МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Назар Рожков
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Назар РОЖКОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Діана ПРИМАЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рожкову Назару Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи управління ризиками витоку персональних даних у цифрових інформаційних системах”,
керівник кваліфікаційної роботи ПРИМАЧЕНКО Діана.
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи: *методи управління ризиками, інформаційні системи, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1 Дослідити теоретичні основи захисту персональних даних та управління ризиками.
   4.2 Проаналізувати ризики витоку персональних даних у цифрових інформаційних системах.
   4.3. Розробити методи та практичні рекомендації щодо зниження ризиків витоку даних.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження теоретичних основ захисту персональних даних та управління ризиками.	08.04.2026	
4.	Аналіз ризиків витоку персональних даних у цифрових інформаційних системах.	15.04.2026	
5.	Розробка методів та практичних рекомендацій щодо зниження ризиків витоку даних.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	05.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Назар РОЖКОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

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

Направляється здобувач Рожков Н.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи управління ризиками витоку персональних даних у цифрових інформаційних системах"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач РОЖКОВ Назар у кваліфікаційній роботі дослідив теоретичні основи захисту персональних даних та управління ризиками, проаналізував ризики витоку персональних даних у цифрових інформаційних системах, розробив методи та практичні рекомендації щодо зниження ризиків витоку даних.

РОЖКОВ Назар показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача РОЖКОВА Назара на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Рожков Н.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Рожкова Назара
на тему “Методи управління ризиками витоку персональних даних у цифрових інформаційних системах”

Актуальність. Однією з найважливіших проблем сучасного інформаційного суспільства є забезпечення належного рівня захисту персональних даних у цифрових інформаційних системах. Стрімкий розвиток цифрових технологій, поширення хмарних сервісів, мобільних застосунків та онлайн-платформ супроводжується постійним зростанням обсягів персональних даних, що обробляються, передаються та зберігаються в електронному вигляді. За таких умов підвищується ризик виникнення інцидентів, пов’язаних із витоком персональних даних, що може призвести до значних фінансових втрат, репутаційних збитків та порушення прав суб’єктів персональних даних.

Особливої актуальності набуває проблема своєчасного виявлення, оцінювання та мінімізації ризиків витоку персональних даних, оскільки традиційні підходи до захисту інформації не завжди здатні ефективно протидіяти сучасним кіберзагрозам. У зв’язку з цим важливим завданням є розроблення та вдосконалення методів управління ризиками витоку персональних даних у цифрових інформаційних системах, що дозволить підвищити рівень інформаційної безпеки та забезпечити дотримання вимог законодавства у сфері захисту персональних даних.

Позитивні сторони.

1.У роботі досліджено теоретичні основи захисту персональних даних та управління ризиками інформаційної безпеки, а також визначено основні фактори, що впливають на виникнення ризиків витоку персональних даних у цифрових інформаційних системах.

2.Кваліфікаційна робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно та логічно, сформульовано обґрунтовані висновки. Основні положення роботи представлено у вигляді таблиць і рисунків.

3.Автором опрацьовано значну кількість наукових джерел, нормативно-правових документів та сучасних наукових публікацій з питань захисту персональних даних, управління ризиками та інформаційної безпеки.

4.За результатами дослідження запропоновано рекомендації щодо вдосконалення процесів управління ризиками витоку персональних даних, спрямовані на підвищення рівня захисту інформації та зниження ймовірності реалізації загроз у цифрових інформаційних системах.

Недоліки.

Доцільно було б приділити більше уваги практичному аналізу сучасних програмних засобів моніторингу, оцінювання та управління ризиками витоку персональних даних, а також порівняльній характеристиці їх ефективності в умовах функціонування цифрових інформаційних систем.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач РОЖКОВ Назар заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів управління ризиками витоку персональних даних у цифрових інформаційних системах. Робота складається зі вступу, трьох розділів, що містять 19 рисунків та 25 таблиць, висновків і списку використаних джерел із 46 найменувань. Загальний обсяг роботи становить 102 аркуші, з яких 6 аркушів займають список використаних джерел.

Метою роботи є дослідження методів управління ризиками витоку персональних даних у цифрових інформаційних системах та розроблення рекомендацій щодо підвищення рівня їх захисту.

Об'єктом дослідження є процеси забезпечення захисту персональних даних у цифрових інформаційних системах.

Предмет дослідження – методи, моделі та засоби управління ризиками витоку персональних даних у цифрових інформаційних системах.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, оцінювання ризиків, моделювання, експертної оцінки, а також системний підхід до управління інформаційною безпекою та захистом персональних даних.

Як результат у роботі досліджено теоретичні основи захисту персональних даних у цифрових інформаційних системах; проаналізовано основні загрози та ризики їх витоку; вивчено сучасні методи управління ризиками та засоби захисту персональних даних; розроблено практичні рекомендації щодо підвищення рівня захисту інформації та зниження ймовірності виникнення інцидентів, пов'язаних із витоком персональних даних.

Галузь застосування. Отримані результати можуть бути використані під час розроблення та вдосконалення систем захисту персональних даних у цифрових інформаційних системах, а також у процесах управління ризиками інформаційної безпеки, спрямованих на запобігання витоку персональних даних та підвищення рівня захищеності інформаційних ресурсів організацій.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, ВИТОК ПЕРСОНАЛЬНИХ ДАНИХ, ЦИФРОВІ ІНФОРМАЦІЙНІ СИСТЕМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, ЗАХИСТ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, ОЦІНЮВАННЯ РИЗИКІВ, ЗАГРОЗИ БЕЗПЕЦІ, КОНФІДЕНЦІЙНІСТЬ ДАНИХ.

ABSTRACT

The qualification work is devoted to the study of the impact of the human factor on the effectiveness of the information security management system. The work consists of an introduction, three chapters containing 19 figures, 25 tables, conclusions and the list of references containing 46 items. The total volume of the work is 102 pages, of which 6 pages is occupied by the list of references.

The purpose of the study is to investigate methods for managing the risks of personal data breaches in digital information systems and to develop recommendations for enhancing the level of protection.

The object the study is the processes involved in ensuring the protection of personal data in digital information systems.

The subject of the study is the methods, models and tools for managing the risks of personal data breaches in digital information systems.

Research methods. In order to solve the above-mentioned scientific task, this study employs methods of analysis and synthesis, comparison, classification, risk assessment, modelling, and expert evaluation, as well as a systematic approach to information security management and the protection of personal data.

As a result, this paper examines the theoretical foundations of personal data protection in digital information systems; analyses the main threats and risks of data leaks; studies modern risk management methods and personal data protection measures; and develops practical recommendations for enhancing information security and reducing the likelihood of incidents involving personal data leaks.

Field of application. The results obtained can be used in the development and improvement of personal data protection systems within digital information systems, as well as in information security risk management processes aimed at preventing personal data leaks and enhancing the security of organisations' information resources.

Keywords: PERSONAL DATA, PERSONAL DATA LEAKAGE, DIGITAL INFORMATION SYSTEMS, INFORMATION SECURITY, RISK MANAGEMENT, INFORMATION PROTECTION, CYBERSECURITY, RISK

ASSESSMENT, SECURITY THREATS, DATA CONFIDENTIALITY.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах цифрової трансформації суспільства та стрімкого зростання обсягів інформації особливого значення набуває проблема захисту персональних даних у цифрових інформаційних системах. Постійне збільшення кількості кіберзагроз, несанкціонованих доступів, витоків інформації та кібератак створює суттєві ризики для конфіденційності, цілісності та доступності персональних даних. Наслідками таких інцидентів можуть бути фінансові збитки, репутаційні втрати організацій, порушення прав громадян та зниження рівня довіри до цифрових сервісів.

З огляду на це, особливої актуальності набуває дослідження методів управління ризиками витоку персональних даних у цифрових інформаційних системах, а також розроблення ефективних підходів до їх виявлення, оцінювання та мінімізації з метою підвищення рівня інформаційної безпеки та забезпечення надійного захисту персональних даних.

Мета роботи полягає у дослідженні методів управління ризиками витоку персональних даних у цифрових інформаційних системах та розроблення рекомендацій щодо підвищення рівня їх захисту.

Об'єкт дослідження – процеси забезпечення захисту персональних даних у цифрових інформаційних системах.

Предмет дослідження – методи, моделі та засоби управління ризиками витоку персональних даних у цифрових інформаційних системах.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні основи захисту персональних даних та управління ризиками.

2. Проаналізувати ризики витоку персональних даних у цифрових інформаційних системах.

3. Розробити методи та практичні рекомендації щодо зниження ризиків витоку даних.

Методи дослідження. Для вирішення поставленого наукового завдання в

роботі використані методи аналізу та синтезу, порівняння, класифікації, оцінювання ризиків, моделювання, експертної оцінки, а також системний підхід до управління інформаційною безпекою та захистом персональних даних.

Як результат у роботі досліджено теоретичні основи захисту персональних даних у цифрових інформаційних системах; проаналізовано основні загрози та ризики їх витоку; вивчено сучасні методи управління ризиками та засоби захисту персональних даних; розроблено практичні рекомендації щодо підвищення рівня захисту інформації та зниження ймовірності виникнення інцидентів, пов’язаних із витоком персональних даних.

Практичне значення одержаних результатів. Застосування отриманих результатів дозволить підвищити рівень захисту персональних даних у цифрових інформаційних системах шляхом своєчасного виявлення, оцінювання та мінімізації ризиків їх витоку. Запропоновані підходи та рекомендації можуть бути використані для вдосконалення процесів управління ризиками інформаційної безпеки, підвищення ефективності механізмів захисту даних, а також обґрунтованого вибору організаційних і технічних заходів безпеки відповідно до особливостей функціонування конкретної інформаційної системи.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА УПРАВЛІННЯ РИЗИКАМИ

1.1 Поняття персональних даних та загрози їх витоку в цифровому середовищі

Персональні дані є одним із ключових інформаційних ресурсів сучасного цифрового суспільства, оскільки забезпечують ідентифікацію фізичних осіб, підтримують функціонування електронних сервісів, інформаційних систем, фінансових установ, державних реєстрів та корпоративних інформаційних середовищ. Стрімкий розвиток інформаційно-комунікаційних технологій, поширення хмарних обчислень, мобільних пристроїв, соціальних мереж та цифрових платформ призвели до значного збільшення обсягів персональних даних, що обробляються, передаються та зберігаються в електронному вигляді. У таких умовах питання забезпечення конфіденційності, цілісності та доступності персональних даних набуває особливого значення, оскільки їх компрометація може спричинити як матеріальні збитки, так і порушення основоположних прав і свобод людини [1].

Поняття персональних даних є базовою категорією у сфері захисту інформації та інформаційної безпеки. Під персональними даними розуміють будь-які відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. До таких даних належать прізвище, ім’я, по батькові, дата народження, місце проживання, номер телефону, адреса електронної пошти, паспортні реквізити, податковий номер, фінансова інформація, біометричні характеристики, геолокаційні дані, відомості про освіту, трудову діяльність та інші характеристики, які дозволяють встановити особу або сформувати її цифровий профіль [2]. Особливістю персональних даних є те, що навіть окремі фрагменти інформації, які самостійно

не дають змоги ідентифікувати людину, у поєднанні з іншими даними можуть забезпечити її точне визначення.

У сучасних умовах персональні дані виступають цінним активом як для організацій, так і для кіберзлочинців. Організації використовують їх для надання послуг, автоматизації бізнес-процесів, персоналізації взаємодії з клієнтами та прийняття управлінських рішень. Водночас незаконне отримання персональних даних відкриває широкі можливості для здійснення шахрайства, викрадення особистості, фінансових злочинів, соціальної інженерії та інших протиправних дій [3]. Саме тому захист персональних даних розглядається не лише як технічне завдання, а й як комплексна організаційно-правова проблема, що охоплює питання регулювання доступу, управління ризиками, контролю обробки інформації та формування культури безпеки.

Розвиток цифрового середовища значно розширив можливості збору та обробки інформації про користувачів. Практично кожна дія людини в мережі Інтернет супроводжується створенням цифрових слідів, які накопичуються інформаційними системами [4]. Використання соціальних мереж, електронної комерції, банківських сервісів, мобільних додатків та державних електронних платформ призводить до постійного зростання кількості персональних даних, що циркулюють у цифровому просторі. Це створює сприятливі умови для виникнення нових загроз безпеці інформації та ускладнює процес контролю за її використанням [5].

Загроза витоку персональних даних являє собою потенційну можливість несанкціонованого отримання, розголошення, копіювання, зміни або знищення інформації, що містить відомості про фізичних осіб [6]. Такі загрози можуть виникати як внаслідок навмисних дій зловмисників, так і через помилки персоналу, технічні несправності або недоліки в організації захисту інформації. Сучасне цифрове середовище характеризується високою взаємозалежністю інформаційних систем, що збільшує площу атаки та створює додаткові ризики для власників персональних даних.

Рис. 1.1 Основні джерела загроз витоку персональних даних у цифровому середовищі

Однією з найбільш поширених загроз є несанкціонований доступ до інформаційних ресурсів. Він може здійснюватися шляхом підбору паролів, використання викрадених облікових даних, експлуатації програмних вразливостей або обходу механізмів автентифікації. Отримавши доступ до інформаційної системи, зловмисник може копіювати бази даних, змінювати інформацію або використовувати її для подальших атак [7]. Особливо небезпечними є випадки компрометації корпоративних систем, які містять великі масиви персональних даних клієнтів та працівників.

Суттєву загрозу становлять атаки соціальної інженерії, які базуються на психологічному впливі на користувачів. Зловмисники можуть використовувати електронні листи, телефонні дзвінки, повідомлення в месенджерах або підроблені вебсайти для отримання конфіденційної інформації. Ефективність таких атак пояснюється людським фактором, який залишається одним із найслабших елементів системи інформаційної безпеки [8]. Навіть за наявності сучасних технічних засобів захисту необережні дії користувачів можуть призвести до розкриття персональних даних.

Важливою категорією загроз є шкідливе програмне забезпечення. Віруси, троянські програми, шпигунське програмне забезпечення та програми-вимагачі здатні здійснювати несанкціонований збір інформації, передавати дані третім особам або блокувати доступ до інформаційних ресурсів. Особливу небезпеку становлять сучасні цільові атаки, які поєднують кілька методів впливу та тривалий час залишаються непоміченими системами захисту.

Серед внутрішніх загроз особливу увагу привертають дії працівників організації. Витік персональних даних може відбуватися внаслідок недотримання вимог безпеки, неправильного налаштування інформаційних систем, втрати носіїв інформації або свідомого розголошення конфіденційних відомостей. Практика свідчить, що значна частина інцидентів безпеки пов’язана саме з людським фактором та недостатнім рівнем підготовки персоналу.

Окремим джерелом ризику є використання хмарних технологій. Хмарні сервіси забезпечують високу доступність та масштабованість інформаційних ресурсів, проте одночасно породжують нові виклики у сфері захисту даних. Передача інформації стороннім провайдерам вимагає впровадження додаткових механізмів контролю, шифрування та моніторингу безпеки [9]. Недостатній рівень захисту хмарної інфраструктури або помилки конфігурації можуть призвести до масового витоку персональних даних.

Зростання популярності мобільних пристроїв також створює додаткові ризики. Смартфони, планшети та ноутбуки часто використовуються для доступу до корпоративних ресурсів і містять значний обсяг персональної інформації. Втрата пристрою, встановлення ненадійних програм або використання незахищених мереж можуть стати причиною компрометації даних. У зв’язку з цим особливого значення набувають засоби мобільної безпеки, шифрування та багатофакторної автентифікації.

Серйозну загрозу становлять витоки інформації через мережеві комунікації. Передача даних через незахищені канали зв’язку створює ризик їх перехоплення третіми особами. Для мінімізації таких загроз застосовуються криптографічні методи захисту, протоколи безпечного з’єднання та технології

віртуальних приватних мереж. Проте навіть використання сучасних засобів захисту не гарантує абсолютної безпеки за умови неналежного адміністрування або наявності вразливостей у програмному забезпеченні.

Наслідки витоку персональних даних можуть мати як індивідуальний, так і суспільний характер. Для фізичних осіб це може означати фінансові втрати, незаконне використання особистої інформації, дискримінацію, втрату репутації та психологічний дискомфорт. Для організацій витоки даних призводять до фінансових збитків, втрати довіри клієнтів, судових позовів, штрафних санкцій та погіршення конкурентних позицій. У масштабах держави масові витоки персональних даних можуть становити загрозу національній безпеці та стабільності функціонування критичної інформаційної інфраструктури.

Таблиця 1.1

Основні загрози витоку персональних даних та їх наслідки

Загроза	Спосіб реалізації	Можливі наслідки
Несанкціонований доступ	Використання викрадених облікових даних, експлуатація вразливостей	Викрадення або зміна персональних даних
Фішинг	Введення користувача в оману через підроблені ресурси	Отримання логінів, паролів, фінансових даних
Шкідливе програмне забезпечення	Встановлення вірусів, троянів, шпигунських програм	Компрометація інформації та порушення роботи систем
Внутрішні порушники	Навмисні або випадкові дії працівників	Витік конфіденційної інформації
Незахищені канали зв'язку	Передача даних без шифрування	Перехоплення інформації сторонніми особами
Помилки конфігурації хмарних сервісів	Неправильне налаштування доступу	Масове розкриття персональних даних
Втрата мобільних пристроїв	Крадіжка або загублення пристрою	Несанкціонований доступ до інформації
Соціальна інженерія	Маніпуляція поведінкою користувачів	Отримання конфіденційних відомостей та доступу до систем

Ефективний захист персональних даних потребує комплексного підходу, який поєднує правові, організаційні та технічні заходи. До таких заходів належать розроблення політик безпеки, впровадження систем контролю доступу, використання криптографічного захисту інформації, проведення аудиту безпеки,

моніторинг подій інформаційної безпеки та регулярне навчання персоналу. Важливим елементом є також управління ризиками, що передбачає систематичне виявлення загроз, оцінювання ймовірності їх реалізації та визначення заходів щодо мінімізації можливих наслідків [10].

Отже, персональні дані є стратегічно важливим інформаційним ресурсом сучасного цифрового суспільства. Їх активне використання забезпечує функціонування цифрової економіки та інформаційних систем, проте одночасно підвищує рівень ризиків, пов’язаних із несанкціонованим доступом та витоком інформації . Зростання кількості кіберзагроз, складність інформаційних технологій та людський фактор обумовлюють необхідність постійного вдосконалення механізмів захисту персональних даних та розвитку ефективних систем управління ризиками в цифровому середовищі.

1.2 Основні принципи та методи управління інформаційними ризиками

Інтенсивний розвиток цифрових технологій, зростання обсягів інформації та широке впровадження інформаційно-комунікаційних систем у діяльність державних установ, підприємств і організацій обумовлюють необхідність забезпечення належного рівня інформаційної безпеки. Одним із ключових напрямів сучасного управління безпекою є управління інформаційними ризиками, яке дозволяє своєчасно виявляти потенційні загрози, оцінювати їх можливий вплив та впроваджувати заходи щодо мінімізації негативних наслідків. Ефективне управління ризиками сприяє забезпеченню стабільного функціонування інформаційних систем, захисту персональних даних та підтриманню безперервності бізнес-процесів.

Інформаційний ризик являє собою ймовірність виникнення події, пов’язаної з порушенням конфіденційності, цілісності або доступності інформації, яка може призвести до матеріальних, фінансових, репутаційних або інших втрат для організації [11]. На відміну від традиційних загроз, ризик

розглядається як поєднання ймовірності реалізації певної загрози та масштабу її можливих наслідків. Таким чином, навіть незначна загроза може становити суттєвий ризик у випадку значного потенційного збитку, а високий рівень загрози може розглядатися як прийнятний ризик за умови мінімальних наслідків для організації.

Управління інформаційними ризиками є безперервним процесом, що охоплює сукупність організаційних, технічних та управлінських заходів, спрямованих на забезпечення належного рівня захисту інформаційних активів. Основною метою такого управління є досягнення балансу між рівнем безпеки інформаційних ресурсів та витратами на їх захист. Практика свідчить, що повне усунення всіх ризиків є неможливим, тому основним завданням стає їх виявлення, аналіз, оцінювання та контроль до прийнятного для організації рівня.

Одним із фундаментальних принципів управління інформаційними ризиками є принцип системності. Він передбачає розгляд інформаційної безпеки як цілісної системи взаємопов’язаних елементів, до складу якої входять інформаційні активи, персонал, технічні засоби, програмне забезпечення, мережна інфраструктура та організаційні процеси [12]. Реалізація цього принципу забезпечує комплексний підхід до оцінювання ризиків і дозволяє враховувати взаємний вплив окремих компонентів інформаційної системи.

Важливим принципом є принцип безперервності управління ризиками. Сучасне інформаційне середовище постійно змінюється під впливом нових технологій, кіберзагроз та змін у законодавстві. Відповідно ризики не можуть оцінюватися одноразово. Необхідним є постійний моніторинг стану інформаційної безпеки, аналіз нових загроз та актуалізація заходів захисту відповідно до змін зовнішнього та внутрішнього середовища.

Суттєве значення має принцип превентивності, відповідно до якого основна увага приділяється попередженню виникнення інцидентів безпеки, а не ліквідації їх наслідків. Запобігання ризикам є більш ефективним та економічно доцільним порівняно з усуненням наслідків реалізованих загроз. Реалізація

даного принципу передбачає своєчасне виявлення вразливостей, проведення аудитів безпеки та впровадження профілактичних заходів.

Одним із базових принципів також є принцип економічної доцільності. Захист інформації потребує фінансових витрат, тому рівень впроваджуваних заходів повинен відповідати цінності інформаційних активів та рівню потенційних збитків. Надмірні витрати на захист можуть бути економічно невиправданими, тоді як недостатній рівень безпеки створює додаткові ризики для діяльності організації.

Важливим є принцип відповідальності, який передбачає чітке визначення обов’язків та повноважень усіх учасників процесу управління ризиками. Ефективна система безпеки неможлива без розподілу відповідальності між керівництвом, адміністраторами інформаційних систем, фахівцями з кібербезпеки та звичайними користувачами [13]. Кожен учасник повинен усвідомлювати власну роль у забезпеченні захисту інформаційних ресурсів.

Сучасні підходи до управління інформаційними ризиками базуються на міжнародних стандартах та рекомендаціях. Особливого поширення набули стандарти серії ISO/IEC 27000, які визначають загальні вимоги до систем управління інформаційною безпекою та процедури оцінювання ризиків. Відповідно до цих стандартів процес управління ризиками включає встановлення контексту, ідентифікацію ризиків, їх аналіз, оцінювання, обробку, моніторинг та постійне вдосконалення системи безпеки.

Рис. 1.2 Процес управління інформаційними ризиками

Першим етапом управління ризиками є ідентифікація інформаційних активів. На цьому етапі визначаються всі ресурси, що мають цінність для організації та потребують захисту. До них належать бази даних, персональні дані, програмне забезпечення, серверне обладнання, мережна інфраструктура, документація та інші інформаційні ресурси. Визначення активів дозволяє сформувати основу для подальшого аналізу загроз та оцінювання ризиків.

Наступним етапом є ідентифікація загроз та вразливостей. Загрозами можуть бути зовнішні кібератаки, шкідливе програмне забезпечення, соціальна інженерія, технічні збої, стихійні лиха або внутрішні порушення політик безпеки. Вразливості являють собою слабкі місця інформаційної системи, які можуть бути використані для реалізації загроз. Виявлення таких вразливостей здійснюється шляхом аудиту безпеки, тестування на проникнення та аналізу конфігурацій систем.

Після визначення загроз здійснюється аналіз ризиків. Основною метою цього етапу є встановлення рівня ризику шляхом оцінювання ймовірності реалізації загрози та масштабу можливих наслідків. Аналіз може проводитися

якісними, кількісними або комбінованими методами. Якісний підхід базується на використанні експертних оцінок та класифікації ризиків за рівнями критичності. Кількісний підхід передбачає використання числових показників, статистичних даних та математичних моделей для визначення рівня ризику.

Одним із найбільш поширених методів є матричний метод оцінювання ризиків. Він передбачає побудову матриці, у якій ризики класифікуються залежно від ймовірності виникнення та рівня потенційного впливу. Використання такого підходу дозволяє швидко визначати найбільш критичні ризики та встановлювати пріоритети щодо їх обробки.

Значного поширення набув метод експертних оцінок, який використовується у випадках недостатності статистичних даних. Його сутність полягає у залученні фахівців для визначення рівня ризику на основі професійного досвіду та знань. Незважаючи на певну суб’єктивність, цей метод є ефективним для оцінювання нових або складних загроз [14].

У сучасних умовах широко застосовуються методи кількісного аналізу ризиків. Вони дозволяють оцінювати можливі фінансові втрати, визначати економічну ефективність заходів безпеки та обґрунтовувати управлінські рішення. Для цього використовуються статистичні методи, теорія ймовірностей, моделювання сценаріїв та інші математичні інструменти.

Після проведення аналізу здійснюється оцінювання ризиків. На цьому етапі визначається рівень прийнятності кожного ризику та приймається рішення щодо необхідності впровадження додаткових заходів захисту. Ризики можуть бути прийнятими, зменшеними, переданими або усуненими залежно від стратегії управління організації.

Таблиця 1.2

Основні методи управління інформаційними ризиками

Метод управління ризиком	**Характеристика**	**Приклад застосування**
Уникнення ризику	Відмова від діяльності, що створює загрозу	Відмова від використання застарілого ПЗ
Зменшення ризику	Впровадження заходів захисту	Шифрування даних, MFA
Передача ризику	Перекладення відповідальності на третю сторону	Кіберстрахування, аутсорсинг
Прийняття ризику	Усвідомлене погодження з ризиком	Збереження низькокритичних вразливостей
Моніторинг ризику	Постійний контроль стану безпеки	Використання SIEM-систем
Попередження ризику	Профілактичні заходи	Навчання персоналу з кібербезпеки

Метод уникнення ризику передбачає відмову від діяльності або технології, яка створює надмірний рівень загроз. Метод зменшення ризику полягає у впровадженні технічних та організаційних засобів захисту. Передача ризику може здійснюватися через страхування або залучення сторонніх постачальників послуг. У випадку низького рівня ризику організація може прийняти його без впровадження додаткових заходів контролю.

Особливу роль у сучасних системах управління ризиками відіграє моніторинг. Його метою є постійне спостереження за станом інформаційної безпеки та своєчасне виявлення змін, які можуть вплинути на рівень ризиків [15]. Для цього використовуються системи моніторингу подій безпеки, засоби аналізу журналів подій, платформи управління інцидентами та інші технологічні рішення.

Ефективність управління інформаційними ризиками значною мірою залежить від рівня підготовки персоналу. Навіть найсучасніші технічні засоби не можуть повністю компенсувати помилки користувачів або нехтування правилами безпеки. Саме тому важливими складовими системи управління ризиками є навчання персоналу, формування культури кібербезпеки та регулярне підвищення обізнаності працівників щодо сучасних загроз.

Отже, управління інформаційними ризиками є невід'ємною складовою сучасної системи захисту персональних даних та інформаційної безпеки загалом. Його ефективність ґрунтується на дотриманні принципів системності, безперервності, превентивності, економічної доцільності та відповідальності. Використання сучасних методів аналізу й оцінювання ризиків дозволяє своєчасно виявляти потенційні загрози, мінімізувати можливі збитки та забезпечувати стабільне функціонування інформаційних систем в умовах постійного розвитку цифрового середовища.

1.3 Нормативно-правове регулювання захисту персональних даних та міжнародні стандарти

Захист персональних даних є одним із пріоритетних напрямів забезпечення інформаційної безпеки в умовах цифрової трансформації суспільства. Активне використання інформаційно-комунікаційних технологій, розвиток електронного урядування, електронної комерції, дистанційних сервісів та глобальних мереж обумовлюють необхідність створення ефективної нормативно-правової бази, яка регламентує порядок збору, обробки, зберігання та передачі персональних даних. Належне правове регулювання забезпечує захист прав фізичних осіб на приватність, визначає обов'язки власників інформаційних систем та встановлює відповідальність за порушення вимог щодо обробки персональної інформації.

Нормативно-правове регулювання захисту персональних даних являє собою систему законодавчих, нормативних та організаційних документів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації про фізичних осіб. Основною метою такого регулювання є створення правових механізмів, які гарантують законність обробки персональних даних, захист прав суб'єктів даних та запобігання їх несанкціонованому використанню.

В Україні правові засади захисту персональних даних визначаються Конституцією України, яка гарантує кожному право на невтручання в особисте і сімейне життя, а також забороняє збирання, зберігання, використання та

поширення конфіденційної інформації про особу без її згоди, за винятком випадків, передбачених законом. Конституційні норми є фундаментом для формування всієї системи правового регулювання у сфері захисту персональних даних та визначають загальні принципи забезпечення інформаційної безпеки громадян.

Ключовим спеціалізованим нормативним актом у даній сфері є Закон України «Про захист персональних даних». У цьому законі визначено поняття персональних даних, принципи їх обробки, права суб'єктів персональних даних, обов'язки володільців і розпорядників інформації, а також порядок здійснення державного контролю за дотриманням законодавства. Закон встановлює вимоги щодо отримання згоди суб'єкта даних, визначення мети обробки інформації та забезпечення належного рівня її захисту від несанкціонованого доступу.

Важливе значення для регулювання інформаційних відносин мають також Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про електронні довірчі послуги», Закон України «Про електронні комунікації» та інші нормативно-правові акти. Їх положення визначають загальні принципи функціонування інформаційного простору, вимоги до захисту інформації в автоматизованих системах та порядок використання сучасних електронних технологій під час обробки персональних даних.

Особливе місце в системі правового забезпечення захисту інформації займають підзаконні нормативні акти, стандарти та методичні рекомендації уповноважених державних органів. Вони деталізують порядок реалізації законодавчих вимог, встановлюють організаційні та технічні заходи безпеки, регламентують проведення аудитів, оцінювання ризиків та впровадження систем управління інформаційною безпекою. Використання таких документів дозволяє організаціям забезпечувати практичне виконання вимог законодавства та підтримувати належний рівень захисту інформаційних ресурсів.

У сучасних умовах нормативно-правове регулювання захисту персональних даних не обмежується національним законодавством. Глобалізація

інформаційних процесів та міжнародний обмін даними обумовлюють необхідність гармонізації національних правових норм із міжнародними стандартами та рекомендаціями. Це особливо актуально для України в контексті європейської інтеграції та адаптації законодавства до вимог Європейського Союзу.

Рис. 1.3 Система нормативно-правового регулювання захисту персональних даних

Одним із найбільш впливових міжнародних нормативних документів у сфері захисту персональних даних є Загальний регламент захисту даних Європейського Союзу (General Data Protection Regulation, GDPR). Цей документ набув чинності у 2018 році та встановив єдині правила обробки персональних даних для всіх країн Європейського Союзу. GDPR визначає принципи законності, добросовісності та прозорості обробки інформації, обмеження цілей використання даних, мінімізації обсягу інформації, точності, обмеження строків зберігання та забезпечення належного рівня безпеки [16].

Особливістю GDPR є орієнтація на права суб'єкта персональних даних. Регламент надає громадянам право на доступ до власної інформації, право на

виправлення неточних даних, право на видалення інформації, право на обмеження обробки, право на перенесення даних та право заперечувати проти їх використання. Водночас документ встановлює суворі вимоги до організацій щодо повідомлення про інциденти безпеки та передбачає значні фінансові санкції за порушення законодавства.

Важливим міжнародним документом є Конвенція Ради Європи №108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Ця конвенція стала першим міжнародним юридично обов'язковим документом у сфері захисту персональних даних та заклала основи сучасного міжнародного регулювання інформаційної приватності. Положення Конвенції визначають основні принципи законної обробки інформації та спрямовані на забезпечення балансу між розвитком інформаційних технологій і захистом прав людини.

Суттєвий вплив на розвиток систем захисту персональних даних мають міжнародні стандарти у сфері інформаційної безпеки. Особливе значення належить стандарту ISO/IEC 27001, який встановлює вимоги до створення, впровадження, функціонування та постійного вдосконалення системи управління інформаційною безпекою [17]. Основною метою даного стандарту є забезпечення системного підходу до захисту інформаційних активів шляхом управління ризиками та впровадження відповідних механізмів контролю.

Стандарт ISO/IEC 27002 доповнює вимоги ISO/IEC 27001 та містить рекомендації щодо практичного впровадження заходів інформаційної безпеки. У ньому визначено широкий перелік контролів, спрямованих на управління доступом, криптографічний захист, фізичну безпеку, моніторинг подій та реагування на інциденти. Використання положень даного стандарту сприяє підвищенню рівня захисту персональних даних та зниженню ризику їх компрометації.

Важливу роль у сфері захисту персональних даних відіграє стандарт ISO/IEC 27701, який є розширенням системи управління інформаційною безпекою та орієнтований безпосередньо на управління конфіденційною інформацією. Цей стандарт визначає вимоги до створення систем управління

приватністю та забезпечує інтеграцію процесів захисту персональних даних у загальну систему інформаційної безпеки організації.

Значну увагу міжнародні стандарти приділяють ризик-орієнтованому підходу до захисту інформації. Зокрема, стандарт ISO/IEC 27005 встановлює методологію управління ризиками інформаційної безпеки та визначає процедури їх ідентифікації, аналізу, оцінювання та обробки. Використання такого підходу дозволяє організаціям ефективно розподіляти ресурси та концентрувати увагу на найбільш критичних загрозах.

Впровадження міжнародних стандартів забезпечує низку переваг для організацій. Серед них підвищення рівня довіри з боку клієнтів і партнерів, зниження ймовірності виникнення інцидентів безпеки, покращення процесів управління ризиками та забезпечення відповідності законодавчим вимогам. Крім того, міжнародні стандарти сприяють уніфікації підходів до захисту інформації та полегшують міжнародне співробітництво у сфері інформаційної безпеки.

У сучасних умовах ефективний захист персональних даних неможливий без поєднання правових механізмів і міжнародних практик управління безпекою. Законодавчі норми визначають обов’язкові вимоги щодо обробки інформації, тоді як міжнародні стандарти надають інструменти для їх практичної реалізації. Така інтеграція забезпечує комплексний підхід до захисту персональних даних та сприяє формуванню сучасної системи інформаційної безпеки.

Отже, нормативно-правове регулювання захисту персональних даних є важливою складовою забезпечення інформаційної безпеки в цифровому середовищі. Національне законодавство України формує правові основи захисту інформації, а міжнародні стандарти та нормативні документи забезпечують використання сучасних підходів до управління ризиками та захисту персональних даних [18]. Гармонізація законодавства з міжнародними вимогами сприяє підвищенню ефективності захисту інформації, розвитку цифрової економіки та зміцненню довіри користувачів до інформаційних систем.

Висновки до розділу 1

У першому розділі було досліджено теоретичні основи захисту персональних даних та управління інформаційними ризиками в умовах цифрового середовища. Визначено сутність персональних даних, їх значення для сучасних інформаційних систем, а також проаналізовано основні загрози та ризики, пов’язані з їх витоком, несанкціонованим доступом і неправомірною обробкою. Встановлено, що зростання обсягів цифрової інформації та розвиток інформаційно-комунікаційних технологій потребують постійного вдосконалення механізмів захисту даних.

Розглянуто основні принципи та методи управління інформаційними ризиками, зокрема принципи системності, безперервності, превентивності, економічної доцільності та відповідальності. Проаналізовано етапи процесу управління ризиками, які включають ідентифікацію активів, виявлення загроз і вразливостей, аналіз та оцінювання ризиків, вибір способів їх обробки, впровадження заходів захисту та моніторинг ефективності системи безпеки. Визначено, що ризик-орієнтований підхід є необхідною умовою забезпечення належного рівня інформаційної безпеки.

Досліджено нормативно-правові засади захисту персональних даних в Україні та міжнародні стандарти у цій сфері. Встановлено, що ефективний захист інформації забезпечується поєднанням вимог національного законодавства, зокрема Закону України «Про захист персональних даних», із положеннями міжнародних документів та стандартів, таких як GDPR, Конвенція Ради Європи №108, ISO/IEC 27001, ISO/IEC 27005 та ISO/IEC 27701. Їх застосування створює правову та організаційну основу для побудови комплексної системи захисту персональних даних і управління інформаційними ризиками.

Розділ 2 АНАЛІЗ РИЗИКІВ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1 Аналіз типових каналів витоку персональних даних у сучасних інформаційних системах

Канал витоку персональних даних доцільно розглядати як технічний або організаційний шлях, через який інформація, що підлягає захисту, може залишити межі контрольованої інформаційної системи та стати доступною особам, які не мають на це відповідних прав. У такому розумінні витік не обмежується прямим викраденням файлів або несанкціонованим доступом до баз даних. Він охоплює будь-яку ситуацію, у якій персональні дані передаються, копіюються, зберігаються або опосередковано розкриваються поза межами встановленої політики безпеки. Особливість сучасних цифрових інформаційних систем полягає в тому, що обробка даних здійснюється через значну кількість взаємопов’язаних компонентів: робочі станції користувачів, сервери, мережеві сервіси, спільні сховища, засоби автентифікації, системи передавання повідомлень і зовнішні канали зв’язку [19]. Кожен із таких компонентів потенційно може стати частиною каналу витоку, якщо контроль доступу, моніторинг або правила передавання інформації реалізовані недостатньо повно.

Таблиця 2.1

Загальна характеристика каналів витоку персональних даних

Вид каналу витоку	Характеристика	Особливість ризику
Дозволений канал передавання	Використовується штатний механізм обміну інформацією, але з порушенням установлених правил безпеки	Дані можуть передаватися через легітимний шлях, тому сам факт передавання не завжди виглядає підозрілим
Спільний інформаційний ресурс	Дані розміщуються у сховищі або ресурсі, до якого може отримати доступ інша особа	Ризик виникає через неправильне розмежування доступу або наявність стороннього доступу до ресурсу
Прихований канал	Для передавання даних використовується канал, який не був призначений для цього	Небезпека полягає в маскуванні самого факту передавання інформації

Канал через авторизованого користувача	Дані залишають систему через особу, яка має законний доступ до них	Шифрування та контроль доступу не усувають ризик після того, як користувач отримав дані у відкритому вигляді

Витік персональних даних може відбуватися як через звичайні дозволені канали обміну інформацією, так і через приховані канали. У першому випадку передавання даних здійснюється через легітимні механізми, які формально призначені для обміну інформацією, однак використовуються з порушенням установлених правил. Наприклад, користувач може мати законний доступ до певного набору персональних даних, але передати їх сторонній особі або розмістити у середовищі, де вони стають доступними неавторизованим суб'єктам. Така ситуація демонструє, що сам факт наявності шифрування, автентифікації чи розмежування прав доступу не завжди гарантує запобігання витоку, оскільки після отримання доступу користувач може працювати з даними вже у відкритому вигляді.

Рис. 2.1. Узагальнена схема формування каналу витоку персональних даних

Приховані канали становлять окрему проблему, оскільки їхня мета полягає не лише в передаванні інформації, а й у маскуванні самого факту такого передавання. У цьому випадку канал, який не був призначений для передавання персональних даних, використовується для прихованого виведення чутливої інформації з порушенням політики безпеки. Небезпека таких каналів полягає в тому, що вони можуть не сприйматися системами контролю як очевидне порушення, особливо якщо зовнішньо їхня активність нагадує звичайну роботу інформаційної системи [20].

Мережеві канали витоку персональних даних формуються під час передавання інформації між користувачами, службами, серверами, зовнішніми ресурсами та іншими вузлами цифрової інформаційної системи. Їхня особливість полягає в тому, що дані залишають межі окремого робочого пристрою або внутрішнього сховища та переміщуються через канали зв’язку, які можуть бути як дозволеними, так і використаними з порушенням політики безпеки. Передавання персональних даних через електронну пошту, вебсайти, служби обміну файлами, віддалені підключення, мережеві сховища або системи повідомлень саме по собі не є порушенням, якщо воно відповідає встановленим правилам доступу, автентифікації та контролю. Однак ці самі канали можуть стати засобом витоку, коли через них передаються відомості особам, які не мають права їх отримувати, або коли користувач надсилає дані за межі організації без належного дозволу. Тому ризик мережевого витоку пов’язаний не лише з наявністю самого каналу зв’язку, а й з тим, яка інформація ним передається, хто є відправником і отримувачем, який спосіб передавання використовується та чи відповідає така передача правилам безпеки.

Таблиця 2.2

Загальна характеристика мережевих каналів витоку персональних даних

Тип мережевого каналу	**Сутність використання**	**Ризик для персональних даних**
Електронна пошта	Передавання повідомлень і вкладених файлів між користувачами	Надсилання персональних даних неавторизованому отримувачу або за межі контрольованої системи
Вебресурси	Передавання даних через звернення до зовнішніх сайтів або служб	Виведення інформації через звичайну мережеву активність, яка може виглядати як штатна робота користувача
Служби обміну файлами	Передавання або розміщення файлів на зовнішніх ресурсах	Потрапляння файлів із персональними даними у середовище з недостатнім контролем доступу
Віддалене підключення	Доступ до системи або ресурсів через мережевий канал	Можливість передавання даних за межі внутрішньої системи через дозволене з’єднання

Важливою характеристикою мережевих каналів є те, що значна частина трафіку може виглядати штатною для інформаційної системи. Повідомлення електронної пошти, звернення до вебресурсів або передавання файлів можуть не викликати підозри на рівні простого мережевого контролю, оскільки зовнішньо відповідають звичайній діяльності користувача [21]. У таких умовах недостатньо аналізувати лише факт з’єднання або адресу отримувача. Необхідно враховувати вміст переданих даних, контекст операції, напрямок руху інформації та відповідність дій користувача дозволеним сценаріям. Особливо небезпечними є ситуації, коли користувач має законний доступ до персональних даних, але використовує мережевий канал для їхнього виведення за межі контрольованого середовища. У такому випадку традиційне розмежування доступу не усуває ризик, оскільки порушення виникає вже після отримання інформації у придатному для використання вигляді.

Окрему групу становлять приховані способи передавання персональних даних через мережу. У таких випадках використовуються канали, які формально призначені для інших службових або технічних завдань, але можуть переносити

приховану інформацію. Дані можуть маскуватися у зверненнях до служби доменних імен, у службових полях мережевих повідомлень, у змінених параметрах пакетів або в особливій послідовності передавання трафіку. Також можливе використання часових затримок між повідомленнями, коли інформація передається не стільки через зміст пакета, скільки через порядок, частоту або момент його надсилання. Небезпека таких каналів полягає в тому, що вони можуть не містити очевидного фрагмента персональних даних у відкритому вигляді, але водночас забезпечувати їх поступове або закодоване виведення.

Рис. 2.2 Узагальнена схема мережевого витоку персональних даних

Канали витоку через спільні ресурси та сховища виникають у ситуаціях, коли персональні дані розміщуються у середовищі, доступ до якого не обмежений належним чином або може бути використаний не лише тими суб’єктами, для яких ці дані призначені. До таких ресурсів належать спільні папки, мережеві диски, файлові сервери, сховища резервних копій, бази даних та інші місця централізованого або розподіленого зберігання інформації.

Таблиця 2.3

Характеристика каналів витоку через спільні ресурси та сховища

Тип спільного ресурсу	**Потенційна умова витоку**	**Наслідок для персональних даних**
Спільна папка	Надмірні права доступу для користувачів	Дані можуть бути переглянуті або скопійовані особами без належних повноважень
Мережевий диск	Неправильне розмежування прав читання та запису	Внутрішній користувач може розмістити дані у доступному для інших середовищі
Файловий сервер	Відсутність контролю за тим, хто отримує доступ до файлів	Ускладнюється відстеження подальшого руху персональних даних
Сховище резервних копій	Збереження копій даних у менш контрольованому середовищі	Персональні дані можуть залишатися доступними навіть після обмеження доступу до основного джерела
База даних	Надання доступу ширшому колу користувачів, ніж необхідно	Дані можуть бути отримані користувачами, які не мають потреби в їх обробці

Основна небезпека полягає в тому, що сховище може виконувати роль проміжної ланки між внутрішнім користувачем, який має доступ до персональних даних, і стороннім отримувачем, який не повинен мати можливості їх переглядати або копіювати. У такому випадку витік не завжди відбувається шляхом прямого надсилання інформації назовні. Дані можуть бути спочатку розміщені у спільному ресурсі, а вже потім отримані іншою особою через неправильні права доступу, слабку автентифікацію або відсутність належного контролю за використанням цього ресурсу [22].

Особливість такого каналу витоку полягає в тому, що сам факт зберігання даних у спільному середовищі може виглядати як звичайна робоча операція. У багатьох інформаційних системах спільні ресурси використовуються для обміну документами, колективної роботи, передавання файлів між підрозділами або тимчасового зберігання інформації. Проте якщо правила доступу до таких ресурсів визначені недостатньо точно, персональні дані можуть стати доступними ширшому колу осіб, ніж це передбачено політикою безпеки. Ризик

підвищується тоді, коли внутрішній користувач має законний доступ до інформації та може самостійно розміщувати її у місцях, доступних іншим користувачам або зовнішнім сторонам. У цьому випадку традиційні засоби контролю доступу до початкового джерела даних уже не гарантують захисту, оскільки після копіювання інформація існує в іншому середовищі з власними правилами доступу.

Спільні ресурси та сховища також створюють проблему контролю подальшого руху даних. Якщо персональні дані переміщені з початкового захищеного місця до менш контрольованого ресурсу, організація може втратити можливість точно визначити, хто отримував до них доступ, коли це відбулося і з якою метою. Тому для запобігання такому типу витоку важливим є не лише обмеження доступу до самих персональних даних, а й контроль місць, у яких вони можуть зберігатися, копіюватися або бути доступними для інших суб’єктів. Спільний ресурс стає небезпечним тоді, коли він поєднує можливість запису з боку внутрішнього користувача та можливість читання з боку неавторизованого отримувача.

Рис. 2.3 Загальна схема витоку персональних даних через спільний ресурс

Саме така комбінація перетворює звичайне сховище на канал витоку, через який персональні дані можуть залишити межі контрольованої інформаційної системи без явного прямого передавання [23].

Канали витоку через робочі пристрої користувачів пов’язані з тим, що персональні дані після надання доступу можуть оброблятися безпосередньо на комп’ютерах, ноутбуках, мобільних пристроях або інших кінцевих засобах роботи з інформацією. На цьому рівні ризик виникає не лише під час передавання даних мережею, а й у процесі їх перегляду, копіювання, редагування, друку або тимчасового збереження. Робочий пристрій є місцем, де захищена інформація часто переходить із зашифрованого або контрольованого стану у форму, придатну для використання користувачем. Тут виникає можливість несанкціонованого копіювання або подальшого поширення даних, навіть якщо початковий доступ до них був наданий законно.

Таблиця 2.4

Канали витоку персональних даних через робочі пристрої користувачів

Канал витоку	**Умова виникнення ризику**	**Можливий наслідок**
Локальне копіювання файлів	Користувач зберігає копію персональних даних на робочому пристрої	Дані виходять за межі початкового контрольованого середовища
Зовнішній носій	Дані копіюються на підключений пристрій зберігання	Персональні дані можуть бути винесені за межі організації
Буфер обміну	Фрагменти інформації копіюються з одного документа до іншого	Частина персональних даних може потрапити до неконтрольованого файла або повідомлення
Знімок екрана	Користувач фіксує вміст екрана із відкритими даними	Інформація зберігається у вигляді зображення, яке складніше контролювати
Друкувальний пристрій	Документ із персональними даними виводиться на друк	Дані переходять у паперову форму та можуть бути отримані іншою особою

Фотографування екрана або документа	Використовується пристрій, який не контролюється інформаційною системою	Витік може відбутися поза межами технічного моніторингу

Наявність шифрування, пароля або розмежування прав доступу не усуває такого ризику повністю, оскільки після успішної автентифікації користувач отримує можливість працювати з інформацією у відкритому вигляді. Якщо додаткові механізми контролю відсутні, персональні дані можуть бути перенесені до іншого файла, скопійовані на зовнішній носій, вставлені в повідомлення, збережені локально або передані через підключений пристрій. Особливо небезпечними є ситуації, коли користувач має легітимні повноваження на перегляд даних, але використовує ці повноваження не для виконання службового завдання, а для створення неконтрольованої копії інформації [24]. До таких дій належать копіювання фрагментів документа через буфер обміну, збереження файлів на переносні носії, створення знімків екрана, виведення документа на друк або фотографування інформації з екрана чи паперового носія. Друкувальні пристрої також можуть формувати окремий канал витоку, оскільки надрукований документ виходить за межі цифрового контролю і може бути отриманий іншою особою, якщо доступ до принтера або роздрукованих матеріалів не обмежений. Подібна проблема виникає і з мобільними телефонами чи іншими пристроями, які не завжди перебувають під повним адміністративним контролем організації. Вони можуть використовуватися для фіксації зображення, перенесення файлів або непрямого копіювання вмісту. Отже, робочі пристрої користувачів є критичною точкою виникнення витоку, оскільки саме на них персональні дані стають доступними для практичного використання. Захист на цьому рівні має враховувати не тільки право доступу до інформації, а й можливість її подальшого копіювання, виведення, збереження або фізичного відтворення користувачем, який уже отримав доступ до даних.

Рис. 2.4 Узагальнена схема витоку персональних даних через робочий пристрій користувача

Приховані та нестандартні канали витоку персональних даних становлять окрему категорію загроз, оскільки вони не пов’язані з прямим і очевидним передаванням інформації через звичайні засоби обміну. Їхня сутність полягає у використанні таких каналів, механізмів або властивостей системи, які первинно не призначені для передавання персональних даних, але можуть бути пристосовані для прихованого виведення інформації за межі контрольованого середовища. На відміну від звичайного надсилання файлів або повідомлень, прихований канал маскує сам факт комунікації або робить передавання інформації менш помітним для засобів контролю. Це ускладнює виявлення витоку, оскільки зовнішньо активність може виглядати як штатна робота системи, звичайний обмін службовими повідомленнями або нормальне використання ресурсів.

Таблиця 2.5

Характеристика прихованих та нестандартних каналів витоку персональних даних

Вид прихованого каналу	**Сутність використання**	**Особливість ризику**
Приховане збереження у службових полях	Дані розміщуються в атрибутах, метаданих або службових параметрах файла	Основний вміст файла може не містити очевидних ознак персональних даних
Приховування у зображеннях або документах	Інформація вбудовується всередину іншого файла	Передавання може виглядати як звичайне надсилання нешкідливого документа
Передавання через часові затримки	Значення передається через інтервали між повідомленнями або порядок дій	Окремі повідомлення можуть не містити даних, але їхня послідовність має прихований зміст
Використання службових полів мережевих повідомлень	Дані приховуються у технічних параметрах пакетів	Канал може маскуватися під звичайний мережевий обмін
Використання системних ресурсів	Інформація передається через зміну стану або особливості роботи ресурсу	Витік може проявлятися не у вмісті, а в поведінці системи

Одним із видів таких каналів є приховане збереження інформації у службових полях файлів, атрибутах, метаданих або інших елементах, які зазвичай не сприймаються як основний вміст документа. У такому випадку персональні дані можуть бути вбудовані не в сам текст або видиму частину файла, а в додаткові параметри, що супроводжують файл. Подібний підхід небезпечний тим, що зовні документ може залишатися звичайним і не містити очевидних ознак чутливої інформації, хоча фактично використовуватиметься як носій прихованих даних. Близьким за змістом є приховування інформації у зображеннях, документах або інших файлах, коли персональні дані розміщуються всередині іншої інформації таким чином, щоб не привертати увагу під час поверхневого перегляду [25].

Іншим типом є передавання через часові характеристики. У цьому випадку значення має не лише сам зміст повідомлення, а й час його надсилання, затримки між окремими повідомленнями, послідовність дій або повторюваність певних операцій. Інформація може кодуватися через інтервали між передаваннями, кількість повідомлень за певний проміжок часу або визначений порядок

мережевої активності. Такі канали складні для виявлення, оскільки окремі повідомлення можуть не містити персональних даних у відкритому вигляді, але їхня послідовність або часовий шаблон може передавати приховане значення.

Нестандартні канали також можуть виникати через використання особливостей системних ресурсів. Тобто ситуації, коли інформація передається через зміну стану спільного ресурсу, особливості роботи пристроїв, параметри мережевих повідомлень або інші технічні характеристики, які не розглядаються як звичайний канал передавання даних. У таких умовах основна загроза полягає не лише у факті витоку, а й у складності його виявлення, оскільки персональні дані можуть бути розподілені, закодовані або приховані в непрямих ознаках роботи системи.

Рис. 2.5 Узагальнена схема прихованого каналу витоку персональних даних

Людський фактор є одним із ключових джерел витоку персональних даних, оскільки саме користувачі, які мають доступ до інформаційної системи, безпосередньо працюють із даними, приймають рішення щодо їх використання та можуть ініціювати їх передавання іншим особам або ресурсам. До таких суб'єктів належать працівники організації, адміністратори, підрядники, тимчасові користувачі та інші особи, яким надано певний рівень доступу до інформації. Особливість цієї загрози полягає в тому, що витік може здійснюватися не через зовнішнє порушення захисту, а через дії особи, яка формально має законні повноваження на перегляд, обробку або передавання персональних даних. У такій ситуації традиційні засоби захисту, зокрема автентифікація, шифрування та розмежування прав доступу, не усувають ризик повністю, оскільки після отримання дозволеного доступу користувач може працювати з інформацією у відкритому вигляді.

Витік, спричинений людським фактором, може мати випадковий або навмисний характер.

Таблиця 2.6

Характеристика витоку персональних даних, спричиненого людським фактором

Тип витоку	**Сутність дії користувача**	**Потенційний наслідок**
Випадковий витік	Користувач помилково надсилає файл, обирає неправильного отримувача або розміщує дані у неналежному ресурсі	Персональні дані стають доступними особам, які не повинні їх отримувати
Навмисний витік	Користувач свідомо передає, копіює або розміщує дані для доступу сторонньої особи	Дані виводяться за межі контрольованої системи з порушенням політики безпеки
Витік через авторизований доступ	Користувач законно отримує доступ до даних, але надалі використовує їх неналежним способом	Контроль доступу не запобігає порушенню після відкриття інформації
Витік через неконтрольовану копію	Користувач створює копію файла, фрагмента документа або вмісту екрана	Дані існують поза початковим захищеним середовищем

Випадковий витік виникає тоді, коли користувач помилково надсилає файл не тому отримувачу, прикріплює до повідомлення неправильний документ,

розміщує дані у неналежному сховищі або використовує канал передавання, який не відповідає рівню чутливості інформації. Такі дії можуть не мати зловмисної мети, однак їхній результат є однаково небезпечним, оскільки персональні дані стають доступними особам, які не повинні їх отримувати. Навмисний витік відрізняється тим, що користувач свідомо використовує свої повноваження для передавання даних сторонній особі, розміщення їх у доступному ресурсі або створення копії з метою подальшого виведення за межі контрольованого середовища [26].

Особливу складність становить загроза з боку внутрішнього користувача, який має легітимний доступ до персональних даних. Такий користувач може не порушувати правила на етапі входу до системи або отримання файлу, але порушення виникає на етапі подальшого використання інформації. Після відкриття документа або отримання даних із системи він може переслати їх іншому користувачу, скопіювати до нового файла, зберегти на носії, передати через мережевий сервіс або розмістити у спільному ресурсі. У цьому випадку джерелом ризику є не лише технічна вразливість, а й поведінка користувача, його наміри, уважність, рівень відповідальності та відповідність його дій політиці безпеки.

Рис. 2.6 Узагальнена схема витоку персональних даних через людський фактор

2.2 Оцінка вразливостей та загроз, що впливають на безпеку персональних даних

Оцінка вразливостей та загроз, що впливають на безпеку персональних даних, має зосереджуватися на визначенні слабких місць, через які порушується контроль над доступом, обробкою та передаванням інформації. Вразливість у цьому контексті є недоліком у технічному захисті, правилах доступу, політиці безпеки або організації роботи користувачів, який створює умови для несанкціонованого розкриття персональних даних. Загроза є потенційною дією або подією, що може використати таку вразливість і призвести до порушення конфіденційності. На відміну від аналізу каналів витоку, оцінка вразливостей спрямована не на опис шляхів передавання інформації, а на встановлення причин, через які ці шляхи можуть бути використані всупереч правилам безпеки.

Загроза з боку внутрішніх користувачів оцінюється як одна з найбільш складних для контролю, оскільки вона пов’язана не з подоланням зовнішнього периметра захисту, а з використанням уже наданих прав доступу. Основною вразливістю в цьому випадку є сама можливість роботи користувача з персональними даними у відкритому вигляді після проходження автентифікації та отримання дозволу на доступ. Працівник, адміністратор, підрядник або інший уповноважений користувач може мати законні підстави для перегляду чи обробки інформації, проте це не гарантує, що подальші дії з нею відповідатимуть політиці безпеки. Тому під час оцінки такої загрози важливо враховувати не лише факт наявності доступу, а й обсяг прав користувача, можливість копіювання, передавання, збереження або розміщення даних в інших середовищах.

Таблиця 2.7

Оцінка вразливостей і загроз, пов’язаних із внутрішніми користувачами

Вразливість	**Загроза**	**Можливий наслідок для персональних даних**
Надмірні права доступу користувача	Отримання доступу до більшого обсягу даних, ніж потрібно для виконання обов’язків	Зростання ймовірності неналежного використання або передавання персональних даних
Робота з даними у відкритому вигляді після автентифікації	Копіювання, пересилання або збереження інформації після її розшифрування	Втрата контролю над подальшим рухом даних
Відсутність контролю дій після відкриття інформації	Створення неконтрольованих копій або передавання даних іншій особі	Дані можуть залишити захищене середовище без порушення початкового доступу
Недостатній контроль дій адміністраторів або підрядників	Використання службових повноважень поза межами дозволених завдань	Розкриття даних через легітимний, але неправильно використаний доступ
Помилки користувача під час роботи з файлами	Випадкове надсилання, розміщення або прикріплення неправильного документа	Ненавмисне розкриття персональних даних неавторизованим особам

Ключовим слабким місцем є недостатнє розмежування прав доступу. Якщо користувач отримує ширший доступ, ніж необхідно для виконання його функцій, зростає ймовірність неналежного використання персональних даних. Іншою

вразливістю є відсутність контролю за діями після відкриття інформації. Шифрування та контроль доступу захищають дані на етапі зберігання або отримання, але не усувають ризик після того, як авторизований користувач розшифрував інформацію та почав із нею працювати. За відсутності додаткових обмежень така інформація може бути скопійована, переслана, перенесена до іншого файла або передана сторонній особі. Це свідчить про те, що вразливість полягає не лише в технічному доступі, а й у недостатньому контролі життєвого циклу даних після їх отримання [27].

Рівень загрози також залежить від характеру дій користувача. Випадкові дії, такі як помилкове надсилання документа або розміщення файла у неналежному ресурсі, створюють ризик ненавмисного витоку. Навмисні дії мають вищий рівень небезпеки, оскільки користувач свідомо використовує свої повноваження для виведення персональних даних за межі контрольованого середовища. Оцінюючи таку загрозу, необхідно враховувати наявність легітимного доступу, обсяг доступних даних, можливість їх копіювання, контроль дій користувача та здатність системи виявляти спроби несанкціонованого передавання.

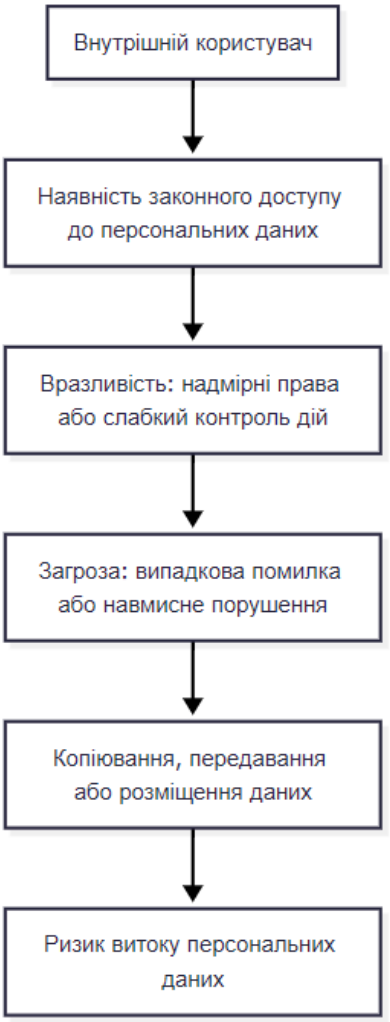

Рис. 2.7 Логіка оцінки загрози з боку внутрішнього користувача

Недоліки контролю доступу є однією з ключових вразливостей, що підвищують ризик витоку персональних даних, оскільки саме механізми доступу визначають, хто може переглядати, змінювати, копіювати або передавати інформацію [28]. Оцінка цієї вразливості має ґрунтуватися не лише на факті наявності системи автентифікації чи розмежування прав, а й на тому, наскільки точно права користувачів відповідають їхнім службовим функціям. Якщо користувач має ширший доступ, ніж необхідно для виконання конкретного завдання, рівень ризику зростає, оскільки збільшується обсяг персональних даних, які можуть бути неналежно використані, випадково розкриті або навмисно передані іншій особі. У такому випадку вразливість полягає не в повній відсутності контролю доступу, а в його недостатній точності та надмірності наданих повноважень.

Таблиця 2.8

Оцінка вразливостей контролю доступу, що впливають на безпеку персональних даних

Вразливість контролю доступу	**Прояв в інформаційній системі**	**Загроза**	**Оцінка ризику**
Надмірні права користувачів	Користувач має доступ до більшого обсягу персональних даних, ніж потрібно для виконання завдань	Випадкове або навмисне використання зайвих даних	Високий
Нечітке розмежування доступу	Різні категорії користувачів мають однакові або недостатньо відокремлені права	Перегляд, зміна або передавання даних без реальної службової потреби	Високий
Відсутність принципу необхідного мінімуму	Доступ надається за посадою, групою або підрозділом без точного обмеження	Розширення кола осіб, які можуть працювати з персональними даними	Середній або високий
Недостатній контроль подальших дій	Після відкриття даних не контролюється їх копіювання, передавання або збереження	Втрата контролю над рухом інформації після легітимного доступу	Високий
Слабкий контроль отримувачів даних	Система не перевіряє, кому саме передаються персональні дані	Передавання інформації неавторизованій особі або сторонньому ресурсу	Високий

Особливо небезпечним є неправильне розмежування доступу між різними категоріями користувачів. Працівники, адміністратори або інші уповноважені особи можуть мати доступ до інформації різного рівня чутливості, однак без чіткого поділу прав виникає можливість перегляду або передавання даних тим суб’єктам, які не мають обґрунтованої потреби в їх обробці [29]. З позиції оцінки загроз це створює умови для реалізації як випадкового, так і навмисного витоку. Випадковий ризик проявляється у тому, що користувач може помилково використати або передати дані, доступ до яких йому фактично не був потрібний.

Навмисний ризик є вищим, оскільки надмірні права дають змогу свідомо отримати, скопіювати або передати більший обсяг персональних даних без необхідності обходити технічні засоби захисту.

Відсутність принципу необхідного мінімуму також ускладнює контроль за рухом персональних даних усередині системи. Якщо доступ надається не за реальними потребами користувача, а за формальною належністю до підрозділу, ролі або групи, система втрачає здатність точно обмежувати обробку інформації. У такому випадку загроза посилюється тим, що користувач може діяти в межах формально дозволених прав, але результат його дій суперечитиме вимогам безпеки. Додатковою вразливістю є слабкий контроль за тим, хто саме передає дані, кому вони передаються і чи відповідає така дія встановленій політиці. Навіть за наявності шифрування або автентифікації захист послаблюється після того, як авторизований користувач отримав доступ до інформації у відкритому вигляді. Отже, недоліки контролю доступу оцінюються як суттєвий чинник ризику, оскільки вони збільшують кількість потенційних джерел витоку, розширюють обсяг доступних даних і знижують здатність системи запобігати неналежному використанню персональної інформації.

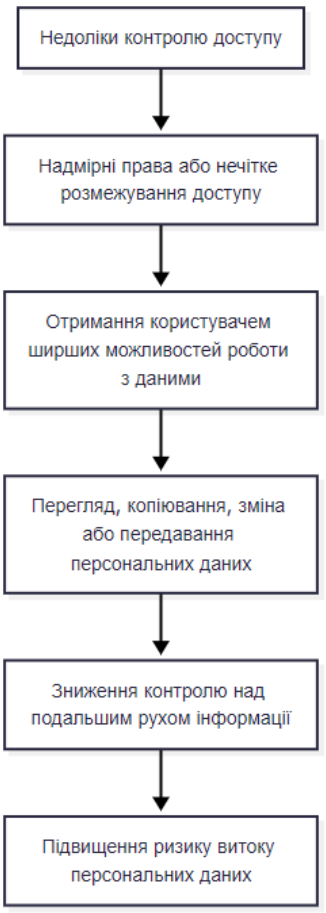

Рис. 2.8 Схема впливу недоліків контролю доступу на ризик витоку персональних даних

Обмеження шифрування як засобу захисту персональних даних полягає в тому, що воно ефективно знижує ризик несанкціонованого доступу лише на окремих етапах життєвого циклу інформації, насамперед під час її зберігання або передавання. У зашифрованому стані дані є менш придатними для використання сторонньою особою, оскільки для їх прочитання потрібні відповідні облікові дані, ключі або інші засоби розшифрування. З позиції оцінки вразливостей це означає, що шифрування зменшує ймовірність розкриття інформації у випадку перехоплення каналу зв’язку, втрати носія або доступу до сховища без належних повноважень [30].

Таблиця 2.9

Оцінка ефективності шифрування на різних етапах обробки персональних даних

Стан персональних даних	**Роль шифрування**	**Обмеження захисту**	**Оцінка ризику**
Дані під час зберігання	Захищає інформацію у сховищі від несанкціонованого прочитання	Не запобігає витоку після легітимного відкриття файла	Середній
Дані під час передавання	Знижує ризик перехоплення інформації у каналі зв'язку	Не контролює подальші дії отримувача після розшифрування	Середній
Дані під час використання	Дає змогу авторизованому користувачу працювати з інформацією	Після розшифрування дані можуть бути скопійовані, переслані або збережені в іншому середовищі	Високий
Дані після копіювання користувачем	Початкове шифрування вже не гарантує захист нової копії	Копія може існувати поза контрольованим середовищем	Високий
Дані після передавання іншій особі	Захист залежить від прав і дій отримувача	Неможливо гарантувати дотримання політики безпеки лише засобами шифрування	Високий

Проте ця захисна властивість не є абсолютною, оскільки персональні дані не можуть постійно залишатися у зашифрованому вигляді. Для виконання робочих операцій авторизований користувач повинен отримати можливість переглядати, обробляти, змінювати або передавати інформацію у формі, придатній для використання.

Основна вразливість виникає після того, як користувач пройшов автентифікацію, отримав доступ до даних і розшифрував їх для роботи. На цьому етапі шифрування вже не запобігає копіюванню, пересиланню, збереженню або розміщенню інформації в іншому середовищі. Отже, ризик витоку переноситься з технічного рівня захисту сховища або каналу передавання на рівень подальших

дій користувача. Якщо система не контролює, що саме відбувається з даними після їх відкриття, шифрування не може самостійно гарантувати збереження конфіденційності. Авторизований користувач може діяти в межах формально наданого доступу, але результат його дій може суперечити політиці безпеки, якщо інформація передається неавторизованому отримувачу або потрапляє до неконтрольованого ресурсу [31].

Оцінка цієї загрози має враховувати різницю між захистом даних у стані зберігання, передавання та використання. Для даних, що зберігаються або передаються, шифрування є важливим і доцільним механізмом зниження ризику. Для даних, що вже використовуються авторизованою особою, його ефективність обмежується, оскільки інформація фактично переходить у відкритий стан. Рівень ризику підвищується, якщо користувач має широкі права доступу, може самостійно створювати копії, переносити файли, надсилати документи або зберігати дані у сторонніх середовищах. Таким чином, шифрування оцінюється як необхідний, але недостатній засіб захисту персональних даних.

Рис. 2.9 Схема формування ризику після розшифрування персональних даних

Воно зменшує ризик несанкціонованого доступу до закритої інформації, але не усуває загрозу витоку після її розшифрування та використання легітимним користувачем

Помилки в політиці безпеки оцінюються як суттєва організаційно-технічна вразливість, оскільки саме політика визначає правила поводження з персональними даними, межі дозволеного доступу, умови передавання інформації та порядок реагування на інциденти. Якщо такі правила сформульовані нечітко або неповно, інформаційна система втрачає однозначну основу для контролю дій користувачів і технічних засобів захисту. Основна небезпека полягає в тому, що персональні дані можуть оброблятися або передаватися формально легітимним способом, але без достатнього

підтвердження того, що така дія відповідає рівню чутливості інформації, ролі користувача та допустимому напрямку передавання [32]. У такій ситуації вразливість виникає не через відсутність окремого захисного механізму, а через невизначеність правил, за якими цей механізм має працювати.

Таблиця 2.10

Оцінка вразливостей, пов’язаних із помилками в політиці безпеки

Помилка в політиці безпеки	**Прояв в інформаційній системі**	**Загроза для персональних даних**	**Оцінка ризику**
Нечітке визначення чутливих даних	Персональні дані не відокремлюються від звичайної інформації	Дані можуть оброблятися без належного рівня захисту	Високий
Відсутність правил щодо дозволених отримувачів	Система або користувач не має чітких обмежень, кому можна передавати дані	Передавання інформації неавторизованій особі	Високий
Невизначені дозволені канали передавання	Дані можуть передаватися будь-яким доступним способом	Неконтрольований рух персональних даних за межі системи	Високий
Неповні правила доступу до спільних ресурсів	Немає чіткої заборони або обмеження на розміщення даних у спільних сховищах	Дані можуть стати доступними ширшому колу осіб	Середній або високий
Нечіткий порядок реагування на інциденти	Не визначено, коли блокувати, фіксувати або повідомляти про порушення	Несвоєчасне виявлення або реагування на витік	Високий

Однією з ключових помилок є нечітке визначення того, які саме дані належать до чутливих і потребують посиленого захисту. Якщо персональні дані не мають належної класифікації, складно оцінити їхню критичність, допустимі способи зберігання, порядок передавання та необхідний рівень контролю. Це підвищує ризик того, що дані будуть оброблятися як звичайна інформація, хоча їх розкриття може спричинити шкоду для суб’єктів даних або організації. Рівень такої вразливості можна оцінити як високий, якщо відсутність класифікації

поєднується з широким доступом користувачів і активним обміном файлами між внутрішніми та зовнішніми сторонами.

Іншою критичною помилкою є відсутність чітких правил щодо того, хто має право передавати персональні дані, кому саме вони можуть бути передані та якими каналами це дозволено робити. Якщо політика не визначає дозволених отримувачів, умов автентифікації, рівня захищеності каналу та обмежень для спільних ресурсів, виникає ризик неконтрольованого руху інформації. У такому випадку користувач може діяти в межах власних технічних можливостей, але без достатньої перевірки допустимості самої операції. Загроза посилюється тоді, коли система не враховує контекст передавання, зокрема відправника, отримувача, час, спосіб передавання та характер інформації [33].

Недостатньо визначений порядок реагування на інциденти також знижує ефективність захисту. Якщо політика не встановлює, які події вважаються інцидентами, коли необхідно блокувати передавання, коли інформувати відповідальних осіб і як документувати порушення, система може несвоєчасно реагувати на витік або не реагувати взагалі.

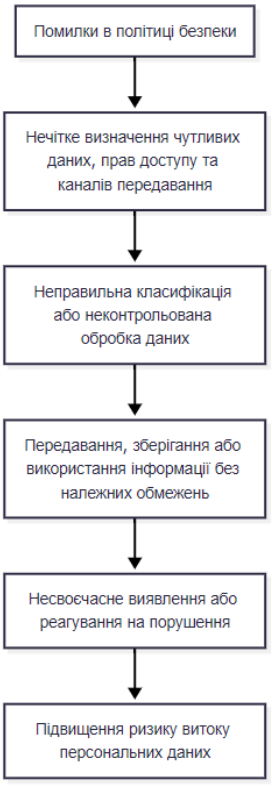

Рис. 2.10 Схема впливу помилок політики безпеки на ризик витоку персональних даних

Проблеми систем запобігання витоку даних оцінюються через їхню здатність не лише фіксувати факт передавання інформації, а й визначати, чи містить така передача персональні дані, чи відповідає вона політиці безпеки та чи не використовується для прихованого виведення інформації. Основним призначенням таких систем є виявлення, моніторинг і захист чутливої інформації від несанкціонованого використання або передавання. Проте їхня ефективність не є абсолютною, оскільки вона залежить від точності правил, якості класифікації даних, повноти налаштувань, доступності контекстної інформації та здатності системи аналізувати не тільки самі дані, а й умови їх передавання.

Таблиця 2.11

Оцінка проблем систем запобігання витоку даних

Проблема системи запобігання витоку	**Прояв в інформаційній системі**	**Загроза для персональних даних**	**Оцінка ризику**
Неповні правила виявлення	Система не має достатньо точних ознак для визначення чутливих даних	Передавання персональних даних може залишитися непоміченим	Високий
Недостатня класифікація даних	Не всі персональні дані правильно визначені як такі, що потребують захисту	Дані можуть оброблятися як звичайна інформація	Високий
Аналіз лише змісту без урахування контексту	Не враховується відправник, отримувач, час, спосіб передавання або роль користувача	Система може неправильно оцінити допустимість операції	Середній або високий
Неповне охоплення середовищ обробки	Контролюється лише мережевий рух або лише робочі пристрої	Частина дій із персональними даними залишається поза контролем	Високий
Складність виявлення прихованих каналів	Дані маскуються у параметрах каналу, службових ознаках або поведінці трафіку	Витік може не містити очевидних персональних даних у відкритому вигляді	Високий
Залежність від налаштувань	Неправильно задані правила блокування, сповіщення або реагування	Система може не заблокувати небезпечну передачу або створити надмірну кількість помилкових спрацювань	Середній

Окремою проблемою є контроль різних станів даних. Персональні дані можуть перебувати у стані зберігання, передавання або використання, і для кожного з цих станів потрібні різні механізми контролю. Мережева система може виявляти дані, що рухаються через корпоративну мережу, але не завжди контролює копіювання на локально підключені пристрої. Водночас засоби контролю на робочих пристроях можуть бути складними для повного впровадження на всіх вузлах системи. Тому ризик підвищується, якщо захист зосереджений лише на одному рівні, а інші точки обробки персональних даних залишаються недостатньо контрольованими [34].

Найвищий рівень складності пов’язаний із прихованими або нестандартними способами витоку. У таких випадках персональні дані можуть не передаватися у відкритому вигляді, а маскуватися в характеристиках каналу, службових параметрах, часових ознаках або поведінці трафіку. Для виявлення таких дій потрібен аналіз не тільки вмісту, а й самого каналу передавання.

Хибні спрацювання та пропущені інциденти є важливими показниками якості оцінки загроз, оскільки вони безпосередньо впливають на здатність системи своєчасно й правильно визначати ризик витоку персональних даних. Хибне спрацювання виникає тоді, коли безпечна або допустима дія користувача помилково класифікується як інцидент. У такому випадку система розпізнає звичайне передавання, зберігання або використання інформації як потенційне порушення, хоча реальної загрози витоку немає. Для організації це створює операційне навантаження, оскільки відповідальні особи змушені перевіряти події, які не становлять небезпеки. Якщо кількість таких спрацювань є значною, ефективність реагування знижується, а увага до реальних інцидентів може послаблюватися.

Пропущений інцидент має протилежний характер і оцінюється як більш небезпечна вразливість, оскільки реальний витік або спроба несанкціонованого передавання персональних даних не виявляється системою. Така ситуація може виникати тоді, коли правила виявлення є неповними, класифікація чутливої інформації недостатньо точною, а система не враховує контекст дії або

особливості каналу передавання. Особливо високий ризик виникає під час аналізу даних, що не мають очевидної структури або передаються не у відкритому вигляді. Якщо система орієнтується лише на відомі шаблони, точні збіги або окремі ознаки, вона може не розпізнати змінений фрагмент документа, приховане передавання або нестандартну поведінку трафіку.

Оцінка хибних спрацювань і пропущених інцидентів є особливо важливою для засобів, які аналізують зміст інформації та контекст її передавання. Аналіз змісту може виявляти персональні дані за відомими зразками або характерними ознаками, однак такі підходи мають обмеження: описані шаблони можуть збігатися з безпечною інформацією, що призводить до хибних спрацювань, або не охоплювати всі можливі форми чутливих даних, що створює ризик пропуску інциденту. Аналіз контексту також потребує точності, оскільки значення мають відправник, отримувач, роль користувача, час, спосіб передавання та інші умови операції. Одна й та сама дія може бути дозволеною в одному контексті та небезпечною в іншому [35].

Для систем, що оцінюють поведінку каналу передавання, проблема ускладнюється тим, що приховані або нестандартні способи витоку можуть імітувати звичайну активність. У такому випадку надто чутливі правила створюють багато помилкових сигналів, а надто слабкі правила підвищують імовірність пропущеного інциденту. Отже, хибні спрацювання оцінюються як чинник зниження ефективності реагування, а пропущені інциденти – як чинник прямого підвищення ризику витоку персональних даних. Оптимальна оцінка має враховувати баланс між точністю виявлення, повнотою правил, аналізом змісту, контексту та характеристик каналу передавання.

2.3 Моделювання та кількісна оцінка ризиків витоку інформації

Загальна логіка моделювання ризику витоку інформації полягає у формалізованому відображенні умов, за яких персональні дані можуть залишити межі контрольованої інформаційної системи. Таке моделювання має описувати

можливий факт витоку, встановлювати взаємозв’язок між джерелом даних, суб’єктом доступу, каналом передавання, отримувачем і засобами контролю, які повинні обмежувати або фіксувати небезпечні дії. Основою моделі є персональні дані як об’єкт захисту, користувач або системний компонент як суб’єкт дії, канал передавання як середовище руху інформації, отримувач як кінцева сторона доступу та система контролю як механізм перевірки допустимості операції. У межах такої моделі ризик виникає тоді, коли користувач має можливість отримати дані, передати їх іншій стороні або розмістити в ресурсі, доступному поза межами встановленої політики безпеки. Тому моделювання повинно враховувати не лише сам факт доступу до персональних даних, а й подальший напрям їх руху, дозволеність отримувача, захищеність каналу та наявність перевірки передавання. Для кількісної оцінки важливо, щоб кожен елемент моделі міг бути охарактеризований певним рівнем ризику. Наприклад, імовірність витоку може зростати за умов широких прав користувача, слабкого контролю каналу або можливості передавання інформації без додаткової перевірки [36]. Вплив інциденту залежить від чутливості персональних даних, обсягу інформації та наслідків її розкриття. Окремо має оцінюватися ефективність засобів контролю. У кількісному поданні така модель може використовувати бальну оцінку параметрів, де кожному чиннику надається умовне значення залежно від його небезпечності. Загальний рівень ризику тоді визначається через поєднання ймовірності реалізації сценарію, можливого впливу та здатності системи контролю запобігти або виявити порушення. Такий підхід дає змогу перейти від загального опису витоку до порівняння сценаріїв за рівнем небезпеки: передавання даних сторонньому отримувачу, доступ через спільний ресурс або використання каналу, який не контролюється достатньою мірою.

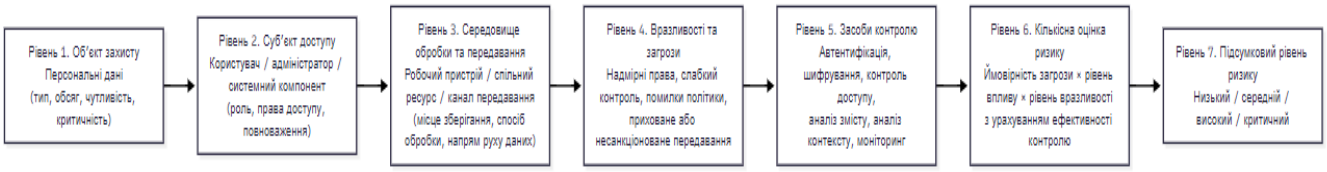

Рис. 2.12 Схема моделювання ризику витоку персональних даних

Основні елементи моделі витоку інформації формують структурну основу для визначення того, як саме персональні дані можуть вийти за межі контрольованої інформаційної системи та які умови підвищують або знижують рівень ризику. Центральним елементом моделі є персональні дані як об’єкт захисту, що має певну чутливість, цінність і можливі наслідки розкриття. Для кількісної оцінки цьому елементу може надаватися показник впливу, оскільки витік різних категорій даних має неоднакову небезпечність. Другим елементом є внутрішній користувач, тобто працівник, адміністратор або інший суб’єкт, який має доступ до інформації та може ініціювати її передавання, копіювання або розміщення в іншому середовищі. Його роль у моделі оцінюється через обсяг прав доступу, рівень повноважень і можливість працювати з даними у відкритому вигляді. Чим ширші права користувача та чим менше контролюється його подальша дія з інформацією, тим вищим є показник імовірності витоку. Зовнішній отримувач у моделі відображає сторону, яка може отримати персональні дані без належного права на доступ. Ризик підвищується, якщо отримувач не проходить належної автентифікації, не має підтвердженого дозволу або перебуває поза контрольованим середовищем організації. Спільний ресурс є проміжним елементом моделі, через який інформація може бути розміщена внутрішнім користувачем і згодом отримана іншою особою. Його небезпечність оцінюється за рівнем обмеження доступу, наявністю контролю читання і запису, а також можливістю визначити, хто саме звертався до даних. Канал передавання показує шлях руху інформації між суб’єктами або ресурсами, а його ризик залежить від захищеності, контрольованості та можливості прихованого використання. Політика безпеки виконує нормативну функцію в

моделі, оскільки визначає, які дані є чутливими, хто має право їх передавати, кому і за яких умов. Система контролю є механізмом перевірки відповідності дій цій політиці та може знижувати підсумковий ризик через автентифікацію, шифрування, аналіз змісту, аналіз каналу й фіксацію подій [37].

Кількісна оцінка ризику витоку інформації є необхідним етапом моделювання, оскільки вона дає змогу перейти від опису можливих сценаріїв до їх порівняння за рівнем небезпечності. Для такої оцінки доцільно використовувати просту бальну шкалу від 1 до 5, де 1 означає мінімальний рівень прояву показника, а 5 – максимальний. Чим чутливішою є інформація, чим більший її обсяг і чим серйознішими можуть бути наслідки її несанкціонованого розкриття, тим вищою має бути оцінка впливу. –

Показник вразливості характеризує слабкість умов, у яких відбувається обробка або передавання даних. Якщо контроль є повним і коректно налаштованим, залишковий ризик знижується. Якщо контроль охоплює лише окремі етапи роботи з даними або не враховує приховані способи передавання, його знижувальний вплив є обмеженим.

У спрощеній моделі загальний ризик можна визначати як поєднання ймовірності та впливу, наприклад за формулою: ризик = ймовірність × вплив. Для точнішої оцінки до цієї логіки можна додати показник вразливості та ефективність контролю, тобто розглядати ризик як результат взаємодії небезпечного сценарію, слабкого місця системи та здатності захисту запобігти інциденту. Наприклад, якщо ймовірність витоку оцінюється у 4 бали, а вплив у 5 балів, базовий ризик становить 20 балів і має розглядатися як високий.

Таблиця 2.12

Інтерпретація підсумкового рівня ризику

Значення ризику	**Рівень ризику**	**Загальна характеристика**
1–5	Низький	Сценарій має обмежену ймовірність або незначний вплив
6–10	Середній	Ризик потребує контролю, але не є критичним
11–15	Високий	Сценарій може призвести до суттєвого витоку персональних даних
16–25	Критичний	Сценарій потребує першочергового реагування та посилення контролю

Якщо при цьому засоби контролю ефективні, підсумковий або залишковий ризик може бути знижений.

Висновки до розділу 2

Проведений аналіз засвідчує, що сучасні інформаційні системи формують розгалужену та багаторівневу структуру потенційних каналів витоку персональних даних. Жоден із компонентів системи – від робочих пристроїв користувачів до мережевих служб і спільних сховищ – не може апріорі вважатися безпечним без відповідного контролю.

Встановлено, що канали витоку поділяються на відкриті (дозволені канали передавання, спільні ресурси, робочі пристрої) та приховані, які маскують сам факт виведення інформації і є найбільш складними для виявлення. Окремо визначено роль людського фактора, що охоплює як навмисні, так і випадкові дії авторизованих користувачів.

Оцінка вразливостей показала, що традиційні засоби захисту – автентифікація та шифрування – є необхідними, але недостатніми. Їхня ефективність принципово обмежується після того, як авторизований користувач отримав доступ до даних у відкритому вигляді. Ризик переноситься з рівня технічного захисту сховища на рівень подальших дій суб'єкта доступу.

Критичними вразливостями визнані надмірні права користувачів, нечітке розмежування доступу, помилки в політиці безпеки та неповне охоплення систем запобігання витоку.

Розглянута кількісна модель ризику, що базується на бальній оцінці показників імовірності та впливу, дозволяє формалізовано порівнювати сценарії витоку за рівнем небезпечності – від низького до критичного. Модель враховує взаємодію між суб'єктом доступу, каналом передавання, отримувачем, спільним ресурсом і системою контролю, що забезпечує системний підхід до аналізу загроз.

Отже, ефективний захист персональних даних потребує комплексного підходу, що поєднує точне розмежування прав доступу, контроль дій користувача після отримання інформації, аналіз каналів передавання та безперервний моніторинг відповідності дій встановленій політиці безпеки.

Розділ 3 РОЗРОБКА МЕТОДІВ ТА ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ ЩОДО ЗНИЖЕННЯ РИЗИКІВ ВИТОКУ ДАНИХ

3.1 Розробка комплексної системи управління ризиками витоку персональних даних

Подальший аналіз виконуватиметься на основі умовної компанії, створеної для моделювання практичної ситуації.

Інвентаризація персональних даних у межах комплексної системи управління ризиками витоку має виконуватися як практичне обстеження всіх інформаційних середовищ організації, у яких персональні дані можуть зберігатися, оброблятися, передаватися або резервуватися. На цьому етапі необхідно встановити фактичне розміщення даних у базах даних, файлових сховищах, електронній пошті, робочих станціях, серверах, хмарних сервісах, резервних копіях, журналах подій та прикладних системах. Особлива увага приділяється не лише основним інформаційним системам, а й допоміжним середовищам, де можуть залишатися копії даних: експортовані таблиці, вкладення в електронних листах, архіви, тимчасові файли, копії звітів, резервні образи систем і службові журнали. Практична мета такого обстеження полягає в тому, щоб організація отримала повну картину того, де саме розміщені персональні дані та хто фактично має до них доступ.

Для проведення інвентаризації доцільно застосовувати перевірку сховищ, баз даних, кінцевих пристроїв і корпоративних сервісів із фіксацією виявлених наборів даних. У процесі обстеження потрібно визначити тип персональних даних, їхній обсяг, систему або сервіс, у якому вони обробляються, відповідального власника, категорії користувачів із доступом, спосіб передавання даних, наявність резервного копіювання та чинні засоби захисту. Такий підхід дозволяє відокремити звичайні контактні або ідентифікаційні дані від фінансових, поведінкових, облікових чи чутливих даних, для яких витік може мати значно вищі наслідки. Також потрібно встановити, чи можуть дані прямо

або опосередковано ідентифікувати особу, оскільки легкість ідентифікації впливає на подальшу оцінку ризику витоку [38].

Практичним результатом інвентаризації є реєстр персональних даних, який використовується як робочий інструмент управління ризиками. У такому реєстрі для кожного набору даних фіксуються назва інформаційної системи, місце зберігання, тип даних, відповідальний підрозділ або власник, користувачі з правами доступу, канали передавання, пов’язані резервні копії, журнали подій, наявні механізми автентифікації, авторизації, шифрування та журналювання. Реєстр також має показувати, які дані передаються зовнішнім підрядникам або обробляються у хмарних сервісах, оскільки такі точки створюють додаткові ризики неконтрольованого доступу. Під час інвентаризації важливо виявити надлишкові копії, застарілі записи, неконтрольовані вивантаження та сховища, які не охоплені політиками безпеки. Це дозволяє одразу визначити слабкі місця: відсутність контролю доступу, незашифровані канали, неповне журналювання, надмірні привілеї користувачів або відсутність резервного копіювання.

Таблиця 3.1

Реєстр інвентаризації персональних даних

Інформаційна система / ресурс	**Тип персональних даних**	**Місце зберігання**	**Відповідальний власник**	**Користувачі з доступом**	**Спосіб передачі**	**Наявні засоби захисту**	**Проблемні місця**
CRM-система	ПІБ, телефон, email, історія звернень	База даних CRM	Відділ продажів	Менеджери, адміністратор	Внутрішня мережа, електронна пошта	Авторизація, журналювання	Надмірний доступ користувачів
Бухгалтерська система	Фінансові дані, ідентифікаційні дані	Сервер БД	Бухгалтерія	Бухгалтери, адміністратор	Захищене з’єднання	Резервне копіювання, обмеження доступу	Потрібен перегляд прав
Електронна пошта	Контактні дані, вкладення з персональними даними	Поштовий сервер / хмара	IT-відділ	Усі працівники	Електронна пошта	Автентифікація, антивірус	Ризик пересилання файлів назовні

Файлове сховище	Копії документів, договори, заяви	Файловий сервер	Кадровий відділ	HR, керівники	Внутрішня мережа	Права доступу, резервні копії	Наявність застарілих копій
Журнали подій	Облікові записи, IP-адреси, дії користувачів	Сервер журналювання	IT-відділ	Адміністратори	Внутрішня мережа	Журналювання, контроль доступу	Потрібен строк зберігання

Таблиця систематизує результати інвентаризації персональних даних і дозволяє визначити, у яких системах зосереджені найбільш критичні набори даних, хто має до них доступ, які засоби захисту вже застосовуються та які слабкі місця потребують подальшого усунення.

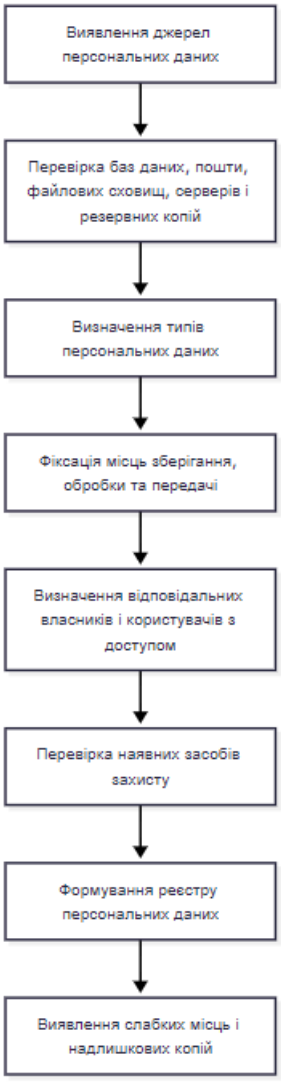

Рис. 3.1 Послідовність інвентаризації персональних даних

Отриманий реєстр повинен бути не разовим документом, а постійно оновлюваною основою для подальшого контролю персональних даних. Його потрібно переглядати після впровадження нових інформаційних систем, зміни прав доступу, підключення зовнішніх сервісів, перенесення даних у хмарне середовище, зміни процесів обробки або виявлення інциденту. Такий підхід забезпечує практичну керованість персональними даними, дозволяє швидко визначити потенційні джерела витоку та створює базу для подальшої оцінки ризиків у комплексній системі захисту [39].

Класифікація персональних даних за рівнем критичності виконується після їх виявлення та фіксації в реєстрі. Практично цей етап передбачає присвоєння кожному набору даних конкретного рівня захисту залежно від змісту, обсягу, можливості ідентифікації особи та потенційних наслідків несанкціонованого доступу. Для робочої моделі доцільно застосувати три рівні: низький, середній і високий або критичний. До низького рівня відносяться базові контактні та біографічні дані, які самі по собі не створюють значного впливу на особу. До середнього рівня належать поведінкові, фінансові та ідентифікаційні дані, особливо якщо вони дозволяють сформувати профіль користувача або зробити висновки про його фінансовий стан. До високого або критичного рівня відносяться чутливі дані, медична інформація, біометричні дані, облікові дані, а також набори, пов’язані з доступом до систем, де обробляються фінансові або чутливі відомості. Облікові дані не слід оцінювати ізольовано: їх критичність визначається тим, до якої системи вони надають доступ і які дані в ній обробляються.

Таблиця 3.2

Класифікація персональних даних за рівнем критичності

Рівень критичності	**Типи персональних даних**	**Практичне значення**	**Мінімальні засоби захисту**
Низький	Контактні дані, базові біографічні дані, службова інформація	Дані не створюють значного ризику самі по собі, але потребують контролю цілісності та доступу	Базове розмежування доступу, журналювання дій, контроль цілісності
Середній	Фінансові дані, поведінкові дані, ідентифікатори, історія дій користувача	Дані можуть дозволити ідентифікувати особу, сформувати профіль або зробити висновки про фінансовий чи поведінковий стан	Обмеження доступу, шифрування під час зберігання і передачі, регулярний перегляд прав, контроль вивантаження
Високий / критичний	Чутливі дані, медичні дані, біометричні дані, облікові дані, дані для доступу до критичних систем	Витік може спричинити значні наслідки для особи або надати доступ до систем з критичними даними	Багатофакторна автентифікація, принцип мінімальних привілеїв, посилене журналювання, маркування даних, постійний моніторинг

Практичним результатом класифікації є таблиця відповідності між типом персональних даних, рівнем критичності та мінімальними вимогами до захисту. Для низького рівня достатньо базового контролю доступу, журналювання та контролю цілісності. Для середнього рівня необхідні обмеження доступу, шифрування під час зберігання і передачі, регулярний перегляд прав користувачів та контроль вивантаження даних. Для критичного рівня застосовується доступ за принципом необхідності знання, багатофакторна автентифікація, посилене журналювання, маркування даних, контроль передавання та постійний моніторинг операцій [40].

Побудова карти потоків персональних даних виконується для фіксації фактичного руху даних між джерелами отримання, внутрішніми інформаційними системами, каналами передавання, місцями зберігання,

резервними копіями та зовнішніми отримувачами. Практично цей етап починається з визначення точки надходження даних: вебформа, електронна пошта, особистий кабінет, паперовий документ, імпорт із зовнішньої системи або ручне внесення працівником. Далі встановлюється, у якій системі дані первинно обробляються, де вони дублюються, хто має доступ до відповідного набору, через які канали вони передаються та чи потрапляють до резервних копій. Особливу увагу потрібно приділяти файловим сховищам, базам даних, електронній пошті, документам і кінцевим пристроям, оскільки саме в таких середовищах можуть зберігатися як структуровані, так і неструктуровані персональні дані. Перед класифікацією і захистом необхідно встановити, де чутливі дані фактично розміщені в системах, застосунках, базах даних і кінцевих пристроях, а також перевірити файлові сховища, репозиторії, електронні листи й документи.

Карта потоків даних має показувати не тільки основний маршрут обробки, а й допоміжні точки ризику: копії у вкладеннях електронної пошти, тимчасові експорти, архіви, резервні копії, доступ підрядників, передавання через зовнішні сервіси та збереження на робочих станціях. У процесі її побудови фіксуються незахищені канали передавання, надмірні права доступу, неконтрольоване вивантаження, відсутність журналювання, передавання даних відомим або невідомим отримувачам і можливість несанкціонованого доступу. Такі точки важливі, оскільки витік може бути пов’язаний із втратою конфіденційності, цілісності або доступності даних, а також із помилковим надсиланням персональних даних електронною поштою чи відкриттям доступу до чужих облікових записів

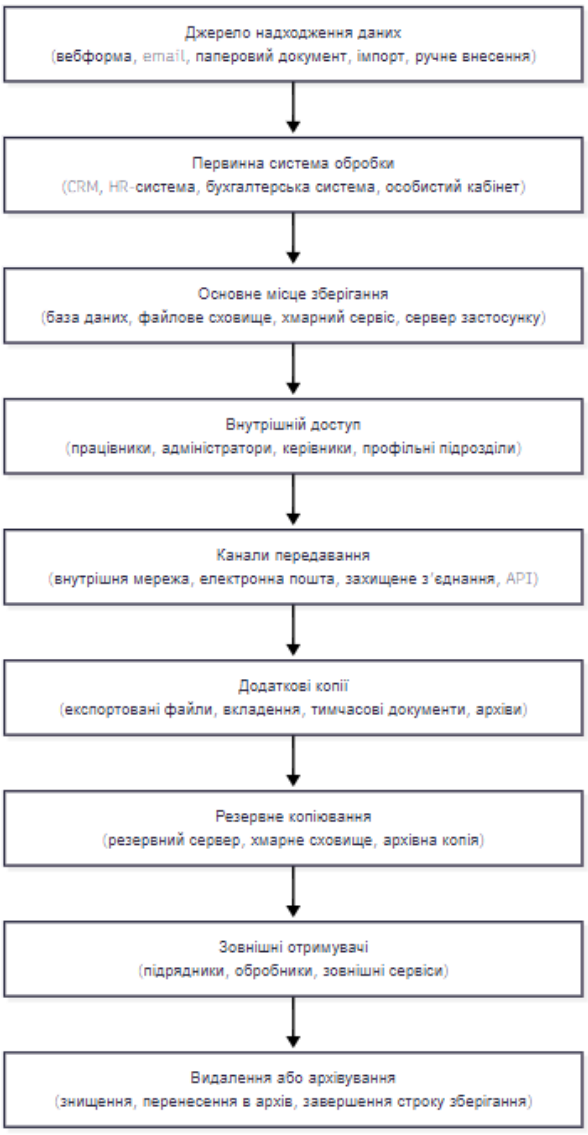

Рис. 3.2 Карта потоків персональних даних

Оцінка ризику витоку виконується окремо для кожного набору персональних даних, внесеного до реєстру. Практично для цього визначається тип даних, їхній обсяг, кількість осіб, яких вони стосуються, кількість користувачів із доступом, спосіб зберігання і передавання, а також наявність технічних засобів захисту. Базовим критерієм є контекст обробки даних, оскільки однакові за формою дані можуть мати різну критичність залежно від системи, у якій вони використовуються, обсягу записів, особливостей суб'єктів даних і можливості формування профілю особи. Для практичної оцінки доцільно враховувати категорію даних: прості, поведінкові, фінансові або чутливі.

Облікові дані оцінюються не окремо, а за критичністю тієї системи, до якої вони надають доступ [41].

Окремо оцінюється легкість ідентифікації особи за скомпрометованими даними. Вона може бути низькою, якщо дані не дозволяють прямо встановити особу, або високою, якщо набір містить ПІБ, адресу, дату народження, електронну пошту, номер документа чи інший ідентифікатор. Додатково враховуються обставини можливого витоку: порушення конфіденційності, зміна даних, втрата доступності або наявність умисних дій. Такі параметри дозволяють оцінити не лише ймовірність несанкціонованого доступу, а й реальний вплив інциденту на фізичних осіб.

Таблиця 3.3

Реєстр оцінки ризиків витоку персональних даних

Набір персональних даних	**Система / місце зберігання**	**Тип даних**	**Кількість осіб**	**Користувачі з доступом**	**Наявні засоби захисту**	**Оцінка ризику 1–5**	**Рівень ризику**	**Практичний висновок**
Контактні дані клієнтів	CRM-система	ПІБ, телефон, email	2 000	Менеджери, адміністратор	Авторизація, журналювання	3	Середній	Потрібен перегляд прав доступу та контроль експорту
Фінансові дані клієнтів	Бухгалтерська система	Рахунки, платежі, договори	850	Бухгалтерія, адміністратор	Обмеження доступу, резервне копіювання	4	Високий	Потрібне шифрування та посилене журналювання
Облікові дані користувачів	Система автентифікації	Логіни, паролі, ролі	120	IT-адміністратори	Політика паролів, обмеження доступу	5	Критичний	Потрібна багатофакторна автентифікація та контроль привілейованого доступу
Документи працівників	Файлове сховище	Копії документів, заяви,	300	HR, керівники	Права доступу, резервні копії	4	Високий	Потрібне маркування файлів і видалення

		договори						зайвих копій
Журнали подій	Сервер журналювання	IP-адреси, облікові записи, дії користувачів	120	IT-адміністратори	Журналювання, контроль доступу	3	Середній	Потрібно визначити строк зберігання та обмежити доступ

Таблиця є практичним результатом оцінки ризику витоку персональних даних. Вона дозволяє порівняти набори даних за рівнем критичності, кількістю осіб, доступом користувачів, наявними засобами захисту та підсумковою оцінкою ризику. За результатами такої оцінки визначаються найбільш проблемні ділянки: системи без шифрування, набори даних із надмірним доступом, облікові дані без багатофакторної автентифікації, файлові сховища із зайвими копіями та журнали подій із недостатнім контролем доступу.

Вибір технічних засобів захисту виконується шляхом прив’язування кожного встановленого ризику до конкретного контрольного заходу, який безпосередньо зменшує ймовірність витоку або його наслідки. Для ризику несанкціонованого доступу до персональних даних впроваджується багатофакторна автентифікація, рольове розмежування доступу, авторизація за службовими обов’язками та принцип мінімальних привілеїв. Доступ до чутливих даних має надаватися лише тим користувачам, яким він потрібний для виконання робочих функцій, із фіксацією дій у журналах подій. Для даних, що передаються або зберігаються, застосовується шифрування, оскільки воно зменшує можливість прочитання інформації у випадку несанкціонованого доступу або втрати носія. Чутливі дані потребують автентифікованого доступу, відповідних механізмів авторизації та регулярного аудиту безпеки.

Для ризику витоку через документи, файлові сховища або електронну пошту застосовується маркування даних, службові мітки у властивостях файлів, позначки в заголовках або колонтитулах документів і в темах електронних листів. Такі мітки дозволяють автоматично застосовувати правила контролю

доступу, запобігання витоку даних і моніторингу подій залежно від рівня чутливості інформації.

Для ризику масового копіювання, несанкціонованого доступу до чутливих даних, підозрілих електронних листів або незвичного мережевого трафіку налаштовуються моніторинг, сповіщення та правила виявлення аномальної активності. Для ризику втрати доступності впроваджується регулярне резервне копіювання, аварійне відновлення та політика безперервності роботи. Практичним результатом є таблиця відповідності, у якій для кожного ризику вказано конкретний технічний засіб, відповідальну систему, очікуваний ефект і статус впровадження

Моніторинг, реагування та перегляд ризиків реалізуються як постійний контроль подій, пов’язаних із доступом до персональних даних і змінами в середовищі їх обробки. У системах, де зберігаються або передаються персональні дані, необхідно фіксувати невдалі спроби входу, багаторазові звернення до файлів, масове копіювання, вивантаження записів, зміну прав доступу, доступ до чутливих таблиць, підозрілий мережевий трафік, підозрілі електронні листи та ознаки шифрування даних сторонніми процесами [42]. Для цього застосовуються журнали подій, засоби сповіщення, правила виявлення аномальної активності та контроль дій користувачів. Раннє виявлення таких подій зменшує вплив витоку, оскільки дозволяє швидко встановити джерело інциденту, задіяні облікові записи, обсяг порушених даних і системи, які потребують ізоляції.

Таблиця 3.5

Моніторинг подій, пов’язаних із ризиком витоку персональних даних

Подія для моніторингу	**Потенційний ризик**	**Джерело фіксації**	**Практична реакція**
Багаторазові невдалі входи	Підбір пароля або спроба несанкціонованого доступу	Журнали автентифікації	Блокування облікового запису, перевірка джерела входу
Масове копіювання файлів	Неконтрольоване вивантаження персональних даних	Файловий сервер, система журналювання	Обмеження доступу, перевірка дій користувача
Вивантаження великої кількості записів	Можливий витік із бази даних	Журнали бази даних	Тимчасове обмеження доступу, перевірка запиту
Зміна прав доступу	Надання зайвих привілеїв	Журнали адміністрування	Перевірка правомірності зміни, повернення попередніх прав
Доступ до чутливих таблиць у неробочий час	Підозріла активність користувача	Журнали бази даних	Перевірка облікового запису, сповіщення адміністратора
Підозрілий мережевий трафік	Передавання даних назовні	Мережеві журнали	Блокування IP-адреси або домену
Ознаки шифрування файлів стороннім процесом	Ризик втрати доступності через шкідливе ПЗ	Система захисту кінцевих пристроїв	Ізоляція пристрою, відновлення з резервної копії

У разі підтвердження інциденту першочергово виконується локалізація: уражений пристрій або програмне забезпечення відключається від мережі, скомпрометований обліковий запис блокується, шкідлива IP-адреса або домен додаються до блокування, паролі змінюються, а доступ до відповідних даних тимчасово обмежується. Якщо порушена доступність або цілісність даних, виконується відновлення з резервних копій. Усі дії фіксуються в журналі реагування із зазначенням часу, виконавця, причини дії та отриманого результату. Після локалізації оцінюється масштаб інциденту, тип порушених даних, кількість осіб, характер порушення конфіденційності, цілісності або доступності та рівень ризику для суб’єктів даних.

3.2 Практичні заходи та технічні засоби запобігання несанкціонованому доступу

Захист робочих станцій, серверів і мобільних пристроїв має виконуватися як практичне укріплення всіх кінцевих точок, через які користувачі або адміністратори отримують доступ до персональних даних. На робочих станціях необхідно обмежити локальні адміністративні права, дозволити встановлення лише перевіреного програмного забезпечення, регулярно оновлювати операційні системи та прикладні програми, а також контролювати підключення зовнішніх носіїв. Це зменшує ризик запуску заражених вкладень, скриптів, програм-стілерів, кейлогерів або шкідливих файлів, які можуть потрапити в систему через фішингові листи, зовнішні пристрої чи скомпрометовані бібліотеки. Шкідливе програмне забезпечення може використовуватися для отримання несанкціонованого доступу до сховищ даних або їх пошкодження, а після проникнення здатне маскувати свої дії під легітимну активність [43].

Для серверів потрібно впровадити контроль конфігурацій, своєчасне виправлення вразливостей, антивірусний захист, засоби виявлення та реагування на кінцевих точках, а також моніторинг підозрілих процесів і змін у системних файлах. Особливо важливо не створювати «сліпі зони» безпеки у сховищах даних, коли сервери не охоплені антивірусним скануванням або засобами виявлення через побоювання щодо продуктивності. У таких умовах шкідливі об’єкти можуть зберігатися у прихованих таблицях, функціях або службових об’єктах бази даних і залишатися непоміченими тривалий час.

Мобільні пристрої мають підключатися до корпоративних ресурсів лише за контрольованими правилами: із захистом пристрою, обмеженням доступу до службових даних, перевіркою оновлень і можливістю блокування доступу у разі втрати або компрометації.

Таблиця 3.6

Контроль захисту робочих станцій, серверів і мобільних пристроїв

Тип пристрою	**Основні ризики**	**Практичні засоби захисту**	**Результат контролю**
Робоча станція	Запуск шкідливих вкладень, використання зовнішніх носіїв, встановлення неперевірених програм	Обмеження локальних адміністративних прав, оновлення ОС, контроль встановлених програм, антивірусний захист, блокування несанкціонованих носіїв	Зменшення ризику зараження пристрою та отримання доступу до персональних даних
Сервер	Експлуатація вразливостей, приховане шкідливе ПЗ, зміна системних файлів, неконтрольований доступ до сховищ	Контроль конфігурацій, регулярне оновлення, засоби виявлення та реагування, антивірусне сканування, моніторинг системних подій	Виявлення підозрілої активності та запобігання прихованому доступу до сховищ даних
Мобільний пристрій	Втрата або крадіжка пристрою, доступ із неконтрольованого середовища, збереження службових даних	Блокування пристрою, перевірка оновлень, обмеження доступу до корпоративних ресурсів, можливість відкликання доступу	Недопущення доступу до персональних даних із втраченого або скомпрометованого пристрою
Зовнішній носій	Неконтрольоване копіювання або перенесення персональних даних	Заборона або обмеження підключення, журналювання операцій, дозвіл лише для перевірених носіїв	Зменшення ризику несанкціонованого винесення даних

Практичним результатом є перелік контрольованих пристроїв із визначеним статусом захисту, де фіксуються власник пристрою, рівень доступу, наявність оновлень, антивірусного захисту, обмеження локальних прав,

дозволені програми та дата останньої перевірки. Такий облік дозволяє своєчасно виявляти неконтрольовані або застарілі пристрої, через які може бути здійснений несанкціонований доступ до персональних даних

Шифрування даних під час зберігання та передавання має застосовуватися до всіх середовищ, де обробляються персональні дані: баз даних, файлових сховищ, хмарних сервісів, резервних копій, архівів і каналів обміну між клієнтом, сервером та внутрішніми вузлами інфраструктури. Для даних, що зберігаються у сховищах, доцільно використовувати симетричне шифрування AES-256, за якого відкриті дані перетворюються на зашифрований набір символів і можуть бути відновлені лише за наявності відповідного ключа. Такий підхід зменшує ризик прочитання інформації навіть у разі компрометації носія, бази даних або резервної копії. Для даних, що передаються мережею, потрібно застосовувати захищені канали зв’язку на основі TLS, оскільки це унеможливлює перехоплення або зміну інформації під час передавання між користувачем і сервером або між серверами [44].

Окремим практичним елементом є керування ключами шифрування. Ключі не повинні зберігатися разом із зашифрованими даними або в основній інфраструктурі сховища, оскільки в такому випадку компрометація системи може одночасно надати доступ і до даних, і до засобу їх розшифрування. Для цього застосовується система керування ключами, яка забезпечує створення, зберігання, ротацію, обмеження доступу та видалення ключів. Також необхідно перевіряти, щоб резервні копії, архіви та експортовані файли не зберігалися у відкритому вигляді. Практичним результатом є таблиця контролю шифрування, де для кожного середовища фіксується тип даних, спосіб шифрування, захист каналу передавання, місце зберігання ключів і відповідальний адміністратор.

Таблиця 3.7

Контроль шифрування персональних даних під час зберігання та передавання

Об'єкт захисту	**Дані, що захищаються**	**Практичний спосіб шифрування**	**Контроль ключів**	**Очікуваний результат**
База даних	Персональні, фінансові, чутливі записи	AES-256 для даних під час зберігання	Ключі зберігаються окремо в системі керування ключами	Дані не читаються у разі компрометації сховища
Файлове сховище	Документи, договори, копії заяв	Шифрування файлів або розділів сховища	Доступ до ключів лише для уповноважених адміністраторів	Обмеження доступу до змісту файлів
Резервні копії	Архіви баз даних і системні копії	Шифрування резервних копій перед збереженням	Окреме зберігання ключів від резервного сховища	Захист копій у разі втрати або викрадення
Канали передавання	Дані між клієнтом, сервером і сервісами	TLS для мережевого обміну	Контроль сертифікатів і строків їх дії	Захист від перехоплення та зміни даних
Експортовані файли	Вивантаження з баз даних, звіти	Шифрування файлів перед передаванням або архівацією	Тимчасові ключі або обмежений доступ	Зменшення ризику витоку під час обміну

Журналювання дій і моніторинг підозрілої активності впроваджуються для постійного технічного контролю доступу до персональних даних і своєчасного виявлення дій, що можуть свідчити про спробу несанкціонованого доступу. У журналах подій необхідно фіксувати автентифікацію користувачів, невдалі спроби входу, звернення до файлів і таблиць із чутливими даними, масове копіювання, вивантаження записів, зміну ролей і привілеїв, підключення з нетипових адрес, підозрілий мережевий трафік, відкриття підозрілих вкладень і ознаки шифрування файлів сторонніми процесами.

Моніторинг має бути налаштований так, щоб підозрілі події автоматично перетворювалися на сповіщення для відповідальних фахівців. До таких подій належать незвично часті звернення до файлів, масові переміщення даних,

несанкціоновані спроби підключення, доступ до чутливих даних, підозрілі електронні листи, незвичний мережевий трафік і запити, характерні для ransomware. Раннє виявлення таких ознак дозволяє швидше локалізувати інцидент і зменшити його вплив. Практичним результатом є матриця моніторингу, у якій для кожної контрольованої події визначаються джерело журналу, ознака ризику, умова спрацювання та первинна реакція.

Таблиця 3.8

Матриця журналювання та моніторингу підозрілої активності

Подія для контролю	**Джерело журналювання**	**Ознака ризику**	**Умова спрацювання**	**Первинна реакція**
Багаторазові невдалі входи	Журнал автентифікації	Підбір пароля або спроба входу сторонньої особи	Кілька помилкових входів за короткий час	Блокування облікового запису, перевірка IP-адреси
Масове копіювання файлів	Файловий сервер	Неконтрольоване винесення персональних даних	Різке збільшення кількості прочитаних або скопійованих файлів	Тимчасове обмеження доступу, перевірка дій користувача
Вивантаження великої кількості записів	Журнал бази даних	Можливий витік із таблиць сховища	Нетиповий експорт або великий запит до чутливої таблиці	Призупинення сесії, перевірка запиту
Зміна ролей або привілеїв	Журнал адміністрування	Несанкціоноване розширення доступу	Надання нових прав без погодження	Відкат змін, перевірка адміністратора
Доступ до чутливих даних у неробочий час	Журнал бази даних або застосунку	Компрометація облікового запису	Доступ поза типовим графіком користувача	Сповіщення відповідального, перевірка сесії
Підозрілий мережевий трафік	Мережеві журнали	Передавання даних назовні	З’єднання з нетиповим доменом або IP-адресою	Блокування адреси, аналіз трафіку
Ознаки ransomware	Журнали кінцевих пристроїв	Втрата доступності даних	Масове перейменування або шифрування файлів	Ізоляція пристрою, запуск процедури відновлення

Резервне копіювання та відновлення доступності даних застосовується для випадків, коли несанкціонований доступ призводить до видалення,

пошкодження, зміни або шифрування персональних даних. Практично резервні копії мають створюватися регулярно для баз даних, файлових сховищ, критичних серверів, журналів подій і конфігурацій систем. Копіювання не повинно охоплювати лише частину даних, оскільки неповна резервна копія не забезпечує повного відновлення після інциденту. Копії необхідно зберігати окремо від основного сховища, бажано в іншому фізичному місці або захищеному хмарному середовищі, щоб атака на основну інфраструктуру не призвела до одночасної втрати всіх резервних екземплярів. Також потрібно обмежити доступ до резервних сховищ, застосовувати шифрування копій і фіксувати всі операції створення, зміни, видалення та відновлення даних. У разі інциденту практичними діями є ізоляція ураженої системи, блокування скомпрометованих облікових записів, зміна паролів і відновлення даних із резервних копій [45].

Окремо необхідно перевіряти працездатність резервних копій через тестове відновлення. Під час перевірки встановлюється, чи можна відновити дані вчасно, повністю і без втрат. Відсутність тестування створює ризик, що резервна копія існує формально, але не може бути використана після реального інциденту. Практичним результатом є журнал резервного копіювання та відновлення, де фіксуються об’єкт копіювання, періодичність, місце зберігання, спосіб захисту, дата останнього тестового відновлення та відповідальна особа. Для зменшення ризику одночасної втрати копій доцільно застосовувати географічне рознесення резервних сховищ, контрольоване шифрування на всіх рівнях і автоматизовану перевірку коректності відновлення.

Таблиця 3.9

Практичний контроль резервного копіювання та відновлення доступності даних

Об’єкт копіювання	**Періодичність**	**Місце зберігання копії**	**Захист копії**	**Перевірка відновлення**	**Практичний результат**
База персональних даних	Щоденно	Окреме резервне сховище / хмара	Шифрування, обмеження доступу	Тестове відновлення раз на місяць	Можливість відновити записи після видалення або шифрування
Файлове сховище	Щоденно або щотижнево	Інше фізичне місце	Шифрування, журналювання доступу	Перевірка вибіркових файлів	Захист документів від втрати або пошкодження
Журнали подій	Щоденно	Захищений архів	Заборона зміни, контроль доступу	Перевірка цілісності архіву	Збереження доказів дій користувачів
Конфігурації серверів	Після кожної зміни	Резервний сервер	Обмеження адміністративного доступу	Тестове розгортання	Швидке відновлення роботи системи
Резервні копії критичних систем	За графіком	Географічно віддалене сховище	Шифрування, окреме зберігання ключів	Повне тестове відновлення	Зменшення ризику одночасної втрати основних і резервних даних

Реагування на спроби несанкціонованого доступу має виконуватися за заздалегідь визначеним порядком, щоб швидко локалізувати інцидент і не допустити подальшого поширення загрози. Після фіксації підозрілої активності першочергово перевіряються журнали автентифікації, мережеві події, дії користувача, звернення до чутливих таблиць або файлів, а також факт зміни прав доступу. Якщо ознаки несанкціонованого доступу підтверджуються, уражений пристрій або програмне забезпечення ізолюється від мережі, скомпрометований обліковий запис блокується, шкідлива IP-адреса або домен додаються до списку

блокування, а паролі відповідних користувачів змінюються [46]. Для локалізації інциденту можуть створюватися тимчасові технічні обмеження: заборона доступу до окремих систем, блокування експорту даних, відкликання активних сесій або тимчасове зниження привілеїв. Такі дії прямо спрямовані на стримування інциденту, ізоляцію джерела загрози та недопущення подальшої компрометації даних.

Після локалізації необхідно визначити, які персональні дані могли бути переглянуті, змінені, видалені або вивантажені, а також який обліковий запис, пристрій чи канал використовувався для доступу. Усі виконані дії фіксуються в журналі реагування із зазначенням часу, відповідального виконавця, ураженої системи, прийнятого рішення та результату. Документування має охоплювати факти інциденту, його наслідки та вжиті заходи усунення. Практичним результатом є журнал первинного реагування, який дозволяє відстежити послідовність дій і перевірити, чи була загроза повністю локалізована.

Таблиця 3.10

Журнал первинного реагування на спробу несанкціонованого доступу

Виявлена подія	**Уражений об'єкт**	**Першочергова дія**	**Додаткова перевірка**	**Практичний результат**
Багаторазові невдалі входи	Обліковий запис користувача	Тимчасове блокування облікового запису	Перевірка IP-адреси та часу входу	Зупинення спроби підбору пароля
Вхід із нетипової адреси	Обліковий запис або VPN-сесія	Відкликання активної сесії	Перевірка журналів автентифікації	Недопущення подальшого доступу
Масове вивантаження даних	База даних або файлове сховище	Блокування експорту та обмеження доступу	Аналіз запитів і обсягу даних	Зменшення ризику витоку
Підозрілий мережевий трафік	Робоча станція або сервер	Блокування IP-адреси чи домену	Аналіз мережевих журналів	Припинення передавання даних назовні
Ознаки шкідливого ПЗ	Пристрій або сервер	Ізоляція від мережі	Перевірка процесів і файлів	Локалізація зараження
Несанкціонована зміна прав	Система керування доступом	Відкат прав і блокування адміністративної дії	Аудит змін ролей і привілеїв	Відновлення коректного доступу

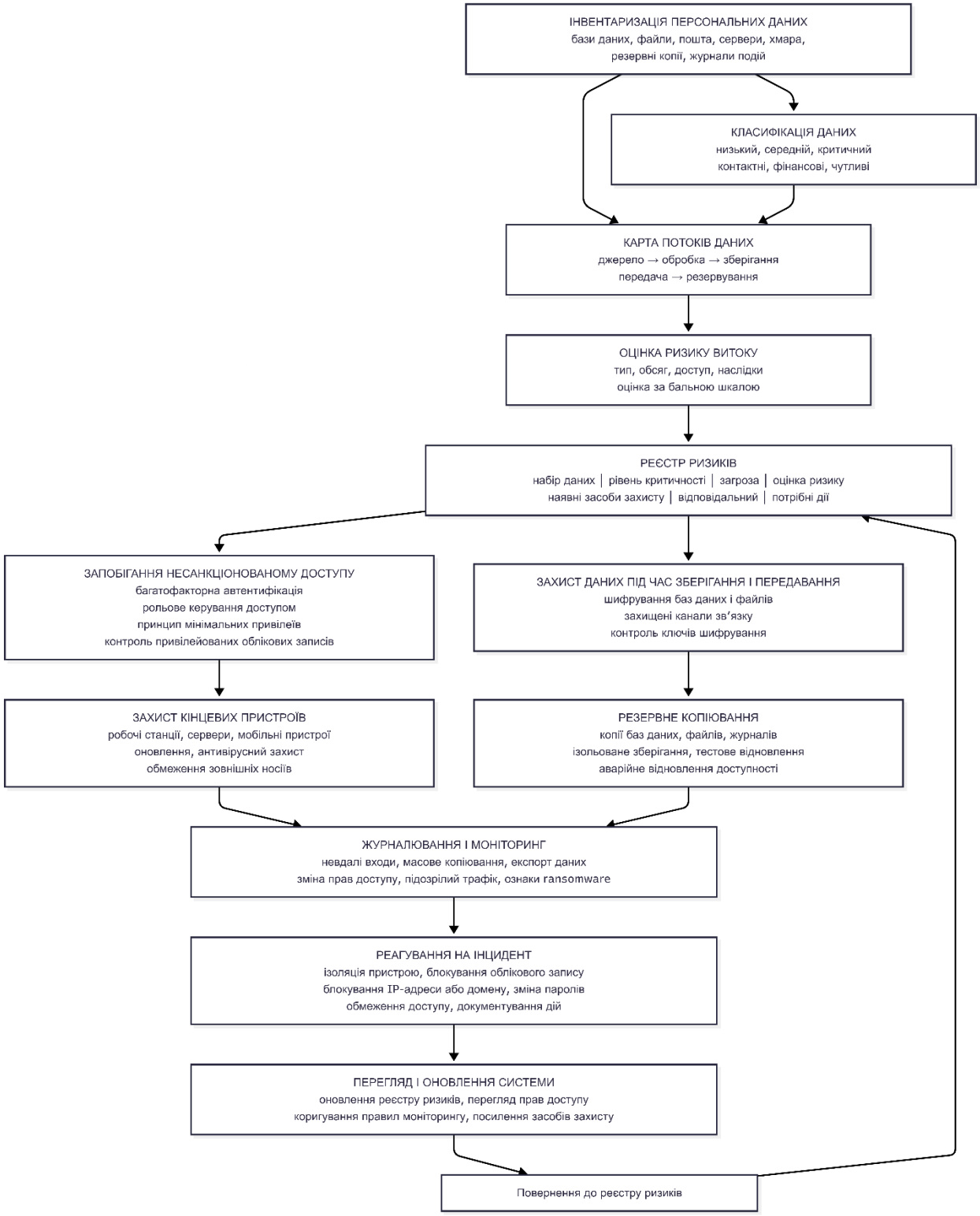

Рис. 3.3 Комплексна система управління ризиками витоку персональних даних

Рисунок відображає комплексну систему управління ризиками витоку персональних даних як замкнений практичний цикл. Центральним елементом системи є реєстр ризиків, який формується на основі інвентаризації, класифікації персональних даних, побудови карти потоків і бальної оцінки ризику. До

кожного ризику прив’язуються конкретні технічні засоби захисту: автентифікація, розмежування доступу, захист кінцевих пристроїв, шифрування, резервне копіювання, журналювання та моніторинг. У разі виявлення підозрілої активності система переходить до реагування на інцидент, після чого результати фіксуються, а реєстр ризиків і захисні заходи переглядаються. Така структура дозволяє не лише виявляти ризики витоку, а й підтримувати постійний контроль за персональними даними на всіх етапах їх обробки.

3.3 Оцінка ефективності запропонованих методів та рекомендації щодо їх впровадження

Визначення показників ефективності захисних заходів виконується для того, щоб оцінювання запропонованої системи ґрунтувалося на вимірюваних результатах, а не на формальному факті впровадження технічних засобів. Для цього доцільно зафіксувати початковий стан захисту персональних даних і встановити набір контрольних метрик, які надалі порівнюються після впровадження заходів. До таких показників належать кількість спроб несанкціонованого доступу, кількість заблокованих підозрілих входів, кількість інцидентів витоку, середній час виявлення підозрілої події, середній час реагування, кількість користувачів із надмірними правами доступу, частка систем із багатофакторною автентифікацією, частка зашифрованих сховищ, наявність актуальних резервних копій і результат тестового відновлення. Такий підхід відповідає практиці вимірювання поточного стану до впровадження змін і повторного оцінювання після їх реалізації, що дозволяє встановити фактичний рівень покращення.

Кожен показник повинен мати джерело отримання даних: журнали автентифікації, журнали баз даних, системи моніторингу, звіти про права доступу, результати перевірки шифрування, записи резервного копіювання та журнали реагування на інциденти. Для оцінки ефективності важливо не лише зібрати метрики, а й сформувати порівнювані значення, які можна

використовувати як базові орієнтири. Саме тому доцільно створити таблицю контрольних показників, у якій фіксуються назва метрики, початкове значення, цільове значення, фактичний результат після впровадження та відповідальний підрозділ. Такий формат дозволяє визначити, які заходи реально знизили ризик витоку, які залишилися недостатньо ефективними та які потребують додаткового коригування. Використання єдиних метрик і порівняльних орієнтирів також дає змогу виявляти прогалини у вимірюванні захисту даних і підтримувати регулярне оновлення показників ефективності

Оцінка стану захисту до та після впровадження заходів виконується як практичне порівняння фактичного рівня безпеки інформаційної системи на двох етапах: до реалізації запропонованих рішень і після їх впровадження. Спочатку фіксується початковий стан захисту персональних даних, зокрема наявність облікових записів без багатофакторної автентифікації, незашифрованих резервних копій, надмірних прав доступу, відсутності журналювання дій користувачів, неконтрольованого вивантаження даних, відкритих каналів передавання або відсутності перевірки відновлення з резервних копій. Таке вимірювання дозволяє встановити реальний розрив між поточним станом системи та необхідним рівнем захисту, а також визначити конкретні ділянки, де ризик несанкціонованого доступу або витоку залишається найвищим. Практика оцінювання змін передбачає вимірювання поточного стану до впровадження та повторне вимірювання після реалізації заходів, щоб підтвердити фактичне покращення.

Після впровадження технічних засобів проводиться повторна перевірка тих самих параметрів. Оцінюється, скільки облікових записів переведено на багатофакторну автентифікацію, які сховища і резервні копії зашифровано, чи зменшено кількість користувачів із надмірними привілеями, чи налаштовано журналювання, чи обмежено експорт даних, чи працюють сповіщення про підозрілу активність і чи підтверджено можливість відновлення даних. Практичним результатом є порівняльна таблиця “до / після”, у якій для кожного

заходу фіксується початковий недолік, виконана дія, фактичний стан після впровадження та залишковий ризик.

Таблиця 3.11

Порівняння стану захисту персональних даних до та після впровадження заходів

Контрольний параметр	**Стан до впровадження**	**Впроваджений захід**	**Стан після впровадження**	**Залишковий ризик**
Облікові записи користувачів	Частина користувачів працює лише з паролем	Увімкнено багатофакторну автентифікацію	Доступ до критичних систем потребує додаткового підтвердження	Низький
Права доступу	Є користувачі з надмірними привілеями	Проведено перегляд ролей і прав доступу	Доступ надається відповідно до службових обов'язків	Середній
Адміністративні облікові записи	Привілейований доступ контролюється недостатньо	Обмежено адміністративні права та посилено контроль дій	Критичні дії адміністраторів фіксуються в журналах	Середній
Резервні копії	Частина копій зберігається без шифрування або без перевірки відновлення	Запроваджено шифрування та тестове відновлення	Резервні копії захищені, придатність до відновлення перевірена	Низький
Журналювання дій	Не всі дії користувачів і адміністраторів фіксуються	Налаштовано журнали автентифікації, доступу та змін прав	Події доступу, експорту і зміни привілеїв фіксуються	Середній
Експорт даних	Можливе неконтрольоване вивантаження файлів або записів	Обмежено експорт і налаштовано сповіщення	Масове вивантаження контролюється та перевіряється	Середній
Шифрування сховищ	Частина баз даних, файлів або архівів зберігається у відкритому вигляді	Застосовано шифрування для сховищ і архівів	Дані не читаються без ключа шифрування	Низький
Канали передавання	Частина обміну може виконуватися без належного захисту	Використано захищені канали передавання	Передавання даних захищене від перехоплення та зміни	Низький

Кінцеві пристрої	Є ризик доступу з неконтрольованих або застарілих пристроїв	Обмежено локальні права, оновлено ПЗ, увімкнено захист пристроїв	До систем допускаються лише контрольовані пристрої	Середній
Моніторинг підозрілої активності	Підозрілі події можуть виявлятися із затримкою	Налаштовано правила сповіщення про аномальні дії	Невдалі входи, масове копіювання та підозрілий трафік контролюються	Середній

Такий формат дозволяє не лише підтвердити виконання рекомендацій, а й визначити, які заходи дали вимірюваний результат, а які потребують додаткового коригування. Для обґрунтованої оцінки ефективності також доцільно враховувати попереджені збитки та зміну показників ризику після застосування засобів захисту

Розрахунок зниження ризику та залишкового ризику виконується шляхом порівняння початкової оцінки загрози з оцінкою після впровадження захисних заходів. Початкова оцінка фіксує стан до впровадження заходів, а залишкова оцінка показує рівень ризику після застосування багатофакторної автентифікації, перегляду прав доступу, шифрування, журналювання, моніторингу або резервного копіювання. Такий підхід дозволяє оцінити не лише факт виконання рекомендацій, а й реальний практичний ефект у вигляді зменшення ймовірності інциденту або його наслідків. Для обґрунтованої оцінки ефективності доцільно використовувати показник попереджених збитків і порівнювати стан до та після впровадження засобів захисту, оскільки саме зменшення можливих втрат є практичним результатом підвищення рівня інформаційної безпеки.

Розрахунок можна виконати за формулою: Зниження ризику = ((початковий ризик − залишковий ризик) / початковий ризик) × 100 %. Наприклад, якщо ризик компрометації облікового запису до впровадження заходів мав оцінку 5, а після впровадження багатофакторної автентифікації, обмеження привілеїв і журналювання знизився до 2, то зниження ризику становить ((5 − 2) / 5) × 100 % = 60 %. Це означає, що після впровадження заходів

ризик не усунуто повністю, але його рівень зменшено з критичного до низького або помірного. Залишковий ризик обов’язково фіксується в реєстрі ризиків, оскільки навіть після застосування технічних засобів можуть зберігатися окремі загрози, пов’язані з людським фактором, помилками конфігурації або новими сценаріями атак. Для подальшого контролю важливо повторно вимірювати показники після впровадження змін і порівнювати їх із початковим станом.

Таблиця 3.12

Розрахунок зниження ризику та залишкового ризику

Ризик	**Початковий ризик**	**Впроваджений захід**	**Залишковий ризик**	**Розрахунок**	**Зниження ризику**
Компрометація облікового запису	5	Багатофакторна автентифікація, перегляд прав, журналювання	2	((5−2)/5)×100	60 %
Несанкціонований доступ до файлового сховища	4	Рольове керування доступом, принцип мінімальних привілеїв	2	((4−2)/4)×100	50 %
Витік через незашифровані резервні копії	4	Шифрування копій, обмеження доступу, тестове відновлення	1	((4−1)/4)×100	75 %
Масове вивантаження персональних даних	5	Журналювання, сповіщення, обмеження експорту	3	((5−3)/5)×100	40 %
Доступ із неконтрольованого пристрою	4	Оновлення, антивірусний захист, обмеження локальних прав	2	((4−2)/4)×100	50 %

Таблиця показує, які ризики знижено найбільше, які залишаються помірними та які потребують подальшого контролю. Найкращий результат отримано для резервних копій, оскільки шифрування й обмеження доступу суттєво зменшують можливість використання даних після компрометації сховища.

Оцінка економічної доцільності впровадження заходів виконується через зіставлення витрат на захист із можливими втратами, яких організація уникає після впровадження цих заходів. Практично для кожного технічного рішення

визначається вартість реалізації, очікуваний ефект і тип збитків, які воно дозволяє зменшити або попередити. До таких збитків належать втрата або пошкодження персональних даних, простої інформаційних систем, витрати на відновлення, реагування на інцидент, юридичні наслідки та репутаційні втрати. Базовим показником доцільності є попереджені збитки від кібератаки, тобто різниця між можливими втратами до впровадження захисного заходу та очікуваними втратами після його впровадження. Такий підхід дозволяє оцінювати захисні заходи не лише як витрати, а як інструмент зменшення потенційної шкоди від інциденту.

Для практичної оцінки можна застосувати спрощену формулу: економічний ефект = очікувані попереджені збитки − витрати на впровадження заходу. Якщо витрати на впровадження багатофакторної автентифікації становлять 40 тис. грн, а очікуване зменшення збитків від компрометації облікових записів оцінюється у 120 тис. грн, економічний ефект становить 120 − 40 = 80 тис. грн. Якщо шифрування резервних копій коштує 30 тис. грн, а дозволяє зменшити можливі втрати на 100 тис. грн, ефект становить 70 тис. грн. Для прийняття рішення також доцільно порівнювати кілька сценаріїв: мінімальний, найбільш імовірний і максимальний очікуваний ефект, оскільки фактичні наслідки інциденту можуть відрізнятися залежно від масштабу атаки та критичності порушених даних.

Таблиця 3.11

Спрощена оцінка економічної доцільності впровадження захисних заходів

Захисний захід	**Витрати на впровадження, тис. грн**	**Очікувані попереджені збитки, тис. грн**	**Розрахунок ефекту**	**Економічний ефект, тис. грн**	**Практичний висновок**
Багатофакторна автентифікація	40	120	120 − 40	80	Доцільно впровадити для критичних систем
Шифрування резервних копій	30	100	100 − 30	70	Доцільно впровадити для всіх резервних сховищ
Журналювання та моніторинг	50	140	140 − 50	90	Доцільно впровадити для раннього виявлення інцидентів
Контроль прав доступу	25	90	90 − 25	65	Доцільно впровадити для зниження внутрішніх ризиків
Тестове відновлення резервних копій	20	75	75 − 20	55	Доцільно впровадити для перевірки доступності даних

Найбільш економічно доцільними є заходи, у яких очікувані попереджені збитки перевищують витрати на впровадження. Отримані значення можна використати для пріоритизації впровадження: спочатку реалізуються заходи з найбільшим ефектом і впливом на зниження ризику витоку персональних даних

Поетапне впровадження запропонованих заходів має здійснюватися за принципом пріоритетності, коли першочергово захищаються критичні системи, сховища персональних даних і облікові записи з розширеними правами доступу.

Після захисту критичних систем виконується розширення заходів на файлові сховища, електронну пошту, резервні копії, мобільні пристрої та канали

передавання даних. На цьому етапі впроваджується маркування документів, контроль вивантаження файлів, налаштування сповіщень про підозрілу активність, перевірка резервного відновлення, оновлення реєстру ризиків і навчання користувачів правилам безпечної роботи з персональними даними. Для контролю виконання доцільно застосовувати цикл “планування – виконання – перевірка – коригування”, за яким після кожного етапу збираються фактичні дані, оцінюється результат і визначається потреба в додаткових змінах. –

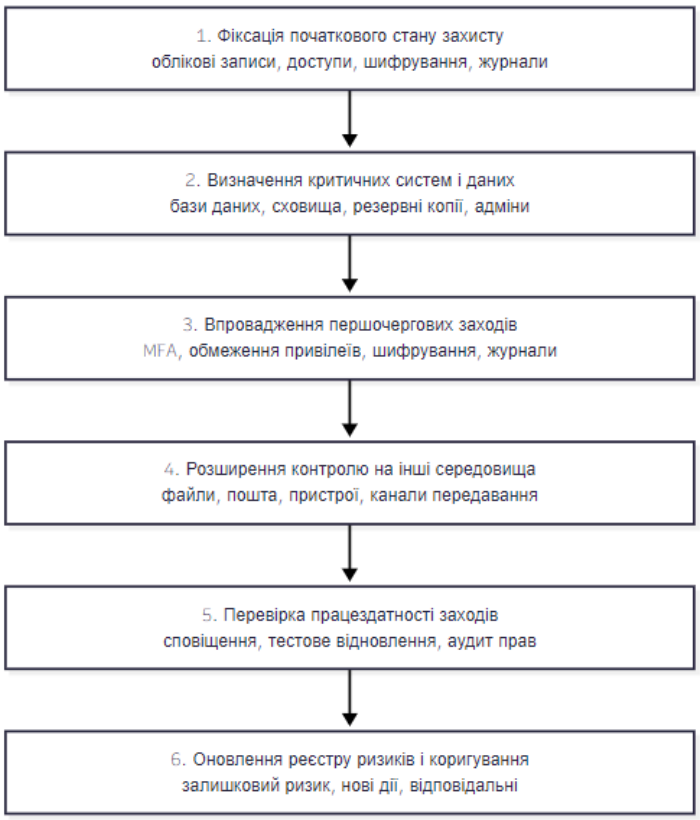

Рис. 3.4 Поетапне впровадження запропонованих заходів

Контроль виконання та регулярний перегляд системи здійснюються після впровадження захисних заходів для підтримання їх актуальності та перевірки фактичної результативності. Практично це означає, що для кожного впровадженого засобу захисту встановлюється періодична перевірка: перегляд прав доступу користувачів, аудит привілейованих облікових записів, аналіз журналів подій, перевірка роботи сповіщень, контроль актуальності шифрування, перевірка резервних копій і тестове відновлення даних. Окремо

потрібно перевіряти, чи не з’явилися нові облікові записи без багатофакторної автентифікації, чи не були повторно надані надмірні права доступу, чи фіксуються події експорту даних, масового копіювання, зміни ролей і доступу до чутливих сховищ. Такий контроль дає змогу виявити не лише технічні збої, а й відхилення від затверджених правил безпеки.

Практичним результатом перегляду є оновлений реєстр ризиків, у якому фіксуються нові ризики, залишкові ризики, виконані коригувальні дії та відповідальні особи. Після інцидентів, змін у системах, підключення нових сервісів або зміни структури доступу оцінка ризиків має повторюватися, оскільки попередній рівень захисту може вже не відповідати фактичному стану середовища. Для оцінювання ефективності доцільно використовувати повторне вимірювання показників і порівняння їх із початковими значеннями, оскільки саме це дозволяє підтвердити, чи дала система практичне покращення. Регулярний перегляд також має включати аналіз прогалин у метриках, оновлення контрольних показників і підготовку звіту про ефективність заходів, що відповідає підходу до періодичного збору, порівняння та вдосконалення показників захисту даних.

Висновки до розділу 3

Розроблена комплексна система управління ризиками витоку персональних даних охоплює повний практичний цикл: від інвентаризації та класифікації даних до впровадження технічних засобів захисту, моніторингу та реагування на інциденти.

Інвентаризація персональних даних умовної організації дозволила сформувати структурований реєстр із визначенням місць зберігання, відповідальних власників, прав доступу та наявних засобів захисту. Виявлені проблемні місця – надмірні права користувачів, відсутність шифрування окремих сховищ, наявність застарілих копій і неповне журналювання – стали основою для подальшої оцінки ризиків. Класифікація даних за рівнями

критичності забезпечила чітку прив'язку між типом інформації та мінімально необхідними засобами захисту.

Побудована карта потоків персональних даних виявила допоміжні точки ризику, зокрема неконтрольоване вивантаження, копії у вкладеннях електронної пошти та доступ підрядників до внутрішніх ресурсів. Оцінка ризиків дозволила визначити критичні ділянки, де ймовірність витоку та його потенційні наслідки є найвищими.

Запропоновані технічні заходи – багатофакторна автентифікація, рольове розмежування доступу, шифрування сховищ і каналів передавання, журналювання та моніторинг підозрілої активності – підтвердили практичну ефективність у порівняльній оцінці стану захисту до і після їх впровадження. Найбільш відчутне зниження ризику досягнуто для резервних копій і привілейованих облікових записів, тоді як ризики, пов'язані з людським фактором і масовим вивантаженням даних, потребують подальшого контролю.

Оцінка економічної доцільності підтвердила, що для всіх запропонованих заходів очікувані попереджені збитки суттєво перевищують витрати на їх реалізацію, що обґрунтовує пріоритетність їх впровадження.

Поетапний план і механізм регулярного перегляду реєстру ризиків забезпечують довготривалу керованість захистом персональних даних і здатність системи адаптуватися до нових загроз.

ВИСНОВКИ

У кваліфікаційній роботі досліджено теоретичні та практичні аспекти управління ризиками витоку персональних даних у цифрових інформаційних системах. Актуальність обраної теми зумовлена стрімким розвитком інформаційно-комунікаційних технологій, розширенням обсягів обробки персональних даних та зростанням кількості кіберзагроз, що створюють ризики несанкціонованого доступу до конфіденційної інформації. Забезпечення належного рівня захисту персональних даних є важливою умовою стабільного функціонування інформаційних систем, дотримання прав громадян та підтримання довіри користувачів до цифрових сервісів.

У першому розділі розглянуто теоретичні основи захисту персональних даних та управління інформаційними ризиками. Досліджено сутність поняття персональних даних, визначено їх роль у сучасному цифровому середовищі та проаналізовано основні загрози, що можуть призвести до витоку інформації. Встановлено, що найбільшу небезпеку становлять несанкціонований доступ до інформаційних ресурсів, атаки соціальної інженерії, шкідливе програмне забезпечення, внутрішні порушення політик безпеки та недоліки організації захисту інформації. Також проаналізовано основні принципи та методи управління інформаційними ризиками, серед яких системність, безперервність, превентивність та ризик-орієнтований підхід. Окрему увагу приділено нормативно-правовому регулюванню захисту персональних даних в Україні та міжнародним стандартам, які визначають сучасні вимоги до забезпечення інформаційної безпеки.

У другому розділі проведено аналіз ризиків витоку персональних даних у цифрових інформаційних системах. Досліджено типові канали витоку інформації, серед яких мережеві комунікації, хмарні сервіси, мобільні пристрої, електронна пошта та внутрішні інформаційні ресурси організацій. Виконано оцінювання вразливостей та загроз, які впливають на безпеку персональних даних, а також визначено фактори, що найбільше сприяють реалізації ризиків.

Проведене моделювання та кількісна оцінка ризиків дозволили встановити рівень їх критичності та визначити пріоритетні напрями вдосконалення систем захисту. Результати аналізу підтвердили необхідність впровадження комплексних заходів безпеки, спрямованих на мінімізацію ймовірності виникнення інцидентів та зменшення можливих наслідків витоку інформації.

У третьому розділі розроблено комплексну систему управління ризиками витоку персональних даних, яка поєднує організаційні, технічні та адміністративні заходи захисту. Запропоновано практичні рекомендації щодо впровадження сучасних засобів автентифікації, контролю доступу, криптографічного захисту інформації, моніторингу подій безпеки та навчання персоналу. Особливу увагу приділено використанню багатофакторної автентифікації, систем виявлення вторгнень, засобів шифрування та регулярного аудиту інформаційної безпеки. Проведене оцінювання ефективності запропонованих заходів показало, що їх комплексне впровадження дозволяє суттєво знизити рівень ризиків витоку персональних даних, підвищити стійкість інформаційних систем до сучасних кіберзагроз та забезпечити відповідність вимогам чинного законодавства і міжнародних стандартів.

За результатами проведеного дослідження встановлено, що ефективне управління ризиками витоку персональних даних повинно базуватися на комплексному підході, який поєднує правові, організаційні та технічні механізми захисту. Досягнення належного рівня інформаційної безпеки можливе лише за умови постійного моніторингу загроз, своєчасного виявлення вразливостей, регулярного оцінювання ризиків та безперервного вдосконалення систем захисту. Запропоновані в роботі методи та рекомендації можуть бути використані організаціями різних форм власності для підвищення рівня захисту персональних даних і вдосконалення процесів управління інформаційними ризиками в умовах цифрової трансформації суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бондарєва Т. І. Організаційні аспекти створення інформаційної системи управління ризиками підприємства. *Time description of economic reforms*. 2022. № 2. С. 58–65. URL: https://doi.org/10.32620/cher.2022.2.08

2. Походенко Б. О. Theoretical foundations of risk management for energy sector enterprises. *Підприємництво та інновації*. 2024. No. 30. P. 27–34. URL: https://doi.org/10.32782/2415-3583/30.4

3. Advanced risk and performance management in the financial sector: a deep learning approach / N. Ryali et al. *2024 2nd international conference on disruptive technologies (ICDT)*, Greater Noida, India, 15–16 March 2024. 2024. URL: https://doi.org/10.1109/icdt61202.2024.10489151

4. An integrated system theory of information security management / K. Hong et al. *Information management & computer security*. 2003. Vol. 11, no. 5. P. 243–248. URL: https://doi.org/10.1108/09685220310500153

5. Brito A. A., Oliveira S. R. B. Perception on the knowledge of privacy and data protection in a software development company: a study based on the application of a survey. *19th CONTECSI international conference on information systems and technology management*. URL: https://doi.org/10.5748/19contecsi/pse/esd/7086

6. Carvalho A. C. d. M. Metrics for risk assessment in data protection impact assessments : master's thesis. 2018. URL: https://hdl.handle.net/10216/116275

7. Data security strategies to avoid data breaches in modern information systems / Chukwudi Tabitha Aghaunor et al. *World journal of advanced research and reviews*. 2025. Vol. 25, no. 1. P. 827–849. URL: https://doi.org/10.30574/wjarr.2025.25.1.3906

8. Enríquez L. A personal data value at risk (pd-var) approach. *Journal of research innovation and technologies (jorit)*. 2024. Vol. 3, no. 2. P. 141–158. URL: https://doi.org/10.57017/jorit.v3.2(6).05

9. Freitas C. O. d. A. Riscos e proteção de dados pessoais. *Revista rede de direito digital, intelectual & sociedade*. 2023. Vol. 2, no. 4. P. 225. URL: https://doi.org/10.5380/rrddis.v2i4.93531

10. Gellert R. Data protection as command and control regulation. *The risk-based approach to data protection*. 2020. P. 54–86. URL: https://doi.org/10.1093/oso/9780198837718.003.0003

11. Gellert R. Risk-Based approach to data protection. Oxford University Press, 2020.

12. Gonçalves A., Correia A., Cavique L. Data protection risk modeling into business process analysis. *Computational science and its applications – ICCSA 2017*. Cham, 2017. P. 667–676. URL: https://doi.org/10.1007/978-3-319-62392-4_48

13. Kogan A., Averyaskina A., Troitskaya N. Theoretical and methodological foundations of pricing for apartment building management services. *Ideas and ideals*. 2023. Vol. 15, no. 1-2. P. 273–290. URL: https://doi.org/10.17212/2075-0862-2023-15.1.2-273-290

14. Meganck S., Leray P., Manderick B. Learning causal bayesian networks from observations and experiments: a decision theoretic approach. *Modeling decisions for artificial intelligence*. Berlin, Heidelberg, 2006. P. 58–69. URL: https://doi.org/10.1007/11681960_8

15. Shetty P. Data privacy and risk management, collaboration is key on tackling privacy risks/issues. *Journal of artificial intelligence & cloud computing*. 2023. P. 1–4. URL: https://doi.org/10.47363/jaicc/2023(2)224

16. Tewald C. Risikomanagement aus der Isolation im Unternehmen herausführen. *Controlling*. 2004. Vol. 16, no. 4-5. P. 261–264. URL: https://doi.org/10.15358/0935-0381-2004-4-5-261

17. Zhao Y. Integrating advanced technologies in financial risk management: a comprehensive analysis. *Advances in economics, management and political sciences*. 2024. Vol. 108, no. 1. P. 92–97. URL: https://doi.org/10.54254/2754-1169/108/20241908

18. Đukić S. Cyber security and data protection. *Moderna arhivistika*. 2025. Vol. 8, no. 1. P. 78. URL: https://doi.org/10.54356/ma/2025/hazd7569

19. Wheatley S., Maillart T., Sornette D. The extreme risk of personal data breaches and the erosion of privacy. The European Physical Journal B. 2016. Vol. 89, no. 1. URL: https://doi.org/10.1140/epjb/e2015-60754-4

20. Shim H., Kim C., Choi Y. H. Volatility clustering in data breach counts. Communications for Statistical Applications and Methods. 2020. Vol. 27, no. 4. P. 487–500. URL: https://doi.org/10.29220/csam.2020.27.4.487

21. Izergin D., Eremeev M. Risk assessment model of compromising personal data on mobile devices. E3S Web of Conferences. 2021. Vol. 270. P. 01013. URL: https://doi.org/10.1051/e3sconf/202127001013

22. Prisca I. Okochi, Stanley A. Okolie, Juliet N. Odii. An improved data leakage detection system in a cloud computing environment. World Journal of Advanced Research and Reviews. 2021. Vol. 11, no. 2. P. 321–328. URL: https://doi.org/10.30574/wjarr.2021.11.2.0385

23. Current status and future prospects of data leakage prevention technology: A brief review / L. Xuming et al. Journal of Physics: Conference Series. 2019. Vol. 1345. P. 022010. URL: https://doi.org/10.1088/1742-6596/1345/2/022010

24. A quantitative assessment method of network information security vulnerability detection risk based on the meta feature system of network security data. KSII Transactions on Internet and Information Systems. 2021. Vol. 15, no. 12. URL: https://doi.org/10.3837/tiis.2021.12.015

25. Information theoretic-based privacy risk evaluation for data anonymization / A. Bkakria et al. Journal of Surveillance, Security and Safety. 2022. URL: https://doi.org/10.20517/jsss.2020.20

26. Kim N., Oh H., Choi J. K. A privacy scoring framework: Automation of privacy compliance and risk evaluation with standard indicators. Journal of King Saud University - Computer and Information Sciences. 2023. URL: https://doi.org/10.1016/j.jksuci.2022.12.019

27. Sankar L., Rajagopalan S. R., Poor H. V. Utility and privacy of data sources: Can Shannon help conceal and reveal information?. 2010 Information Theory and Applications Workshop (ITA), La Jolla, CA, USA, 31 January – 5 February 2010. 2010. URL: https://doi.org/10.1109/ita.2010.5454092

28. The Trusted Server: A secure computational environment for privacy compliant evaluations on plain personal data / N. von Bomhard et al. PLOS ONE. 2018. Vol. 13, no. 9. P. e0202752. URL: https://doi.org/10.1371/journal.pone.0202752

29. Big data security and privacy in healthcare: A Review / K. Abouelmehdi et al. Procedia Computer Science. 2017. Vol. 113. P. 73–80. URL: https://doi.org/10.1016/j.procs.2017.08.292

30. Serrão C., Cardoso E. Handling confidentiality and privacy on cloud-based health information systems. Journal of Information Privacy and Security. 2017. Vol. 13, no. 2. P. 51–68. URL: https://doi.org/10.1080/15536548.2017.1322415

31. The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach / M. Dimodugno et al. Journal of Physics: Conference Series. 2021. Vol. 2090, no. 1. P. 012017. URL: https://doi.org/10.1088/1742-6596/2090/1/012017

32. Mohammed Z. Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. Organizational Cybersecurity Journal: Practice, Process and People. 2021. Vol. 2, no. 1. P. 41–59. URL: https://doi.org/10.1108/ocj-05-2021-0014

33. Ke Z., Yongzhen L. Research on Internet data security and privacy protection. Journal of Physics: Conference Series. 2021. Vol. 2005, no. 1. P. 012004. URL: https://doi.org/10.1088/1742-6596/2005/1/012004

34. Computer security for data collection technologies / C. Cobb et al. Development Engineering. 2018. Vol. 3. P. 1–11. URL: https://doi.org/10.1016/j.deveng.2017.12.002

35. A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces / L. Zhang et al. International Journal of Information Security. 2021. URL: https://doi.org/10.1007/s10207-021-00566-3

36. Assessing system of systems information security risk with OASoSIS / D. Ki-Aries et al. Computers & Security. 2022. Vol. 117. P. 102690. URL: https://doi.org/10.1016/j.cose.2022.102690

37. Haynes D., Robinson L. Delphi study of risk to individuals who disclose personal information online. Journal of Information Science. 2021. P. 016555152199275. URL: https://doi.org/10.1177/0165551521992756

38. Shaikh F. A., Siponen M. Information Security Risk Assessments following Cybersecurity Breaches: The Mediating Role of Top Management Attention to Cybersecurity. *Computers & Security*. 2022. P. 102974. URL: https://doi.org/10.1016/j.cose.2022.102974

39. Razikin K., Soewito B. Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*. 2022. URL: https://doi.org/10.1016/j.eij.2022.03.001

40. Sánchez-García I. D., Feliu Gilabert T. S., Calvo-Manzano J. A. Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. *Computers & Security*. 2023. Vol. 128. P. 103170. URL: https://doi.org/10.1016/j.cose.2023.103170

41. Mohammed Z. Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People*. 2021. Vol. 2, no. 1. P. 41–59. URL: https://doi.org/10.1108/ocj-05-2021-0014

42. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy / S. Akter et al. *Annals of Operations Research*. 2022. URL: https://doi.org/10.1007/s10479-022-04844-8

43. Jagannathan J., Mohamed Parvees M. Y. Security breach prediction using Artificial Neural Networks. *Measurement: Sensors*. 2022. P. 100448. URL: https://doi.org/10.1016/j.measen.2022.100448

44. Exploring user behavioral data for adaptive cybersecurity / J. H. Addae et al. *User Modeling and User-Adapted Interaction*. 2019. Vol. 29, no. 3. P. 701–750. URL: https://doi.org/10.1007/s11257-019-09236-5

45. Suzuki Y. E., Monroy S. A. S. Prevention and mitigation measures against phishing emails: a sequential schema model. *Security Journal*. 2021. URL: https://doi.org/10.1057/s41284-021-00318-x

46. Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity / K. Sharma et al. *Organizational Cybersecurity Journal: Practice, Process and People*. 2021. Ahead-of-print, ahead-of-print. URL: https://doi.org/10.1108/ocj-03-2021-0009