київ, 2023. 165 с.

72. Степко О. Аналіз головних складових інформаційної безпеки держави. НАУ. URL: https://jrnl.nau.edu.ua/index.php/IMV/article/view/3214/3172

73. Стратегія інформаційної безпеки. Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

74. Стратегія розвитку архівної справи на період до 2025 року. Проєкт. URL: https://www.kmu.gov.ua/news/strategiya-rozvitku-arhivnoyi-spravi-do-2025-roku

75. Стратегія ЮНЕСКО щодо розвитку архівної справи та діловодства. Records and Archives Management Programme. URL: http://surl.li/ijzgog

76. У 2023 році державні архіви оцифрували у 15 разів більше документів, ніж у 2018. Читомо. URL: http://surl.li/qbpgzo

77. Фурашев В.М., Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2(34). URL: http://surl.li/nwrisr

78. Цифровий фонд користування документами Національного архівного фонду: створення, зберігання, облік та доступ до нього: методичні рекомендації / Державна архівна служба України, УНДІАСД; уклад.: Л.В.Дідух, Н.В.Залєток, Т.М. Ковтанюк. Київ, 2018. 131 с.

79. Charter on the Preservation of Digital Heritage (Хартія про збереження цифрової спадщини, 2003 р.). URL: https://www.unesco.org/en/legal-affairs/charter-preservation-digital-heritage

80. International Council of Archives. URL: https://www.ica.org/

81. Kovalska Lesia, Kovalskyi Hryhorii, Vozyanov Ivan. The concept of “document” in the epistemological system of knowledge: A methodological discourse in the philosophy of science. Library Science. Record Studies. Informology. 2024, 2, 40-49.

ДОДАТКИ

ДОДАТОК А

Принципи інформаційної безпеки

ДОДАТОК Б

Основні поняття з питання кібербезпеки архівних інформаційних ресурсів в законодавстві

РАДА ВЕРХОВНА РАДА УКРАЇНИ
Законодавство України

Електронний кабінет

ЗАКОН УКРАЇНИ

Про Національний архівний фонд та архівні установи

(Відомості Верховної Ради України (ВВР), 1994, № 15, ст.86)

архівна справа - галузь життєдіяльності суспільства, що охоплює науково, організаційно, правово, технологічно, економічно та інші питання діяльності юридичних і фізичних осіб, пов'язані із документуванням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться;

діловодство - сукупність процесів, що забезпечують документування управлінської інформації і організацію роботи із службовими документами;

архівна установа, архів, архівний підрозділ, архівний відділ - це відповідно установа чи структурний підрозділ, що забезпечує облік і зберігання архівних документів, використання відомостей, що в них містяться, та формування Національного архівного фонду і або здійснює управління, науково-дослідну та інформаційну діяльність у сфері архівної справи і діловодства;

державна архівна установа - архівна установа, що здійснює свою діяльність за рахунок коштів Державного бюджету України, а також Галузевий державний архів Національного банку України, який здійснює свою діяльність за рахунок коштів, передбачених кошторисом адміністративних витрат Національного банку України;

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

5) кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

ДОДАТОК В

Загрози національній безпеці в інформаційній сфері визначені «Доктриною інформаційної безпеки України»

Написати звернення | Подати петицію | Підписатися на розсилку | Запит на інформацію

ПРЕЗИДЕНТ УКРАЇНИ | ВОЛОДИМИР ЗЕЛЕНСЬКИЙ

Офіційне інтернет-представництво

НОВИНИ ФОТО ВІДЕО ДОКУМЕНТИ ПРЕЗИДЕНТ ОФІС ПРЕС

Укази Розпорядження Конституція України Всі документи

Головна › Документи › Укази

УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017

Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

Відповідно до статті 107 Конституції України, частини другої статті 2 Закону України «Про основи національної безпеки України» п о с т а н о в л я ю:

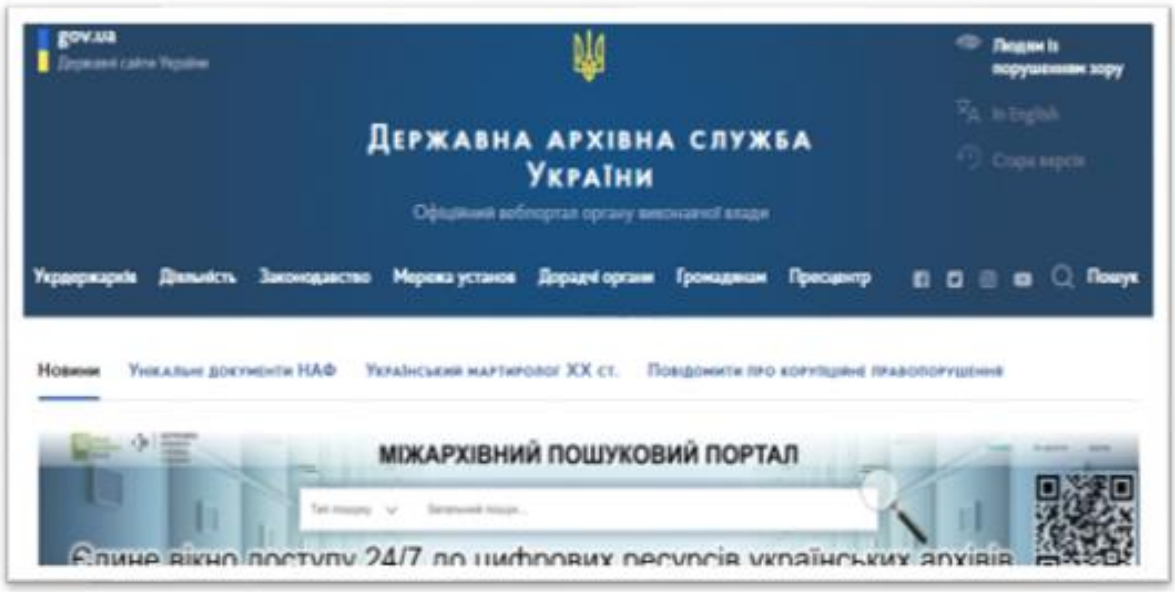
1. Увести в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» (додається).

2. Затвердити Доктрину інформаційної безпеки України (додається).

3. Цей Указ набирає чинності з дня його опублікування.

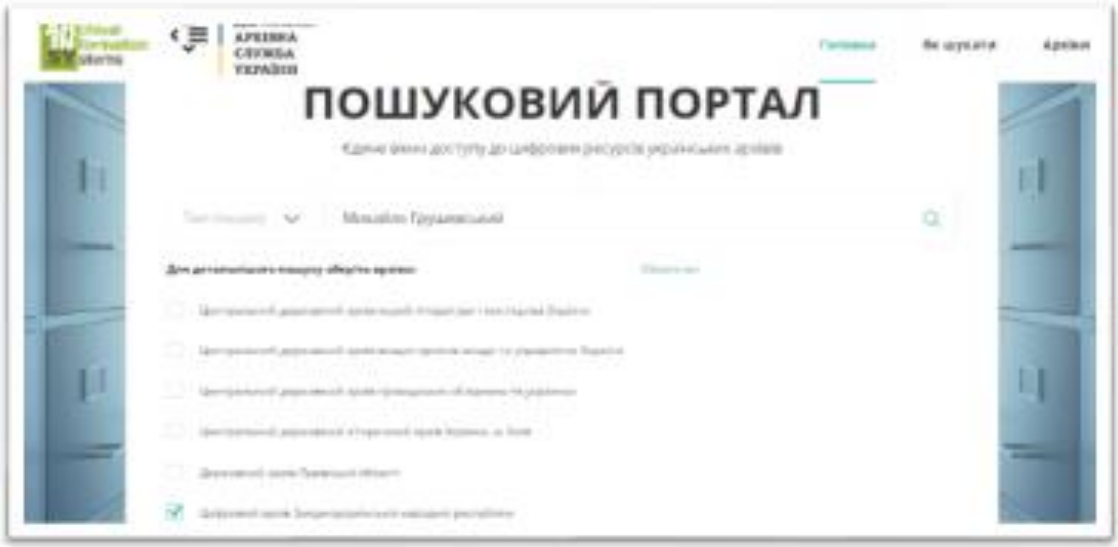
ДОДАТОК Г

Стара і оновлена версії вебпорталу Державної архівної служби України



ДОДАТОК Д

Алгоритм роботи меню «Міжархівного пошукового порталу»



ДОДАТОК Е

Кількість запитів користувачів, які опрацювали українські архіви протягом 2023 р.

У 2023 р. опрацьовано 342 388 запитів		
185 006	–	соціально-правового характеру (про реєстрацію актів цивільного стану, національність, трудовий стаж і розмір заробітної плати, політичні репресії та розкуркулення, перебування на окупованих територіях, евакуацію, вивезення до Німеччини, присвоєння нагород, медалей, наукових ступенів та вчених звань, навчання тощо).
78 569	–	майнових запитів.
37 861	–	тематичних запит (про реорганізацію, ліквідацію підприємств, установ та організацій, зміни в адміністративно-територіальному поділі, історії культових споруд, краєзнавчих даних тощо).
35 879	–	біографічних запитів (життя та уточнення біографічних фактів фізичних та історичних осіб).
5 073	–	генеалогічних запитів.

ДОДАТОК Ж

Зразок журналу для ведення обліку документів з грифом ДСК

Додаток 4
до Інструкції.

ЖУРНАЛ

реєстрації вихідних
та внутрішніх документів
з грифом «Для службового користування»

_____

(назва підприємства, установи, організації, ПІБ підприємця)

_____

(адреса, телефони)

Розпочато «____» _____ 20___ р.

Закінчено «____» _____ 20___ р.

ДОДАТОК К

Заходи з організації інформаційної безпеки в державних архівних установах

1. **Конфіденційність інформації:** Забезпечення захисту від несанкціонованого доступу до конфіденційної інформації, яка може бути власністю індивідів, організацій або держави.
2. **Цілісність даних:** Гарантування, що інформація залишається невикробленою, невідмінною та непошкодженою під час передачі, обробки або зберігання.
3. **Доступність інформації:** Забезпечення доступу до інформації для тих, хто має право користуватися нею, і водночас уникання перешкод для легітимних користувачів.
4. **Захист від кіберзагроз:** Попередження та захист від кібератак, вірусів, хакерських атак та інших загроз інформаційно-комунікаційних систем.
5. **Захист персональних даних:** Збереження конфіденційності та безпеки особистої інформації кожного індивіда.
6. **Управління ризиками:** Проведення оцінки ризиків і розробка стратегій для запобігання та реагування на можливі загрози.
7. **Законодавча база:** Існування відповідних законів і стандартів, які регулюють сферу інформаційно-комунікаційної безпеки.
8. **Свідомість і освіта:** Залучення суспільства до питань інформаційної безпеки шляхом освіти та підвищення рівня інформаційної грамотності.

ДОДАТОК Л

Антивірусна програма Avast Antivirus для комп’ютерів на базі Windows