МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ

Кафедра музеєзнавства, пам'яткознавства
та інформаційно-аналітичної діяльності

На правах рукопису

РЕЗНІЧЕНКО МИРОСЛАВ ОЛЕКСАНДРОВИЧ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ЦИФРОВИХ АРХІВАХ: НОВІТНІ ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Робота на здобуття освітнього ступеня «Бакалавр»
за освітньо-професійною програмою
«Документаційне забезпечення управління та інформаційно-аналітична діяльність»
спеціальності 029 «Інформаційна, бібліотечна та архівна справа»

Науковий керівник:
кандидат педагогічних наук,
доцент
Мельничук Юлія Євгеніївна

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол № _____
засідання кафедри музеєзнавства,
пам'яткознавства та інформаційно-
аналітичної діяльності
від _____2025 р.
Завідувачка кафедри проф. Гаврилюк С. В._____

Луцьк – 2025

ЗМІСТ

ВСТУП ……...3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ ТА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ЦИФРОВИХ АРХІВАХ..... 6
1.1. Поняття та особливості захисту даних у цифрових архівах. 6
1.2. Огляд сучасних регламентів та стандартів у сфері захисту даних 15
РОЗДІЛ 2. АКТУАЛЬНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ТА МЕТОДІВ ЗАХИСТУ ДАНИХ У ЦИФРОВИХ АРХІВАХ……...23
2.1. Основні ризики, пов’язані із захистом даних у цифрових архівах 23
2.2. Перспективні технології захисту даних..... 31
ВИСНОВКИ..... 39
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 41

ВСТУП

Актуальність дослідження теми захисту персональних даних у цифрових архівах зумовлена стрімким розвитком цифровізації та зростанням обсягів обробки інформації в сучасному світі. З кожним роком все більше організацій і державних установ покладаються на цифрові архіви для зберігання важливих документів, серед яких є конфіденційна та персональна інформація. В умовах таких трансформацій необхідність забезпечення належного захисту цих даних стає вкрай важливою, оскільки втрата або компрометація персональних відомостей може призвести до серйозних наслідків, зокрема порушення прав громадян та значних фінансових збитків для організацій.

Захист даних на цифрових архівах потребує інтеграції новітніх технологій та методів, які здатні адаптуватися до постійно змінюваних загроз. Використання блокчейну, криптографічних методів та штучного інтелекту дозволяє створювати надійні, стійкі до зловмисних дій системи зберігання та обробки даних. Системи на основі штучного інтелекту можуть виявляти аномалії в поведінці користувачів або атаки в режимі реального часу, що значно підвищує рівень безпеки архівів. Водночас розвиток шифрування та біометричних технологій відкриває нові можливості для забезпечення захисту доступу до інформації.

Враховуючи постійне збільшення загроз кібербезпеки та необхідність відповідати вимогам законодавства, що регулює захист персональних даних, дослідження новітніх технологій захисту в цифрових архівах є надзвичайно важливим. Збереження конфіденційності даних і забезпечення їх безпеки має прямий вплив на довіру користувачів та надійність роботи організацій. Тому розробка нових підходів до захисту та інтеграція сучасних технологій у сферу управління цифровими архівами є важливою складовою забезпечення інформаційної безпеки.

Мета дослідження полягає у вивченні новітніх технологій і методів захисту персональних даних у цифрових архівах.

Для досягнення означеної мети автором дослідження поставлено наступні **завдання:**

– проаналізувати поняття та особливості захисту даних у цифрових архівах;

– розглянути сучасні регламенти та стандарти у сфері захисту даних;

– окреслити основні ризики, пов’язані із захистом даних у цифрових архівах;

– окреслити перспективні технології захисту даних.

Об’єктом дослідження є цифрові архіви та їх інформаційні системи.

Предметом дослідження є технології та методи забезпечення безпеки персональних даних у цифрових архівах.

Стан наукової розробки проблеми. Теоретичні засади дослідження новітніх технологій та методів захисту даних у цифрових архівах досліджувались М. Бліхарем [2], О. Боскіним та П. Чорним [3], В. Брижко [4], О. Диким та М. Флюнтом [10], О. Доптою [11] та ін. У цих працях науковці досліджують поняття та особливості захисту даних, розглядають основні нормативні засади забезпечення безпеки даних у цифровому середовищі. Актуальні проблеми захисту персональних даних у цифрових архівах є об’єктом наукових розвідок для В. Ващук [5], О. Вихриста та Р. Петрової [6], Я. Іщак та О. Кислуна [13], Д. Ковальова та В. Школьнікова [14], та ін. У цих роботах науковці вивчають вплив зловмисного ПЗ, вірусів, фішингу та хакерських атак на цілісність та безпеку даних цифрових архівів. Недостатньо розкритою залишається проблема пошуку перспективних технологій для захисту даних у цифрових архівах, що потребує більш детальних досліджень цієї теми у науковому середовищі України та актуалізує тему кваліфікаційної роботи.

Методи дослідження. Під час написання кваліфікаційної роботи було використано наступні методи дослідження:

– аналізу та синтезу – використано при аналізі теоретичних засад захисту даних у цифрових архівах;

– метод конкретизації – застосовано при вивченні актуальних проблем та перспектив розвитку захисту даних у цифрових архівах;

– метод узагальнення – був корисним при формулюванні загальних висновків до теми дослідження.

Наукова новизна дослідження полягає в аналізі та систематизації новітніх технологій захисту персональних даних у цифрових архівах, зокрема вивченні можливостей використання блокчейну та штучного інтелекту для виявлення кіберзагроз і запобігання несанкціонованому доступу.

Практичне значення дослідження полягає у можливості розробки рекомендацій на основі матеріалів дослідження щодо інтеграції інноваційних технологій захисту даних у цифрові архіви, що дозволить підвищити рівень їх безпеки в умовах сучасних кіберзагроз. Матеріали кваліфікаційної роботи також можуть бути корисним для організацій і установ, що працюють з великими обсягами конфіденційної інформації, що допоможе ефективно захищати дані та забезпечувати їх цілісність.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ НОВІТНІХ ТЕХНОЛОГІЙ ТА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ЦИФРОВИХ АРХІВАХ

1.1. Поняття та особливості захисту даних у цифрових архівах.

Сучасне демократичне, соціальне та правове суспільство ґрунтується на повазі до прав, свобод і безпеки людини, а також на необхідності їх захисту відповідно до принципів законності та верховенства права. Гарантуючи дотримання цих прав і свобод, держава забезпечує захист приватного життя громадян від несанкціонованого втручання, виконує одну зі своїх ключових функцій. Дотримання права на приватність є фундаментом справедливості та гармонії в суспільстві [23, с. 60].

Персональні дані – це відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована на їх основі. До них належать дані, які дозволяють встановити особу безпосередньо або опосередковано, зокрема через ідентифікаційні ознаки: ім’я, дата народження, місце проживання, номер телефону, електронна адреса, біометричні чи генетичні характеристики, фінансова інформація, інформація про здоров’я або соціальний статус.

В українському законодавстві відсутнє словосполучення «безпека приватності персональних даних» або «безпека персональних даних». Натомість використовується термін «інформаційна безпека», який закріплений у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V. У пункті 13 розділу III цього закону інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства та держави, який забезпечує уникнення шкоди через: неповноту, невчасність або

недостовірність інформації; негативний інформаційний вплив; негативні наслідки використання інформаційних технологій; несанкціоноване розповсюдження, використання чи порушення цілісності, конфіденційності та доступності інформації. При цьому питання «процесу» забезпечення захищеності не розглядається [4, с. 37].

А. В. Пазюк зазначає, що персональна інформація відображає унікальність кожної людини, проте через доступність і поширеність засобів її збору та використання існує ризик неправомірного застосування таких даних. Це може призводити до розголошення деталей приватного життя, завдання шкоди репутації або добробуту особи. У західній правовій доктрині для позначення правового інституту, який захищає приватне життя людини, використовується термін «приватність». Він походить від слова «приватний», що протиставляється публічному (суспільному), позначає належність до особистої, недоступної для загалу, сфери життя людини [22, с. 4].

Основними загрозами для персональної інформації в цифрових архівах є ризики несанкціонованого доступу, який може призвести до викрадення або неправомірного використання даних, зокрема через хакерські атаки чи витоки інформації. Значну небезпеку становлять технічні збої, які можуть спричинити втрату або пошкодження даних, а також помилки у налаштуванні систем захисту чи недостатній рівень шифрування. Додатково, людський фактор, такий як ненавмисні дії співробітників або їхнє недбале ставлення до політик безпеки, також може створити вразливості. Іншим викликом є зловмисні дії з боку внутрішніх користувачів архівів, які мають доступ до конфіденційної інформації. Водночас, використання застарілих або ненадійних технологій підвищує ризики порушення конфіденційності, цілісності й доступності даних.

Сучасні електронні документообігові системи (ЕДО) стикаються з численними загрозами, які ставлять під загрозу їхню безпеку та ефективність. Однією з найважливіших вимог до таких систем є забезпечення безпечного електронного обміну документами. Відповідно до

Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, захист інформації визначається як діяльність, спрямована на запобігання несанкціонованим діям із інформацією в системі. При цьому відповідальність за захист покладається на власника системи [25].

Серед основних загроз, що існують для ЕДО, варто виділити такі:

– Загроза цілісності інформації. Це може бути пошкодження, знищення або перекручення даних, що відбувається як через ненавмисні причини (помилки чи збої), так і в результаті зловмисних дій.

– Загроза конфіденційності. Ця загроза включає будь-які порушення конфіденційності, як-от крадіжка чи перехоплення інформації, а також зміна маршрутів доставки документів.

– Загроза роботі системи. Реалізація таких загроз може призвести до порушення або повного припинення функціонування ЕДО. До причин належать навмисні атаки, помилки користувачів, збої в програмному забезпеченні чи апаратному забезпеченні.

– Загроза доступності. Йдеться про дії, які ускладнюють або унеможливлюють доступ до системи. Наприклад, це може бути блокування доступу або створення умов, за яких доступ займає надто багато часу, що робить неможливим виконання певних задач [33, с. 7].

Персональні дані є важливим ресурсом, який в умовах цифрової епохи набуває все більшого значення. Вони включають інформацію, що ідентифікує особу, і відіграють ключову роль у багатьох сферах суспільного життя, як-от економіка, медицина, освіта, бізнес, державне управління тощо. Однак разом із широким використанням персональних даних зростають і загрози, пов’язані з їх неправомірним використанням, зокрема порушенням конфіденційності, несанкціонованим доступом та витоком інформації. Дослідження підтверджує, що ефективне управління ризиками у системах електронного документообігу є невід’ємною частиною їхньої роботи,

оскільки забезпечення безпеки є ключовою умовою їхнього успішного функціонування.

Термін «цифровий архів» і увага до його розвитку почали активно застосовуватися відносно нещодавно, у відповідь на глобальну тенденцію створення цифрової архівної спадщини шляхом оцифрування документів. В Україні архівні установи переважно зберігають паперові документи, їхні копії (фотографічні, скановані тощо), а також електронні документи, що класифікує такі архіви як «гібридні». Виклики інформаційного суспільства на міжнародному рівні визначають одним зі стратегічних напрямів організації доступу до архівів саме оцифрування документів та забезпечення їх доступності через Інтернет. Сучасні архіви активно розширюють діяльність із цифровізації своїх колекцій, що спрямована на збереження національної культурної спадщини, участь у світових цифрових проєктах архівів, музеїв і бібліотек для взаємообміну інформацією, а також забезпечення користувачів зручним доступом до документів через інтернет-сервіси [29, с. 31].

Сьогодні створення цифрової архівної спадщини є глобальною тенденцією, яка отримує значну фінансову підтримку. Архівні служби багатьох країн: США, Канада, Франція, Іспанія, Польща та інші, вже оцифрували значну частину своїх документів. В Україні оцифрування Національного архівного фонду розглядається як стратегічний напрям, спрямований на збереження документів та забезпечення доступу до них у цифровому форматі [7, с. 12].

Процес оцифрування документів включає перетворення фізичних паперових носіїв в електронний формат, що дозволяє ефективно зберігати, обробляти та використовувати інформацію у цифрових системах. Основним етапом оцифрування є сканування, під час якого використовуються сучасні сканери різних типів – від настільних пристроїв до високопродуктивних моделей для масової оцифровки. Після сканування здійснюється обробка зображень за допомогою спеціалізованих програм, які покращують якість отриманих зображень, видаляють шуми та виправляють можливі дефекти.

Одним із ключових інструментів на цьому етапі є технологія оптичного розпізнавання символів (OCR), що дозволяє конвертувати зображення тексту в редагований цифровий формат.

Для організації та збереження оцифрованих документів використовуються системи управління документами (DMS), які забезпечують структурування даних, зручний пошук, індексацію та доступ до інформації. Такі системи інтегруються із хмарними платформами для забезпечення резервного копіювання та спільного використання файлів.

Також важливим етапом є збереження метаданих – структурованої інформації про документ (назва, дата створення, автор тощо), яка спрощує управління архівом і забезпечує його цілісність.

Серед популярних інструментів і технологій для оцифрування документів виділяються Adobe Acrobat для роботи з PDF-файлами, ABBYY FineReader для розпізнавання тексту, а також спеціалізовані бібліотечні або архівні системи на кшталт Archivematica, що оптимізують процеси збереження та доступу до цифрових матеріалів.

Для організації та збереження оцифрованих документів використовуються системи управління документами (DMS), які забезпечують структурування даних, зручний пошук, індексацію та доступ до інформації. Такі системи інтегруються із хмарними платформами для забезпечення резервного копіювання та спільного використання файлів.

Також важливим етапом є збереження метаданих – структурованої інформації про документ (назва, дата створення, автор тощо), яка спрощує управління архівом і забезпечує його цілісність [30].

Важливу роль відіграє створення резервних копій даних. Цей процес забезпечує додатковий рівень захисту від втрати інформації через технічні збої, кібератаки чи фізичне пошкодження серверів. Резервні копії зазвичай зберігають у географічно розподілених місцях, що дозволяє мінімізувати ризики, пов’язані з локальними катастрофами.

Ще одним критичним аспектом є впровадження систем моніторингу й перевірки цілісності даних. Регулярна перевірка стану файлів дозволяє виявляти можливі пошкодження та своєчасно проводити відновлення інформації. Такі системи часто використовують контрольні суми для верифікації коректності збережених даних.

Окрему увагу приділяють захисту даних від кібератак. Для цього застосовуються сучасні методи шифрування, а також багаторівнева система доступу, яка передбачає ідентифікацію та аутентифікацію користувачів.

Захист даних має ключове значення, оскільки забезпечує безпеку та конфіденційність важливої інформації. Персональні дані, зокрема дані кредитних карток чи медичні записи, можуть стати об’єктом інтересу кіберзлочинців і використовуватися для крадіжки особистої інформації, шахрайства або інших протиправних дій. Для компаній захист даних є не менш важливим, адже його відсутність може призвести до репутаційних втрат, значних фінансових збитків та серйозних юридичних наслідків [12].

Захист від кіберзагроз, як-от віруси, атаки типу DDoS та фішинг, є важливим елементом забезпечення безпеки інформаційних систем. Віруси становлять одну з найпоширеніших загроз, оскільки вони здатні пошкоджувати або видаляти файли, порушувати роботу програмного забезпечення і викрадати дані. Для протидії вірусам використовуються антивірусні програми, які регулярно оновлюються для виявлення нових загроз, а також заходи з обмеження доступу до підозрілих файлів і програм.

Атаки типу DDoS (розподілене блокування доступу) спрямовані на перевантаження серверів або систем, що унеможливлює їхню нормальну роботу. Для захисту від таких атак застосовуються системи моніторингу мережевого трафіку, брандмауери, а також технології для розподілу навантаження, які запобігають надмірному трафіку.

Фішинг – це новий вид шахрайства, метою якого є виманювання у користувачів мереж Інтернет персональни даних клієнтів сервісів із переведення або обміну валюти, інтернет магазинів. Наразі, фішинг є одним

із найпоширеніших способі злочинності в Інтернеті, з платіжними картками, спрямований на одержання конфіденційної інформації про реквізити картки та інші персональні дані [32, с. 131]. Для захисту від фішингу важливе значення має навчання користувачів, впровадження фільтрів спаму та використання багатофакторної аутентифікації.

Політика безпеки в організаціях, що працюють із цифровими системами, є стратегічним документом, який визначає правила, процедури та практики для забезпечення захисту інформації. Вона охоплює всі аспекти управління безпекою, зокрема технічні, організаційні та поведінкові заходи, спрямовані на захист конфіденційності, цілісності та доступності даних.

Основною метою політики безпеки є створення умов для запобігання несанкціонованому доступу до інформаційних систем, витоку даних, кібератакам та іншим загрозам. Для цього в документі визначаються ключові принципи захисту, зокрема розподіл прав доступу, впровадження багаторівневого захисту, регулярний моніторинг та аналіз безпеки систем.

Системи шифрування даних є ключовим елементом інформаційної безпеки, що забезпечують конфіденційність та цілісність інформації під час її зберігання або передачі. Існують два основних типи шифрування: симетричне та асиметричне, кожен із яких має свої особливості та сфери застосування.

Симетричне шифрування передбачає використання одного ключа, яким користуються всі сторони для шифрування та дешифрування даних. Цей ключ залишається секретним і спільним для учасників процесу. Асиметричне шифрування базується на застосуванні двох різних ключів: один використовується для шифрування, а інший – для дешифрування. Ключ для шифрування називають «відкритим ключем», оскільки він доступний для інших, тоді як ключ для дешифрування є «закритим ключем» і зберігається у таємниці [39].

Часто у сучасних системах безпеки обидва типи шифрування комбінуються. Наприклад, асиметричне шифрування використовується для

передачі симетричних ключів, а вже ці ключі застосовуються для шифрування великих обсягів даних. Такий підхід дозволяє поєднати переваги обох методів, забезпечувати високий рівень безпеки й ефективності.

Використання брандмауерів та антивірусних програм є основними засобами захисту інформаційних систем від кіберзагроз. Брандмауер (firewall) у комп'ютерній мережі являє собою програмно-апаратний засіб, що встановлюється на межі мережі й забезпечує двосторонній обмін лише дозволеними даними відповідно до заданих правил. Зазвичай брандмауери використовуються для захисту внутрішньої корпоративної мережі від несанкціонованого доступу із зовнішніх джерел. Водночас вони також можуть виконувати функцію фільтрації вихідного трафіку, обмежувати доступ користувачів внутрішньої мережі до зовнішніх ресурсів або контролювати передавання даних назовні [11, с. 38].

Антивірусні програми, у свою чергу, призначені для виявлення, блокування та видалення шкідливих програм, як-от віруси, трояни, шпигунське та рекламне програмне забезпечення. Вони працюють на основі сигнатурного аналізу, порівнюють файли з базою відомих загроз, а також поведінкового аналізу, який дозволяє виявляти нові загрози за їхньою підозрілою активністю. Сучасні антивірусні програми часто інтегруються з хмарними сервісами для оперативного оновлення баз загроз і використовують штучний інтелект для підвищення точності аналізу.

Поєднання брандмауерів і антивірусних програм забезпечує багаторівневий захист інформаційних систем. Брандмауери обмежують доступ до мережі, запобігають проникненню загроз, тоді як антивіруси зосереджуються на виявленні та нейтралізації вже існуючих шкідливих програм. Такий комплексний підхід є основою ефективної стратегії кібербезпеки, забезпечують як захист від зовнішніх атак, так і контроль внутрішніх загроз.

Навчання персоналу з питань кібербезпеки є важливим елементом загальної стратегії захисту організації від кібератак та інших загроз. За

даними IBM, понад 90% кіберінцидентів спричинені людськими помилками. Зі збільшенням кількості фішингових атак важливість навчання співробітників основам кібергігієни зростає, оскільки їхня недостатня обізнаність може мати серйозні наслідки для безпеки організації [21]. Оскільки людський фактор часто стає причиною порушення безпеки, формування обізнаності співробітників про потенційні ризики та способи їх уникнення є ключовим завданням.

Основна мета навчання – підвищити рівень знань працівників щодо сучасних загроз, як-от фішингові атаки, шкідливе програмне забезпечення, несанкціонований доступ до систем і витік даних. Персонал навчається розпізнавати підозрілі електронні листи, посилання та файли, а також дотримуватися базових принципів безпеки, наприклад, створювати надійні паролі, уникати використання особистих пристроїв для роботи та повідомляти про будь-які інциденти.

Практичні тренінги дозволяють моделювати реальні кіберзагрози, щоб співробітники могли випробувати свої навички реагування в умовах, максимально наближених до реальних. Це може включати симуляцію фішингових атак або відпрацювання дій у разі підозри на витік інформації.

Також важливим є постійне оновлення знань персоналу, оскільки кіберзагрози швидко еволюціонують. Організації повинні регулярно проводити семінари, вебінари та тренінги, доповнювати їх інформаційними матеріалами, як-от інструкції або внутрішні бюлетені про нові типи атак і способи їх запобігання.

Ефективний захист даних базується на впровадженні багаторівневих заходів, які включають технічні, організаційні та правові аспекти. Технічні заходи, зокрема шифрування, багатофакторна аутентифікація, резервне копіювання та використання антивірусних програм, забезпечують надійний захист інформації. Організаційні заходи, зокрема навчання персоналу, регулярний аудит безпеки та чітке визначення прав доступу, мінімізують людський фактор як потенційну загрозу.

Отже, захист даних у цифрових архівах є ключовим елементом забезпечення інформаційної безпеки в умовах стрімкої цифровізації. Архіви містять важливу, часто конфіденційну інформацію, вразливу до несанкціонованого доступу, змін або знищення. Особливості цифрових архівів, зокрема велика кількість даних, довготривале зберігання та необхідність доступності, зумовлюють потребу в комплексних системах захисту. Ефективна система безпеки повинна поєднувати технічні, організаційні та правові засоби. Водночас важливо забезпечити баланс між безпечністю та зручністю користування архівами. Таким чином, захист цифрових архівів – це безперервний процес, який потребує адаптації до нових загроз і технологій.

1.2. Огляд сучасних регламентів та стандартів у сфері захисту даних

Міжнародні стандарти та регламенти захисту персональних даних є основою для забезпечення безпеки та конфіденційності інформації в умовах глобалізованого цифрового середовища. Вони визначають єдині підходи та вимоги до обробки, зберігання та передачі персональних даних, що дозволяє узгоджувати правові та технічні аспекти захисту інформації між різними країнами та організаціями.

GDPR є одним із найважливіших регуляторних актів щодо захисту персональних даних у Європейському Союзі. У ньому уточнено визначення персональних даних, розмежовано ролі сторін, які працюють з інформацією, та встановлено суворі штрафи за порушення вимог. Законотворча діяльність ЄС у сфері захисту даних не зупинилася на ухваленні GDPR. Регламент не охоплює обробку персональних даних у сфері кримінального правосуддя, оскільки ця галузь потребує особливого правового підходу. Тому в 2016 році одночасно з GDPR була ухвалена директива, яка регулює захист фізичних

осіб під час автоматизованої обробки персональних даних державними органами з метою запобігання, розслідування, виявлення та переслідування кримінальних злочинів [38].

Стандарти ISO/IEC у сфері захисту інформації є універсальними інструментами, які забезпечують ефективний підхід до управління інформаційною безпекою в організаціях різних рівнів. Ці стандарти розроблені Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) з метою уніфікації принципів та методів захисту даних.

ISO/IEC 27001 є основним стандартом, що визначає вимоги до системи управління інформаційною безпекою (ISMS). Він ґрунтується на підході до управління ризиками та включає заходи для забезпечення конфіденційності, цілісності та доступності інформації. Стандарт передбачає проведення регулярного аналізу ризиків, визначення політики безпеки, впровадження заходів захисту та моніторинг ефективності цих заходів. Організація, що відповідає вимогам ISO/IEC 27001, може отримати сертифікацію, що підтверджує її здатність захищати інформаційні активи.

Додатковим до ISO/IEC 27001 є ISO/IEC 27002, який надає детальні рекомендації щодо впровадження заходів безпеки. Цей стандарт містить практичні приклади та опис кращих практик, які можна адаптувати для конкретної організації.

Для захисту персональних даних важливим є ISO/IEC 27701, який є розширенням ISO/IEC 27001 і стосується управління конфіденційністю інформації. Він встановлює вимоги до системи управління конфіденційністю (PIMS), що забезпечує дотримання правових регламентів, як-от GDPR, та створює механізми для управління персональною інформацією.

Інші стандарти, як-от ISO/IEC 27017 і ISO/IEC 27018, стосуються безпеки даних у хмарних середовищах, де особлива увага приділяється захисту інформації у процесі її обробки та зберігання у хмарних сервісах.

Міжнародні стандарти інформаційної безпеки представляють собою комплексну систему, яка охоплює як обов'язкові вимоги, так і рекомендації щодо забезпечення інформаційної безпеки. Розробка нових стандартів є безперервним процесом, що адаптується до нових викликів та інцидентів у сфері ІБ, має на меті створення універсальної та надійної моделі захисту даних та інформації, зокрема в кіберпросторі. Сімейство міжнародних стандартів не лише забезпечує основу для ефективних механізмів інформаційної безпеки, але й слугує орієнтиром для подальшого розвитку систем управління інформаційною безпекою (СУІБ) та впровадження програм захисту на локальному рівні [10, с. 86].

Важливим документом у міжнародному масштабі є Конвенція 108 Ради Європи – перша міжнародна угода, яка регулює захист персональних даних. Модифікована версія Конвенції 108, ухвалена у 2018 році, розширює її застосування на сучасні цифрові виклики, включно із новими технологіями обробки даних, та підсилює вимоги щодо відповідальності сторін [9].

На глобальному рівні також діють рекомендації ОЕСР (Організації економічного співробітництва та розвитку). Вони зосереджуються на принципах транскордонного обміну персональними даними та формулюють основні правила обробки інформації, зокрема обмеження збору, забезпечення цілісності даних та підзвітність.

Крім цього, Рамкові угоди США та ЄС, зокрема Privacy Shield, а також його нові модифікації, регулюють передачу даних між країнами, забезпечують баланс між економічними інтересами та захистом приватності користувачів.

Впровадження міжнародних стандартів у сфері захисту даних супроводжується низкою викликів, що виникають як на глобальному, так і на національному рівнях. Однією з головних проблем є гармонізація законодавства. Багато країн мають власні регламенти, які не завжди узгоджуються з міжнародними нормами, зокрема GDPR чи стандартами

ISO/IEC. Це створює труднощі для транснаціональних компаній, які змушені адаптувати свої процеси до різних вимог у кожній юрисдикції.

Ще одним викликом є фінансова та технічна готовність організацій. Впровадження міжнародних стандартів вимагає значних ресурсів для модернізації інфраструктури, впровадження систем шифрування, налаштування контролю доступу та регулярних аудитів безпеки. Невеликі компанії чи державні установи, особливо в країнах, що розвиваються, часто стикаються з обмеженням фінансування та браком кваліфікованих кадрів.

Розрив у технологічному розвитку між країнами також є серйозною перешкодою. Технологічно розвинені країни мають доступ до сучасних рішень у сфері кібербезпеки, тоді як менш розвинені держави відчувають нестачу таких можливостей. Це призводить до нерівномірного рівня захисту даних на глобальному рівні.

Ще однією проблемою є опір організацій та держав до змін. Деякі компанії сприймають впровадження міжнародних стандартів як додатковий бюрократичний тягар, що ускладнює їхню діяльність. Крім того, у країнах із слабким контролем за дотриманням законодавства міжнародні норми часто залишаються формальними і не впроваджуються на практиці.

Важливим викликом залишається забезпечення балансу між захистом даних та інноваціями. Жорсткі вимоги до обробки персональних даних можуть обмежувати розвиток нових технологій, як-от штучний інтелект або великі дані, які активно працюють із інформацією користувачів.

Актуальні міжнародні угоди та рамкові документи відіграють важливу роль у гармонізації підходів до захисту даних у різних країнах, сприяють глобальній взаємодії в умовах цифрового суспільства та підвищують стандарти безпеки обробки персональної інформації.

В Україні питання захисту персональних даних регулюється Законом «Про захист персональних даних» [26], який значною мірою базується на європейських стандартах. Закон України «Про захист персональних даних», ухвалений у 2010 році, є основним нормативно-правовим актом, що регулює

порядок обробки та захисту персональної інформації громадян. Цей закон визначає персональні дані як відомості або сукупність відомостей про фізичну особу, яка може бути ідентифікована за допомогою таких даних.

Основні положення закону зосереджені на забезпеченні прав суб'єктів персональних даних, а також встановленні обов'язків для володільців і розпорядників цих даних. Закон передбачає, що обробка персональних даних повинна здійснюватися законно та прозоро, а збір інформації має проводитися лише з конкретною та чітко визначеною метою. Недопустимим є використання даних для цілей, що не відповідають заявленим під час їх збору.

Важливим аспектом закону є необхідність отримання згоди суб'єкта персональних даних на їх обробку, за винятком випадків, передбачених законодавством (наприклад, у межах виконання державних завдань чи судових рішень). Суб'єкти персональних даних мають право доступу до своїх даних, право вимагати їх виправлення, видалення чи обмеження обробки, якщо дані є неточними або обробляються незаконно.

Закон також покладає на володільця персональних даних обов'язок впроваджувати заходи безпеки для захисту інформації від несанкціонованого доступу, зміни чи знищення. Це включає як технічні, так і організаційні механізми захисту. Крім того, володілець зобов'язаний реєструвати бази даних у відповідних органах та забезпечувати їх належну конфіденційність.

Особлива увага приділяється відповідальності за порушення вимог закону, що включає як адміністративні, так і кримінальні санкції. Це створює основу для забезпечення належного рівня захисту персональних даних і стимулює організації дотримуватися встановлених вимог.

Важливим нормативним актом у сфері захисту персональних даних є Загальний регламент із захисту персональних даних (General Data Protection Regulation – GDPR. Цей документ не лише значно підвищив стандарти захисту персональних даних у країнах-членах ЄС, але й встановив механізми для застосування передбачених ним санкцій до компаній за межами

Європейського Союзу, зокрема українські підприємства. Попри те, що Україна не є членом ЄС, правила, закріплені у GDPR, можуть безпосередньо стосуватися суб'єктів, які перебувають під українською юрисдикцією. Відповідно до статті 3 GDPR, регламент має екстратериторіальну дію, тобто його положення поширюються не лише на країни-члени ЄС, а й на фізичних та юридичних осіб інших держав у випадках, що передбачені документом. Це означає, що компанії, які обробляють персональні дані громадян ЄС або надають їм послуги, зобов'язані дотримуватися вимог GDPR, навіть якщо вони розташовані за межами Європейського Союзу [18, с. 599].

Обидва документи ґрунтуються на принципах законності, прозорості та цільового використання персональних даних. В українському законодавстві, як і в GDPR, передбачено право суб'єкта персональних даних на доступ до своїх даних, виправлення помилок та їх видалення у разі незаконної обробки. Водночас GDPR деталізує ці права значно глибше та вводить поняття «права на забуття», що в українському законодавстві ще не повною мірою імплементоване.

Щодо обов'язків володільців даних, український закон вимагає забезпечення безпеки персональних даних, проте не настільки жорстко регулює питання впровадження технічних і організаційних заходів безпеки, як GDPR. Наприклад, у GDPR передбачена обов'язкова процедура оцінки впливу на захист даних (DPIA) для операцій, що становлять високий ризик для прав суб'єктів, а також обов'язок призначення офіцера із захисту даних (DPO) у певних випадках, чого український закон не вимагає.

Одним із ключових викликів є транскордонна передача персональних даних. GDPR встановлює жорсткі умови для передачі даних за межі ЄС, дозволяють це лише країнам, законодавство яких визнано таким, що забезпечує адекватний рівень захисту. Українське законодавство потребує подальшої гармонізації з цими вимогами, щоб створити умови для вільного обміну даними з європейськими країнами.

Держава забезпечує захист персональних даних, створюють необхідні умови для їх ефективної охорони та оперативного відновлення порушених прав осіб, пов’язаних із такими даними. Учасники правовідносин, що стосуються персональних даних, зобов’язані вживати заходів для захисту цих даних від незаконної обробки та доступу. Вони повинні здійснювати комплекс правових і технічних дій, спрямованих на досягнення максимально можливого рівня безпеки персональних даних в інтернеті. Сукупність нормативно-правових актів, що регулюють цю сферу, утворює правову основу для захисту персональних даних в мережі. Разом вони спрямовані на забезпечення ефективного механізму інформаційної безпеки, запобігання несанкціонованому використанню персональних даних та швидке відновлення порушених прав особи, пов’язаних із їх поширенням [2, с. 23].

Роль держави у підвищенні рівня обізнаності населення щодо захисту персональної інформації є надзвичайно важливою, оскільки саме державні органи володіють ресурсами та повноваженнями для організації ефективних просвітницьких ініціатив. Перш за все, держава може виступати ініціатором інформаційних кампаній, спрямованих на роз’яснення громадянам їхніх прав у сфері захисту персональних даних та потенційних загроз, що виникають через неналежне поводження з особистою інформацією.

Крім цього, держава здатна розробляти навчальні програми та включати відповідні теми до освітніх курсів у школах, вищих навчальних закладах та на спеціалізованих тренінгах. Створення онлайн-платформ і ресурсів, які надають громадянам доступ до рекомендацій, інструкцій та прикладів щодо захисту даних, є ще одним дієвим інструментом у підвищенні цифрової грамотності населення.

Законодавчі ініціативи також відіграють ключову роль. Держава може ухвалювати нормативно-правові акти, які регулюють використання персональних даних і зобов’язують компанії та установи проводити навчання для своїх працівників. Крім того, державні органи можуть співпрацювати з громадськими організаціями та бізнесом для створення спільних програм, які

допомагають підвищити рівень обізнаності та впроваджують найкращі практики.

Нарешті, держава може підтримувати ініціативи, що стосуються реагування на інциденти у сфері персональних даних, таким чином показують приклад відповідального ставлення до захисту інформації та стимулюють населення уважніше ставитися до безпеки своєї персональної інформації.

Таким чином, сучасні регламенти та стандарти відіграють важливу роль у формуванні ефективної системи захисту даних. Нормативні документи встановлюють чіткі вимоги до обробки, зберігання та передачі інформації. Дотримання вимог законодавства у сфері захисту даних не лише підвищує рівень безпеки цифрових архівів, а й сприяє формуванню довіри користувачів та партнерів. Стандарти забезпечують уніфікований підхід до ризик-менеджменту, моніторингу інцидентів і контролю доступу. Проте важливо враховувати специфіку законодавства кожної країни та адаптувати практики відповідно до локального контексту. Саме тому впровадження регламентованих норм є невід’ємною умовою сталого функціонування цифрових інформаційних систем.

РОЗДІЛ 2
АКТУАЛЬНІ ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ТА МЕТОДІВ ЗАХИСТУ ДАНИХ У ЦИФРОВИХ АРХІВАХ

2.1. Основні ризики, пов'язані із захистом даних у цифрових архівах

У сучасному цифровому середовищі архіви стають дедалі більш вразливими до різноманітних кіберзагроз. Ефективний захист даних потребує розуміння потенційних ризиків, які можуть призвести до втрати, викривлення або несанкціонованого доступу до інформації. Аналіз цих ризиків є ключовим етапом у побудові надійної системи безпеки цифрових архівів. Зокрема, основними ризиками захисту даних у цифрових архівах є наступні (рис. 2.1).

Рис. 2.1 – Основні загрози безпеці даних цифрових архівів

Джерело: створено автором

Розглянемо кожну із загроз більш детально.

Шкідливе програмне забезпечення, або ж зловмисне ПЗ, – це комп’ютерний код, створений з метою завдати шкоди комп’ютерам користувачів або використовувати будь-які програмовані пристрої, сервери чи мережі у власних інтересах зловмисників. Таке програмне забезпечення може проявлятися у різних формах: блокування доступу, знищення чи крадіжка даних, викрадення коштів, використання ресурсів комп’ютера, розповсюдження дезінформації, зараження інших систем та інші шкідливі дії. Основними мотивами кіберзлочинців є фінансова вигода, шпигунство, викрадення конфіденційної інформації або нанесення шкоди конкурентам чи противникам [5, с. 196].

Перш за все, загроза зловмисного програмного забезпечення виходить далеко за межі звичайного комп’ютера. Будь-який пристрій, що має доступ до Інтернету, потенційно вразливий до зараження. Наслідки такого зараження можуть бути надзвичайно серйозними. Зокрема, зловмисне програмне забезпечення може надати сторонній особі повний контроль над комп’ютером або іншим пристроєм, що може проявлятися у встановленні небажаних програм, зміні системних налаштувань чи паролів, а також у викраденні конфіденційної чи інтелектуальної інформації. Усе, що зберігається або завантажується на пристрій, потенційно стає доступним для зловмисника, який контролює шкідливий код [40, с. 161].

Протистояння між фахівцями з кібербезпеки та розробниками шкідливого програмного забезпечення спричинило постійний розвиток методів виявлення загроз. Одним із перспективних підходів, що набув широкого поширення останнім часом, стало використання глибокого навчання, зокрема згорткових нейронних мереж (CNN), для ідентифікації та класифікації різновидів шкідливих програм.

CNN, як різновид глибоких нейронних мереж, виявили високу ефективність у завданнях розпізнавання зображень. Їх основна перевага полягає в здатності автоматично навчатися та виявляти релевантні характеристики без необхідності ручного виділення ознак. Цей підхід

привернув увагу дослідників до можливості його застосування в задачах класифікації шкідливого ПЗ.

Одним із ключових етапів у цьому процесі є вилучення характерних ознак. На відміну від зображень або текстових даних, зловмисне ПЗ зазвичай існує у вигляді двійкових файлів. Згорткові нейронні мережі здатні навчатися обробці цих двійкових форматів, подавати їх як послідовності даних, та виявляти значущі шаблони, необхідні для точного визначення типу шкідливої програми [36, с. 49].

Зловмисне програмне забезпечення становить серйозну загрозу для цифрових архівів, оскільки може спричинити втрату, пошкодження або викрадення збережених даних. Віруси, трояни та програми-вимагачі здатні шифрувати або знищувати цінні цифрові ресурси, ускладнювати або унеможливлювати їх відновлення. Особливо небезпечними є атаки, спрямовані на архіви з конфіденційною чи історичною інформацією, що мають високу цінність. У разі компрометації таких систем наслідки можуть бути незворотними, зокрема для наукових, юридичних або культурних установ.

Комп’ютерний вірус – це невелика, але складна програма, створена висококваліфікованим програмістом, яка здатна до самореплікації та виконання шкідливих дій. Сьогодні відомо понад 50 тисяч різновидів таких вірусів. Точна дата появи першого комп’ютерного вірусу залишається предметом дискусій, проте більшість експертів вважають, що перші віруси з’явилися у 1986 році. Одним із перших відомих вірусів був «Brain», створений пакистанським програмістом на прізвище Алві, який інфікував понад 18 тисяч комп’ютерів у США. Спочатку віруси мали дослідницьке призначення, але згодом їх використання набуло зловмисного характеру, що призвело до появи правових норм щодо відповідальності за кіберзлочини у багатьох країнах. Віруси діють виключно на програмному рівні – вони проникають у файли або приєднуються до них, інфікують таким чином

систему. Щоб вірус активувався, потрібно запустити заражений файл, після чого шкідливий код починає діяти автономно [13, с. 13].

Шкідливий програмний код часто маскується під щось привабливе або корисне (наприклад, зображення популярного спортсмена), але насправді виконує небажані або непередбачувані дії, зокрема пошкоджує дані. Прояви вірусів можуть бути різними, зокрема:

1. Значне уповільнення роботи комп'ютера.
2. Неочікувана поява сторонніх повідомлень на екрані.
3. Поява різноманітних відеоефектів, наприклад, перевертання екрану.
4. Раптове зникнення інформації з екрана.
5. Генерація непередбачених звуків.
6. Порушення нормальної роботи програм, деякі з них можуть вести себе дивно.
7. Поява великої кількості пошкоджених файлів даних і текстових файлів на дисках.
8. Повне руйнування файлової системи на одному з дисків.
9. Операційна система раптово не розпізнає жорсткий диск.
10. Довільна зміна розміру деяких файлів.
11. Несподівані проблеми з доступом до файлів і диска у Windows 3.11 або Windows 95.
12. Видалення всіх незахищених файлів користувача та системних файлів.
13. Заміну існуючих драйверів на невідповідні для системи, що може призвести до помилок, уповільнення роботи та збоїв у роботі важливих сервісних програм [24, с. 231].

Комп'ютерні віруси становлять серйозну загрозу для даних цифрових архівів, оскільки можуть пошкоджувати або викрадати важливу інформацію. Віруси здатні заражати архіви, руйнувати файли або змінювати їх вміст, що робить неможливим відновлення втрачених даних. Особливо небезпечними є

віруси, які можуть зашифрувати файли, вимагати викуп або знищити архіви, що містять конфіденційну чи історичну інформацію. Порушення цілісності та доступності даних у цифрових архівах може призвести до серйозних наслідків, зокрема втрати культурних або наукових матеріалів, що мають унікальну цінність.

Фішінг – це форма кіберзлочинства, яка полягає в шахрайському здобутті конфіденційної інформації, такої як паролі, номери кредитних карток або дані про банківські рахунки. Зловмисники, що займаються фішінгом, видають себе за надійні джерела, зокрема банки чи інші інтернет-сервіси, і надсилають повідомлення або листи, щоб обманом змусити жертв розкрити свої особисті дані. Вони часто використовують різні методи, щоб збити користувачів з пантелику:

1. Фішингові листи – зловмисники надсилають електронні листи, що виглядають як офіційні повідомлення від надійних компаній або установ. Листи можуть містити посилання на фальшиві веб-сайти, які запитують особисті дані.

2. Фішингові веб-сайти – створюються підроблені сайти, що імітують офіційні сторінки банків чи онлайн-магазинів, на яких користувачі можуть випадково ввести свої особисті дані, та бути впевненими, що вони взаємодіють з офіційним ресурсом.

3. Соціальний фішінг – зловмисники використовують інформацію з соціальних мереж для створення персоналізованих атак, що виглядають більш переконливо і можуть переконати користувача надати свої особисті дані [14, с. 73].

Атаки фішерів стають дедалі більш витонченими, з використанням методів соціальної інженерії, щоб налякати жертву і змусити її передати особисту інформацію. Повідомлення часто містять загрози, наприклад, блокування рахунку у разі невиконання вимог, наприклад «якщо ви не надасте свої дані протягом тижня, ваш рахунок буде заблоковано». Іноді зловмисники навіть стверджують, що інформація потрібна для покращення

антифішингових систем, пропонують перейти за посиланням і ввести логін та пароль.

Цільовий фішинг є більш складним і технічним, що збільшує потенційні збитки. Зловмисники ретельно вивчають своїх жертв, аналізуюьб їхні профілі в соціальних мережах та інші персональні дані, щоб зробити повідомлення більш переконливим. Фішери прагнуть викликати у жертви швидку реакцію, тому часто використовують тривожні теми, наприклад, «щоб відновити доступ до свого банківського рахунку…», що змушує користувача перейти за фальшивим посиланням. Вони також маскують фішингові сайти під реальні організації, використовують помилки в адресах або субдомени, щоб ускладнити їх виявлення [3, с. 179].

Фішинг створює серйозні ризики для користувачів, наприклад, фінансові втрати, пошкодження репутації та втрату довіри. Його наслідки особливо відчутні для бізнесу, де кожен інцидент фішингової атаки може призвести до значних збитків і погіршити імідж бренду. Компанії, які піддаються фішинговим атакам, можуть втратити довіру клієнтів, що є важливим конкурентним фактором. Окрім того, компанії можуть нести юридичну відповідальність, якщо не забезпечили належний захист персональних даних своїх клієнтів, що лише погіршує ситуацію [37, с. 215].

Фішинг є серйозною загрозою для цифрових архівів, оскільки зловмисники можуть використовувати цей метод для отримання доступу до конфіденційної інформації, зокрема даних архівів. Якщо користувачі або співробітники архіву випадково розкривають свої облікові дані через фішингові атаки, зловмисники можуть отримати контроль над архівами, викрасти чи пошкодити важливі документи. Такі атаки можуть призвести до втрати або зміни цінних даних, що ускладнить їх відновлення. Більш того, фішинг може бути використаний для проникнення в систему архіву, щоб вставити шкідливе програмне забезпечення, що також загрожує цілісності даних.

Кібербезпека – це захист життєво важливих інтересів громадянина, суспільства та держави під час використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства та цифрового середовища комунікацій. Вона включає своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України в кіберпросторі, відповідно до п. 5 ч.1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. Цей закон визначає правові та організаційні основи забезпечення національних інтересів України в кіберпросторі, а також основні цілі державної політики в сфері кібербезпеки [27].

В умовах воєнного стану необхідно визначити ефективні форми та методи забезпечення інформаційної безпеки громадян для захисту суспільства не тільки від деструктивного інформаційного впливу з боку держав-агресорів та терористичних організацій, що сприяють дестабілізації ситуації в країні, але й від інших негативних інформаційних факторів, які можуть дезорганізувати національний інформаційний простір. Використання інформаційних технологій для здійснення ворожих актів агресії проти громадян, несанкціоноване використання інформаційних ресурсів інших країн, протиправна діяльність в інформаційному просторі, що має на меті дестабілізацію суспільства, поширення інформації, що сприяє міжетнічній та міжплемінній ворожнечі, а також ідеї та теорії, що пропагують ненависть, дискримінацію і насильство, маніпулювання інформацією та інші загрози створюють серйозні ризики для інформаційної безпеки [28, с. 35].

Основні загрози від кібератак під час воєнного стану включають:

1. Втрата інформації – кібератаки можуть призвести до викрадення або знищення важливої інформації, як-от військові плани, дані про розробку зброї, а також конфіденційна інформація державних установ та посадових осіб, що може серйозно зашкодити національній безпеці та обороноздатності країни.

2. Шантаж – зловмисники можуть використовувати викрадену інформацію для шантажу державних органів, військових або цивільних осіб з метою досягнення своїх інтересів або впливу на їхню поведінку.

3. Пошкодження критичної інфраструктури – кібератаки можуть бути спрямовані на важливі інфраструктурні об’єкти: енергетичні мережі, телекомунікаційні системи та водопостачання, що може призвести до серйозних наслідків для національної безпеки.

4. Вплив на військові операції – кібератаки можуть спричинити збій у військових операціях, зокрема за допомогою атак на системи зв’язку, навігації та управління, що ускладнить або унеможливить ефективну координацію між частинами армії, а також створить хаос в русі військової техніки [15, с. 84].

Хакерські атаки є серйозною загрозою для цифрових архівів, оскільки можуть призвести до викрадення або пошкодження цінної інформації. Зловмисники можуть проникати в архіви для отримання доступу до конфіденційних документів, вивести їх на продаж або використати в корисливих цілях. Атаки можуть включати злом паролів, встановлення шкідливих програм, шифрування даних (вимагачі) або зміни в архівованих файлах. Наслідки таких атак можуть бути катастрофічними для збереження інформації, оскільки без належного захисту цифрові архіви можуть бути цілком знищені або втрачені, що вплине на цілісність та доступність важливих даних.

Отже, основні ризики, пов’язані із захистом даних у цифрових архівах, включають ймовірність несанкціонованого доступу до конфіденційної інформації, що може призвести до її крадіжки або витоку. Недостатній рівень захисту може дозволити зловмисникам маніпулювати або знищувати важливі файли, що матиме серйозні наслідки для організацій чи державних установ. Ризик втрати даних у зв’язку із технічними збоями, вірусами або помилками в програмному забезпеченні також є серйозною загрозою, оскільки це може призвести до непоправних втрат інформації. Крім того, недостатній рівень

безпеки на етапі зберігання та архівації може призвести до того, що файли стануть доступними для сторонніх осіб через вразливості в системах або мережах. Збереження старих і застарілих копій даних без належного оновлення і моніторингу також збільшує ймовірність їх компрометації.

2.2. Перспективні технології захисту даних

Перспективні технології захисту даних мають на меті забезпечення надійної безпеки та конфіденційності інформації в умовах постійно зростаючих кіберзагроз. Інноваційні методи, зокрема шифрування даних, блокчейн, а також технології штучного інтелекту для виявлення аномалій, стають все більш актуальними для захисту даних у цифрових архівах та на інших платформах. Зазначені технології можуть значно підвищити рівень безпеки, сприяьт ефективному протистоянню сучасним кібератакам. Проаналізуємо особливості кожної із технологій.

Шифрування інформації відбувається за допомогою відкритого тексту, який є вихідними даними для обробки, а також з використанням ключа і математичних алгоритмів, що виконують обчислення над цією інформацією. Процес шифрування перетворює відкритий текст на нечитаємий формат, тобто на зашифровані дані. Після цього, коли інформація надсилається одержувачу, вона може бути повернута до початкового вигляду через процес дешифрування. Для доступу до зашифрованих даних як відправник, так і одержувач повинні мати відповідні ключі шифрування, які представляють собою послідовність випадкових символів [41].

Процес шифрування реалізується за допомогою криптографічних ключів та математичних алгоритмів, які різняться за рівнем безпеки та функціональністю. Існують три основні методи шифрування:

1. Симетричне шифрування використовує один криптографічний ключ для шифрування та дешифрування даних. Його переваги полягають у

високій ефективності, мінімальних затримках і низьких вимогах до обчислювальних ресурсів. Однак основний недолік цього методу – ризик компрометації ключа, що може дозволити сторонній особі отримати доступ до даних і змінювати їх.

2. Асиметричне шифрування використовує пару ключів: відкритий і закритий. Відкритий ключ доступний для всіх, хто хоче відправити інформацію, а закритий зберігається у секреті у отримувача. Цей підхід знижує ризик компрометації ключа і забезпечує вищий рівень безпеки та автентифікації, оскільки лише той, хто має закритий ключ, може дешифрувати дані.

3. Хешування – це процес перетворення даних будь-якого розміру у фіксований результат, що зазвичай є комбінацією цифр і літер. Хешування використовується для перевірки цілісності даних, оскільки зашифровану інформацію не можна відновити до початкового вигляду. Хоча хешування може бути корисним у поєднанні з іншими методами для підвищення безпеки, його зазвичай не вважають ефективним методом захисту самостійно [42].

На сьогоднішній день важливим аспектом безпеки є не лише шифрування даних, але й захист інформації, що зберігається на наших пристроях. Це обумовлено можливістю зараження пристроїв шкідливим програмним забезпеченням, яке може шукати конфіденційні дані та передавати їх кіберзлочинцям. Для запобігання таким загрозам застосовується шифрування файлів, яке захищає файлові системи, робить їх доступними лише тим, хто має відповідний ключ, зазвичай у вигляді пароля чи фрази для дешифрування. Після введення правильних облікових даних, файл стає доступним для читання. Цей метод може бути інтегрований в операційну систему або файлову систему, де застосовуються складні алгоритми для забезпечення захисту файлів. Окрім вбудованих засобів безпеки, додаткове програмне забезпечення забезпечує багаторівневий захист, збереження цілісності та безпечну передачу даних, що дозволяє

використовувати кілька пристроїв для зберігання та доступу до зашифрованої інформації. Також деякі компанії використовують шифрування даних у хмарі, хоча це менш поширене через складність управління зашифрованими файлами в хмарних сервісах [19, с. 81].

Захист конфіденційності та цілісності даних є критично важливим у сучасному інформаційному середовищі. Шифрування є одним із найбільш ефективних методів захисту даних від несанкціонованого доступу в операційних системах. Такі операційні системи, як Windows, Linux, Unix і MacOS, мають вбудовані рішення для шифрування даних: BitLocker, LUKS, GELI та FileVault відповідно. Одним із найпоширеніших інструментів для шифрування є BitLocker, який доступний в Windows. Він забезпечує шифрування всіх даних на системному розділі, додаткових пристроях чи зовнішніх носіях, використовує AES-шифрування з 128-бітним або 256-бітним ключем. У свою чергу, LUKS, який використовується в Linux, забезпечує шифрування даних на рівні блоків за допомогою різних алгоритмів шифрування, зокрема AES, Twofish і Serpent [35, с. 183].

Шифрування даних є важливим інструментом захисту інформації в цифрових архівах, оскільки дозволяє забезпечити конфіденційність та цілісність архівованих матеріалів. За допомогою шифрування можна захистити як окремі файли, так і цілі архіви, щоб лише авторизовані особи могли отримати доступ до них. Цей метод захисту особливо важливий для архівів, які містять чутливу або конфіденційну інформацію, наприклад, персональні дані або корпоративні документи. Застосування шифрування у цифрових архівах гарантує, що навіть у разі несанкціонованого доступу до архіву дані залишатимуться недоступними без відповідного ключа дешифрування.

Блокчейн сприяє збору даних за допомогою сенсорних технологій та відкриває можливості для використання програмних інструментів, які аналізують інформацію в реальному часі, що дозволяє системам підтримки прийняття рішень обробляти потоки даних і допомагати у прийнятті рішень

на різних рівнях. Блокчейн підвищує ефективність обміну інформацією в ланцюгу поставок, робить процес життєвого циклу товарів більш прозорим, спрощує збір нових даних і сприяє більш швидкому прийняттю рішень. У світі, де доступними є багато даних, сучасні методи прийняття рішень обмежують потенціал бізнесу для використання великих даних, тому інтеграція нових програмних засобів і методів у розумні фабрики стає необхідною для оцінки екологічних наслідків виробництва. Україна, зокрема, визнана лідером у впровадженні блокчейн-технологій, і відповідно до прогнозів, близько 10% світового ВВП буде створюватися за допомогою цих технологій. Європейські країни також активно працюють над впровадженням блокчейну, створюють партнерства для обміну досвідом та утримання лідерських позицій у цій галузі [20, с. 18].

Однією з основних переваг блокчейн-рішень є те, що вони дозволяють організаціям обмінюватися даними новими способами, що раніше були недоступні, що відкриває можливості для покращення співпраці, підвищення операційної ефективності та збільшення прибутку. Проте питання збереження конфіденційності даних стає ще більш актуальним у таких середовищах, оскільки дані зберігаються в спільних реєстрах, доступних кільком учасникам блокчейну. Компанія ConsenSys, яка займається розробкою блокчейн-технологій, зазначає, що конфіденційність не є властивістю будь-якого блокчейну, а скоріше існують різні рівні конфіденційності, які можна застосувати до кожного з них. Розробники повинні ретельно визначати, хто має доступ до читання та запису транзакцій, а також як транзакції перевіряються, транслюються та зберігаються. Окрім цього, важливими є питання щодо оновлення та застосування заходів безпеки та дозволів. Рішення про власність даних і їх використання організаціями та програмами ще більше ускладнюють дискусії щодо конфіденційності [1, с. 8].

Блокчейн пропонує сучасне вирішення проблем безпеки завдяки своїй децентралізованій архітектурі, яка суттєво знижує ризики втручання зловмисників у функціонування систем.

Серед основних завдань, які ця технологія вирішує в сфері кіберзахисту, можна виділити:

– захист інформації від несанкціонованого доступу – дані зберігаються у вигляді зашифрованих блоків із унікальними підписами, що унеможливлює їхнє підроблення або несанкціоноване редагування;

– прозорість та контрольованість транзакцій – усі дії в системі фіксуються в реєстрі, що дає змогу простежити походження кожної транзакції та перевірити її достовірність;

– відсутність централізованого керування – це унеможливлює централізовані атаки на сервери чи бази даних;

– захист від фальсифікації – будь-яка спроба змінити інформацію миттєво стає очевидною всім учасникам завдяки взаємозв’язаній структурі блоків;

– оперативне підтвердження транзакцій – завдяки смарт-контрактам процес обробки угод автоматизується й прискорюється без залучення посередників.

Блокчейн є розподіленою базою даних, у якій кожен блок містить хеш попереднього, що гарантує цілісність ланцюга. Його децентралізований характер робить систему надзвичайно стійкою до зламів і кіберзагроз [6, с. 428].

Цей метод базується на концепції «довірених джерел» – спеціально авторизованих вузлів мережі, які мають право змінювати та доповнювати персональні дані. Кожен з цих вузлів має індивідуальний рівень довіри, який змінюється динамічно залежно від історії його дій. Архітектура системи побудована як ієрархія вузлів перевірки, де кожен рівень відповідає за окремі етапи валідації даних. На першому рівні перевіряється коректність форматів і відповідність структурі даних; другий рівень займається криптографічною

перевіркою цифрових підписів і повноважень джерела; третій – проводить глибоку перехресну перевірку та звірку з наявними записами. Ключовим компонентом є система управління життєвим циклом даних, яка дає змогу контролювати зміни, зберігати історію редагувань. Ця функція реалізується через смарт-контракти, що автоматично обробляють запити на зміну даних та проводять необхідні перевірки. Метод також враховує вимоги законодавства щодо захисту персональної інформації, завдяки системі керування згодами користувачів та механізмам реалізації права на забуття [31, с. 30].

Блокчейн може ефективно використовуватись для захисту даних у цифрових архівах завдяки своїй незмінній і децентралізованій природі. Кожен запис у цифровому архіві фіксується у вигляді блоку з криптографічним підписом, що унеможливлює його підробку або несанкціоноване редагування. Завдяки хронологічному збереженню записів забезпечується прозорість та повна історія змін. Смарт-контракти дозволяють автоматизувати контроль доступу до архівів та забезпечити виконання правил зберігання даних, що значно підвищує рівень безпеки, надійності й довіри до цифрових архівів.

Єдиного загальновизнаного визначення поняття «штучний інтелект» не існує, проте найпоширеніші підходи до його тлумачення зосереджуються на кількох основних аспектах. По-перше, штучний інтелект вивчає методи вирішення задач, що потребують людського мислення, зокрема застосування аналогії, дедукції, індукції, накопичення знань і вміння їх використовувати. По-друге, ШІ займається розробкою рішень для задач, які складно або неможливо розв’язати традиційними способами. І нарешті, штучний інтелект розглядається як система, здатна до навчання та потенційно здатна замінити людину-експерта в певних інтелектуальних процесах. Таким чином, штучний інтелект можна загалом визначити як напрям комп’ютерної лінгвістики та інформатики, що досліджує найефективніші способи самостійного аналізу, прийняття рішень і формалізації задач, подібних до тих, які вирішує людина або не здатна вирішити взагалі [8].

При розгляді штучного інтелекту важливо враховувати його ключові компоненти. Однією з них є Data Science – наука про аналіз даних, яка охоплює процеси збору, обробки, моделювання, оцінки ризиків і прогнозування на основі сучасних інформаційних та телекомунікаційних технологій. Machine Learning (машинне навчання) – це складова ШІ, яка дозволяє комп'ютерам навчатися і покращувати виконання завдань без явного програмування, використовувати статистичні методи. Deep Learning (глибинне навчання) автоматизує процес виділення ознак із даних, мінімізує потребу в ручній обробці інформації. Computer Vision (комп'ютерний зір) – напрям, який дозволяє системам розпізнавати й відслідковувати об'єкти за допомогою алгоритмів обробки зображень. На практиці ШІ вже активно застосовується в бізнесі: чат-боти для клієнтської підтримки, фільтри спаму, автоматизація рутинних процесів, прогнозування продажів, інтелектуальні асистенти (Siri, Cortana, Google Now), системи безпеки та аналітики, що підвищують ефективність підприємств [17, с. 82].

Трансформаційні процеси, що відбуваються під впливом глобалізації та цифровізації, зумовлюють неминуче впровадження й розвиток технологій штучного інтелекту в економіці. Ті держави та компанії, які швидко адаптуються до нових викликів і активно інтегрують ШІ у свою діяльність, отримають конкурентні переваги та зможуть забезпечити собі провідні позиції в цивілізаційному поступі. В Україні вже здійснено перші кроки у цьому напрямі: Міністерство цифрової трансформації розробило Концепцію штучного інтелекту та активізувало підготовку фахівців, які здатні реалізовувати відповідні проєкти. Такі ініціативи сприяють зміцненню ролі України на міжнародній арені як держави, що динамічно впроваджує інновації в економічну діяльність [34].

Очевидно, що майбутнє належить технологіям штучного інтелекту, адже в умовах зростаючої цифровізації їх інноваційна природа здатна забезпечити стабільні конкурентні переваги як окремим компаніям, так і цілим країнам. Водночас, як і будь-яка технологія, ШІ може бути

використаний як на благо, так і на шкоду. Однією з головних загроз є потенційна втрата контролю над його розвитком, коли розумні машини можуть почати ухвалювати рішення самостійно, що створює ризики для бізнесу та суспільства. Проте ці виклики можна подолати завдяки значним перевагам, які отримують організації в результаті ефективного використання штучного інтелекту [16].

Штучний інтелект відіграє важливу роль у захисті даних цифрових архівів, забезпечує автоматичне виявлення загроз і аномальної активності в режимі реального часу. Алгоритми машинного навчання здатні розпізнавати спроби несанкціонованого доступу та реагувати на них до того, як станеться витік інформації. Крім того, ШІ допомагає класифікувати й сортувати дані за рівнем конфіденційності, що сприяє кращому управлінню доступом. Глибинне навчання може використовуватись для розпізнавання та відновлення пошкоджених або змінених файлів, зберігати цілісність цифрових архівів.

Можна підсумувати, що перспективні технології захисту даних відіграють ключову роль у забезпеченні безпеки інформаційних систем в умовах стрімкої цифровізації. Серед найефективніших підходів – використання блокчейну для створення незмінних та прозорих записів, а також впровадження штучного інтелекту для виявлення кіберзагроз у режимі реального часу. Широкі можливості відкриває також шифрування, яке унеможливлює перехоплення даних під час їх передачі. Важливим напрямом залишається розвиток багаторівневих систем автентифікації та біометричних рішень, що значно підвищують рівень захисту доступу. Отже, інтеграція інноваційних технологій захисту даних є необхідною умовою стабільного функціонування організацій і держав.

ВИСНОВКИ

Захист інформації в цифрових архівах є фундаментальним напрямом загальної системи інформаційної безпеки в умовах активної цифрової трансформації. Оскільки архіви зберігають важливу та часто конфіденційну інформацію, вони залишаються вразливими до несанкціонованого доступу, спотворення чи втрати даних. Враховуючи специфіку цифрових архівів – великі обсяги інформації, тривалі строки зберігання й необхідність забезпечення постійного доступу – виникає потреба у впровадженні комплексного підходу до захисту. Така система має поєднувати технічні рішення, організаційні заходи та правове регулювання. При цьому важливо зберігати рівновагу між безпекою даних та зручністю користування архівами. Отже, забезпечення надійного захисту цифрових архівів – це динамічний і безперервний процес, що потребує постійного вдосконалення у відповідь на нові труднощі.

Сучасні регламенти та стандарти мають вирішальне значення для створення ефективної системи захисту даних. Законодавчі норми визначають чіткі вимоги щодо обробки, зберігання та передачі інформації, що сприяє підвищенню безпеки цифрових архівів. Дотримання таких вимог не лише забезпечує належний рівень захисту, але й сприяє підвищенню довіри серед користувачів і партнерів. Стандарти надають уніфікований підхід до управління ризиками, моніторингу інцидентів і контролю доступу, що є важливим для стабільності інформаційних систем. Проте важливо враховувати відмінності в законодавствах різних країн та адаптувати ці норми до локальних умов. Тому інтеграція регламентованих стандартів є необхідною для сталого та безпечного функціонування цифрових архівів.

Основні ризики, пов’язані із захистом даних у цифрових архівах, включають можливість несанкціонованого доступу до конфіденційної інформації, що може призвести до її крадіжки чи витоку. Недостатній захист може дозволити зловмисникам змінювати або знищувати важливі файли, що

створює серйозні загрози для організацій та державних установ. Також існує ризик втрати даних через технічні проблеми, віруси або помилки в програмному забезпеченні, що може спричинити непоправні втрати інформації. Інші загрози виникають через слабкі місця в системах зберігання та архівації, що дозволяють стороннім особам отримати доступ до файлів через вразливості в мережах або програмному забезпеченні. Збереження застарілих копій без регулярного оновлення та моніторингу підвищує ймовірність компрометації інформації.

Перспективні технології захисту даних є важливим елементом забезпечення безпеки інформаційних систем в епоху швидкої цифровізації. Серед найбільш ефективних методів – використання блокчейну для створення незмінних та прозорих записів, а також застосування штучного інтелекту для виявлення кіберзагроз у реальному часі. Шифрування даних залишається одним з основних засобів захисту під час їх передачі. Важливим напрямом також є розвиток багаторівневих систем автентифікації та біометричних технологій, які значно підвищують безпеку доступу. Таким чином, інтеграція новітніх технологій захисту даних є вкрай важливою для стабільної роботи як підприємств, так і державних структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балацька В., Опірський І. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2023. Вип. 4.20. С. 6–19. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/463. (дата звернення: 18.04.2025).

2. Бліхар М. М., Правові основи захисту персональних даних в інтернеті. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2023 № 62 URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc62/4.pdf (дата звернення: 25.04.2025).

3. Боскін О., Чорний П. Аналіз загрози фішингу. *Сучасна молодь в світі інформаційних технологій.* 2021. С. 179.

4. Брижко В. М. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. 2020. № 1 (32). С. 33–46. URL: http://nbuv.gov.ua/UJRN/Infpr_2020_1_5 (дата звернення: 20.04.2025).

5. Ващук В. Шкідливе програмне забезпечення та основні його категорії. *Розвиток сучасної науки та освіти: реалії, проблеми якості*. 2022. С. 196. URL: http://www.tsatu.edu.ua/tm/wp-content/uploads/sites/14/materyaly.pdf#page=197. (дата звернення: 28.04.2025).

6. Вихрист О., Петрова Р. Використання блокчейн-технологій у створенні безпечних інформаційних систем. *Інформаційні технології і автоматизація – 2024* / Матеріали XVII міжнародної науково-практичної конференції. Одеса, 31 жовтня – 1 листопада 2024 р. Одеса, Видавництво ОНТУ, 2024. С. 428–429. URL: https://er.knutd.edu.ua/bitstream/123456789/28788/1/%D0%A2%D0%B8%D1%82%D1%83%D0%BB_%D0%9E%D0%B4%D0%B5%D1%81%D0%B0_%D1%82%D0%B5%D0%B7%D0%B8.pdf#page=428. (дата звернення: 23.04.2025).

7. Вплив копіювально-розмножувальної техніки на збереженість архівних документів : метод. Рекомендації. Укрдержархів, УНДІАСД. 2012. С. 12.

8. Глибовець М., Олецький О. Системи штучного інтелекту. URL: http://kist.ntu.edu.ua/textPhD/ArtificIntell.pdf. (дата звернення: 21.04.2025).

9. День захисту персональних даних: 40 років «Конвенції 108». Офіс Ради Європи в Україні. 2021. URL: https://www.coe.int/uk/web/kyiv/-/data-protection-day-40-years-of-convention-108 (дата звернення: 24.04.2025).

10. Дикий О. В., Флюнт, М. О. Стандарти інформаційної безпеки: компаративне дослідження. *Право та державне управління*. 2019. Вип. 2 (35). URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://pdujournal.kpu.zp.ua/archive/2_2019/tom_1/16.pdf (дата звернення: 24.04.2025).

11. Допта О. Захист мережі з використанням брандмауерів. *Матеріали III Всеукраїнської студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання».* 2010. Вип. 1. С. 38. URL: http://elartu.tntu.edu.ua/handle/123456789/11222 (дата звернення: 26.04.2025).

12. Захист ваших даних: Що потрібно знати про захист даних. ITEЗ. 2024. URL: https://itez.com.ua/data-protection.html (дата звернення: 24.04.2025).

13. Іщак Я., Кислун О. Комп'ютерні віруси. *Перспективні напрямки розвитку сучасних інформаційних систем та технологій*: Матеріали Всеукраїнської науково-практичної студентської конференції. Кропивницький: ЦНТУ, 2021. С. 13–14. URL: https://kntu.kr.ua/file/content/8133/materialy-vseukrainskoi-naukovo-praktychnoi-konferentsii-perspektyvni-napriamky-rozvytku-suchasnykh-informatsiinykh-system-ta-tekhnolohii-15-kvitnia-2021r-.pdf#page=13. (дата звернення: 27.04.2025).

14. Ковальов Д., Школьніков В. Фішинг як загроза в мережі Інтернет. *Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану*. 2024. С. 73. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/083f0180-f141-4bf0-b6aa-8ad67ec59f51/content. (дата звернення: 29.04.2025).

15. Красько І., Буренко О. Загрози від кібератак в умовах воєнного стану. *Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану*. 2024. С. 84–85. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/19da884d-3262-461a-9202-1a9fecd23f8d/content.

16. Кузьомко В., Бурангулова В. Можливості використання штучного інтелекту в діяльності сучасних підприємств. *Економіка та суспільство*. 2021. Вип. 32. URL: https://economyandsociety.in.ua/index.php/journal/article/view/808. (дата звернення: 20.04.2025).

17. Машлій Г., Мосій О. Дослідження управлінських аспектів використання штучного інтелекту. *Економіка та управління підприємствами*. 2020. С. 80–89. URL: https://galicianvisnyk.tntu.edu.ua/pdf/57/601.pdf. (дата звернення: 26.04.2025).

18. Михайлик А. Щодо законодавчого забезпечення захисту персональних даних працівників в Україні відповідно до міжнародних стандартів. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 598-601 URL: https://hdl.handle.net/11300/19570 (дата звернення: 25.04.2025).

19. Морозюк А., Ніколюк П. Шифрування даних. *Комп'ютерні технології обробки даних.* 2022. С. 80–82.

URL: https://jktod.donnu.edu.ua/article/view/13052. (дата звернення: 30.04.2025).

20. Ніколаєв С., Вороненко В. Блокчейн як фактор цифрової трансформації економіки України. *Вісник Сумського державного університету*. Серія Економіка. 2021. № 2. С. 16–23. URL: https://essuir.sumdu.edu.ua/handle/123456789/85043. (дата звернення: 19.04.2025).

21. Організація навчання працівників обізнаності з кібербезпеки з ITS CSAT. *IT Specialist*. 13 вересня 2024. URL: https://my-itspecialist.com/organizing-employee-cybersecurity-awareness-with-its-csat (дата звернення: 27.04.2025).

22. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.11 «Міжнародне право». Київ, 2004. 15 с.

23. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Журнал «Інформація і право».* 2016. № 4 (19). URL: https://ippi.org.ua/pilipchuk-vg-brizhko-vm-informatsiina-bezpeka-ta-privatnist-u-sferi-zakhistu-personalnikh-danikh-sto (дата звернення: 21.04.2025).

24. Почапська О. Комп'ютерні віруси як загроза інформаційній безпеці. *Наука. Освіта. Молодь*. 2017. Ч. 2. С. 230–232. URL: https://library.udpu.edu.ua/library_files/stud_konferenzia/2017_2/89.pdf. (дата звернення: 23.04.2025).

25. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 22.04.2025).

26. Про захист персональних даних: Закон України № 2297-VI від 01.06.2010. URL: https://www.president.gov.ua/documents/2297vi-11567 (дата звернення: 24.04.2025).

27. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (датазвернення: 21.04.2025).

28. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». Вінниця: ХНУВС, 2023. 176 с.

29. Радько Г. Г. Електронний архів: структура та функціонування. Запоріжжя : ЗНУ, 2020. 85 с.

30. Робота з метаданими. Adobe. 21 травня 2021. URL: https://helpx.adobe.com/ua/bridge/using/metadata-adobe-bridge.html (дата звернення: 22.04.2025).

31. Ситник Р., Гнатушенко В. Метод забезпечення достовірності та цілісності персональних даних, що обробляються в блокчейн-системі. *Системні технології*. 2025. № 3 (158). С. 28–35. URL: https://journals.nmetau.edu.ua/index.php/st/article/download/1993/1254/2476. (дата звернення: 29.04.2025).

32. Тарасенко А. Фішинг в сучасних умовах. Редакційна колегія, 2019. С. 131.

33. Тема 3. Цифрова безпека на персональному рівні. Державний університет «Житомирська політехніка». URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://learn.ztu.edu.ua/pluginfile.php/367828/mod_resource/content/0/%D0%A2%D0%B5%D0%BC%D0%B0%203_%D0%B7%D0%B0%D0%BA%D1%96%D0%BD%D1%87%D0%B5%D0%BD%D0%BD%D1%8F.pdf (дата звернення: 24.04.2025).

34. Технології майбутнього: як штучний інтелект впливає на наше життя?. Пороги: незалежний молодіжний портал. URL: https://porogy.zp.ua/2024/12/tehnologiyi-majbutnogo-yak-shtuchnyj-intelekt-vplyvaye-na-nashe-zhyttya/. (дата звернення: 26.04.2025).

35. Тимощук В., Стебельський М. Шифрування даних в операційних системах. *Матеріали VI Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання».* 2023. С. 183–184. URL: https://elartu.tntu.edu.ua/bitstream/lib/41262/2/183-184.pdf. (дата звернення: 23.04.2025).

36. Федюшин О. І. CNN та їх використання для класифікації Malware. *Проблеми інформатизації* : тези доповідей одинадцятої міжнар. наук.-техн. конф., 16–17 листопада 2023 р. Баку–Харків–Бельсько-Бяла, 2023. Т. 2, секція 3,6. С. 49. URL: https://openarchive.nure.ua/entities/publication/18a45b4d-deb3-4ff9-a470-a494d4c9f4fb. (дата звернення: 30.04.2025).

37. Чухалов І., Степанов А. Боротьба з фішингом в інформаційній сфері. *The 4th International scientific and practical conference «Scientific research: modern challenges and future prospects»* (November 18-20, 2024) MDPC Publishing, Munich, Germany. 2024. С. 214–218. URL: https://sci-conf.com.ua/wp-content/uploads/2024/11/SCIENTIFIC-RESEARCH-MODERN-CHALLENGES-AND-FUTURE-PROSPECTS-18-20.11.24.pdf#page=214. (дата звернення: 20.04.2025).

38. Шушпанова А. Р. Особливості впровадження вимог загального регламенту захисту даних (GDPR) в разі використання хмарних технологій. *Кафедра безпеки інформації та телекомунікацій*. 2018. Вип. 149. URL: http://ir.nmu.org.ua/handle/123456789/154349 (дата звернення: 21.04.2025).

39. Що таке шифрування та як воно працює? *Kingston Technology Corporation*. Травень 2023. URL: https://www.kingston.com/ua/blog/data-security/what-is-encryption (дата звернення: 27.04.2025).

40. Яблонський В. Шкідливе програмне забезпечення. *Розвиток сучасної науки та освіти: реалії, проблеми якості.* 2022. С. 161. URL: http://www.tsatu.edu.ua/tm/wp-content/uploads/sites/14/materyaly.pdf#page=162. (дата звернення: 22.04.2025).

41. Saini K. What Is Data Encryption: Types, Algorithms, Techniques and Methods. *SimpliLearn.* Apr 27, 2025. URL: https://www.simplilearn.com/data-encryption-methods-article. (дата звернення: 30.04.2025).

42. What is encryption?. *IBM.* URL: https://www.ibm.com/think/topics/encryption. (дата звернення: 29.04.2025).