МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ

Кафедра музеєзнавства, пам'яткознавства
та інформаційно-аналітичної діяльності

На правах рукопису

КУКЛА ВАДИМ ВАЛЕРІЙОВИЧ

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ Й ОРГАНІЗАЦІЯ ЗБЕРІГАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

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 історичних наук, доцент
Дмитренко А. А.

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол № _____
засідання кафедри музеєзнавства,
пам'яткознавства та інформаційно-
аналітичної діяльності
від _____ 2025 р.
Завідувач кафедри проф. Гаврилюк С. В._____

Луцьк – 2025

АНОТАЦІЯ

Кукла В. В. Забезпечення захисту й організація зберігання електронних документів. Кваліфікаційна робота на правах рукопису на здобуття освітнього ступеня «Бакалавр». Волинський національний університет імені Лесі Українки, Луцьк, 2025.

У кваліфікаційній роботі висвітлено результати дослідження проблем забезпечення захисту та організації зберігання електронних документів у сучасному інформаційному суспільстві. Проаналізовані теоретичні аспекти і практичні підходи до побудови ефективного середовища для зберігання електронної документації.

У першому розділі визначено сутність поняття «електронний документ», охарактеризовано його відмінності від традиційного паперового аналога та проаналізовано основні методи захисту, зокрема шифрування, електронний підпис, контроль доступу та системи резервного копіювання. Особливу увагу приділено правовим аспектам використання електронного підпису та його ролі в забезпеченні юридичної значущості документа. Окреслено основні типи загроз для електронних документів: технічні збої, несанкціонований доступ, зловмисне програмне забезпечення ін.

У другому розділі досліджено актуальні технологічні рішення у сфері захисту інформації, зокрема, системи електронного архівування, хмарні сховища з підвищеним рівнем безпеки, засоби автентифікації користувачів та технології блокчейн. Особлива увага приділена перспективам розвитку систем захисту в умовах цифрової трансформації, глобалізації кіберзагроз та зростання обсягу оброблюваних даних. Розкрито важливість інтегрованого підходу до безпеки, який поєднує технічні інструменти з нормативним регулюванням та підвищенням цифрової грамотності персоналу.

Ключові слова: електронний документ, інформаційна безпека, цифрова трансформація, захист даних, електронний підпис, кіберзагрози.

ЗМІСТ

ВСТУП

Актуальність дослідження проблем захисту електронних документів зростає у зв'язку з їхньою інтеграцією в усі сфери сучасного життя, наприклад, бізнес, державне управління, освіту та інші галузі. Електронні документи забезпечують зручність й оперативність обміну інформацією, але одночасно з їх використанням з'являються нові ризики. Найбільшими з них є загрози несанкціонованого доступу, втрати або фальсифікації даних, що може призвести до серйозних фінансових і репутаційних збитків. Тому захист цих документів набуває важливого значення для збереження довіри до систем та процесів, в яких вони використовуються.

Вкрай важливим є дотримання правових норм, що регулюють захист персональних даних і електронний документообіг. Закони та нормативні акти вимагають від організацій та державних установ забезпечення належного захисту електронних документів, що включає використання методів автентифікації, криптографії та інших технічних засобів, що гарантують цілісність і конфіденційність інформації. Тому дослідження в галузі безпеки електронних документів є важливим не тільки з технічної, але й з правової точки зору, оскільки воно безпосередньо впливає на виконання правових вимог і захист прав громадян.

В умовах сучасних кіберзагроз важливість впровадження ефективних технологій збереження та захисту електронних документів стає ще більш очевидною. Кіберзлочинці постійно вдосконалюють свої методи атак, що вимагає від організацій постійного оновлення засобів захисту. Від правильного вибору і впровадження технологій захисту залежить стабільність і безпека інформаційної інфраструктури як на рівні окремих підприємств, так і в державному секторі загалом. Тому дослідження новітніх методів і підходів до захисту електронних документів є надзвичайно актуальним для забезпечення безпеки в цифровому середовищі.

Мета дослідження – дослідження ефективних підходів до забезпечення захисту електронних документів і організації їхнього зберігання. Для досягнення означеної мети автором дослідження поставлено наступні **завдання:**

– проаналізувати поняття електронного документу та методи його захисту;

– розглянути основні загрози для електронного документу;

– окреслити сучасні технологічні рішення у сфері захисту електронних документів;

– сформувати перспективи розвитку систем захисту в умовах цифрової трансформації та зростаючих кіберзагроз.

Об’єктом дослідження є процеси забезпечення захисту та організації зберігання електронних документів у сучасному інформаційному середовищі.

Предметом дослідження є методи, засоби та технології, що забезпечують ефективний захист і організацію зберігання електронних документів, а також нормативно-правові та технічні підходи до їх реалізації.

Стан наукової розробки проблеми. Теоретичні засади дослідження зберігання та захисту електронних документів вивчались В. Варейчук [2], С. Гаркушею [3], Д. Ковальовим [14], О. Ковальчук [15], О. Лабою [20] та ін. У цих працях розкрито сутність поняття «електронний документ», а також методи його захисту; проаналізовано основні загрози для електронного документу. Актуальні тенденції розробки системи захисту електронних документів є об’єктом наукових розвідок для А. Досенко [6], Н. Думанської [7], Д. Караман [12], О. Насатова та Г. Плєхової [24] та ін. Названі вчені досліджують сучасні технологічні рішення, що мають на меті мінімізувати вплив кіберзагроз на цілісність та безпеку електронних документів. Недостатньо розкритою залишається проблема пошуку перспективних

методів захисту електронних документів, що вимагає більш ґрунтовних досліджень цієї теми у наукових колах України та світу.

Методи дослідження. В ході написання кваліфікаційної роботи було використано наступні методи дослідження:

– аналізу та синтезу – використано при аналізі теоретичних засад дослідження зберігання та захисту електронних документів;

– метод індукції та дедукції – застосовано при вивченні актуальних тенденцій та перспектив розробки систем захисту електронних документів;

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

Наукова новизна дослідження полягає у ґрунтовному аналізі сучасних методів захисту електронних документів з урахуванням новітніх технологій. У роботі систематизовано актуальні загрози та досліджено модель захисту, яка поєднує технічні та правові інструменти безпеки. Окрім того, дослідження розглядає перспективи впровадження інноваційних рішень у вимірі цифрової трансформації.

Практичне значення дослідження полягає в можливості застосування отриманих результатів для вдосконалення систем електронного документообігу в державному та приватному секторах. Матеріали кваліфікаційної роботи сприяють підвищенню рівня безпеки даних, зниженню ризиків кібератак та забезпеченню відповідності чинному законодавству. Результати можуть бути використані як основа для розробки внутрішніх політик інформаційної безпеки в організаціях.

Апробація результатів дослідження. Основні положення і висновки дослідження були представлені на наступних конференціях:

1. Актуальні проблеми розвитку природничих та гуманітарних VIII Міжнародна науково-практична конференція (14 листопада 2024 року, м. Луцьк).

2. Гуманітарний простір науки: досвід та перспективи»: 44-а Міжнародна науково-практична інтернет-конференція (30 травня 2025 року, м. Переяслав-Хмельницький).

Публікації. Результати бакалаврської роботи опубліковані у формі тез:

1. Кукла В. Забезпечення захисту й організація зберігання електронних документів. *Актуальні проблеми розвитку природничих та гуманітарних наук: збірник матеріалів VIII Міжнар. наук. практ. конф*. (14 листопада 2024 р., м. Луцьк) / відп. ред. Шуляк Н. О., Зінченко М. О. Луцьк, 2024.

2. Кукла В. Забезпечення збереження й безпеки електронних документів. *Гуманітарний простір науки: досвід та перспективи»*: Матеріали Міжнародної науково-практичної інтернет-конференції, 30 травня 2025 року. Вип. 44. Переяслав-Хмельницький, 2025.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗБЕРІГАННЯ ТА ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

1.1. Поняття електронного документу та методи його захисту

Електронний документ – це інформаційне повідомлення, зафіксоване в електронній формі, яке має юридичну силу та може бути використане в діловодстві. У зв'язку зі стрімким розвитком цифрових технологій постає необхідність забезпечення надійного захисту таких документів від несанкціонованого доступу, змін або знищення.

Електронний документ має кілька ключових особливостей. По-перше, він є окремим документом, який відрізняється від інших електронних документів, включно з різними його версіями. По-друге, електронному документу властива логічна структура, що забезпечує взаємозв'язок між його елементами, як-от текстові частини, таблиці, зображення чи заголовки, які разом формують цілісний документ. Це відрізняє його від інших форм даних. По-третє, електронні документи дедалі частіше набувають мультимедійного характеру (Compound-Document), що допускає інтеграцію звуку та відео [44, с. 19].

У науковій літературі існують різні підходи до визначення цього поняття. Одні дослідники наголошують на технологічному аспекті, підкреслюючи, що електронний документ – це інформаційний ресурс, представлений у форматі, придатному для автоматизованої обробки. Інші зосереджують увагу на його юридичному значенні, зазначаючи, що електронний документ є носієм правової інформації, що має силу документа на рівні з паперовими аналогами, за умови дотримання вимог щодо автентичності та захисту.

Також серед наукових підходів виділяють концепції, які зосереджуються на структурі документа. Електронний документ розглядається як сукупність текстових, графічних, мультимедійних та інших

елементів, упорядкованих у логічній формі, що забезпечує цілісність і доступність інформації.

Електронний документ є базовою, автономною одиницею, яка формується, зберігається та використовується в електронних системах документообігу. Однак вважається, що електронний документ сам по собі, без відповідного контексту, не може бути достатньо інформативним. Він набуває повноти значення лише в поєднанні з контекстуальною інформацією або іншими пов’язаними електронними документами [40].

Використання електронних документів має низку переваг і недоліків, які важливо враховувати залежно від контексту їх застосування.

Серед основних переваг електронних документів варто зазначити зручність і оперативність їхнього обігу. Завдяки цифровій формі інформація легко передається, зберігається та обробляється, що значно прискорює робочі процеси. Електронні документи також дозволяють суттєво зекономити матеріальні ресурси, оскільки зменшують потребу у використанні паперу та фізичних носіїв. Іншою важливою перевагою є можливість інтеграції мультимедійних елементів, як-от зображення, аудіо чи відео, що робить документи більш інформативними. До того ж електронні документи забезпечують легкий доступ до архівів і дозволяють автоматизувати їхній пошук та обробку.

Попри очевидні переваги, впровадження систем електронного документообігу має і певні недоліки, які можуть стримувати підприємство від переходу на такі технології. По-перше, впровадження системи вимагає значних фінансових витрат, які залежать від кількості користувачів та масштабу підприємства. Після придбання системи необхідно виділити час на її встановлення, налаштування та адаптацію до потреб організації, що може зайняти тривалий період. Додатково, для забезпечення стабільної роботи системи підприємству потрібен кваліфікований адміністратор, який відповідатиме за її обслуговування, вирішення технічних питань і підтримку користувачів. Усіх співробітників, які будуть працювати з електронним

документообігом, необхідно навчити, що також потребує ресурсів. Щоб уникнути втрати інформації, необхідно організувати створення резервних копій бази документів, а для захисту даних передбачити розмежування доступу, впровадження електронних підписів та системи захисту від зовнішніх загроз. Крім того, якщо у партнерів підприємства не використовується електронний документообіг, може виникнути необхідність підтримувати одночасно і паперову, і електронну форми документообігу, що створює додаткове навантаження. Усі ці фактори вимагають ретельного аналізу, щоб оцінити доцільність впровадження системи в конкретних умовах підприємства [3, с. 262].

Ще однією проблемою у термінології та правовому регулюванні є невідповідність наявних в Україні нормативних актів міжнародним стандартам в області електронного діловодства. Наприклад, Європейський Союз відмовився від використання терміну «електронний цифровий підпис», замінивши його на «електронний підпис». Термін «електронний підпис» вперше був введений Європейською Комісією в оновленій версії проекту Директиви ЄС 1999/93/EG з метою уникнення прив'язки правового регулювання до конкретної технології [20, с. 55].

Згідно з даними ООН, у 2008 році Україна займала 41-ше місце серед 193 країн у рейтингу готовності до електронного уряду за індексом EGDI. Однак у 2010 році вона втратила 13 позицій, опустившись на 54-те місце, а в 2012 році рейтинг знизився ще на 14 позицій – до 68-го місця. У 2014 році спад тривав, і Україна опустилася ще на 19 позицій, посівши 87-ме місце. У 2018 році ситуація дещо покращилася: країна піднялася до 82-го місця, а в 2020 році досягла 69-го місця у світовому рейтингу. Це свідчить про поступове зростання України у сфері цифрового урядування, що включає розвиток електронного документообігу на підприємствах, в установах, організаціях, а також у органах державної влади [16].

Формати зберігання та обробки електронних документів відіграють ключову роль у забезпеченні ефективності їх використання в електронному

документообігу. Вони визначають, як інформація організовується, зберігається та обробляється у цифровому середовищі, впливаючи на сумісність, безпеку та доступність даних.

Сучасні формати електронних документів можна умовно поділити на кілька груп. Одні з них, як-от PDF (Portable Document Format), забезпечують збереження структури, макету та дизайну документа незалежно від платформи чи пристрою. Цей формат широко використовується для офіційних документів завдяки підтримці електронних підписів і шифрування.

Інші формати, наприклад, DOCX (Microsoft Word) або ODT (Open Document Text), орієнтовані на зручність редагування, що робить їх придатними для створення та внесення змін у текстові документи. Водночас вони дозволяють інтеграцію мультимедійних елементів, як-от зображення чи таблиці.

Для таблиць і структурованих даних популярними є формати XLSX (Microsoft Excel) та CSV (Comma-Separated Values). Перший забезпечує багатофункціональність у роботі з числовими даними, а другий є зручним для імпорту й експорту інформації між різними системами.

Для довготривалого зберігання документів із забезпеченням автентичності використовуються спеціалізовані формати, як-от PDF/A, який оптимізований для архівування та виключає можливість змін.

Інтеграція мультимедійних елементів або комплексних даних може вимагати використання форматів XML (Extensible Markup Language) або JSON (JavaScript Object Notation). Вони дозволяють структурувати дані, полегшуючи їх обробку та сумісність із різними програмними рішеннями.

Згідно зі статтею 9 Закону № 851, електронний документообіг охоплює всі процеси, пов’язані зі створенням, обробкою, відправленням, передачею, отриманням, зберіганням, використанням і знищенням електронних документів (ЕД). Усі ці дії здійснюються із забезпеченням перевірки їхньої цілісності, а за потреби – із підтвердженням факту отримання таких документів [28].

Незалежно від змін, електронний документообіг повинен виконувати три ключові функції: доставку документів до адресата, забезпечення працівників підприємства управлінською інформацією, що міститься у документах, та здійснення багаторівневого контролю за виконанням документів. Завдяки впровадженню комплексної комп'ютеризації всі ці завдання здатна реалізувати спеціалізована комп'ютерна програма. Роль користувача зводиться до моніторингу роботи програми та виправлення помилок у разі, якщо вони виникають і не можуть бути автоматично усунені самою системою [33].

Цифровий світ активно розвивається, і логічним кроком стало перенесення практики підписів у цифрове середовище. Вперше концепцію цифрових підписів запропонували Діффі та Хеллман [46]. У своїй роботі вони теоретично описали схему цифрового підпису, припускаючи її можливе існування. Основна ідея полягала в тому, що кожен користувач повинен мати відкритий (загальнодоступний) ключ для перевірки підпису, одночасно зберігаючи секретний (конфіденційний) ключ для створення цього підпису. У цій схемі підпис для певного повідомлення є унікальним значенням, яке залежить від самого повідомлення та конфіденційного ключа підписанта. При цьому будь-хто може перевірити автентичність підпису за допомогою відкритого ключа. Система побудована таким чином, що перевірка підпису є простою процедурою, тоді як його підробка надзвичайно складна. Це забезпечується тим, що конфіденційний ключ є секретним і обов'язковим для створення підпису, а без нього зімітувати автентичність неможливо [30, с. 10].

Електронні документи знайшли широке застосування у різних сферах діяльності, значно спрощуючи та оптимізуючи робочі процеси.

У бізнесі електронні документи стали невід'ємною частиною операційної діяльності. Вони використовуються для обміну комерційною інформацією, оформлення угод, створення звітності та ведення внутрішнього документообігу. Завдяки електронним підписам документи мають юридичну

силу, що дозволяє компаніям скоротити час на погодження контрактів і знизити витрати, пов’язані з друком та зберіганням паперових документів.

У державному секторі електронні документи активно впроваджуються для підвищення ефективності управління. Вони забезпечують швидкий обмін інформацією між відомствами, сприяють автоматизації адміністративних процесів і створенню електронних архівів. Особливо важливим є використання електронних документів у сфері електронного урядування, де громадяни можуть подавати заявки, отримувати довідки та взаємодіяти з державними органами без відвідування установ.

Освітня сфера також активно інтегрує електронні документи. Вони використовуються для оформлення та обміну академічними довідками, сертифікатами, звітністю, а також для створення й зберігання навчальних матеріалів. Використання електронних систем документообігу в освітніх установах дозволяє забезпечити ефективну комунікацію між викладачами, адміністрацією та студентами, спрощуючи доступ до необхідної інформації.

Забезпечення надійного захисту даних є необхідною умовою для ефективного функціонування як окремих організацій, так і суспільства в цілому. У зв’язку з цим вивчення та впровадження методів інформаційної безпеки є не лише актуальним, але й критично важливим завданням.

Криптографічні методи захисту даних є основою забезпечення інформаційної безпеки, особливо в контексті електронних документів. Вони спрямовані на шифрування інформації для захисту її від несанкціонованого доступу, забезпечення цілісності даних і підтвердження автентичності їхнього джерела.

Сьогодні криптографія як наукова дисципліна та криптографічний захист інформації як окрема сфера діяльності охоплюють широкий спектр питань. Вони включають шифрування даних, впровадження сучасних технологій в електронну торгівлю, використання у системах автоматизованого управління, звітності та контролю. Розробка високопродуктивних методів шифрування та розшифрування з високим

рівнем криптографічної стійкості є ключовим елементом у забезпеченні інформаційної безпеки. Методи криптографічного захисту інформації включають системи шифрування даних, алгоритми, що запобігають нав'язуванню фальшивої інформації (MAC-коди та алгоритми електронного цифрового підпису), а також криптографічні протоколи, що забезпечують розподіл ключів, автентифікацію та підтвердження факту передачі або прийому інформації [21, с. 373].

Симетричне шифрування є методом криптографії, у якому для шифрування та дешифрування даних використовується один і той самий ключ. Такий підхід став широко застосовуваним у другій половині 20-го століття, спочатку для забезпечення безпеки комунікацій в урядових і військових структурах. Наразі симетричні ключі активно використовуються в різноманітних комп'ютерних системах для захисту персональних даних. Основою симетричного шифрування є спільний ключ, який використовується обома сторонами для шифрування і дешифрування інформації. Цей ключ дозволяє перетворити відкритий текст (тобто вихідні дані або повідомлення) на зашифрований текст за допомогою спеціального алгоритму, відомого як шифр. Процес шифрування полягає в обробці відкритого тексту цим шифром, у результаті чого утворюється зашифрований текст, який може бути дешифрований лише за наявності того ж самого ключа [39].

Головною перевагою симетричного шифрування є його висока швидкість і низькі обчислювальні витрати, що робить його ефективним для роботи з великими обсягами даних. Проте одним із ключових викликів є забезпечення безпечної передачі та зберігання секретного ключа. Якщо ключ потрапить до зловмисника, це поставить під загрозу всю захищену інформацію.

Симетричне шифрування широко використовується у протоколах передачі даних, як-от SSL/TLS, а також у системах зберігання даних для захисту файлів і баз даних. Найбільш відомими алгоритмами симетричного шифрування є AES (Advanced Encryption Standard), DES (Data Encryption

Standard) та його модифікація Triple DES. Незважаючи на свої обмеження, симетричне шифрування залишається невід'ємною частиною сучасної криптографії, забезпечуючи базовий рівень захисту в багатьох системах.

Асиметричне шифрування є криптографічною системою, яка базується на використанні двох ключів: відкритого та закритого. На відміну від симетричних методів, де застосовується один спільний ключ, асиметричний підхід забезпечує розширені можливості й унікальні характеристики для вирішення завдань, які є складними для інших криптографічних методів. Завдяки парі ключів асиметричне шифрування дозволяє ефективно вирішувати проблеми безпечного обміну даними, автентифікації та цифрового підпису. Цей метод став невід'ємною складовою сучасних технологій кібербезпеки, забезпечуючи високий рівень захисту інформації в комп'ютерних системах та мережах [7].

Електронний підпис є ключовим інструментом забезпечення автентичності електронних документів у сучасному цифровому середовищі. Він виступає як цифровий аналог власноручного підпису, підтверджуючи особу підписанта та цілісність документа. Згідно зі статтею 207 Цивільного кодексу України, правочин вважається укладеним у письмовій формі, якщо воля сторін передана за допомогою телетайпного, електронного або іншого технічного засобу зв'язку [37]. Таким чином, ця норма прирівнює електронні документи до паперових і дозволяє їх підписання електронним підписом.

Технічно електронний підпис базується на використанні криптографічних алгоритмів, зокрема технології відкритого ключа. У процесі підписання створюється унікальний зашифрований код, який прив'язаний до конкретного документа та особи, що його підписує. Це гарантує, що документ не був змінений після накладення підпису, а його авторство легко можна підтвердити.

Окрім автентичності, електронний підпис виконує роль інструмента юридичної легітимації документа. У багатьох країнах, зокрема Україні, законодавство визнає електронний підпис як рівнозначний власноручному за

умови, що він відповідає встановленим стандартам. Це робить можливим офіційний документообіг у цифровій формі, спрощуючи й прискорюючи юридичні та ділові процеси. Електронний підпис також забезпечує конфіденційність і безпеку. Завдяки шифруванню лише уповноважені особи можуть отримати доступ до змісту документа, а будь-яка спроба його підробки чи зміни стає очевидною. Це особливо важливо для фінансових, юридичних та інших чутливих документів.

Отже, електронний документ є важливим елементом сучасного документообігу, який забезпечує зручність, оперативність і збереження інформації в цифровому середовищі. Водночас е-документ вимагає ефективного захисту від загроз, пов’язаних із кібератаками, несанкціонованим доступом та фальсифікацією. Методи захисту електронних документів відіграють ключову роль у забезпеченні безпеки електронних документів. Комплексне застосування технічних і правових засобів дозволяє зберігати цілісність, конфіденційність та юридичну значущість цифрових документів. Надійний захист електронного документообігу є необхідною умовою для розвитку цифрової економіки та електронного врядування.

1.2. Основні загрози для електронного документу

Для забезпечення високого рівня безпеки електронних документів і надійного функціонування систем електронного документообігу необхідно створити ефективні умови захисту системи від можливих загроз. Система захисту електронних документів являє собою сукупність програмно-технічних засобів, спрямованих на ідентифікацію та усунення потенційних загроз інформаційній безпеці. Для її створення важливо детально визначити спектр можливих загроз, проаналізувати вразливості системи, оцінити ризики їх реалізації та розмір потенційних збитків у разі порушення безпеки [32, с. 60].

Як ми вже згадували, загрози безпеці електронних документів є результатом різноманітних факторів, які можуть виникати як через зовнішні

атаки (наприклад, хакерські вторгнення), так і через внутрішні недоліки (помилки персоналу, недостатній рівень захисту). Втрата або модифікація важливих даних може мати серйозні наслідки, зокрема для компаній та організацій, де такі документи використовуються для прийняття важливих рішень або виконання зобов’язань.

Також існує ризик від використання ненадійних або застарілих технологій, що не забезпечують належного захисту від зовнішніх загроз, або відсутність належних протоколів для захисту даних під час їх передачі через інтернет. Зовнішні ризики можуть бути також пов’язані з фізичними загрозами, як-от крадіжка або пошкодження носіїв інформації, що зберігаються за межами організації.

Несанкціонований доступ до електронних документів є однією з найбільших загроз для безпеки інформації. Він передбачає отримання доступу до конфіденційних або важливих даних особами, які не мають на це права. Такий доступ може бути здійснений різними методами, серед яких хакерські атаки, соціальна інженерія, фішинг, або використання уразливостей в системах безпеки.

Причини несанкціонованого доступу до інформації можуть бути різноманітними і пов’язані як з технічними, так і з організаційними факторами. Однією з основних причин є помилки конфігурації, зокрема неправильне налаштування прав доступу, брандмауерів або обмежень на кількість запитів до баз даних. Це може створювати вразливості, через які зловмисники можуть отримати доступ до системи. Ще однією причиною є недостатній рівень захисту засобів авторизації, що може призвести до викрадення паролів або смарт-карт, а також до несанкціонованого доступу через фізичний доступ до малозахищеного обладнання. Ситуація ускладнюється, якщо робочі місця співробітників залишаються незаблокованими під час їхньої відсутності. Іншими факторами є помилки в програмному забезпеченні, які можуть виникати через недоліки у коді, що дозволяє зловмисникам скористатися уразливостями для отримання доступу

до даних. Також значним ризиком є зловживання службовими повноваженнями, наприклад, викрадення резервних копій або несанкціоноване копіювання інформації на зовнішні носії при наявності відповідних прав доступу. Продовженням цього є прослуховування каналів зв'язку в разі використання незахищених з'єднань в межах локальних обчислювальних мереж, що може призвести до перехоплення даних. Крім того, використання клавіатурних шпигунів, вірусів та троянів на комп'ютерах співробітників також створює додаткові ризики для безпеки інформації [10].

Також важливо враховувати загрозу втрати конфіденційності, яка виникає через витоки даних. Це може статися в результаті діяльності шкідливого програмного забезпечення, фішингових атак або внутрішніх витоків через недобросовісних співробітників.

На сьогодні фішинг-атаки можуть набувати різних форм. Зазвичай зловмисники використовують цей метод для викрадення у жертви її логінів, паролів, номерів кредитних карток або іншої фінансової інформації. Ця форма шахрайства здобула значну популярність серед злочинців, оскільки маніпулювати людиною значно легше, ніж скомпрометувати інтернет-мережу або програмне забезпечення. Для здійснення фішинг-атаки зловмиснику достатньо надіслати просте повідомлення з вимогою надати доступ до особистої інформації. З часом фішинг-атаки стали більш складними та професіональними. Раніше електронні листи з фішинговими посланнями можна було легко виявити завдяки невідомим або замаскованим відправникам, граматичним помилкам або підмінам у словах та посиланнях, що виглядали схожими на оригінальні. Сьогодні ж такі повідомлення створюються фахівцями, які забезпечують їх високий рівень якості, без явних помилок. Дизайн веб-сайтів, на які ведуть фішингові посилання, часто повністю або дуже схоже відтворює оригінали, що робить такі атаки значно складнішими для виявлення, навіть із використанням сучасних засобів захисту [26, с. 60].

Фішинг є видом кіберзлочинності, що полягає в обманному отриманні конфіденційної інформації, такої як паролі, банківські реквізити або номери кредитних карток. Зловмисники маскуються під надійні джерела – банки, компанії чи онлайн-сервіси – і надсилають повідомлення з метою змусити користувачів розкрити особисті дані. Серед основних методів фішингу вирізняють:

1. Фішингові електронні листи – це повідомлення, які виглядають як офіційні звернення від відомих організацій і містять посилання на фальшиві веб-ресурси, де користувача просять ввести особисту інформацію.

2. Фішингові веб-сайти – підроблені сайти, що копіюють зовнішній вигляд справжніх онлайн-ресурсів (банків, магазинів тощо) з метою отримання даних користувача.

3. Соціальний фішинг – метод, при якому злочинці використовують інформацію з соціальних мереж, щоб створити індивідуалізовані повідомлення, які виглядають переконливо й змушують користувача поділитися особистими даними [14, с. 73].

Фішинг фактично є однією з форм соціальної інженерії, що базується на необізнаності користувачів щодо основ мережевої безпеки. Багато людей не підозрюють, що надійні сервіси ніколи не надсилають повідомлень із проханням надати логін, пароль чи інші конфіденційні дані. Вперше техніку фішингу детально описали ще у 1987 році, а сам термін уперше з’явився 2 січня 1996 року в групі новин alt.online-service.America-Online у мережі Usenet. Існує також ймовірність, що згадки про цей термін траплялися раніше – наприклад, у хакерських журналах [45].

Фішингові атаки стають дедалі витонченішими, при цьому активно застосовуються методи соціальної інженерії. Основна мета зловмисників – залякати користувача, вигадати критичну ситуацію, яка змусить його розкрити конфіденційні дані. Найчастіше такі повідомлення містять погрози, наприклад, щодо блокування рахунку в разі невиконання вказівок («якщо ви не надасте свої дані протягом тижня, ваш рахунок буде заблоковано»).

Цікаво, що іноді фішери в якості приводу вимагають надати дані нібито з метою покращення систем захисту від фішингу («щоб убезпечити себе, перейдіть за посиланням і введіть логін та пароль»).

Цільовий фішинг використовує ще складніші та технологічно розвинуті схеми, ніж звичайний. Зловмисники ретельно вивчають своїх потенційних жертв: аналізують профілі в соціальних мережах, дізнаються про їх звички, використовувані сервіси, коло спілкування тощо. Завдяки такій інформації фішингові листи виглядають дуже переконливо.

Оскільки людина схильна емоційно реагувати на важливі для неї події, фішери прагнуть викликати тривогу та змусити діяти негайно. Саме тому повідомлення з заголовком «щоб відновити доступ до банківського рахунку...» часто привертає увагу і спонукає користувача перейти за вказаним посиланням для отримання подальшої інформації [1, с. 179].

Не менш серйозною є проблема порушення цілісності електронних документів. Хакери чи інші зловмисники можуть змінити або знищити дані, що призведе до втрати їхньої надійності та правової цінності. Поширеним прикладом є атаки типу «ransomware», коли доступ до документів блокується, а їх цілісність може бути поставлена під загрозу.

З появою програмування з’явилися і віруси, що здатні атакувати програмно-апаратні комплекси. Деякі з них потайки проникають у систему і збирають приватну інформацію, інші шкодять «залізу» або важливим системним файлам, а деякі просто розважають користувача і не здаються особливо небезпечними – вірусів існує безліч, і їхні варіанти постійно зростають. Однією з найбільш небезпечних категорій вірусів є шифрувальники (також відомі як здирники або ransomware), які, потрапивши в комп’ютер, шифрують файли певних форматів, блокують до них доступ, а потім висувають вимогу викупу, вказують суму, яку треба перерахувати на певний рахунок. Після надходження грошей обіцяють розшифрувати файли. Однак сумна реальність така, що шифрувальники часто не мають

інструментів для відстеження, з якого комп'ютера надійшли гроші, тому жертви залишаються і без коштів, і без своїх файлів [11].

Окрім цього, існує загроза втрати доступності документів через збої в роботі серверів, апаратні несправності або атаки типу DDoS, які паралізують функціонування систем. Така ситуація може спричинити серйозні проблеми, особливо в організаціях, які покладаються на безперервний доступ до інформації.

Широке поширення мереж на основі протоколу TCP/IP спричинило появу методів обходу захисту та розробку програм для здійснення неправомірних дій у таких мережах. Однією з найпопулярніших загроз останнім часом стали ddos-атаки. Цей недорогий і ефективний метод використовують для атак на державні та корпоративні ресурси з різними цілями, як-от конкурентна боротьба, здирництво, прикриття інших вторгнень або завдання іміджевого збитку.

Dos (Denial of Service) можна перекласти як «відмова в обслуговуванні», а ddos означає «розподілену відмову в обслуговуванні». ddos-атака передбачає низку дій, спрямованих на перевантаження серверу та викликання зависання системи через велику кількість хибних запитів [41, с. 237].

Основні ознаки ddos-атак можна визначити за такими параметрами:

1. Кількість ARP-запитів. Цю інформацію можна переглянути через командний рядок. Для маршрутизаторів Cisco використовуються команди show arp або show ip arp, а для інших – «arp –a» або «arp –v». Також можна перевірити це через інтерфейс. За нормальних умов мережі кількість ARP-запитів залишається стабільною, з незначними коливаннями. При ddos-атаки кількість ARP-запитів збільшується порівняно з нормальною ситуацією.

2. Використання пам'яті маршрутизатора. Для Cisco маршрутизаторів це можна перевірити за допомогою команди router#show memory, а для інших – через інтерфейс (не всі моделі підтримують цю функцію). Під час звичайної роботи пам'ять маршрутизатора

використовується стабільно в межах певного діапазону, в той час як під час ddos-атаки спостерігається значне збільшення навантаження на пам’ять.

3. Використання процесорного часу. Цю інформацію можна отримати через командний рядок. Для Cisco маршрутизаторів використовується команда Router# show proc cpu sort, а для інших – через telnet до IP-адреси маршрутизатора, після чого вводиться логін та пароль для доступу до налаштувань. Це відображає таблицю завантаження процесора. Під час нормальної роботи мережі використання процесора коливається в межах мінімальних значень, в той час як при ddos-атаці спостерігається значне збільшення навантаження на процесор.

4. Кількість записів у таблиці NAT/PAT. Для маршрутизаторів Cisco використовуються команди Router# show ip route або Router# show ipv6 route, для інших – «show ip nat translation». За нормальних умов кількість записів у таблиці NAT/PAT залишається стабільною протягом часу. Під час ddos-атаки кількість записів значно зростає порівняно з нормальною роботою мережі [2, с. 419].

Підробка та зміна електронних документів є серйозними загрозами для їхньої цілісності та достовірності. Зловмисники можуть змінювати вміст електронних документів з метою фальсифікації даних, що має тяжкі наслідки, особливо у таких сферах, як фінанси, право, медичні записи чи ділова документація. Підроблені документи можуть бути використані для обману, маніпулювання результатами або навіть скоєння фінансових злочинів. Вони можуть бути змінені за допомогою спеціального програмного забезпечення, яке дозволяє редагувати або видаляти важливі частини інформації, залишаючи враження, що документ є автентичним.

Існує кілька методів підробки, зокрема зміну тексту документа, вставку нових елементів або заміну важливих даних без залишення слідів. Одним із найбільш складних для виявлення методів є використання технік маніпулювання метаданими, які можуть не змінювати зовнішній вигляд

документа, але приховують зміни на рівні його властивостей або історії редагувань.

Шкідливе програмне забезпечення, таке як віруси, трояни і шпигунські програми, є однією з основних загроз для безпеки електронних документів. Віруси здатні поширюватися від одного комп'ютера до іншого, змінюючи або пошкоджуючи дані, що зберігаються на пристроях. Вони можуть активуватися при відкритті заражених файлів чи відвідуванні шкідливих вебсайтів, що створює серйозні ризики для конфіденційності та цілісності інформації.

«Троянський кінь» («Trojan Horse») – це тип шкідливого програмного забезпечення, який може включати в себе програми-вандали, «дроппери» для вірусів, «злі жарти», а також деякі види програм-люків, логічних бомб, програм для вгадування паролів і програм для прихованого адміністрування. Останні чотири категорії можуть існувати не тільки як «трояни», а й як окремі програмні продукти, які також здатні викликати шкідливі ефекти в операційній системі. «Троянський кінь» – це програма, що, окрім своїх основних функцій, зазначених в документації, виконує додаткові, не зафіксовані в документації дії. Він може виглядати як корисна програма або процес, однак в її коді приховані шкідливі функції, які активуються під певними умовами і виконують небажані або шкідливі операції [15, с. 19].

Шпигунські програми, або "спайвери", працюють у фоновому режимі і збирають особисту інформацію без ведома користувача. Вони можуть реєструвати натискання клавіш, стежити за активністю в інтернеті та передавати зібрані дані стороннім особам. Це може призвести до викрадення логінів, паролів, фінансових даних та іншої важливої інформації, що складає серйозну загрозу безпеці електронних документів.

Захист від шкідливого програмного забезпечення вимагає використання антивірусних програм, оновлення систем безпеки, а також обережності користувачів при відкритті невідомих файлів чи переході за сумнівними посиланнями.

Технічні причини втрати даних можуть бути різноманітними і часто пов’язані з несправностями обладнання або програмного забезпечення. Однією з основних причин є апаратні збої, які можуть виникнути через поломку жорстких дисків, пошкодження носіїв інформації або відмову сервера. Такі поломки призводять до втрати доступу до даних або до їхнього пошкодження, що робить неможливим відновлення інформації.

Іншою технічною причиною є помилки в програмному забезпеченні. Неправильна робота програм, що відповідають за зберігання та обробку даних, може призвести до їхньої часткової або повної втрати. Наприклад, баги в операційних системах або помилки в алгоритмах резервного копіювання можуть спричинити несанкціоноване видалення або корупцію файлів. Також інколи виявляються помилки в обробці даних, коли програми неправильно інтерпретують або зберігають інформацію, що може призвести до її пошкодження.

Збої в електричному живленні, зокрема раптові відключення електрики або нестабільне живлення, також можуть спричинити втрату даних. Вони можуть порушити роботу процесів збереження файлів або привести до неповного запису даних на носій. В умовах неякісного захисту від електричних стрибків ці проблеми можуть мати серйозні наслідки для збереження інформації.

Також варто зазначити, що вірогідність втрати даних збільшується у разі відсутності належної системи резервного копіювання. Без регулярних копій даних відновлення після технічних збоїв може бути неможливим або надзвичайно складним.

Створення та реалізація електронної системи вимагає комплексного підходу, що включає низку стандартних заходів. Зокрема, необхідно провести аналіз основних властивостей і функцій електронних документів, здійснити класифікацію загроз інформаційної безпеки, вивчити вимоги до її забезпечення, а також визначити та розробити відповідні механізми захисту інформації [33, с. 54].

Сучасне цифрове середовище є надзвичайно вразливим до різноманітних атак та порушень безпеки. Як внутрішні, так і зовнішні фактори можуть суттєво вплинути на цілісність, конфіденційність і доступність електронних документів. З одного боку, внутрішні загрози часто виникають через несанкціонований доступ працівників, помилки у конфігурації систем або зловживання службовими повноваженнями. З іншого боку, зовнішні загрози, наприклад, кібератаки, віруси, фішинг або зловмисні програми, стають серйозними викликами для безпеки.

Технічні помилки, апаратні збої та відсутність належного захисту інформації підвищують ймовірність втрати даних або компрометації документів. Важливою проблемою є також невідповідність національних нормативних актів міжнародним стандартам у сфері електронного діловодства, що ускладнює забезпечення належного рівня захисту.

Таким чином, основними загрозами для електронних документів є їхня вразливість до несанкціонованого доступу, модифікації, пошкодження або втрати. Хакерські атаки, зокрема фішинг чи шкідливі програми, можуть спричинити викрадення або зміну вмісту документів. Іншою серйозною загрозою є недостатній рівень захисту даних при їхньому зберіганні або передачі, що може призвести до витоку конфіденційної інформації. Крім того, відсутність надійної автентифікації та електронного підпису може знизити довіру до документів, що впливає на їх юридичну значущість. Для мінімізації таких загроз необхідно впроваджувати комплексні заходи захисту, наприклад, криптографію, системи моніторингу та регулярне оновлення програмного забезпечення.

РОЗДІЛ 2
АКТУАЛЬНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗРОБКИ СИСТЕМИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

2.1. Сучасні технологічні рішення у сфері захисту електронних документів

Сучасні технологічні рішення у сфері захисту електронних документів спрямовані на забезпечення їх цілісності, конфіденційності та доступності. Завдяки розвитку криптографічних методів, систем аутентифікації та електронного підпису, з’являються нові підходи до захисту даних, що дозволяють ефективно протистояти кіберзагрозам. У цьому вимірі важливим є постійне вдосконалення технологій для адаптації до нових проблем у цифровому середовищі.

Електронний документ, який використовується у діловодстві з незакінченим терміном дії, має зберігатися в робочому каталозі автоматизованого робочого місця працівника або на сервері відповідно до встановлених процедур зберігання електронних документів, зокрема всі необхідні реквізити та електронні цифрові підписи. Документ, юридична сила якого втрачається через анулювання сертифіката електронного цифрового підпису, зазначеного в ньому, повинен бути переданий до електронного архіву для тимчасового зберігання. При цьому термін зберігання електронних документів на носіях інформації має бути не меншим за термін, визначений законодавством для аналогічних паперових документів [25, с. 254].

Хмарні технології стали невід’ємною частиною сучасного управління електронними документами, адже вони забезпечують доступність, гнучкість та високий рівень безпеки даних. Завдяки таким платформам, як Google Drive, Dropbox і Microsoft OneDrive, користувачі можуть зберігати файли в мережі інтернету, що дозволяє отримувати доступ до них з будь-якого пристрою, підключеного до інтернету.

Google Drive відрізняється глибокою інтеграцією з іншими сервісами Google: Google Docs, Sheets і Slides, що дозволяє легко створювати, редагувати та спільно працювати над документами в режимі реального часу. Dropbox, своєю чергою, популярний серед професіоналів завдяки простоті у використанні, зручній синхронізації між пристроями та широким можливостям інтеграції з іншим програмним забезпеченням. Microsoft OneDrive інтегрується з пакетом Office, що особливо зручно для бізнес-користувачів, які активно працюють з документами у Word, Excel чи PowerPoint.

Однією з головних переваг хмарних сервісів є їхня масштабованість: обсяг пам’яті можна розширити відповідно до потреб користувача. Безпека даних також знаходиться на високому рівні завдяки шифруванню, резервному копіюванню та можливостям управління доступом. Важливою особливістю є також підтримка спільної роботи, що дозволяє користувачам одночасно редагувати документи, залишати коментарі та обговорювати зміни.

Локальні сервери відіграють важливу роль у забезпеченні зберігання та захисту корпоративних даних, особливо для компаній, які прагнуть зберігати контроль над своїми інформаційними ресурсами. Встановлення локальних серверів дозволяє організаціям створювати централізовані сховища для документів, баз даних та іншої критично важливої інформації, забезпечуючи швидкий доступ до них у внутрішній мережі. Це особливо важливо для компаній, які працюють із конфіденційними даними або суворо дотримуються законодавчих норм захисту інформації.

Однією з ключових переваг локальних серверів є висока ступінь безпеки. Всі дані залишаються під фізичним контролем компанії, що зменшує ризики несанкціонованого доступу чи витоку інформації, характерні для хмарних сервісів. Мережу захищають за допомогою налаштувань безпеки в комутаторах L2/L3 і будь-яких маршрутизаторах. Використання механізмів автентифікації адміністратора, журнали пристроїв і часті

оновлення ПЗ допомагають підтримувати безпеку обладнання локальної мережі [5].

Хмарні технології стали важливою складовою сучасної інформаційної інфраструктури, даючи компаніям можливість використовувати обчислювальні ресурси та дані без необхідності створення власної IT-інфраструктури. Основою хмарних рішень є концепція надання IT-ресурсів як послуг через інтернет, що забезпечує доступ до потужних серверів, сховищ даних і програмного забезпечення на віддалених платформах. Хмарні сервіси сприяють різноманітній діяльності користувачів у сучасному інформаційно-комунікаційному середовищі, завдяки численним групам та інтернет-спільнотам, що взаємодіють у медійному просторі в реальному часі. Для координації таких спільнот використовується спеціалізований інструментарій, який надає користувачам широкий доступ до інформаційного та розважального контенту [6, с. 258].

До основних типів хмарних послуг належать:

1. SaaS (Software as a Service) – модель надання програмного забезпечення як послуги через інтернет. Користувачі отримують доступ до програм, що функціонують на серверах постачальника, без потреби в їх встановленні та обслуговуванні. До таких сервісів можна віднести Google Workspace та Microsoft 365. Ця модель дозволяє зменшити витрати на купівлю та підтримку програмного забезпечення і швидко адаптуватися до змін у бізнес-процесах.

2. PaaS (Platform as a Service) – модель, що надає платформи для розробки, тестування та розгортання програм. Компанії можуть використовувати інструменти для створення та управління програмами без необхідності підтримки серверної інфраструктури. Прикладами є Microsoft Azure та Google App Engine. Ця модель допомагає скоротити час для виведення нових продуктів на ринок, підвищити ефективність розробки та знизити витрати на IT-інфраструктуру.

3. IaaS (Infrastructure as a Service) – модель, яка надає в оренду віртуальні сервери, сховища даних та мережеві ресурси через інтернет. Клієнти можуть налаштовувати та керувати обчислювальними ресурсами відповідно до своїх потреб. Прикладами таких сервісів є Amazon Web Services (AWS) та Google Cloud. Модель IaaS дозволяє підприємствам масштабувати ресурси залежно від поточних потреб, мінімізуючи капітальні витрати [34, с. 213].

Для забезпечення надійної кібербезпеки в хмарних технологіях необхідний комплексний підхід і ретельне управління ризиками. Ось кілька стратегій, які можуть допомогти ефективно контролювати загрози:

1. Шифрування даних – використання надійних методів шифрування, як-от алгоритм AES-256 з довгими ключами, для захисту конфіденційної інформації, а також регулярне оновлення ключів для забезпечення постійної безпеки.

2. Постійний моніторинг безпеки – оперативний моніторинг активності з метою виявлення потенційних загроз, що може включати системи, які аналізують великі обсяги даних для виявлення аномалій і сповіщають про можливі ризики.

3. Двофакторна аутентифікація – використання додаткових рівнів захисту для запобігання несанкціонованому доступу, наприклад, одночасне введення пароля і одноразового коду (OTP) або застосування біометрії.

4. Регулярні оновлення та патчі – важливість своєчасного оновлення програмного забезпечення і встановлення патчів для виправлення вразливостей системи.

5. Захист мережі – встановлення та підтримка мережевих заходів безпеки, як-от брандмауери і системи моніторингу, для фільтрації трафіку і блокування загроз.

6. Навчання та підвищення обізнаності користувачів – проведення тренінгів і семінарів для підвищення обізнаності співробітників про кіберзагрози і надання доступу до навчальних матеріалів та онлайн-ресурсів.

Хмарні технології надають численні переваги, але для їх ефективного використання важливо ретельно підходити до забезпечення безпеки. Реалізація зазначених стратегій допоможе зберегти дані в безпеці та мінімізувати ризики порушень у хмарних середовищах [24, с. 128].

Апаратна безпека, така як розпізнавання відбитків пальців, маркери безпеки та повне шифрування диска, також можна використовувати для підвищення безпеки мережі. Додаткові пакети безпеки для захисту та підтримки периметра мережі можна встановити локально або придбати за моделлю SaaS.

Зі збільшенням кількості пристроїв «Інтернету Речей» (IoT) та зростанням рівня підключеності, питання безпеки передачі даних стає надзвичайно важливим. Однак традиційні криптографічні методи вимагають значних ресурсів, що ускладнює їх використання в малопотужних пристроях із обмеженою енергоємністю та обчислювальними можливостями.

Наразі активно розвиваються методи так званої «легкої» криптографії (lightweight cryptography), які забезпечують високий рівень захисту даних при мінімальному споживанні ресурсів, як-от площа мікросхеми, енергія та час виконання. Ці методи ідеально підходять для використання в пристроях IoT, що дозволяє забезпечити безпечну передачу даних.

Використання енергоефективної та легкої криптографії в системах IoT не лише гарантує безпеку передачі інформації, але й продовжує термін служби пристроїв, особливо за умови застосування автономних, малопотужних джерел живлення, що є важливим для ефективної роботи IoT-систем. Особливо популярними в таких системах стали методи аутентифікованого шифрування з асоційованими даними (AEAD). AEAD поєднує алгоритми шифрування та аутентифікації, шифруючи лише частину передаваних даних (наприклад, прикладну інформацію), тоді як аутентифікується весь набір даних. Це забезпечує захист чутливої інформації та гарантує цілісність усіх даних пакету, зокрема незашифровані елементи, зокрема заголовки, адреси вузлів, технічні характеристики, статистичну

інформацію та мітки часу. Відкриті, але аутентифіковані дані сприяють ефективній маршрутизації і доставці пакетів даних до кінцевого адресата, одночасно гарантуючи цілісність і автентичність інформації та її надійне джерело [12, с. 481].

Ще одним важливим аспектом є стабільність роботи. Локальні сервери не залежать від швидкості інтернет-з'єднання, тому забезпечують швидкий і безперебійний доступ до даних навіть за умов тимчасових проблем із мережею. Це робить їх ідеальним вибором для великих корпорацій і компаній, які не можуть дозволити собі переривання доступу до інформації.

Система електронного документообігу – це програмний інструмент, що забезпечує роботу з електронними документами на всіх етапах їхнього життєвого циклу: від створення та редагування до зберігання.

Сучасні рішення в цій галузі пропонують не лише базові функції, зокрема пошук та класифікація, але й розширені можливості для автоматизації, зокрема маршрутизацію документів. Оскільки документи тісно пов'язані з бізнес-процесами, сучасні системи електронного документообігу оснащені інструментами для ефективного управління як самими документами, так і процесами, що з ними пов'язані [8].

Однією з головних переваг DMS є централізація даних. Усі документи зберігаються у структурованій базі даних, що спрощує їх пошук і забезпечує доступність для авторизованих користувачів. Крім цього, системи управління документами підтримують інтеграцію зі стандартами електронного документообігу, наприклад, ISO 15489, що робить їх придатними для використання в юридичних і корпоративних процесах.

Важливим елементом сучасних DMS є функціонал забезпечення безпеки. Вони включають інструменти для управління доступом, що дозволяють визначати рівні прав для різних категорій користувачів, а також можливості шифрування даних і відстеження активності в системі. Завдяки цьому можна мінімізувати ризики витоку інформації та забезпечити відповідність вимогам конфіденційності.

Сучасні методи обробки, передачі та зберігання інформації спричинили появу ризиків, пов’язаних із втратою, спотворенням або несанкціонованим доступом до даних. Загроза інформаційній безпеці визначається як сукупність умов і факторів (процесів, дій або явищ), які створюють потенційну небезпеку, що може призвести до таких наслідків, як витік, модифікація чи знищення інформації. Усі дії, здатні завдати шкоди системі, класифікуються як загрози безпеці електронного документообігу. Сьогодні відомий широкий спектр загроз інформаційній безпеці, який включає сотні різних сценаріїв. Аналіз можливих загроз інформаційній безпеці є важливим етапом у визначенні повного набору вимог до створення ефективної системи захисту [31, с. 120].

Сучасні тенденції розвитку технологій значною мірою впливають на системи зберігання, обробки й захисту інформації, інтегруючи передові рішення, зокрема блокчейн, машинне навчання та автоматизація.

Блокчейн – це революційна технологія, яка дозволяє безпечно, надійно та прозоро зберігати всі дані за допомогою мережі комп’ютерів. Цією базою даних користуються для проведення операцій з криптовалютою та для зберігання інформації в багатьох інших цілях. Цифровий реєстр даних мережі блокчейну складається з ланцюгів, які містять інформацію про всі проведені операції. Історія операцій утворює блоки, в яких всі дані розташовані в хронологічному порядку. Збереження цієї інформації підтримується великою кількістю комп’ютерів по всьому світу [36].

Блокчейн функціонує за принципом децентралізації: дані не зберігаються на одному сервері, а розподіляються між багатьма комп’ютерами, які взаємодіють між собою. Кожен комп’ютер у мережі, або вузол, зберігає копію всіх транзакцій. Якщо одна частина системи стає об’єктом нападу, інші вузли продовжують працювати, зберігаючи дані без змін.

Кожна транзакція в блокчейні записується у блоці, який з’єднується з іншими блоками, утворюючи ланцюг, що гарантує незмінність історії даних:

якщо хтось спробує змінити один блок, йому доведеться змінити всі наступні блоки, що зробити практично неможливо без дозволу більшості учасників мережі [42].

Блокчейн активно застосовується у фінансовому секторі для забезпечення безпеки транзакцій і конфіденційності користувачів. Наприклад, криптовалюти зокрема Monero та ZCash спеціально створені для забезпечення анонімності своїх користувачів. Monero використовує кільцеві підписи та технологію «Confidential Transactions», які дозволяють приховати не тільки ідентичність учасників, а й суму переказу, що дає можливість здійснювати транзакції з повною анонімністю, що є вкрай важливим у вимірі зростаючої уваги до захисту особистої інформації та безпеки в фінансовій сфері. Таким чином, блокчейн стає важливим інструментом для створення нових фінансових систем, де дані користувачів надійно захищені від сторонніх [47].

Блокчейн стає важливим інструментом для забезпечення конфіденційності в державному секторі. У Естонії, зокрема, уряд активно використовує блокчейн для захисту особистих даних громадян у державних реєстрах, як-от податкові та земельні записи. Завдяки децентралізованій архітектурі блокчейн дані зберігаються на численних серверах, що ускладнює несанкціонований доступ і зменшує ймовірність кібератак. Це дозволяє громадянам контролювати доступ до своїх даних та відслідковувати їх використання. Таким чином, блокчейн може стати надійною основою для електронного управління та безпечного зберігання даних, що підвищує довіру до урядових установ [27, с. 296].

Машинне навчання активно впроваджується для вдосконалення процесів аналізу та управління даними. Алгоритми на основі штучного інтелекту здатні автоматично класифікувати документи, визначати їхній пріоритет, виявляти аномалії або потенційні загрози, зокрема підозріла активність користувачів. Завдяки машинному навчанню системи стають

більш адаптивними, навчаючись на основі накопичених даних для підвищення ефективності роботи й точності прогнозів.

Автоматизація є ще однією важливою тенденцією, яка трансформує бізнес-процеси. Сучасні системи управління документами інтегрують інструменти автоматизації, що дозволяють мінімізувати людське втручання у рутинні операції, зокрема створення, маршрутизація та архівування документів. Це не лише підвищує швидкість роботи, але й знижує ймовірність помилок. Крім того, автоматизація сприяє інтеграції різних систем у єдине інформаційне середовище, що дозволяє ефективніше використовувати ресурси організації.

Вибір найбільш ефективного програмного забезпечення для управління документами значною мірою залежить від конкретних потреб користувача, що можуть відрізнятися залежно від масштабу організації, типу роботи та вимог до функціональності.

Для малого бізнесу ключовими факторами стають простота використання, доступність і базові функції, зокрема зберігання, пошук і спільна робота з документами. У цьому випадку хмарні сервіси, наприклад, Google Drive або Dropbox, можуть бути оптимальним вибором, оскільки вони не вимагають значних інвестицій у технічну інфраструктуру та легко інтегруються з іншими інструментами.

Середні компанії часто потребують більш розширених можливостей, як-от налаштування прав доступу, інтеграція з корпоративними системами й автоматизація рутинних процесів. Для них підійдуть такі рішення, як Microsoft SharePoint або M-Files, які пропонують гнучкість у налаштуванні, високу продуктивність та відповідність корпоративним стандартам.

Великі корпорації, які працюють із великими обсягами даних і чутливою інформацією, зазвичай потребують комплексних рішень із розширеними функціями безпеки, можливістю масштабування та інтеграцією зі складними бізнес-процесами. Такі системи, як Alfresco чи IBM FileNet,

забезпечують необхідний рівень контролю й дозволяють організувати електронний документообіг із врахуванням міжнародних стандартів.

Отже, сучасні технологічні рішення у сфері захисту електронних документів включають використання криптографії, біометричної аутентифікації та технології блокчейн для забезпечення цілісності та конфіденційності інформації. Шифрування даних і цифрові підписи забезпечують захист від несанкціонованого доступу та фальсифікацій. Блокчейн завдяки своїй децентралізованій природі надає можливість зберігання даних, що робить їх менш вразливими до кібератак. Крім того, біометричні технології дозволяють забезпечити надійний контроль доступу до чутливої інформації. У поєднанні ці методи створюють ефективний механізм захисту електронних документів, знижують ризики несанкціонованого втручання та підвищують рівень безпеки в цифровому середовищі.

2.2. Перспективи розвитку систем захисту в умовах цифрової трансформації та зростаючих кіберзагроз

В умовах цифрової трансформації, коли все більше процесів переходить в онлайн-формат, зростають вимоги до ефективності систем захисту інформації. З розвитком новітніх технологій з’являються нові проблеми у сфері кібербезпеки, що вимагає постійного вдосконалення засобів захисту. Адаптація до цих змін є ключовим фактором для забезпечення безпеки даних у майбутньому.

Перспективними методами, які можна використовувати для захисту систем електронних документів, є наступні: квантова криптографія, інтелектуальні системи виявлення кіберзагроз, технології захисту на основі поведінкової аналітики, концепція довіри за замовчуванням (Zero Trust), сегментація мережі з метою захисту даних.

Розглянемо кожен із напрямів більш детально.

У сучасному світі інформація є одним з найцінніших ресурсів, тому завдання шифрування – забезпечення її конфіденційності, цілісності та анонімності – стають більш актуальними, ніж будь-коли. Завдяки розвитку класичної криптографії, зокрема завдяки використанню стійких схем шифрування та цифрових підписів із відкритими ключами, ці завдання реалізуються досить успішно.

Проте будь-яка криптографічна система рано чи пізно піддається зламуванню. На сьогодні найбільшу загрозу для класичної криптографії становить застосування принципів квантової механіки в обчисленнях. Квантова механіка не тільки може загрожувати розкриттю класичних шифрів, але й відкриває можливості для створення принципово нових, потенційно незламних криптографічних систем.

Квантова криптографія досліджує можливість генерації криптографічних ключів, чия секретність забезпечується основними законами квантової механіки. Розвиток цієї науки розпочався в 1984 році з розробки першого квантового протоколу розподілу ключів BB84. За цим протоколом інформація передається через кодування станів фотонів на відправляючому кінці та їх подальше вимірювання на приймальному. Якщо зловмисник спробує перехопити ці фотони, принцип невизначеності Гейзенберга дозволяє легітимним користувачам виявити таке вторгнення завдяки збільшенню кількості помилок при реєстрації фотонів. Важливою характеристикою є критична помилка для протоколу BB84, яка становить близько 11%.

Отже, головною перевагою квантових криптографічних протоколів є те, що навіть за наявності необмежених можливостей у зловмисників для перехоплення ключової інформації факт прослуховування каналу завжди можна буде виявити, що робить квантову криптографію привабливою для захисту від шпигунства та шахрайства [17, с. 152].

Квантові технології все ще перебувають на ранніх етапах розвитку, але їх прогрес відбувається дуже швидко. У міру їх удосконалення можна

очікувати зростання кількості їхніх застосувань у повсякденному житті. Ось кілька перспектив розвитку квантових технологій:

1. Квантові комп’ютери мають величезний потенціал для вирішення завдань значно швидше, ніж традиційні комп’ютери. Вони можуть бути використані для розробки нових ліків, моделювання кліматичних процесів і створення інноваційних матеріалів. Зі збільшенням потужності та доступності квантових комп’ютерів, ми станемо свідками революції в таких галузях, як фармацевтика, виробництво, фінанси та штучний інтелект.

2. Квантові сенсори мають потенціал бути набагато точнішими й чутливішими, ніж традиційні сенсори. Вони можуть застосовуватися для виявлення хімічних речовин, моніторингу витоків та оцінки стану навколишнього середовища. З розвитком цих технологій вони стануть більш поширеними, що позитивно вплине на безпеку, охорону здоров’я та стан довкілля.

3. Квантова криптографія значно перевищує безпеку традиційних методів шифрування, оскільки вона не може бути зламана навіть за допомогою найпотужніших комп’ютерів, що обумовлено використанням властивостей квантової механіки, які не піддаються моделюванню на класичних комп’ютерах [22, с. 119].

Інтелектуальні системи управління та аналізу даних (ІСУАД) є однією з найбільш перспективних технологій, здатних змінити різні аспекти бізнесу та наукових досліджень. Ці системи поєднують алгоритми штучного інтелекту (ШІ) та сучасні методи аналізу даних, що дозволяє не тільки оптимізувати процеси, але й здобувати нові знання з великих обсягів інформації. В умовах швидких змін у бізнес-середовищі компанії, які не використовують новітні технології для аналізу даних, можуть відстати від своїх конкурентів.

Попри великий потенціал ІСУАД, багато підприємств стикаються з проблемами їх впровадження через складність налаштування та інтеграції, нестача кваліфікованих кадрів, а також через проблеми з якістю та

доступністю даних. Крім того, важливими є питання етики та захисту конфіденційності, зокрема, у контексті збільшення обсягів оброблюваних персональних даних. Однак з розвитком технологій ШІ та зростанням обсягів даних ІСУАД стають дедалі більш доступними та ефективними.

З розвитком цифрових технологій, як-от Інтернет речей (IoT), блокчейн і великі дані, ІСУАД відкривають нові можливості для застосування. Наприклад, у фінансах ці системи використовуються для оцінки ризиків, автоматизації торгівлі та виявлення шахрайства. В охороні здоров'я вони сприяють діагностиці, персоналізованому лікуванню та управлінню медичними ресурсами. В логістиці ІСУАД допомагають оптимізувати маршрути, управлінню запасами та прогнозуванню попиту, а в маркетингу – для аналізу поведінки споживачів, створення персоналізованих рекомендацій та сегментації ринку [29, с. 132].

CRM-система – це поєднання стратегій, практик та технологій, які компанії використовують для управління взаємодією з клієнтами та аналізу даних протягом їхнього життєвого циклу. Основні завдання системи включають організацію клієнтської бази, автоматизацію процесів, управління роботою співробітників, продажами та аналітикою. CRM-системи збирають інформацію про клієнтів через різні канали взаємодії, я веб-сайт, телефон, чат, електронну пошту, маркетингові матеріали та соціальні мережі. Зазвичай ці системи широко використовуються в інтернет-магазинах, сервісах (від салонів краси до клінінгових послуг), навчанні (курси, майстер-класи), онлайн-продажах (одяг, взуття, аксесуари тощо), готелях, ресторанах та нерухомості. Однак багато бізнесів не приділяють належної уваги безпеці даних, що зберігаються в CRM, що підвищує ризики для конфіденційності клієнтів.

Резервні копії даних є критично важливими, але часто ними нехтують або забувають про їх належну організацію. У випадку з десктопними системами, важливо налаштувати регулярне резервне копіювання даних, наприклад, через RegionSoft Application Server. Для хмарних CRM-систем

необхідно заздалегідь уточнити умови резервного копіювання: які дані зберігаються, з якою частотою, де і за якою ціною. Це важливо, оскільки базові безкоштовні варіанти резервного копіювання зазвичай обмежуються лише останніми даними, тоді як повноцінне й безпечне копіювання може бути платним. Не забувайте регулярно перевіряти відновлюваність резервних копій.

Щодо безпеки доступу, важливо встановити обмеження на рівні прав доступу до функцій і даних. Крім того, для захисту мережі потрібно обмежити використання CRM лише в межах офісної підмережі, заборонити доступ із мобільних пристроїв та публічних мереж (коворкінг, кафе тощо). Особливо обережно слід ставитися до мобільної версії CRM-системи – вона повинна бути спрощеною та обмеженою для забезпечення безпеки [35, с. 169].

На сучасному ринку програмних рішень для інформаційної безпеки представлено велику кількість інструментів для моніторингу та аналізу діяльності користувачів. Серед них особливо виділяються системи запобігання втраті даних, контролю доступу та аналізу поведінки користувачів. Системи запобігання втраті даних (DLP – Data Loss Prevention) допомагають вирішити проблему випадкових та навмисних витоків конфіденційної інформації. В основному, DLP-системи дозволяють ідентифікувати, контролювати та захищати дані, що використовуються на різних етапах – на кінцевих точках (наприклад, дії користувачів), в русі (наприклад, через мережу) та в стані спокою (наприклад, зберігання даних), що досягається за допомогою глибокого аналізу вмісту пакетів, контекстного аналізу безпеки транзакцій, врахування атрибутів ініціатора, об’єкта даних, носія, часу, місця призначення тощо, в рамках централізованої системи управління [40].

Система DLP є складним автоматизованим рішенням, що відслідковує спроби передачі конфіденційної або важливої інформації з інформаційної системи за межі організації. Для цього на сервер організації та на всі

пристрої в офісі встановлюється програма, яка в реальному часі перевіряє всі операції з інформацією. Якщо система виявляє спробу відправки важливих даних на недозволену адресу, вона блокує передачу. Наприклад, якщо співробітник спробує надіслати таблицю Excel з контактами клієнтів з корпоративної пошти на особисту, система DLP зупинить цей процес і повідомить відповідального фахівця про порушення, що створює «цифровий периметр» навколо організації, аналізуючи всю вхідну, вихідну та внутрішню інформацію. Виявлення конфіденційних даних у потоку інформації здійснюється шляхом контент-аналізу та пошуку специфічних ознак, як-от гриф документа, мітки чи хеш-функції.

DLP-система вирішує кілька завдань контролю, зокрема:

– моніторинг поштового та веб-трафіку;

– контроль переписки в месенджерах (Skype, Telegram, WhatsApp);

– моніторинг передачі даних в хмарні додатки;

– контроль інформаційного обміну через комунікаційні порти (com-, lpt-, usb-, irda-порти тощо);

– спостереження за пристроями введення-виведення (наприклад, CD, знімні накопичувачі) та бездротовими засобами доступу (bluetooth, firewire, wi-fi);

– моніторинг друку на локальних і мережевих принтерах;

– перевірка збереження інформації на робочих станціях і в мережевих сховищах.

Також DLP-система забезпечує контроль за діяльністю співробітників на робочих станціях, наприклад:

– спостереження за буфером обміну, використання кейлоггерів, моніторинг відвідуваних сайтів, контроль пошукових запитів і додатків;

– контроль за робочим місцем користувача (аудіо, відео, скріншоти);

– тіньове копіювання всіх перехоплених файлів;

– консолідацію даних в єдиному сховищі та надання візуальної аналітики для перехоплених даних [23, с. 53].

Концепція Zero Trust набуває все більшої популярності в умовах зростання кіберзагроз. Основний принцип цієї концепції полягає в тому, що жоден користувач чи пристрій не має довіри за замовчуванням, незалежно від того, звідки вони підключаються до мережі. Це означає, що кожна спроба доступу до ресурсів мережі повинна бути перевірена, аутентифікована та авторизована.

Стратегія Zero Trust зосереджується на переконанні, що організації не повинні автоматично довіряти будь-яким даним, незалежно від того, чи знаходяться вони всередині, чи за межами мережі, і повинні перевіряти кожну спробу підключення до своїх систем перед наданням доступу.

Простота концепції Zero Trust полягає в тому, щоб розглядати кожен запит на доступ до системи як потенційну загрозу і надавати доступ лише після ретельної перевірки, що відрізняється від традиційного підходу безпеки, який припускав, що всі учасники мережі організації є надійними. Zero Trust вимагає постійної перевірки всіх користувачів та пристроїв, що намагаються увійти в системи організації, значно зміцнюючи захист від витоків даних і кібератак [38, с. 167].

Модель нульової довіри є підходом до кібербезпеки, який автоматично обмежує доступ до цифрових ресурсів організації і надає його лише тим користувачам, які пройшли автентифікацію та мають відповідні права доступу, що не залежить від фізичного місцезнаходження пристрою в мережі чи його приналежності (корпоративний або приватний пристрій). Ця модель допомагає виявляти програми-вимагачі завдяки ретельній перевірці особи кожного користувача та пристрою при кожному спробі доступу до ресурсів. Вимагаючи постійної автентифікації, модель нульової довіри знижує ймовірність несанкціонованого доступу та поширення шкідливих програм у мережі.

З точки зору виявлення програм-вимагачів, модель нульової довіри доповнює наявні заходи безпеки, забезпечуючи додаткові рівні захисту. Наприклад, вона зосереджена на моніторингу і аналізі мережевого трафіку для виявлення незвичної активності, що може свідчити про потенційну атаку. Постійна перевірка доступу та моніторинг аномальної поведінки значно підвищують шанси виявити програми-вимагачі на ранніх етапах.

Крім того, зосередження уваги на мінімізації доступу, необхідного для виконання завдань, також сприяє виявленню програм-здирників. Обмежуючи привілеї користувачів і пристроїв, модель зменшує потенційний вплив атак зловмисників. Якщо користувач або пристрій з обмеженим доступом намагається виконати підозрілі дії або отримати доступ до несанкціонованих файлів, це може викликати сповіщення і стимулювати розслідування для мінімізації загрози.

Поєднання моделі нульової довіри з іншими методами виявлення програм-вимагачів, як-от статичний аналіз файлів, моніторинг аномалій виконання і використання розширеного аналізу шкідливого програмного забезпечення, забезпечує комплексний підхід до виявлення і нейтралізації атак. Завдяки впровадженню моделі нульової довіри, організації можуть підвищити свою здатність виявляти і реагувати на загрози з боку програм-вимагачів, зменшуючи потенційну шкоду від таких атак [39, с. 181].

Сегментація мережі передбачає поділ мережевої інфраструктури на ізольовані сегменти з контрольованим обміном між ними. Мікросегментація є більш дрібнозернистою формою сегментації, яка логічно розбиває мережу до рівня окремих робочих навантажень або додатків. Метою цих підходів є мінімізація потенційної шкоди від кіберінцидентів через ізоляцію сегментів. Кожен сегмент стає відокремленим від інших, що ускладнює несанкціонований доступ до чутливих ресурсів. Якщо зловмисник проник в один сегмент, його рух системою обмежується.

Сегментація створює додаткові рівні захисту всередині системи, що зменшує кількість точок входу для атак і ускладнює проникнення

зловмисників вглиб системи, що також обмежує латеральне переміщення, тобто поширення атаки по мережі. Сегментація полегшує виявлення та локалізацію вторгнень, оскільки активність в ізольованому сегменті легше моніторити та аналізувати. Дослідження показали, що впровадження мікросегментації може підвищити стійкість мережі та знизити її вразливість на 60-90% завдяки скороченню площі атаки. Мікросегментація також уповільнює або запобігає переміщенню зловмисника між вузлами, надаючи більше шансів виявити атакуючого до того, як він завдасть значної шкоди.

Основна проблема, яка виникає при сегментації – це складність впровадження та підтримки сегментованої архітектури. Тонке налаштування численних меж доступу вимагає ретельного планування та адміністрування. Мікросегментація може істотно підвищити складність мережі і супроводжується додатковими витратами на розгортання та управління. Організації відзначають, що наддрібна сегментація додає витрат порівняно з отриманим зниженням кількості інцидентів, хоча загалом вона підсилює захищеність системи. Таким чином, важливо знайти баланс між рівнем безпеки та керованістю мережі при впровадженні цього підходу [13, с. 150].

Таким чином, перспективи розвитку систем захисту в умовах цифрової трансформації передбачають впровадження інноваційних підходів, зокрема Zero Trust, мікросегментації та використання штучного інтелекту для виявлення аномальної поведінки. Ці технології дозволяють ефективніше контролювати доступ до ресурсів і знижувати ризики від кіберзагроз. Водночас організації повинні адаптувати свої стратегії до швидкого розвитку кіберзагроз, що потребує постійного вдосконалення існуючих заходів безпеки. Зростаюча інтеграція IoT, хмарних технологій та віддаленої роботи вимагає розробки гнучких та масштабованих систем захисту. Усі ці тенденції підвищують важливість розвитку кібербезпеки як критичного елементу для забезпечення стабільності і надійності цифрової економіки.

ВИСНОВКИ

Електронні документи стали важливою складовою сучасного документообігу, що забезпечує зручність, швидкість і надійне збереження інформації в цифровому форматі. Однак вони вимагають належного захисту від загроз, пов’язаних з кібератаками, несанкціонованим доступом та фальсифікацією. Методи захисту електронних документів є ключовими для забезпечення їх безпеки. Використання як технічних, так і правових заходів гарантує збереження цілісності, конфіденційності та юридичної сили цифрових документів. Надійний захист електронного документообігу є вкрай важливим для розвитку цифрової економіки та ефективного електронного управління.

Основними загрозами для електронних документів є їх вразливість до несанкціонованого доступу, модифікації, пошкодження або втрати. Хакерські атаки, зокрема фішинг або шкідливі програми, можуть призвести до викрадення або змінення вмісту документів. Іншою серйозною загрозою є недостатній рівень захисту даних під час зберігання або передачі, що може спричинити витік конфіденційної інформації. Відсутність надійної автентифікації та електронного підпису також може знизити довіру до документів, що впливає на їх юридичну значущість.

Сучасні технології для захисту електронних документів включають застосування криптографії, біометричної аутентифікації та блокчейн-технології для забезпечення цілісності та конфіденційності даних. Шифрування інформації і цифрові підписи допомагають захистити документи від несанкціонованого доступу та фальсифікацій. Завдяки децентралізованій структурі блокчейн забезпечує зберігання даних, що робить їх менш вразливими до атак. Біометричні технології гарантують надійний контроль доступу до важливої інформації. Коли ці методи використовуються разом, вони формують ефективний механізм захисту

електронних документів, зменшуючи ймовірність несанкціонованого втручання та підвищуючи безпеку в цифровому середовищі.

Перспективи розвитку систем захисту в умовах цифрової трансформації включають інтеграцію інноваційних підходів, як-от модель Zero Trust, мікросегментація та використання штучного інтелекту для виявлення аномалій. Ці технології забезпечують більш ефективний контроль доступу до ресурсів та допомагають знижувати ризики від кіберзагроз. Однак організації повинні постійно адаптувати свої стратегії до швидко змінюваного середовища кіберзагроз, що вимагає постійного вдосконалення існуючих заходів безпеки. Розширення використання IoT, хмарних технологій і віддаленої роботи вимагає створення гнучких та масштабованих систем захисту. Усі ці тенденції підвищують значення кібербезпеки як ключового елементу для забезпечення стабільності та надійності цифрової економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Боскін О., Чорний П. Аналіз загрози фішингу. *Сучасна молодь в світі інформаційних технологій*. Херсон, 2021. С. 179–181. URL: http://dspace.ksau.kherson.ua/bitstream/handle (дата звернення: 10.02. 2025).

2. Варейчук В. Е. DDoS-атаки та їх ознаки у безпровідних wi-fi мережах. *Радіоелектроніка та молодь у XXI столітті* : матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. Харків : ХНУРЕ, 2024. Т. 3. С. 419–420. URL: https://openarchive.nure.ua/entities/publication/c2a32418-7fbc-4cef-96e5-42943bbea776. (дата звернення: 05.05.2025).

3. Гаркуша С. А. Електронний документообіг: переваги та недоліки впровадження. *Інфраструктура ринку*. 2020. № 50. С. 259–262. URL: http://market-infr.od.ua/journals/2020/50_2020_ukr/45.pdf(дата звернення: 05.11.2024).

4. Гринович А. А., Пухальська Г. В. Електронний цифровий підпис: особливості застосування, переваги та проблеми. *Вісник Хмельницького національного університету*. 2009. № 1(2). С. 19–21.

5. Дехтярьова Ю. Що таке локальна мережа і навіщо вона потрібна? *Itedu.center*. 2022. URL: https://itedu.center/ua/blog/articles/lan_wan_man/?srsltid=AfmBOooDqQOZtFcjc7oQLCyXjYvhUEqt3FTMEUkh1MoHVGED5YR5_spm (дата звернення: 10.11.2024).

6. Досенко А. Хмарні технології: прикладні технології сучасних платформ. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: Філологія. Журналістика. 2022. Вип. 33(72). С. 257–262. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/view/528/551. (дата звернення: 06.05.2025).

7. Думанська Н. О. Шифрування даних в інформаційних системах. Математичні методи, моделі та інформаційні технології в управлінні. 23 с. URL:

https://www.researchgate.net/publication/385807233_MEHANIZMI_BEZPEKI_INFORMACII_TA_IH_VIKLIKI (дата звернення: 09.11.2024).

8. Електронний документообіг: види систем та їхні функції. *Intecracy Deals*. 2021. URL: https://dealssign.com/blog/elektronnij-dokumentoobig-vidi-sistem-ta-yixni-funkciyi/(дата звернення: 11.11.2024).

9. Журавчак Д. Концепція нульової довіри для захисту active directory для виявлення програм-вимагачів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2023. Вип. 2.22. С. 179–190. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/489 (дата звернення: 16.05.2025).

10. Загрози безпеки AIC, причини виникнення загроз. *Букліб*. URL: https://buklib.net/books/28541/ (дата звернення: 09.11.2024)

11. Здирники, шифрувальники, ransomware – що це і як з ними боротися. SIM Networks. URL: https://www.sim-networks.com/ukr/kb/ransomware-how-to-win. (дата звернення: 02.05.2025)

12. Караман Д. Г. Апаратна реалізація методів аутентифікованого шифрування з асоційованими даними для систем IoT. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доп. 31-ї Міжнар. наук.-практ. конф. MicroCAD-2023*, 17-20 травня 2023 р. / ред. Є. І. Сокол ; уклад. Г. В. Лісачук. Харків : НТУ «ХПІ», 2023. С. 481. URL: https://repository.kpi.kharkov.ua/items/9ef9de51-b8b4-4f82-ab0a-8da10d04aabf (дата звернення: 10.05.2025).

13. Кобільник Б., Сидоренко В. Сучасні методи забезпечення захисту критичної інфраструктури держави. *Research in Science, Technology and Economics: Collection of Scientific Papers «International Scientific Unity» with Proceedings of the 2nd International Scientific and Practical Conference*. March 5-7, 2025. Luxembourg, Luxembourg. С. 148–152. URL: https://lib.udau.edu.ua:8443/server/api/core/bitstreams/c771478f-0b91-412d-b00a-3554f2bbd3fe/content#page=148. (дата звернення: 16.05.2025).

14. Ковальов Д. 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: 02.05.2025).

15. Ковальчук О. В. Загрози, що виникають в результаті застосування шкідливого програмного забезпечення на мобільних пристроях. Тернопіль, 2018. 115 с. URL: http://dspace.tneu.edu.ua/handle/316497/27899 (дата звернення: 19.11.2024).

16. Копняк К. В., Покиньчереда В. В. Електронний документообіг в публічному управлінні: проблеми впровадження, переваги та перспективи. *Державне управління: удосконалення та розвиток.* 2020. № 10. URL: http://sel.vtei.edu.ua/card.php?id=25674 (дата звернення: 09.11.2024).

17. Кузнецова А., Семендяй С. Квантова криптографія. *Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених* (м. Чернігів, 18–19 березня 2021 р.) : збірник тез доповідей. Чернігів : НУ «Чернігівська політехніка» 2021. С. 152–153. URL: https://ir.stu.cn.ua/jspui/bitstream/123456789/22722/1/zbirnyk-2021-novitni-tehnologiyi-sajt.pdf#page=152 (дата звернення: 15.05.2025).

18. Кукла В. Забезпечення захисту й організація зберігання електронних документів. *Актуальні проблеми розвитку природничих та гуманітарних наук: збірник матеріалів VIII Міжнар. наук. практ. конф.* (14 листопада 2024 р.) / відп. ред. Шуляк Н. О., Зінченко М. О. Луцьк, 2024. С. 344–349.

19. Кукла В. Забезпечення збереження й безпеки електронних документів. *Гуманітарний простір науки: досвід та перспективи»*: Матеріали Міжнародної науково-практичної інтернет-конференції, 30 травня 2025 року. Вип. 44. Переяслав-Хмельницький, 2025.

20. Лаба О. Електронне діловодство: проблеми та перспективи розвитку. *Студії з архівної справи та документознавства.* 2011. Т. 19. Кн. 2.

С. 53–56. URL: http://nbuv.gov.ua/UJRN/sasd_2011_19_2_9 (дата звернення: 19.11.2024).

21. Мінгальова Ю. І. Новітні криптографічні методи захисту інформації. *Матеріали II Всеукраїнської науково-практичної інтернет-конференції, присвяченої 95-річчю Херсонського державного університету*. 2012.С. 373–378. URL: http://eprints.zu.edu.ua/id/eprint/13902 (дата звернення: 11.11.2024).

22. Мрачковський О. Квантова технологія: перспективи розвитку. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України:* матеріали Науково-практичної конференції (Львів, 22 грудня 2023 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2024. С. 118–120. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6900/1/22_12_2023.pdf#page=118 (дата звернення: 15.05.2025).

23. Мужанова Т. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2021. Вип. 1.13. С. 50–62. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/281 (дата звернення: 15.05.2025).

24. Насатов О., Плєхова Г. Хмарні технології та кібербезпека. *Математичне моделювання та інформаційні технології сучасності*. 2024. С. 127–129.

25. Нікітіна В., Нестор Д. Особливості збереження і захисту електронних документів. *Інформація, комунікація, суспільство.* 2014. 254 с. URL: https://www.researchgate.net/profile/Solomia-Fedushko/publication/331276453_Proceedings_of_the_International_Academic_Conference_ICS-2014/links/5c6fc13392851c69503696b0/Proceedings-of-the-International-Academic-Conference-ICS-2014.pdf#page=254 (дата звернення: 08.11.2024).

26. Опірський І., Винар А. Аналіз використання хмарних сервісів для фішингових атак. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. Вип. 1(9). С. 59–68. URL: https://doi.org/10.28925/2663-4023.2020.9.5968 (дата звернення: 19.11.2024).

27. Поляков Д. Блокчейн на основі шифрування даних і механізми збереження конфіденційності великих даних. *Наукові відкриття та фундаментальні наукові дослідження: світовий досвід:* збірник наукових праць з матеріалами V Міжнародної наукової конференції, м. Полтава, 8 листопада 2024 р. / Міжнародний центр наукових досліджень. Вінниця: ТОВ «УКРЛОГОС Груп, 2024. С. 294–300. URL: https://ket.stu.cn.ua/wp-content/uploads/2024/11/zbirnyk-naukovyh-pracz.pdf#page=294 (дата звернення: 10.05.2025).

28. Про електронні документи та електронний документообіг: Закон України № 851IV від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/85115#Text (дата звернення: 09.11.2024).

29. Ревенко М. Інтелектуальні системи управління та аналізу даних. *Наукові праці Першої міжнар. наук.-практ. конф. «Штучний інтелект та інформаційні технології»* (AIIT-2024), 3–4 червня 2024 р. (Київ, Україна). Київ: НУХТ, 2024. С. 132–133. URL: https://dspace.nuft.edu.ua/server/api/core/bitstreams/04559034-d7a2-4eee-a053-3072e8f4cb21/content (дата звернення: 15.05.2025).

30. Рижий Я. О. Технологія використання цифрового підпису в системах електронного документообігу: кваліфікаційна робота магістра: 125 Кібербезпека. Хмельниц. нац. ун-т. Хмельницький. 2023. 115 с. URL: https://elar.khmnu.edu.ua/handle/123456789/14868 (дата звернення: 11.11.2024).

31. Розломій І. О. Організація і оцінка ефективності системи захищеного документообігу. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2015. Вип. 6(1). С. 119–124. URL: http://nbuv.gov.ua/UJRN/Vkdpu_2015_6(1)__20 (дата звернення: 10.11.2024).

32. Розломій І. О. Виявлення та нейтралізація загроз безпеки електронних документів на основі аналізу їх життєвого циклу. *Вісник Київського національного університету технологій та дизайну.* Серія «Технічні науки». 2016. № 1(94). С. 57–64. URL: https://er.knutd.edu.ua/handle/123456789/1787 (дата звернення: 19.11.2024).

33. Розломій І. О., Косенюк Г. В. Основні механізми захисту електронних документів від фальсифікацій. *Вісник Черкаського державного технологічного університету*. 2016. Вип. 2. С. 53–58. URL: https://bulletin-chstu.com.ua/web/uploads/pdf/Bulletin%20of%20Cherkasy%20State%20Technological%20University_2016_Vol_21_No.2_53-58.pdf (дата звернення: 10.11.2024).

34. Семененко Ю. Хмарні технології як фактор підвищення ефективності діяльності компанії. *Herald of Khmelnytskyi National University. Economic sciences.* 2024. Вип. 334.5. С. 211–218. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/view/528 (дата звернення: 09.05.2025).

35. Тимошенко Є. Способи захисту даних в CRM системах. *Новітні технології у науковій діяльності і навчальному процесі :* зб. тез Всеукр. наук.-практ. конф. студентів, аспірантів та молодих учених (м. Чернігів, 18–19 березня 2021 р.) : збірник тез доп. Чернігів : НУ «Чернігівська політехніка», 2021. С. 169–170. URL: https://ir.stu.cn.ua/handle/123456789/24385 (дата звернення: 15.05.2025).

36. Хмельницька І. Все про блокчейн: як працює, хто користується, де застосовують. *ТСН*. 2023. URL:https://tsn.ua/groshi/vse-pro-blokcheyn-yak-pracyuye-hto-koristuyetsya-de-zastosovuyut-2378878.html (дата звернення: 09.11.2024).

37. Цивільний кодекс України: Закон України № 435-IV від 16.01.2003. URL:https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 09.11.2024).

38. Яцишин Ю., Власюк Г. Використання концепції Zero Trust для забезпечення кібербезпеки. *Research in Science, Technology and Economics: Collection of Scientific Papers «International Scientific Unity» with Proceedings of the 2nd International Scientific and Practical Conference.* March 5–7, 2025. Luxembourg. С. 166–169. URL: https://lib.udau.edu.ua:8443/server/api/core/bitstreams/c771478f-0b91-412d-b00a-3554f2bbd3fe/content#page=166 (дата звернення: 16.05.2025).

39. Bishop D. Introduction to Cryptography with Java Applets. Boston – Toronto – London – Singapore: Jones and Bartlett Publishers, 2003. 387 p. URL: https://repository.dinus.ac.id/docs/ajar/Introduction_to_Cryptography_with_Java_Applets.pdf (дата звернення: 15.05.2025).

40. Data loss prevention – Glossary. CSRC. *NIST Computer Security Resource Center*. URL: https://csrc. nist.gov/glossary/term/data_loss_prevention (дата звернення: 16.05.2025).

41. Einfluss von Informationstechnologien auf Archivierungsverfahren. AWV. *Arbeitsgemeinschaft für Wirtschaftliche Verwaltung*. V. Eichborn 1997. S. 8. URL: https://journals.wlb-stuttgart.de/ojs/index.php/an/article/view/4299 (дата звернення: 07.11.2024).

42. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 10.05.2025).

43. Özçelik I.,Brooks R. Distributed Denial of Service Attacks. *Real-world Detection and Mitigation*. New York, 2020. 422 p. URL: https://dokumen.pub/distributed-denial-of-service-attacks-1nbsped-1138626813-9781138626812.html (дата звернення: 18.05.2025).

44. The Phishing Guide (Part 1). Understanding and Preventing Phishing Attacks. URL: http://www.technicalinfo.net/papers/Phishing.html (дата звернення: 02.05.2025).

45. Whitfield D., Hellman M. New directions in cryptography. *IEEE transactions on Information Theory*. 1976. № 22(6). P. 644–654. URL: https://ieeexplore.ieee.org/document/1055638 (дата звернення: 10.11.2024).

46. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 10.05.2025).