МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **125 Кібербезпека**
Освітня програма: **Кібербезпека у фінансових технологіях**

Група: АБ-41Б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

«ІНСТРУМЕНТИ АНАЛІЗУ ТА ЗАХИСТУ ВІД ЗЛОВЖИВАНЬ ПЕРСОНАЛЬНИМИ ДАНИМИ У СФЕРІ ТАРГЕТОВАНОЇ РЕКЛАМИ»

ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти **Спориш Елеонори Євгенівни**

Робота допущена до захисту в ЕК
протокол кафедри ІТММ №13 від 31.05.2025р.

Завідувач кафедри ІТММ
к.п.н.
_____ Н.І. Стяглик

Науковий керівник
к.ф.-м.н, доцент
_____ Г.В. Макарова

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма Кібербезпека у фінансових технологіях

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ **Н. І. Стяглик**
Підпис ініціали, прізвище
"08" лютого 2025 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Спориш Елеонора Євгенівна

(прізвище, ім'я, по батькові студента)

1. Тема роботи «Інструменти аналізу та захисту від зловживань персональними даними у сфері тергетованої реклами»

керівник роботи Макарова Ганна Валеріївна, к.ф.-м.н, доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від "08" лютого 2025 року № 4601-5/335

2. Строк подання студентом роботи 15 травня 2025 року

3. Перелік питань, які потрібно розробити:

У розділі 1: присвячено аналіз зловживань персональними даними, включаючи їхні види, джерела загроз, методи оцінки ризиків витоку та огляд інструментів для моніторингу безпеки.

У розділі 2: міститься огляд та класифікація інструментів захисту персональних даних, включаючи технології шифрування, системи управління доступом і програмне забезпечення для запобігання витокам.

У розділі 3: висвітлюється практичні аспекти впровадження захисту персональних даних, зокрема розробку політик, навчання персоналу, аудит систем безпеки та реагування на інциденти.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 08 лютого 2025 року

Студент Е. Є. Спориш
підпис ініціали, прізвище

Керівник роботи Г. В. Макарова
підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ

«Інструменти аналізу та захисту від зловживань персональними даними у сфері таргетованої реклами»

Спориш Елеонори Євгенівни

Дипломна робота містить: 56 сторінок, 3 таблиць, список літератури з 29 найменувань.

Об'єктом дослідження є процеси аналізу та захисту персональних даних у цифрових системах.

Предметом дослідження виступають інструменти, методи та технології, які застосовуються для виявлення загроз і запобігання зловживанням персональними даними.

Мета роботи полягає в дослідженні інструментів аналізу та захисту персональних даних, оцінці їхньої ефективності та розробці рекомендацій щодо їхнього впровадження для запобігання зловживанням.

Для досягнення цієї мети визначено такі завдання:

- Провести аналіз типів зловживань персональними даними та джерел загроз.
- Вивчити сучасні методи аналізу ризиків витоку даних.
- Оцінити інструменти захисту персональних даних, включаючи технології шифрування, системи управління доступом і програмне забезпечення для запобігання витокам.
- Розробити практичні рекомендації щодо впровадження політики захисту даних, навчання персоналу та реагування на інциденти.

Актуальність дослідження обумовлена зростаючими ризиками зловживання персональними даними в умовах цифровізації та активного розвитку інформаційних технологій. Особливої ваги це питання набуває в Україні через посилення кіберзагроз у зв'язку з воєнним станом та цифровою трансформацією державного і приватного секторів.

За результатами дослідження проаналізовано типи загроз і зловживань персональними даними, оцінено сучасні інструменти захисту, такі як шифрування, системи управління доступом та програмне забезпечення для запобігання витокам. Розроблено рекомендації щодо впровадження ефективної політики захисту даних.

Практична новизна полягає у систематизації актуальних методів аналізу й захисту персональних даних з урахуванням українського правового та технічного контексту, а також у створенні практичних рекомендацій щодо підвищення рівня інформаційної безпеки в організаціях.

Одержані результати можуть бути використані у державних установах, комерційних організаціях, навчальних закладах для покращення захисту персональних даних, розробки внутрішніх політик безпеки, а також для підвищення цифрової грамотності користувачів у сфері кібербезпеки.

КЛЮЧОВІ СЛОВА: ПЕРСОНАЛЬНІ ДАНІ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ШИФРУВАННЯ, ВИТІК ДАНИХ, ІНФОРМАЦІЙНІ

ТЕХНОЛОГІЇ, ЦИФРОВІЗАЦІЯ, АНАЛІЗ РИЗИКІВ, ПОЛІТИКА БЕЗПЕКИ, КІБЕРЗАГРОЗИ.

ABSTRACT

FOR THE BACHELOR'S QUALIFICATION THESIS

«Tools for Analysis and Protection Against the Misuse of Personal Data in Targeted Advertising»

by Sporysh Eleonora Yevhenivna

This thesis, presented in 56 pages and supported by 3 tables and 29 references, explores the issues of analyzing and securing personal data within digital systems, especially in the context of targeted advertising.

The study focuses on identifying effective tools and technologies that can detect and prevent the misuse of personal data. Key areas of research include threat identification, risk analysis of data leaks, and evaluation of security solutions such as encryption, access control, and data loss prevention systems.

The main objective of the work is to assess how these tools function in practice and provide practical recommendations for implementing data protection strategies. This includes staff awareness, data policies, and incident response planning.

The relevance of this topic is linked to the increasing risks of data misuse in today's digital world. For Ukraine, these challenges are particularly pressing due to rising cyber threats during martial law and the ongoing digital transformation of public and private institutions.

Research outcomes include the classification of threats, analysis of security tools, and development of guidelines to improve data protection. The novelty of the work lies in adapting modern analysis and defense approaches to the Ukrainian legal and technical environment, aiming to support institutions in strengthening their cybersecurity frameworks.

The results can be applied across various sectors – government, business, and education – for improving data protection policies and raising awareness about cybersecurity practices.

KEYWORDS: PERSONAL DATA, CYBERSECURITY, INFORMATION PROTECTION, ENCRYPTION, DATA LEAKAGE, INFORMATION TECHNOLOGY, DIGITALIZATION, RISK ANALYSIS, SECURITY POLICY, CYBER THREATS.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AES – Advanced Encryption Standard (Стандарт шифрування даних, симетричний алгоритм).

ALE – Annual Loss Expectancy (Очікувані річні втрати, показник для кількісного аналізу ризиків).

CRM – Customer Relationship Management (Система управління взаємовідносинами з клієнтами).

DDoS – Distributed Denial of Service (Розподілена атака типу «відмова в обслуговуванні»).

DLP – Data Loss Prevention (Запобігання втраті даних, клас систем для захисту інформації).

ECC – Elliptic Curve Cryptography (Криптографія на основі еліптичних кривих, асиметричне шифрування).

GDPR – General Data Protection Regulation (Загальний регламент захисту даних Європейського Союзу).

HTTPS – HyperText Transfer Protocol Secure (Безпечний протокол передачі гіпертексту).

IAM – Identity and Access Management (Управління ідентифікацією та доступом).

IDS/IPS – Intrusion Detection/Prevention System (Система виявлення/запобігання вторгненням).

IoT – Internet of Things (Інтернет речей).

MDM – Mobile Device Management (Управління мобільними пристроями).

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технологій США).

OSINT – Open Source Intelligence (Розвідка на основі відкритих джерел).

RSA – Rivest-Shamir-Adleman (Алгоритм асиметричного шифрування).

SIEM – Security Information and Event Management (Управління інформацією та подіями безпеки).

SQL – Structured Query Language (Мова структурованих запитів, використовується для роботи з базами даних).

SSL/TLS – Secure Sockets Layer/Transport Layer Security (Протоколи захисту передачі даних).

SUBD – Systema Upravlinnia Bazamy Dannyh (Система управління базами даних, укр.).

TDE – Transparent Data Encryption (Прозоре шифрування даних, технологія для баз даних).

UEBA – User and Entity Behavior Analytics (Аналіз поведінки користувачів і об’єктів).

VPN – Virtual Private Network (Віртуальна приватна мережа).

ЗМІСТ

ВСТУП

Сучасне інформаційне суспільство характеризується стрімким розвитком цифрових технологій, що забезпечують обробку, зберігання та передачу величезних обсягів даних. Персональні дані, які включають інформацію про фізичних осіб, їхні ідентифікаційні характеристики, фінансові, медичні та інші аспекти життя, стали одним із найцінніших ресурсів цифрової економіки. Водночас зростання обсягів даних супроводжується підвищенням ризиків їхнього зловживання, зокрема витоків, несанкціонованого доступу, шахрайства та кібератак. За даними глобальних звітів, таких як звіти Verizon Data Breach Investigations Report, кількість кіберінцидентів, пов'язаних із персональними даними, щорічно зростає, що завдає значних фінансових і репутаційних збитків організаціям та окремим особам. В Україні проблема захисту персональних даних є особливо актуальною через активну цифровізацію державних і приватних секторів, а також виклики, пов'язані з воєнним станом, що підвищують вразливість інформаційних систем.

Актуальність теми бакалаврської роботи зумовлена необхідністю розробки та впровадження ефективних інструментів аналізу та захисту персональних даних, які здатні мінімізувати ризики зловживань. Захист персональних даних є не лише технічним завданням, а й важливим правовим, соціальним та етичним питанням. В Україні правові засади захисту персональних даних регулюються Законом України «Про захист персональних даних» №2297-VI від 01.06.2010, а також гармонізуються з міжнародними стандартами, такими як Загальний регламент захисту даних (GDPR) Європейського Союзу. Проте практична реалізація захисту даних часто стикається з обмеженнями, пов'язаними з недостатньою технічною інфраструктурою, низьким рівнем обізнаності користувачів і складністю протидії сучасним кіберзагрозам.

Мета роботи полягає в дослідженні інструментів аналізу та захисту персональних даних, оцінці їхньої ефективності та розробці рекомендацій щодо їхнього впровадження для запобігання зловживанням. Для досягнення цієї мети визначено такі завдання:

1. Провести аналіз типів зловживань персональними даними та джерел загроз.
2. Вивчити сучасні методи аналізу ризиків витоку даних.
3. Оцінити інструменти захисту персональних даних, включаючи технології шифрування, системи управління доступом і програмне забезпечення для запобігання витокам.
4. Розробити практичні рекомендації щодо впровадження політики захисту даних, навчання персоналу та реагування на інциденти.

Об’єктом дослідження є процеси аналізу та захисту персональних даних у цифрових системах. Предметом дослідження виступають інструменти, методи та технології, які застосовуються для виявлення загроз і запобігання зловживанням персональними даними.

Методи дослідження включають системний аналіз, порівняльний аналіз, узагальнення наукових джерел, а також вивчення нормативно-правової бази. У роботі використано як теоретичні підходи (аналіз літератури, правових актів), так і практичні (огляд програмного забезпечення, кейс-стаді).

Наукова новизна роботи полягає в систематизації сучасних інструментів аналізу та захисту персональних даних з урахуванням специфіки українського контексту, а також у розробці практичних рекомендацій для організацій щодо мінімізації ризиків зловживань. Практична значущість роботи зумовлена можливістю застосування отриманих результатів для вдосконалення систем захисту даних у державних і комерційних установах, а також для підвищення обізнаності щодо кібербезпеки серед користувачів.

Структура роботи складається зі вступу, трьох основних розділів, висновків, списку використаних джерел і додатків. У першому розділі розглядаються теоретичні аспекти зловживань персональними даними та методи їхнього аналізу. Другий розділ присвячено інструментам захисту даних, а третій – практичним аспектам їхнього впровадження. Така структура дозволяє послідовно розкрити тему дослідження та досягти поставленої мети.

РОЗДІЛ 1. АНАЛІЗ ЗЛОВЖИВАНЬ ПЕРСОНАЛЬНИМИ ДАНИМИ

1.1. Поняття та види персональних даних

Персональні дані є ключовим елементом сучасного інформаційного суспільства, оскільки вони охоплюють широкий спектр інформації, пов'язаної з фізичними особами. Згідно з Законом України «Про захист персональних даних» №2297-VI від 01.06.2010, персональними даними вважається будь-яка інформація, що дає змогу прямо чи опосередковано ідентифікувати фізичну особу [24]. До таких даних належать ім'я, прізвище, дата народження, адреса, номер телефону, електронна пошта, а також біометричні дані, фінансові відомості чи інформація про здоров'я. У міжнародній практиці, зокрема відповідно до Загального регламенту захисту даних (GDPR), персональні дані поділяються на загальні (наприклад, контактні дані) та чутливі (расове походження, релігійні переконання, дані про здоров'я), що потребують посиленого захисту [5].

Персональні дані класифікуються за різними критеріями, що допомагає зрозуміти їхню природу та способи обробки. За типом інформації виділяють ідентифікаційні дані (паспортні дані, ІПН), контактні дані (телефон, адреса), фінансові дані (банківські рахунки, кредитна історія) та поведінкові дані (історія покупок, активність у соціальних мережах). За способом збору розрізняють дані, надані добровільно (наприклад, заповнення анкет), і дані, отримані автоматично (cookies, геолокація). Така класифікація є основою для розробки стратегій захисту даних, оскільки кожен тип має свої вразливості [1]. Наприклад, фінансові дані частіше стають об'єктом шахрайства, тоді як поведінкові дані використовуються для таргетованої реклами чи маніпуляцій.

З точки зору обробки, персональні дані поділяються на структуровані (зберігаються в базах даних, наприклад, CRM-системах) і неструктуровані (тексти, зображення, відео). Структуровані дані легше аналізувати та захищати за допомогою автоматизованих інструментів, таких як системи управління базами даних (СУБД), тоді як неструктуровані дані потребують складніших

методів, наприклад, аналізу за допомогою штучного інтелекту [1]. У контексті великих даних (Big Data) персональні дані набувають особливої цінності, оскільки їхній аналіз дозволяє прогнозувати поведінку користувачів, але водночас підвищує ризики зловживань через великі обсяги інформації.

Правовий аспект також відіграє важливу роль у визначенні персональних даних. В Україні захист персональних даних регулюється не лише вищезгаданим законом, а й іншими нормативними актами, які встановлюють порядок їхньої обробки, зберігання та передачі [24]. На міжнародному рівні GDPR запровадив суворі вимоги до згоди користувачів на обробку даних, що стало стандартом для багатьох країн [5]. Це підкреслює важливість чіткого визначення категорій даних, оскільки від цього залежить рівень захисту, який необхідно застосовувати.

Види персональних даних також залежать від контексту їхнього використання. У медичній сфері, наприклад, дані про здоров’я є особливо чутливими, оскільки їхній витік може призвести до серйозних наслідків для особи [15]. У фінансовому секторі банківські дані, такі як номери карток чи транзакційна історія, є основною мішенню кіберзлочинців. У соціальних мережах поведінкові дані, зібрані через алгоритми відстеження, часто використовуються для профілювання, що може порушувати приватність користувачів. Таким чином, розуміння видів персональних даних є передумовою для аналізу ризиків і розробки ефективних інструментів їхнього захисту.

Важливим аспектом є також етичний вимір обробки персональних даних. Зловживання даними, навіть у межах закону, може викликати недовіру з боку користувачів. Наприклад, надмірне використання поведінкових даних для маркетингових цілей може сприйматися як порушення приватності [5]. Отже, організації, які обробляють персональні дані, повинні враховувати не лише технічні та правові аспекти, а й суспільні очікування щодо їхнього використання.

1.2. Типи зловживань персональними даними

Зловживання персональними даними є однією з ключових проблем сучасного цифрового середовища, що охоплює широкий спектр протиправних дій, спрямованих на незаконне використання інформації про фізичних осіб. Зловживання можуть мати різні форми, включаючи крадіжку даних, шахрайство, несанкціонований доступ, а також використання даних у спосіб, що суперечить інтересам особи [3]. За даними звіту Verizon Data Breach Investigations Report 2023, понад 80% кіберінцидентів пов'язані з персональними даними, що підкреслює масштабність проблеми.

Одним із найпоширеніших типів зловживань є крадіжка персональних даних (data breach). Це може відбуватися через хакерські атаки, фішинг, шкідливе програмне забезпечення або соціальну інженерію. Наприклад, фішингові кампанії обманом змушують користувачів розкривати паролі чи банківські дані, які потім використовуються для фінансового шахрайства [14]. Такі інциденти часто спрямовані на фінансові дані, оскільки вони мають високу цінність на чорному ринку. Згідно з дослідженнями, середня вартість витоку даних для компаній у 2023 році склала близько 4,45 млн доларів США [3].

Іншим типом зловживань є несанкціоноване використання даних. Це включає продаж даних третім сторонам без згоди користувача, використання даних для профілювання чи таргетованої реклами, а також передачу даних у порушення законодавства. Наприклад, соціальні мережі можуть передавати поведінкові дані рекламодавцям, що порушує принципи прозорості, визначені GDPR [6]. В Україні такі випадки також трапляються, зокрема через недостатній контроль за обробкою даних у приватному секторі [14].

Шахрайство з персональними даними є ще однією серйозною загрозою. Воно включає такі дії, як оформлення кредитів на ім'я жертви, створення фальшивих акаунтів або використання вкрадених даних для доступу до фінансових ресурсів. У медичній сфері шахрайство може проявлятися у використанні даних про здоров'я для незаконного отримання страхових виплат

[15]. Такі дії не лише завдають матеріальних збитків, а й підривають довіру до організацій, які обробляють дані.

Зловживання також можуть бути пов’язані з внутрішніми загрозами, коли співробітники організацій умисно чи через недбалість розкривають персональні дані. Наприклад, неналежне налаштування баз даних або відсутність контролю доступу може призвести до витоку інформації [3]. В Україні подібні інциденти часто фіксуються у державних установах через застарілу інфраструктуру та низький рівень кіберграмотності [14].

Окремим типом зловживань є маніпуляція даними, спрямована на вплив на поведінку осіб. Наприклад, аналіз поведінкових даних дозволяє створювати психологічні профілі користувачів, які використовуються для політичних кампаній чи комерційних маніпуляцій. Скандал із Cambridge Analytica є прикладом такого зловживання, коли дані користувачів Facebook були використані для впливу на виборчі процеси [6]. Це підкреслює необхідність посилення етичних стандартів у роботі з даними.

Наслідки зловживань персональними даними є багатогранними. Для фізичних осіб це може означати фінансові втрати, порушення приватності, психологічний стрес. Для організацій – репутаційні ризики, штрафи та втрату довіри клієнтів. В Україні, де цифровізація активно розвивається, проблема зловживань потребує комплексного підходу, що поєднує правові, технічні та освітні заходи [15]. Розуміння типів зловживань є основою для розробки стратегій їхнього запобігання, що буде розглянуто в наступних розділах.

1.3. Джерела загроз для персональних даних

Загрози для персональних даних є багатогранними і походять із різних джерел, що обумовлено складністю сучасних інформаційних систем і зростанням обсягів даних, які обробляються. Ці джерела можна класифікувати на зовнішні, внутрішні та технологічні, кожне з яких має свої особливості та вимагає специфічних заходів протидії. Зовнішні загрози включають дії зловмисників, внутрішні – помилки чи зловмисні дії працівників, а технологічні

– вразливості в програмному забезпеченні чи обладнанні [7]. Розуміння джерел загроз є ключовим для розробки ефективних стратегій захисту персональних даних.

Зовнішні загрози є найпоширенішими і включають хакерські атаки, фішинг, шкідливе програмне забезпечення (malware) та соціальну інженерію. Хакерські атаки спрямовані на отримання несанкціонованого доступу до баз даних, що містять персональні дані, через експлуатацію вразливостей у системах. Наприклад, атаки типу SQL-ін’єкцій або DDoS можуть призвести до компрометації великих обсягів даних [3]. Фішинг, своєю чергою, використовує обманні методи, такі як підроблені електронні листи чи вебсайти, для отримання конфіденційних даних, таких як паролі чи банківські реквізити. В Україні фішингові атаки набули поширення через зростання онлайн-сервісів, зокрема в банківській сфері [14]. Шкідливе програмне забезпечення, наприклад, віруси-вимагачі (ransomware), блокує доступ до даних і вимагає викуп, що становить серйозну загрозу для організацій і приватних осіб.

Внутрішні загрози є не менш небезпечними, оскільки походять від працівників або інших осіб, які мають легітимний доступ до систем. Такі загрози можуть бути навмисними (наприклад, крадіжка даних для продажу) або ненавмисними (помилки в конфігурації систем чи втрата носіїв інформації). За даними досліджень, близько 30% витоків даних пов’язані з внутрішніми загрозами, що підкреслює важливість контролю доступу та навчання персоналу [7]. В Україні внутрішні загрози часто виникають через низький рівень кіберграмотності та відсутність чітких політик безпеки в організаціях [14]. Наприклад, неналежне зберігання паролів або використання особистих пристроїв для доступу до корпоративних систем може призвести до компрометації даних.

Технологічні загрози пов’язані з вразливостями в програмному забезпеченні, апаратному забезпеченні або інфраструктурі. Застаріле програмне забезпечення, яке не отримує оновлень безпеки, є однією з основних причин витоків даних. Наприклад, уразливості в популярних системах управління

базами даних, таких як MySQL чи Oracle, часто експлуатуються зловмисниками [3]. У контексті хмарних технологій, які активно використовуються для зберігання персональних даних, неправильно налаштовані сховища (наприклад, Amazon S3) можуть стати джерелом масштабних витоків. Крім того, зростання популярності Інтернету речей (IoT) створює нові виклики, оскільки багато пристроїв мають слабкий захист і можуть бути використані як точки входу для атак [7].

Соціальні та політичні фактори також можуть бути джерелом загроз. У період воєнного стану в Україні зростає ризик кібератак, спрямованих на державні реєстри, що містять персональні дані громадян. Такі атаки можуть мати на меті не лише крадіжку даних, а й дестабілізацію суспільства [14]. Крім того, глобальні тенденції, такі як торгівля даними на чорному ринку, стимулюють зловмисників до пошуку нових методів атак. Наприклад, персональні дані, отримані внаслідок витоків, можуть використовуватися для шантажу чи шахрайства.

Наслідки реалізації цих загроз є значними як для окремих осіб, так і для організацій. Для громадян це може означати втрату конфіденційності, фінансові збитки або психологічний дискомфорт. Для компаній – штрафи, репутаційні втрати та витрати на відновлення систем. Таким чином, аналіз джерел загроз є необхідною передумовою для розробки комплексних заходів захисту, які враховують як технічні, так і організаційні аспекти [3].

1.4. Методи аналізу ризиків витоку даних

Аналіз ризиків витоку персональних даних є важливим етапом у забезпеченні їхньої безпеки, оскільки дозволяє виявити потенційні загрози, оцінити їхній вплив і розробити заходи для їхнього запобігання. Методи аналізу ризиків поєднують якісні та кількісні підходи, які допомагають організаціям систематично оцінювати вразливості та пріоритизувати захисні заходи [8]. Ці методи базуються на стандартах, таких як ISO/IEC 27005, і адаптуються до специфіки обробки персональних даних.

Одним із основних методів є якісний аналіз ризиків, який передбачає ідентифікацію загроз і оцінку їхньої ймовірності та впливу на основі експертних суджень. Цей метод включає створення переліку активів (наприклад, баз даних із персональними даними), визначення можливих загроз (хакерські атаки, внутрішні витоки) і оцінку їхнього впливу за шкалою, наприклад, від «низького» до «критичного» [8]. У контексті персональних даних якісний аналіз часто використовується для оцінки ризиків, пов'язаних із чутливими даними, такими як медична чи фінансова інформація [15]. Наприклад, витік даних про здоров'я може мати критичний вплив через порушення приватності та потенційні юридичні наслідки.

Кількісний аналіз ризиків є більш формалізованим і передбачає використання числових показників для оцінки ймовірності та вартості потенційних втрат. Цей метод включає розрахунок очікуваних збитків (Annual Loss Expectancy, ALE), який враховує частоту інцидентів і їхній фінансовий вплив. Наприклад, організація може оцінити, що ймовірність витоку даних становить 10% на рік, а потенційні збитки – 1 млн грн, що дає ALE у розмірі 100 тис. грн [8]. Утім, кількісний аналіз потребує точних даних, що може бути складно в умовах обмеженої статистики, особливо в Україні, де ринок кібербезпеки ще розвивається [19].

Ще одним поширеним методом є аналіз сценаріїв, який передбачає моделювання можливих інцидентів і оцінку їхніх наслідків. Наприклад, організація може змоделювати сценарій фішингової атаки, яка призводить до компрометації бази даних клієнтів, і оцінити, які системи та процеси є найбільш вразливими [19]. Цей метод часто використовується разом із тестуванням на проникнення (penetration testing), яке дозволяє виявити слабкі місця в системах шляхом симуляції атак. В Україні такі тести стають дедалі популярнішими серед великих компаній, зокрема в банківському секторі [15].

Стандартизовані фреймворки, такі як NIST SP 800-30 або COBIT, також широко застосовуються для аналізу ризиків. Вони пропонують структурований підхід, який включає ідентифікацію активів, оцінку загроз, аналіз вразливостей і

розробку плану управління ризиками. Наприклад, NIST SP 800-30 рекомендує використовувати матрицю ризиків, де загрози оцінюються за ймовірністю та впливом, що допомагає визначити пріоритетні заходи захисту [8]. В Україні ці стандарти адаптуються до місцевих умов, зокрема через рекомендації Уповноваженого Верховної Ради з прав людини [23].

Автоматизовані інструменти, такі як Microsoft Purview або IBM Security Guardium, відіграють важливу роль у сучасному аналізі ризиків. Вони дозволяють виявляти вразливості в реальному часі, аналізувати потоки даних і оцінювати відповідність регуляторним вимогам, таким як GDPR чи українське законодавство [21]. Наприклад, Microsoft Purview може автоматично класифікувати персональні дані та виявляти ризики, пов’язані з їхньою обробкою, що значно полегшує роботу організацій [21]. В Україні такі інструменти поки що використовуються переважно великими корпораціями, але їхня популярність зростає [19].

Аналіз ризиків також включає оцінку людського фактора, оскільки помилки працівників є однією з основних причин витоків даних. Навчання персоналу та імітація фішингових атак допомагають оцінити рівень підготовки працівників і виявити слабкі місця в організаційних процесах [23]. В Україні такі заходи рекомендуються Міністерством внутрішніх справ як частина стратегії протидії кіберзлочинності [15].

Методи аналізу ризиків витоку даних є комплексними і поєднують технічні, організаційні та правові аспекти. Їхнє застосування дозволяє організаціям не лише виявляти потенційні загрози, а й розробляти ефективні стратегії захисту, що враховують специфіку обробки персональних даних.

1.5. Огляд інструментів для моніторингу зловживань

Моніторинг зловживань персональними даними є важливим компонентом системи кібербезпеки, оскільки дозволяє своєчасно виявляти несанкціонований доступ, витоки даних або інші протиправні дії. Інструменти для моніторингу зловживань включають програмне забезпечення для аналізу даних, системи

виявлення вторгнень, а також платформи для управління безпекою інформації. Ці інструменти допомагають організаціям не лише реагувати на інциденти, а й запобігати їм шляхом аналізу підозрілої активності в реальному часі [9]. В Україні такі інструменти набувають популярності через зростання кіберзагроз і вимоги законодавства щодо захисту персональних даних [22].

Одним із ключових інструментів для моніторингу є системи запобігання втраті даних (Data Loss Prevention, DLP). Такі системи, як Symantec DLP або Microsoft Purview, дозволяють відстежувати рух персональних даних у корпоративних мережах, хмарних сховищах і на кінцевих пристроях. Вони використовують політики безпеки для виявлення несанкціонованого копіювання, передачі чи видалення даних. Наприклад, Microsoft Purview автоматично класифікує чутливі дані, такі як номери кредитних карток чи паспортні дані, і блокує їхню передачу через незахищені канали [21]. В Україні DLP-системи активно застосовуються у фінансовому секторі, де захист клієнтських даних є критично важливим [20].

Системи управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) є ще одним важливим інструментом. Такі платформи, як Splunk або IBM QRadar, збирають і аналізують журнали подій із різних джерел (сервери, мережеві пристрої, додатки), щоб виявляти аномалії, які можуть свідчити про зловживання. Наприклад, SIEM-системи можуть виявити незвичну кількість запитів до бази даних або спроби входу з невідомих IP-адрес [9]. В Україні SIEM-системи використовуються великими організаціями, але їхнє впровадження ускладнене через високу вартість і потребу в кваліфікованому персоналі [20].

Інструменти для аналізу відкритих джерел (Open Source Intelligence, OSINT) також відіграють важливу роль у моніторингу зловживань. Такі інструменти, як Maltego або SpiderFoot, дозволяють відстежувати витоки даних у темному веб (Dark Web) або на публічних платформах. Наприклад, OSINT може виявити, чи були персональні дані організації виставлені на продаж у даркнеті після хакерської атаки [19]. В Україні OSINT набуває популярності

серед правоохоронних органів і приватних компаній, які займаються кібербезпекою [19]. Ці інструменти особливо корисні для виявлення зовнішніх загроз, таких як торгівля вкраденими даними.

Мобільні та хмарні платформи для моніторингу, такі як Google Chronicle або AWS Security Hub, забезпечують аналіз безпеки в хмарних середовищах. Вони дозволяють відстежувати доступ до даних, виявляти вразливості та аналізувати поведінку користувачів. Наприклад, AWS Security Hub може виявити неправильно налаштовані хмарні сховища, які часто стають причиною витоків даних [9]. В Україні хмарні рішення стають дедалі популярнішими через зростання використання хмарних сервісів, таких як Microsoft Azure чи Amazon Web Services [21].

Інструменти для моніторингу поведінки користувачів (User and Entity Behavior Analytics, UEBA) використовують штучний інтелект для виявлення аномальної активності. Наприклад, платформа Exabeam аналізує шаблони поведінки працівників і може сигналізувати про підозрілі дії, такі як завантаження великих обсягів даних у неробочий час [9]. Такі інструменти є особливо актуальними для протидії внутрішнім загрозам, які в Україні становлять значну частку інцидентів через низький рівень кіберграмотності [20]. UEBA-системи дозволяють організаціям швидко реагувати на потенційні зловживання, мінімізуючи збитки.

Для наочності нижче наведено таблицю, яка порівнює основні інструменти для моніторингу зловживань за їхніми функціональними можливостями, типом загроз, які вони виявляють, і сферою застосування.

Таблиця 1.1

Порівняльний аналіз інструментів для моніторингу зловживань персональними даними

Інструмент	Основні функції	Типи загроз	Сфера застосування	Переваги	Недоліки
Microsoft Purview	Класифікація даних, DLP, моніторинг передачі даних	Витоки, несанкціонована передача	Фінанси, охорона здоров'я, корпорації	Інтеграція з хмарними сервісами	Висока вартість
Splunk (SIEM)	Аналіз логів, виявлення аномалій	Хакерські атаки, внутрішні загрози	Великі організації, держсектор	Гнучкість, масштабованіст	Складність налаштування
Maltego (OSINT)	Аналіз відкритих джерел, відстеження витоків у даркнеті	Торгівля даними, зовнішні загрози	Кібербезпека, правоохоронні органи	Доступність, широкий охват	Обмежена автоматизація
AWS Security Hub	Моніторинг хмарних середовищ, аналіз вразливостей	Неправильна конфігурація, витоки	Хмарні сервіси, IT-компанії	Хмарна інтеграція	Залежність від AWS-екосистеми
Exabeam (UEBA)	Аналіз поведінки, виявлення аномалій	Внутрішні загрози, шахрайство	Корпорації, фінансові установи	Використання ШІ, точність	Потреба в навчанні персоналу

Ця таблиця демонструє, що вибір інструменту залежить від типу загроз, розміру організації та її технічних можливостей. В Україні впровадження таких інструментів ускладнене через обмежені бюджети та нестачу фахівців, але їхнє використання є необхідним для відповідності законодавчим вимогам і захисту даних [22].

1.6. Висновки до розділу

Перший розділ бакалаврської роботи присвячений аналізу зловживань персональними даними, що є ключовим етапом для розуміння проблематики їхнього захисту. У ході дослідження було встановлено, що персональні дані охоплюють широкий спектр інформації, від ідентифікаційних до поведінкових даних, які класифікуються за типом, способом збору та контекстом використання [1]. Їхня цінність у цифровій економіці зумовлює високий рівень загроз, серед яких виділяються крадіжка даних, шахрайство та несанкціоноване використання [6].

Джерела загроз для персональних даних включають зовнішні атаки (хакерство, фішинг), внутрішні фактори (помилки чи зловмисні дії працівників) і технологічні вразливості (застаріле програмне забезпечення, неправильно налаштовані системи) [7]. В Україні ці загрози посилюються через воєнний стан і швидку цифровізацію, що вимагає посилення заходів безпеки [14].

Методи аналізу ризиків, такі як якісний, кількісний аналіз і моделювання сценаріїв, дозволяють оцінити ймовірність і наслідки витоків даних, сприяючи розробці ефективних захисних стратегій [8]. У цьому контексті автоматизовані інструменти, такі як Microsoft Purview, відіграють важливу роль у підвищенні точності аналізу [21].

Огляд інструментів для моніторингу зловживань показав, що DLP-системи, SIEM, OSINT, хмарні платформи та UEBA-інструменти забезпечують комплексний підхід до виявлення та запобігання зловживанням [9]. В Україні їхнє впровадження є перспективним, але потребує подолання фінансових і кадрових обмежень [20]. Таким чином, аналіз зловживань персональними даними підкреслює необхідність поєднання правових, технічних і організаційних заходів для забезпечення їхньої безпеки, що буде розглянуто в наступних розділах.

РОЗДІЛ 2. ІНСТРУМЕНТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Класифікація інструментів захисту даних

Захист персональних даних є багатогранним процесом, що вимагає використання різноманітних інструментів для забезпечення конфіденційності, цілісності та доступності інформації. Інструменти захисту даних можна класифікувати за кількома критеріями, такими як їхня функціональність, сфера застосування, технічна реалізація та рівень автоматизації. Така класифікація дозволяє організаціям вибирати оптимальні рішення залежно від типу даних, загроз і регуляторних вимог [10]. В Україні ці інструменти набувають особливого значення через зростання кіберзагроз і вимоги Закону України «Про захист персональних даних» [24].

За функціональністю інструменти захисту даних поділяються на кілька основних категорій: шифрування, управління доступом, запобігання втраті даних (DLP), моніторинг і аудит безпеки, а також антивірусне програмне забезпечення. Технології шифрування, такі як AES або RSA, захищають дані від несанкціонованого доступу шляхом їхнього кодування [3]. Системи управління доступом (Identity and Access Management, IAM), наприклад, Okta чи Microsoft Azure Active Directory, обмежують доступ до даних лише для авторизованих користувачів. DLP-системи, такі як Symantec DLP, відстежують і блокують несанкціоновану передачу даних [21]. Моніторинг і аудит безпеки включають SIEM-системи, такі як Splunk, які аналізують журнали подій для виявлення аномалій [9]. Антивіруси, такі як ESET чи Kaspersky, захищають від шкідливого програмного забезпечення, яке може компрометувати дані [14].

За сферою застосування інструменти поділяються на ті, що використовуються в локальних мережах, хмарних середовищах або на кінцевих пристроях. Наприклад, локальні інструменти, такі як брандмауери Cisco, захищають корпоративні мережі, тоді як хмарні рішення, як AWS Security Hub, забезпечують безпеку даних у хмарних сховищах [9]. Мобільні рішення, наприклад, Mobile Device Management (MDM) від VMware, контролюють доступ

до даних із смартфонів чи планшетів, що є актуальним в умовах зростання віддаленої роботи [10]. В Україні хмарні інструменти стають дедалі популярнішими через перехід компаній до хмарних платформ, таких як Microsoft Azure [21].

За рівнем автоматизації розрізняють автоматизовані, напівавтоматизовані та ручні інструменти. Автоматизовані системи, такі як Microsoft Purview, самостійно класифікують дані та виявляють порушення політик безпеки [21]. Напівавтоматизовані інструменти, наприклад, системи тестування на проникнення (penetration testing), такі як Metasploit, потребують участі фахівців для аналізу результатів [19]. Ручні методи, такі як аудит безпеки чи навчання персоналу, є менш ефективними в умовах великих обсягів даних, але залишаються важливими для підвищення кіберграмотності [23]. В Україні ручні методи часто застосовуються через обмежені бюджети, але поступово замінюються автоматизованими рішеннями [20].

За технічною реалізацією інструменти поділяються на апаратні, програмні та гібридні. Апаратні рішення включають захищені носії інформації, такі як USB-токени YubiKey, які використовуються для двофакторної автентифікації [14]. Програмні інструменти, як-от антивіруси чи DLP-системи, є більш гнучкими та легшими в інтеграції. Гібридні рішення, наприклад, брандмауери з інтегрованими функціями DLP, поєднують переваги обох підходів [3]. В Україні апаратні рішення менш поширені через їхню високу вартість, але програмні інструменти активно використовуються в державному та приватному секторах [24].

Нижче наведено таблицю, яка систематизує основні категорії інструментів захисту даних за їхньою функціональністю, прикладами та перевагами.

Таблиця 2.1

Класифікація інструментів захисту персональних даних

Категорія	Приклади інструментів	Основні функції	Переваги	Недоліки
Шифрування	AES, RSA, VeraCrypt	Кодування даних для захисту від доступу	Високий рівень безпеки	Потреба в управлінні ключами
Управління доступом	Okta, Azure Active Directory	Обмеження доступу за ролями	Гнучкість, інтеграція з системами	Складність налаштування
Запобігання втраті даних	Symantec DLP, Microsoft Purview	Моніторинг і блокування передачі даних	Автоматизація, точність	Висока вартість
Моніторинг і аудит	Splunk, IBM QRadar	Виявлення аномалій, аналіз логів	Комплексний аналіз	Потреба в кваліфікованих фахівцях
Антивірусне ПЗ	ESET, Kaspersky	Захист від шкідливого ПЗ	Простота використання	Обмежена ефективність проти нових загроз

Ця таблиця демонструє різноманітність інструментів і їхню адаптивність до різних потреб. Вибір інструменту залежить від типу даних, рівня загроз і фінансових можливостей організації.

2.2. Технології шифрування та їх застосування

Технології шифрування є основою захисту персональних даних, оскільки вони забезпечують конфіденційність інформації шляхом перетворення її у формат, який неможливо прочитати без спеціального ключа. Шифрування застосовується на різних рівнях – від зберігання даних до їхньої передачі – і є обов’язковим компонентом відповідності регуляторним вимогам, таким як GDPR чи Закон України «Про захист персональних даних» [5]. У сучасних

системах використовуються різні алгоритми шифрування, кожен із яких має свої особливості та сфери застосування [3].

Симетричне шифрування, наприклад, алгоритм Advanced Encryption Standard (AES), використовує один ключ для шифрування та дешифрування. AES із довжиною ключа 256 біт є стандартом для захисту даних у банківських системах, хмарних сховищах і мобільних додатках. Його перевагою є висока швидкість обробки, що робить його ефективним для великих обсягів даних [3]. Наприклад, AES застосовується в інструментах, таких як VeraCrypt, для шифрування дисків і файлів. В Україні банки використовують AES для захисту транзакційних даних, що відповідає вимогам Національного банку України [22].

Асиметричне шифрування, таке як RSA або Elliptic Curve Cryptography (ECC), використовує пару ключів – відкритий і закритий. Відкритий ключ шифрує дані, а закритий – дешифрує. RSA широко застосовується для безпечного обміну ключами та цифрових підписів, наприклад, у протоколах HTTPS і SSL/TLS, які захищають передачу даних у веббраузерах [5]. ECC, завдяки меншій довжині ключа при високому рівні безпеки, використовується в мобільних пристроях і IoT. В Україні асиметричне шифрування застосовується в системах електронного підпису, таких як «Дія.Підпис» [24].

Гомоморфне шифрування є новітньою технологією, яка дозволяє обробляти зашифровані дані без їхнього дешифрування. Це особливо корисно для хмарних обчислень, де дані потрібно аналізувати, не розкриваючи їх. Наприклад, гомоморфне шифрування може використовуватися для аналізу медичних даних без порушення конфіденційності [10]. В Україні ця технологія поки що перебуває на етапі досліджень, але має потенціал для застосування в державних реєстрах [20].

Шифрування на рівні баз даних і файлових систем забезпечує захист даних у стані спокою (data at rest). Інструменти, такі як Oracle Transparent Data Encryption або Microsoft SQL Server Always Encrypted, дозволяють шифрувати дані в базах даних, що є критично важливим для захисту чутливої інформації, наприклад, у медичній чи фінансовій сферах [21]. В Україні такі рішення

застосовуються в державних установах для захисту реєстрів, але їхнє впровадження ускладнене через високу вартість [22].

Шифрування також відіграє ключову роль у захисті даних під час передачі (data in transit). Протоколи TLS і VPN забезпечують безпечний обмін інформацією через інтернет. Наприклад, VPN-сервіси, такі як NordVPN, використовують AES-256 для захисту даних користувачів від перехоплення [3]. В Україні використання VPN стало особливо актуальним у період воєнного стану для забезпечення безпеки комунікацій [14].

Нижче наведено таблицю, яка порівнює основні технології шифрування за їхніми характеристиками та застосуванням.

Таблиця 2.2

Порівняння технологій шифрування

Технологія	Тип шифрування	Основні алгоритми	Застосування	Переваги	Недоліки
Симетричне шифрування	Один ключ	AES-256, DES	Шифрування файлів, баз даних	Висока швидкість	Складність управління ключами
Асиметричне шифрування	Пара ключів	RSA, ECC	Цифрові підписи, HTTPS, VPN	Висока безпека	Низька швидкість обробки
Гомоморфне шифрування	Обробка зашифрованих даних	SEAL, HElib	Хмарні обчислення, медичні дані	Захист під час аналізу	Висока обчислювальна складність
Шифрування баз даних	Захист у стані спокою	TDE, Always Encrypted	Бази даних, реєстри	Прозора інтеграція	Обмежена гнучкість

Ця таблиця показує, що вибір технології шифрування залежить від потреб організації та типу даних, які необхідно захистити. В Україні шифрування є обов’язковим елементом кібербезпеки, але потребує подальшого розвитку інфраструктури та навчання фахівців.

2.3. Системи управління доступом до даних

Системи управління доступом до даних (Identity and Access Management, IAM) є критично важливим інструментом захисту персональних даних, оскільки вони забезпечують контроль над тим, хто, коли і як може отримати доступ до інформації. IAM-системи дозволяють організаціям обмежувати доступ до чутливих даних, таких як фінансові чи медичні відомості, лише для авторизованих користувачів, мінімізуючи ризики внутрішніх і зовнішніх загроз. У контексті зростання кіберзагроз і регуляторних вимог, таких як GDPR та Закон України «Про захист персональних даних», ці системи стають незамінними для забезпечення безпеки [13]. В Україні IAM-системи активно застосовуються у банківському секторі, державних установах і великих корпораціях [25].

Основним принципом роботи IAM є забезпечення ідентифікації, автентифікації та авторизації користувачів. Ідентифікація визначає, хто намагається отримати доступ (наприклад, за логіном чи ID). Автентифікація підтверджує особу користувача через паролі, біометричні дані чи двофакторну автентифікацію (2FA). Авторизація визначає, які дії користувач може виконувати, наприклад, переглядати, редагувати чи видаляти дані [10]. Наприклад, система Okta дозволяє налаштувати рольовий доступ (Role-Based Access Control, RBAC), де працівники отримують доступ лише до тих даних, які необхідні для їхньої роботи. Це знижує ризик витоків через неналежне використання даних працівниками [23].

Системи IAM поділяються на кілька типів залежно від їхньої архітектури та функціональності. Локальні системи, такі як Microsoft Active Directory, встановлюються в корпоративних мережах і підходять для організацій із власною інфраструктурою. Хмарні IAM, наприклад, Microsoft Azure Active Directory або AWS Identity and Access Management, забезпечують гнучкість і масштабованість, що є актуальним для компаній, які використовують хмарні сервіси [21]. Гібридні системи поєднують локальні та хмарні підходи, що дозволяє інтегрувати старі системи з новими технологіями. В Україні хмарні

IAM набувають популярності через перехід до хмарних платформ, таких як Microsoft Azure, але локальні рішення все ще домінують у державному секторі через вимоги до локалізації даних [25].

Однією з ключових функцій IAM є двофакторна автентифікація (2FA), яка значно підвищує рівень безпеки. 2FA вимагає додаткового підтвердження особи, наприклад, через SMS-код, додаток-аутентифікатор (Google Authenticator, Microsoft Authenticator) або апаратний токен (YubiKey). За даними досліджень, використання 2FA знижує ризик компрометації облікових записів на 99% [14]. В Україні 2FA активно впроваджується в банківських додатках і державних сервісах, таких як «Дія», для захисту персональних даних громадян [13]. Наприклад, доступ до електронного підпису в «Дія» вимагає додаткової верифікації, що відповідає рекомендаціям Міністерства внутрішніх справ [14].

Іншою важливою функцією IAM є управління привілейованим доступом (Privileged Access Management, PAM). PAM-системи, такі як CyberArk або BeyondTrust, контролюють доступ адміністраторів до критично важливих систем, таких як бази даних чи сервери. Вони дозволяють записувати сеанси доступу, обмежувати тимчасовий доступ і автоматично змінювати паролі після використання. Це особливо актуально для протидії внутрішнім загрозам, які в Україні становлять значну частку інцидентів через низький рівень кіберграмотності [25]. Наприклад, неналежне управління привілейованим доступом може призвести до витоку даних, як це було в кількох гучних інцидентах у державних установах [13].

IAM-системи також підтримують відповідність регуляторним вимогам, таким як GDPR, яке вимагає чіткого контролю доступу до персональних даних і документування всіх операцій із ними [10]. У контексті українського законодавства IAM допомагають організаціям виконувати вимоги Закону України «Про захист персональних даних», зокрема щодо обмеження доступу та забезпечення прозорості обробки даних [24]. Наприклад, системи, такі як SailPoint, дозволяють автоматично генерувати звіти про доступ до даних, що полегшує проходження аудитів [21].

Попри численні переваги, IAM-системи мають певні виклики. Налаштування таких систем може бути складним і вимагати значних ресурсів, особливо для малих організацій. У Україні впровадження IAM ускладнене через брак кваліфікованих фахівців і обмежені бюджети, особливо в державному секторі [25]. Крім того, неправильна конфігурація IAM може призвести до надмірного обмеження доступу, що знижує продуктивність, або, навпаки, до надто широкого доступу, що підвищує ризики [14]. Для подолання цих проблем необхідно проводити регулярне навчання персоналу та аудит систем.

Системи управління доступом також інтегруються з іншими інструментами захисту, такими як DLP чи SIEM, для створення комплексного підходу до безпеки. Наприклад, Microsoft Azure Active Directory може працювати разом із Microsoft Purview для моніторингу доступу та виявлення несанкціонованої передачі даних [21]. В Україні такі інтеграції поки що обмежені, але їхня популярність зростає разом із цифровізацією [13].

Системи управління доступом до даних є незамінним інструментом для захисту персональних даних, оскільки вони дозволяють контролювати доступ, мінімізувати ризики внутрішніх і зовнішніх загроз і забезпечувати відповідність регуляторним вимогам. В Україні їхнє впровадження є перспективним, але потребує подолання організаційних і фінансових бар'єрів.

2.4. Програмне забезпечення для запобігання витокам

Програмне забезпечення для запобігання витокам даних (Data Loss Prevention, DLP) є ключовим інструментом захисту персональних даних, спрямованим на виявлення, моніторинг і блокування несанкціонованої передачі чи використання інформації. DLP-системи допомагають організаціям мінімізувати ризики витоків, спричинених як зовнішніми загрозами, так і внутрішніми факторами, наприклад, помилками чи зловмисними діями працівників. У контексті регуляторних вимог, таких як GDPR та Закон України «Про захист персональних даних», DLP відіграє важливу роль у забезпеченні відповідності стандартам безпеки [16]. В Україні ці системи набувають

популярності, особливо у фінансовому, медичному та державному секторах, де захист чутливих даних є критично важливим [27].

DLP-системи функціонують на основі політик безпеки, які визначають, які дані є чутливими, і встановлюють правила їхньої обробки. Основні функції DLP включають класифікацію даних, моніторинг їхнього руху та блокування несанкціонованих дій. Наприклад, DLP може виявити спробу відправлення файлу з персональними даними через електронну пошту чи хмарний сервіс і автоматично заблокувати таку дію [11]. Популярні DLP-системи, такі як Symantec DLP, Forcepoint DLP і Microsoft Purview, використовують комбінацію сигнатурного аналізу, машинного навчання та аналізу поведінки для точного виявлення чутливих даних, таких як номери паспортів, банківських карток чи медичні записи [21].

За типом розгортання DLP-системи поділяються на мережеві, хостові та хмарні. Мережеві DLP, наприклад, Symantec Network Prevent, контролюють дані, що передаються через корпоративні мережі, включаючи електронну пошту, вебтрафіки чи FTP. Хостові DLP, такі як McAfee Total Protection, встановлюються на кінцевих пристроях (комп’ютери, смартфони) і відстежують дії користувачів, наприклад, копіювання даних на USB-накопичувачі [11]. Хмарні DLP, такі як Microsoft Purview, інтегруються з хмарними сервісами (Microsoft 365, Google Drive) і забезпечують захист даних у хмарних середовищах. В Україні хмарні DLP стають популярними через зростання використання хмарних платформ, але мережеві та хостові рішення залишаються поширеними в організаціях із локальною інфраструктурою [20].

Однією з ключових можливостей DLP є автоматична класифікація даних. Сучасні системи використовують шаблони (регулярні вирази) і машинне навчання для ідентифікації чутливих даних, таких як ІПН, номери телефонів чи медична інформація. Наприклад, Microsoft Purview може автоматично розпізнавати дані, що підпадають під вимоги GDPR, і застосовувати до них відповідні політики захисту [21]. В Україні такі функції є особливо актуальними для відповідності Закону України «Про захист персональних даних», який

вимагає чіткого визначення та захисту чутливих даних [16]. Крім того, DLP-системи дозволяють створювати звіти про інциденти, що полегшує проходження аудитів безпеки [27].

DLP також ефективно протидіє внутрішнім загрозам, які в Україні становлять значну частку витоків через низький рівень кіберграмотності. Наприклад, система Forcepoint DLP може виявити, якщо працівник намагається надіслати конфіденційний документ на особистий email, і повідомити адміністратора або заблокувати дію [11]. Такі можливості допомагають організаціям не лише запобігати витокам, а й підвищувати обізнаність працівників щодо правил обробки даних. Міністерство внутрішніх справ України рекомендує використовувати DLP у поєднанні з навчанням персоналу для зниження ризиків внутрішніх порушень [14].

Попри численні переваги, впровадження DLP-систем пов’язане з певними викликами. По-перше, налаштування політик безпеки вимагає глибокого розуміння структури даних організації, що може бути складним для малих компаній. По-друге, DLP може створювати помилкові спрацьовування (false positives), наприклад, блокуючи легітимні дії користувачів, що знижує продуктивність [21]. В Україні додатковим бар’єром є висока вартість ліцензій і брак фахівців із досвідом роботи з DLP, особливо в державному секторі [20]. Для подолання цих проблем рекомендуються поетапне впровадження DLP і використання хмарних рішень, які знижують витрати на інфраструктуру [27].

DLP-системи також інтегруються з іншими інструментами безпеки, такими як IAM і SIEM, для створення комплексного підходу до захисту. Наприклад, Microsoft Purview може працювати разом із Azure Active Directory для контролю доступу та моніторингу передачі даних, забезпечуючи єдину екосистему безпеки [21]. В Україні такі інтеграції поки що обмежені, але мають значний потенціал у контексті цифровізації державних і комерційних сервісів [16].

Ще однією важливою функцією DLP є реагування на інциденти. Системи можуть автоматично ізолювати скомпрометовані пристрої, шифрувати чутливі

дані перед передачею або повідомляти адміністраторів про порушення. Наприклад, Symantec DLP дозволяє налаштувати автоматичне шифрування файлів, які містять персональні дані, перед їхнім надсиланням через незахищені канали [11]. В Україні такі функції є особливо актуальними для захисту державних реєстрів, які часто стають мішенню кібератак [14].

Програмне забезпечення для запобігання витокам є потужним інструментом захисту персональних даних, що поєднує моніторинг, класифікацію та блокування несанкціонованих дій. В Україні впровадження DLP-систем сприяє підвищенню рівня безпеки, але потребує подолання фінансових і організаційних бар'єрів, а також інтеграції з іншими інструментами для забезпечення комплексного захисту.

2.5. Висновки до розділу

Другий розділ бакалаврської роботи присвячений дослідженню інструментів захисту персональних даних, які є основою для забезпечення їхньої конфіденційності, цілісності та доступності в умовах зростання кіберзагроз. Проведений аналіз дозволив систематизувати ключові інструменти, оцінити їхню ефективність і визначити особливості їхнього застосування в Україні.

Класифікація інструментів захисту даних показала, що вони поділяються за функціональністю (шифрування, управління доступом, DLP, моніторинг, антивіруси), сферою застосування (локальні, хмарні, мобільні), рівнем автоматизації та технічною реалізацією [10]. Така систематизація допомагає організаціям вибирати оптимальні рішення залежно від їхніх потреб і ресурсів. В Україні хмарні інструменти, такі як Microsoft Purview, набувають популярності, але локальні рішення залишаються поширеними через регуляторні вимоги до локалізації даних [24].

Технології шифрування, такі як AES, RSA та гомоморфне шифрування, є основою захисту даних як у стані спокою, так і під час передачі [3]. Вони забезпечують високий рівень безпеки, але потребують належного управління ключами та адаптації до конкретних сценаріїв, наприклад, захисту державних

реєстрів в Україні [22]. Симетричне та асиметричне шифрування широко застосовуються в банківських і державних системах, тоді як гомоморфне шифрування має перспективу для хмарних обчислень.

Системи управління доступом до даних (IAM) відіграють ключову роль у контролі доступу до персональних даних, мінімізуючи ризики внутрішніх і зовнішніх загроз [13]. Функції, такі як двофакторна автентифікація (2FA) і управління привілейованим доступом (PAM), значно підвищують безпеку, що підтверджується їхнім активним використанням у сервісах, таких як «Дія» [14]. Проте в Україні впровадження IAM ускладнене через брак фахівців і складність інтеграції з застарілими системами.

Програмне забезпечення для запобігання витокам (DLP) забезпечує моніторинг і блокування несанкціонованої передачі даних, що є особливо важливим для захисту чутливої інформації, такої як медичні чи фінансові дані [11]. Системи, такі як Symantec DLP і Microsoft Purview, дозволяють автоматично класифікувати дані та реагувати на інциденти, але їхнє впровадження в Україні обмежене високою вартістю та потребою в кваліфікованому персоналі [20].

Інструменти захисту персональних даних формують комплексний підхід до безпеки, поєднуючи технічні, організаційні та правові аспекти. В Україні їхнє застосування сприяє виконанню законодавчих вимог і підвищенню рівня кібербезпеки, але потребує подолання фінансових, технічних і кадрових обмежень. Подальший розвиток цих інструментів і їхня інтеграція з іншими системами безпеки є необхідними для ефективної протидії зловживанням персональними даними, що буде розглянуто в наступному розділі.

РОЗДІЛ 3. ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ЗАХИСТУ ДАНИХ

3.1. Розробка політики захисту персональних даних

Розробка політики захисту персональних даних є фундаментальним кроком для забезпечення безпеки інформації в організаціях. Політика захисту даних визначає принципи, правила та процедури обробки, зберігання й передачі персональних даних, а також встановлює відповідальність працівників і керівництва за їх дотримання. У контексті українського законодавства, зокрема Закону України «Про захист персональних даних» №2297-VI, така політика є обов'язковою для організацій, які обробляють персональні дані [12]. Крім того, вона допомагає відповідати міжнародним стандартам, таким як GDPR, і знижувати ризики зловживань, включаючи витоки, шахрайство та несанкціонований доступ [17]. У цьому підрозділі запропоновано практичний підхід до розробки політики захисту персональних даних, який включає алгоритм створення політики та рекомендації щодо її впровадження.

Розробка політики захисту персональних даних вимагає системного підходу, який враховує організаційні, технічні та правові аспекти. Запропонований алгоритм складається з п'яти основних етапів, кожен із яких спрямований на створення ефективної та адаптованої до потреб організації політики.

1. Аналіз контексту організації та даних. Першим кроком є визначення обсягу персональних даних, які обробляє організація, їхньої чутливості та джерел. Це включає ідентифікаційні дані (ПІБ, ІПН), фінансові (банківські рахунки), медичні чи поведінкові дані. Наприклад, фінансова установа може обробляти дані про транзакції, тоді як медична організація – інформацію про здоров'я. Для цього використовуються інструменти класифікації даних, такі як Microsoft Purview, які автоматично визначають чутливі дані [21]. В Україні цей етап також передбачає аналіз відповідності Закону України «Про захист

персональних даних», який вимагає чіткого визначення категорій даних і цілей їхньої обробки [12]. Результатом є детальний перелік даних, їхніх джерел (CRM-системи, бази даних, хмарні сервіси) і пов’язаних ризиків.

2. Оцінка ризиків і загроз. На цьому етапі проводиться аналіз ризиків витоку чи зловживання даними з використанням методів, описаних у розділі 1.4, таких як якісний і кількісний аналіз [8]. Наприклад, організація може оцінити ймовірність фішингових атак чи внутрішніх витоків через неналежне управління доступом. В Україні особливу увагу слід приділяти зовнішнім загрозам, пов’язаним із кібератаками в умовах воєнного стану, а також внутрішнім загрозам через низький рівень кіберграмотності [17]. Результати оцінки формують основу для визначення пріоритетних заходів захисту, таких як шифрування чи двофакторна автентифікація.
3. Розробка структури політики. Політика повинна мати чітку структуру, яка включає такі розділи:
   - Мета і сфера застосування: Визначення цілей політики (захист конфіденційності, відповідність законодавству) і перелік систем/процесів, на які вона поширюється.
   - Визначення та класифікація даних: Опис категорій персональних даних і критеріїв їхньої чутливості.
   - Правила обробки даних: Процедури збору, зберігання, передачі та знищення даних, включаючи вимоги до шифрування (наприклад, AES-256) і управління доступом [3].
   - Ролі та відповідальність: Визначення обов’язків працівників, адміністраторів і керівництва щодо захисту даних.
   - Реагування на інциденти: Процедури виявлення, повідомлення та усунення порушень безпеки, наприклад, витоків даних.

— Аудит і перегляд: Періодичність перевірки політики (наприклад, раз на рік) і механізми її оновлення. У контексті України політика має враховувати вимоги Уповноваженого Верховної Ради з прав людини щодо повідомлення про обробку даних і захисту прав суб'єктів [12].

4. Інтеграція технічних і організаційних заходів. Політика повинна передбачати використання технічних інструментів, таких як DLP-системи (Symantec DLP, Microsoft Purview) для моніторингу передачі даних і IAM-системи (Okta, Azure Active Directory) для контролю доступу [21]. Організаційні заходи включають навчання персоналу, розробку інструкцій і впровадження двофакторної автентифікації (2FA), що знижує ризики компрометації облікових записів [14]. В Україні особливу увагу слід приділяти навчанню працівників, оскільки внутрішні загрози часто виникають через необізнаність [17]. Наприклад, імітація фішингових атак може допомогти оцінити готовність персоналу до реальних загроз.
5. Тестування, впровадження та моніторинг. Перед впровадженням політика тестується в пілотному режимі, наприклад, у межах одного відділу. Це дозволяє виявити недоліки, такі як надмірне обмеження доступу чи недостатня чіткість процедур. Після тестування політика затверджується керівництвом і доводиться до відома всіх працівників через тренінги чи внутрішні портали. Моніторинг виконання політики здійснюється за допомогою аудитів безпеки та інструментів SIEM (Splunk, IBM QRadar), які аналізують журнали подій для виявлення порушень [9]. В Україні регулярні аудити рекомендуються Уповноваженим з прав людини для забезпечення відповідності законодавству [12].

Для ефективного впровадження політики захисту персональних даних в Україні пропонується врахувати такі рекомендації:

— Адаптація до локального контексту: Політика має враховувати специфіку українського законодавства, зокрема вимоги до локалізації

даних і повідомлення суб'єктів про обробку [12]. Наприклад, організації, які працюють із державними реєстрами, повинні забезпечити шифрування даних і обмежений доступ відповідно до стандартів безпеки.

- Пріоритет на автоматизацію: Використання автоматизованих інструментів, таких як Microsoft Purview, дозволяє зменшити людський фактор і підвищити точність виявлення чутливих даних [21]. Для малих організацій із обмеженим бюджетом рекомендуються хмарні DLP-рішення, які знижують витрати на інфраструктуру.
- Фокус на внутрішніх загрозах: В Україні значна частка витоків даних пов'язана з помилками чи зловмисними діями працівників [17]. Тому політика повинна включати регулярне навчання, тестування на фішинг і чіткі інструкції щодо використання даних.
- Інтеграція з іншими процесами: Політика має бути частиною загальної системи кібербезпеки, інтегруючись із IAM, DLP і SIEM-системами. Наприклад, Azure Active Directory може працювати разом із Purview для одночасного контролю доступу та моніторингу передачі даних [21].
- Гнучкість і оновлення: Політика повинна регулярно переглядатися (наприклад, раз на рік або після значних інцидентів) для врахування нових загроз, таких як кібератаки, пов'язані з воєнним станом, чи змін у законодавстві [14].

Запропонований алгоритм розробки політики захисту персональних даних є універсальним і може застосовуватися в організаціях різного масштабу – від малих підприємств до державних установ. У контексті України він враховує локальні виклики, такі як обмежені бюджети, низький рівень кіберграмотності та підвищені ризики кібератак. Політика, розроблена за цим алгоритмом, забезпечує відповідність законодавчим вимогам, знижує ризики зловживань і підвищує довіру клієнтів до організації. Наприклад, фінансова установа, яка впровадила таку політику, може уникнути штрафів за порушення GDPR чи українського законодавства і захистити дані клієнтів від шахрайства [17].

Практична реалізація політики також сприяє формуванню культури кібербезпеки в організації. Регулярне навчання та використання автоматизованих інструментів, таких як DLP і IAM, дозволяють не лише запобігати інцидентам, а й швидко реагувати на них, мінімізуючи збитки. У майбутньому цей підхід може бути доповнений аналізом ефективності впроваджених заходів і адаптацією до нових технологій, таких як гомоморфне шифрування чи блокчейн для захисту даних [10].

Розробка політики захисту персональних даних є комплексним процесом, який поєднує правові, технічні та організаційні заходи. Її впровадження в Україні сприятиме підвищенню рівня безпеки даних і відповідності сучасним стандартам, що є передумовою для ефективного захисту від зловживань.

3.2. Навчання персоналу з питань безпеки даних

Навчання персоналу з питань безпеки даних є одним із ключових елементів захисту персональних даних, оскільки людський фактор залишається основною причиною багатьох інцидентів, пов’язаних із витоками інформації. В Україні, де низький рівень кіберграмотності працівників є значною проблемою, навчання набуває особливої актуальності [18]. Воно спрямоване на підвищення обізнаності щодо загроз, формування навичок безпечної роботи з даними та забезпечення відповідності вимогам законодавства, зокрема Закону України «Про захист персональних даних» №2297-VI [24]. У цьому підрозділі запропоновано практичний підхід до організації навчання персоналу, який включає розробку програми навчання, методи оцінки ефективності та рекомендації для впровадження в українських організаціях.

Навчання персоналу з питань безпеки даних має бути систематичним, регулярним і адаптованим до потреб організації. Запропонований підхід складається з чотирьох етапів, які охоплюють планування, проведення, оцінку та вдосконалення програми навчання.

1. Планування програми навчання. На першому етапі визначаються цілі, аудиторія та зміст програми. Цілі можуть включати підвищення

обізнаності про фішинг, навчання використання двофакторної автентифікації (2FA) або ознайомлення з політикою захисту даних [14]. Аудиторія поділяється на групи залежно від ролей: адміністратори систем потребують поглиблених знань про IAM і DLP-системи, тоді як звичайні працівники – базових навичок безпечної роботи з даними [21]. Зміст програми має охоплювати:

- Основи кібербезпеки: розпізнавання фішингових листів, безпечне використання паролів.
- Правові аспекти: вимоги Закону України «Про захист персональних даних» і GDPR [12].
- Практичні інструменти: використання VPN, шифрування, антивірусів (наприклад, ESET) [14].
- Реагування на інциденти: дії у разі виявлення витоку даних. В Україні особливу увагу слід приділяти локальним загрозам, таким як кібератаки в умовах воєнного стану [18].

2. Проведення навчання. Навчання може проводитися у різних форматах: очні тренінги, онлайн-курси, симуляції та інтерактивні ігри. Очні тренінги ефективні для малих організацій, де можна провести практичні заняття, наприклад, із налаштування 2FA через Google Authenticator [14]. Онлайн-курси, такі як платформи KnowBe4 або Coursera, дозволяють масштабувати навчання для великих компаній і є економічно вигідними [26]. Симуляції фішингових атак, які імітують реальні загрози, допомагають оцінити реакцію працівників і навчити їх розпізнавати підозрілі листи [18]. В Україні онлайн-навчання є перспективним через доступність і можливість охопити віддалених працівників, але потребує адаптації до української мови та локального контексту [24].
3. Оцінка ефективності навчання. Для оцінки ефективності використовуються тести, практичні завдання та аналіз поведінки

працівників після навчання. Тести можуть перевіряти знання про типи загроз (фішинг, ransomware) або правила обробки даних [12]. Практичні завдання включають симуляцію інцидентів, наприклад, виявлення підозрілого листа чи налаштування шифрування файлу за допомогою VeraCrypt [3]. Аналіз поведінки проводиться за допомогою DLP-систем, які відстежують, чи зменшилася кількість порушень, таких як надсилання чутливих даних через незахищені канали [21]. В Україні оцінка ефективності часто ускладнена через брак автоматизованих інструментів, але використання хмарних DLP, таких як Microsoft Purview, може спростити цей процес [21].

4. Вдосконалення та регулярне оновлення. Програма навчання має регулярно оновлюватися (наприклад, раз на півроку) з урахуванням нових загроз, змін у законодавстві чи технологіях. Наприклад, поява нових методів фішингу чи оновлення GDPR може вимагати додавання нових модулів [17]. Зворотний зв'язок від працівників допомагає вдосконалити програму, наприклад, зробити її більш інтерактивною чи скоротити тривалість занять. В Україні регулярне оновлення є особливо важливим через швидке зростання кіберзагроз, пов'язаних із воєнним станом, і потребу в адаптації до місцевих реалій [18].

Для ефективного навчання персоналу в українських організаціях пропонується врахувати такі рекомендації:

— Фокус на локальних загрозах: Навчання має враховувати специфіку України, зокрема ризики кібератак на державні та комерційні системи в умовах воєнного стану. Наприклад, працівники повинні знати, як розпізнавати фішингові листи, що маскуються під офіційні повідомлення від державних органів [18].

— Використання доступних інструментів: Для організацій із обмеженим бюджетом рекомендуються безкоштовні або недорогі платформи, такі як Google Security Awareness або локальні курси від IT Education Center [19]. Хмарні рішення, такі як Microsoft Purview, можуть

використовуватися для моніторингу ефективності навчання без значних витрат [21].

— Інтерактивність і практичність: Симуляції фішингових атак і практичні завдання, такі як налаштування VPN чи шифрування файлів, підвищують залученість працівників. Наприклад, імітація атаки може показати, скільки працівників відкрили підозріле посилання, що мотивує їх бути обережнішими [14].
— Регулярність і обов'язковість: Навчання має бути обов'язковим для всіх працівників і проводитися щонайменше раз на рік. Нових працівників слід навчати протягом першого місяця роботи, щоб уникнути порушень через необізнаність [12].
— Інтеграція з політикою безпеки: Навчання має бути частиною політики захисту даних, описаної в підрозділі 3.1, і доповнювати технічні заходи, такі як IAM і DLP [21]. Наприклад, працівники повинні знати, як використовувати 2FA в Azure Active Directory для доступу до корпоративних систем.

Запропонований підхід до навчання персоналу є універсальним і може застосовуватися в організаціях різного масштабу – від малих підприємств до державних установ. У контексті України він враховує локальні виклики, такі як низький рівень кіберграмотності, обмежені бюджети та підвищені кіберризики. Навчання, проведене за цим підходом, знижує ймовірність внутрішніх витоків даних, які становлять значну частку інцидентів в Україні, і сприяє формуванню культури кібербезпеки [18].

Практична реалізація програми навчання дозволяє організаціям не лише відповідати вимогам законодавства, а й підвищувати ефективність інших інструментів захисту, таких як DLP чи IAM. Наприклад, працівники, які пройшли навчання, рідше порушують політики безпеки, що знижує навантаження на DLP-системи [21]. У довгостроковій перспективі це сприяє зниженню фінансових і репутаційних ризиків, пов'язаних із зловживаннями персональними даними.

Навчання персоналу з питань безпеки даних є невід'ємною частиною комплексного захисту персональних даних. Його систематичне впровадження в Україні сприятиме підвищенню кіберграмотності, зниженню ризиків і відповідності регуляторним вимогам, що є важливим кроком до ефективного запобігання зловживанням.

3.3. Аудит та тестування систем захисту

Аудит і тестування систем захисту персональних даних є критично важливими процесами для оцінки ефективності впроваджених заходів безпеки, виявлення вразливостей і забезпечення відповідності регуляторним вимогам, таким як Закон України «Про захист персональних даних» №2297-VI та GDPR [22]. Ці процеси дозволяють організаціям не лише перевірити надійність технічних і організаційних заходів, а й своєчасно усунути недоліки, що знижує ризики зловживань, таких як витоки даних чи несанкціонований доступ. В Україні, де кіберзагрози посилюються через воєнний стан і швидку цифровізацію, аудит і тестування набувають особливої актуальності [28]. У цьому підрозділі запропоновано практичний підхід до організації аудиту та тестування систем захисту, який включає алгоритм їх проведення, методи оцінки та рекомендації для українських організацій.

Аудит і тестування систем захисту є взаємодоповнювальними процесами, які охоплюють аналіз політик, технічних засобів і поведінки користувачів. Запропонований підхід складається з чотирьох етапів, які забезпечують комплексну оцінку безпеки та сприяють її вдосконаленню.

1. Планування аудиту та тестування. На першому етапі визначаються цілі, обсяг і методи оцінки. Цілі можуть включати перевірку відповідності законодавству, оцінку ефективності DLP чи IAM-систем, або виявлення вразливостей у хмарних сховищах [21]. Обсяг аудиту охоплює всі системи, що обробляють персональні дані: бази даних, мережеві пристрої, кінцеві пристрої та хмарні сервіси. Методи включають аналіз документації, тестування на проникнення (penetration testing) і

сканування вразливостей. В Україні планування має враховувати вимоги Уповноваженого Верховної Ради з прав людини щодо регулярного аудиту обробки персональних даних [23]. Наприклад, фінансова установа може запланувати аудит для перевірки захисту транзакційних даних відповідно до стандартів Національного банку України [22].

2. Проведення аудиту. Аудит передбачає аналіз технічних і організаційних заходів безпеки. Технічний аудит включає перевірку конфігурації систем шифрування (наприклад, AES-256), IAM (Azure Active Directory), DLP (Symantec DLP) і SIEM (Splunk) [11]. Наприклад, аудит може виявити, що база даних не використовує прозоре шифрування (TDE), що підвищує ризик витоку [21]. Організаційний аудит оцінює відповідність політики захисту даних (описаної в підрозділі 3.1) і рівень підготовки персоналу. Для цього використовуються опитування, перевірка документації та аналіз журналів подій. В Україні аудит часто фокусується на внутрішніх загрозах, оскільки помилки працівників є поширеною причиною інцидентів [18]. Результати аудиту документуються у звіті, який включає перелік вразливостей і рекомендації щодо їх усунення.
3. Тестування систем захисту. Тестування передбачає активну перевірку систем на стійкість до загроз. Основні методи включають:
    — Тестування на проникнення (penetration testing): Імітація хакерських атак для виявлення слабких місць, наприклад, уразливостей у вебдодатках чи неправильно налаштованих брандмауерах. Інструменти, такі як Metasploit або Burp Suite, дозволяють перевірити стійкість до SQL-ін’єкцій чи XSS-атак [19].

— Сканування вразливостей: Використання сканерів, таких як Nessus або OpenVAS, для виявлення застарілого програмного забезпечення чи відкритих портів [28].
— Симуляція фішингових атак: Перевірка реакції працівників на підозрілі листи, що допомагає оцінити ефективність навчання, описаного в підрозділі 3.2 [14].

В Україні тестування на проникнення є особливо актуальним для державних реєстрів, які часто стають мішенню кібератак [22]. Наприклад, тестування може виявити, що хмарне сховище неправильно налаштоване, дозволяючи несанкціонований доступ до даних.

4. Аналіз результатів і вдосконалення. Після аудиту та тестування аналізуються отримані дані для визначення пріоритетних заходів. Вразливості класифікуються за рівнем критичності (низький, середній, високий), а рекомендації включають технічні (оновлення ПЗ, налаштування шифрування) та організаційні (посилення політик доступу, додаткове навчання) дії [28]. Наприклад, якщо аудит виявив відсутність 2FA, організація може впровадити Google Authenticator або YubiKey [14]. В Україні результати аудиту мають бути задокументовані для подання Уповноваженому з прав людини під час перевірок [23]. Регулярне повторення аудиту (наприклад, раз на рік) і тестування (раз на півроку) забезпечує постійне вдосконалення систем захисту.

Для ефективного аудиту та тестування систем захисту в українських організаціях пропонується врахувати такі рекомендації:

— Фокус на локальних вимогах: Аудит має відповідати Закону України «Про захист персональних даних» і враховувати вимоги до захисту державних реєстрів, особливо в умовах воєнного стану [22]. Наприклад, аудит державних установ повинен перевіряти локалізацію даних і використання шифрування.

— Використання автоматизованих інструментів: Інструменти, такі як Nessus для сканування вразливостей або Microsoft Purview для аналізу відповідності, знижують витрати часу та підвищують точність [21]. Для малих організацій рекомендуються безкоштовні інструменти, такі як OpenVAS, які доступні для базового сканування [28].
— Пріоритет на внутрішніх загрозах: В Україні значна частка витоків пов'язана з діями працівників, тому аудит має включати перевірку дотримання політик IAM і DLP, а тестування – симуляцію внутрішніх атак [18]. Наприклад, тестування може перевірити, чи можуть працівники обійти DLP, надсилаючи чутливі дані через особистий email.
— Інтеграція з іншими процесами: Аудит і тестування мають бути частиною політики захисту даних (підрозділ 3.1) і доповнювати навчання персоналу (підрозділ 3.2). Наприклад, результати симуляції фішингу можуть бути використані для вдосконалення тренінгів [14].
— Регулярність і документація: Аудит і тестування слід проводити регулярно, а результати документувати для звітності перед регуляторними органами. В Україні це є обов'язковим для організацій, які обробляють великі обсяги персональних даних [23].

Запропонований підхід до аудиту та тестування систем захисту є універсальним і може застосовуватися в організаціях різного масштабу – від малих підприємств до державних установ. У контексті України він враховує локальні виклики, такі як підвищені кіберризики, обмежені бюджети та необхідність відповідності законодавству. Регулярний аудит і тестування дозволяють виявляти вразливості, такі як застаріле ПЗ чи слабкі паролі, і запобігати зловживанням, таким як витоки даних чи шахрайство [28].

Практична реалізація цього підходу сприяє підвищенню рівня безпеки шляхом інтеграції з іншими інструментами, такими як DLP (Symantec DLP) і IAM (Azure Active Directory), що забезпечує комплексний захист [21]. Наприклад, аудит може виявити, що DLP неправильно налаштована, а

тестування – підтвердити її ефективність після виправлення. У довгостроковій перспективі це знижує фінансові та репутаційні ризики, підвищує довіру клієнтів і забезпечує відповідність регуляторним вимогам.

Аудит і тестування систем захисту є невід'ємною частиною стратегії захисту персональних даних. Їхнє систематичне впровадження в Україні сприятиме підвищенню кібербезпеки, зниженню ризиків зловживань і виконанню законодавчих стандартів, що є важливим для сталого розвитку цифрової інфраструктури.

3.4. Реагування на інциденти зловживань даними

Реагування на інциденти зловживань персональними даними є критично важливим процесом для мінімізації наслідків витоків, шахрайства чи несанкціонованого доступу. Ефективне реагування дозволяє організаціям швидко виявляти інциденти, обмежувати їхній вплив, відновлювати нормальну роботу систем і запобігати повторним порушенням. У контексті України, де кіберзагрози посилюються через воєнний стан і швидку цифровізацію, а також через вимоги Закону України «Про захист персональних даних» №2297-VI, розробка чіткого плану реагування є обов'язковою [15]. Цей підрозділ пропонує практичний підхід до організації реагування на інциденти, який включає алгоритм дій, інструменти для реалізації та рекомендації для українських організацій.

Реагування на інциденти зловживань даними вимагає структурованого підходу, який поєднує технічні, організаційні та правові заходи. Запропонований алгоритм складається з п'яти основних етапів, які забезпечують швидке та ефективне управління інцидентами.

1. Виявлення інциденту. Перший етап передбачає швидке виявлення зловживання даними, такого як витік, фішингова атака чи несанкціонований доступ. Для цього використовуються інструменти моніторингу, такі як SIEM-системи (Splunk, IBM QRadar), які аналізують журнали подій і виявляють аномалії, наприклад, незвичну

активність у базі даних [9]. DLP-системи, такі як Microsoft Purview, можуть сигналізувати про несанкціоновану передачу чутливих даних, наприклад, надсилання файлу з персональними даними на зовнішній email [21]. У контексті України важливим є також моніторинг зовнішніх загроз, таких як кібератаки на державні реєстри, що може здійснюватися за допомогою OSINT-інструментів, таких як Maltego [19]. Працівники, навчені за програмою, описаною в підрозділі 3.2, також відіграють ключову роль, повідомляючи про підозрілі дії, наприклад, фішингові листи [18].

2. Обмеження та ізоляція інциденту. Після виявлення інциденту необхідно обмежити його поширення. Це може включати блокування скомпрометованих облікових записів через IAM-системи (Azure Active Directory), ізоляцію заражених пристроїв за допомогою мережевих брандмауерів або припинення передачі даних через DLP [21]. Наприклад, якщо виявлено витік даних через фішинг, організація може тимчасово відключити доступ до системи для всіх користувачів, крім адміністраторів, і активувати двофакторну автентифікацію (2FA) [14]. В Україні швидке обмеження інциденту є особливо важливим через високий ризик атак на критичну інфраструктуру, що вимагає координації з правоохоронними органами, такими як кіберполіція [15].
3. Аналіз і розслідування. На цьому етапі проводиться детальний аналіз інциденту для визначення його причини, масштабу та наслідків. SIEM-системи надають журнали подій, які допомагають встановити, які дані були скомпрометовані і як відбувся доступ [9]. Наприклад, аналіз може показати, що витік стався через неправильно налаштоване хмарне сховище (Amazon S3), що є поширеною проблемою [28]. У разі складних атак використовуються інструменти криміналістичного аналізу, такі як EnCase або Autopsy, для збору доказів [19]. В Україні розслідування має враховувати вимоги Уповноваженого Верховної Ради з прав людини щодо повідомлення про інциденти протягом 72

годин, що відповідає стандартам GDPR [23]. Результати аналізу документуються для подальшого звітування та вдосконалення безпеки.

4. Усунення наслідків і відновлення. Після розслідування організація усуває наслідки інциденту та відновлює нормальну роботу систем. Це може включати відновлення даних із резервних копій, оновлення паролів через IAM-системи, виправлення вразливостей (наприклад, встановлення патчів для застарілого ПЗ) і посилення шифрування (AES-256) [3]. Для користувачів, чиї дані були скомпрометовані, необхідно надати повідомлення та рекомендації, наприклад, змінити паролі чи активувати 2FA [14]. В Україні цей етап часто ускладнений через обмежені ресурси, але хмарні інструменти, такі як Microsoft Purview, дозволяють автоматизувати частину процесів, наприклад, відновлення доступу до даних [21]. Крім того, організації повинні співпрацювати з кіберполіцією для притягнення винних до відповідальності [15].
5. Аналіз після інциденту та вдосконалення. Останній етап передбачає аналіз причин інциденту та оновлення заходів безпеки для запобігання повторним порушенням. Це включає перегляд політики захисту даних (підрозділ 3.1), посилення навчання персоналу (підрозділ 3.2) і повторний аудит систем (підрозділ 3.3). Наприклад, якщо інцидент стався через слабкі паролі, організація може впровадити обов’язкове використання парольних менеджерів, таких як LastPass [14]. В Україні аналіз після інциденту є важливим для адаптації до нових загроз, таких як цілеспрямовані кібератаки, і відповідності вимогам законодавства [23]. Результати аналізу використовуються для створення звітів для регуляторних органів і внутрішнього вдосконалення.

Для ефективного реагування на інциденти зловживань даними в українських організаціях пропонується врахувати такі рекомендації:

— Автоматизація реагування: Використання SIEM (Splunk) і DLP (Microsoft Purview) дозволяє автоматизувати виявлення та обмеження інцидентів, що знижує час реакції [21]. Для малих організацій із

обмеженим бюджетом рекомендуються хмарні рішення, які не потребують значних витрат на інфраструктуру [28].

— Фокус на локальних загрозах: В Україні особливу увагу слід приділяти реагуванню на кібератаки, пов’язані з воєнним станом, наприклад, атаки на державні реєстри. Організації мають налагодити співпрацю з кіберполіцією та CERT-UA для швидкого обміну інформацією про загрози [15].
— Навчання та симуляції: Регулярні симуляції інцидентів, такі як фішингові атаки чи імітація витоку даних, допомагають підготувати персонал до реальних ситуацій. Це доповнює програму навчання, описану в підрозділі 3.2 [18].
— Документація та звітність: Відповідно до Закону України «Про захист персональних даних», організації повинні повідомляти про інциденти Уповноваженому з прав людини протягом 72 годин і надавати детальні звіти [23]. Автоматизовані інструменти, такі як Microsoft Purview, спрощують підготовку таких звітів [21].
— Інтеграція з іншими процесами: Реагування на інциденти має бути частиною загальної системи безпеки, включаючи аудит (підрозділ 3.3) і політику захисту даних (підрозділ 3.1). Наприклад, результати аналізу інциденту можуть бути використані для оновлення політик IAM або DLP [9].

Запропонований підхід до реагування на інциденти зловживань даними є універсальним і може застосовуватися в організаціях різного масштабу – від малих підприємств до державних установ. У контексті України він враховує локальні виклики, такі як підвищені кіберризики, обмежені ресурси та необхідність відповідності законодавству. Реалізація цього підходу дозволяє організаціям швидко виявляти інциденти, мінімізувати збитки та запобігати повторним порушенням, що є критично важливим у період воєнного стану [15].

Практична цінність підходу полягає в його інтеграції з іншими інструментами безпеки, такими як SIEM, DLP і IAM, що забезпечує комплексний

захист [21]. Наприклад, швидке виявлення витоку через Splunk і блокування через Microsoft Purview може зменшити масштаб інциденту на 70%, за даними досліджень [28]. У довгостроковій перспективі це сприяє зниженню фінансових і репутаційних ризиків, підвищенню довіри клієнтів і відповідності регуляторним вимогам.

Реагування на інциденти зловживань даними є невід'ємною частиною стратегії захисту персональних даних. Його систематичне впровадження в Україні сприятиме підвищенню кібербезпеки, зниженню ризиків і сталому розвитку цифрової інфраструктури.

3.5. Висновки до розділу

Третій розділ бакалаврської роботи присвячений практичним аспектам впровадження захисту персональних даних, що є ключовим для забезпечення їхньої безпеки в умовах зростання кіберзагроз і регуляторних вимог. Проведений аналіз дозволив розробити практичні підходи до створення політики захисту даних, навчання персоналу, аудиту систем, реагування на інциденти та систематизувати рекомендації для їх реалізації в Україні.

Розробка політики захисту персональних даних є основою для створення структурованої системи безпеки. Запропонований алгоритм, який включає аналіз даних, оцінку ризиків, розробку структури політики, інтеграцію технічних і організаційних заходів, а також тестування, дозволяє організаціям відповідати вимогам Закону України «Про захист персональних даних» і GDPR [12]. В Україні цей процес ускладнений обмеженими бюджетами та низькою кіберграмотністю, але використання автоматизованих інструментів, таких як Microsoft Purview, сприяє його спрощенню [21].

Навчання персоналу з питань безпеки даних є критично важливим для зниження ризиків внутрішніх загроз, які в Україні становлять значну частку інцидентів [18]. ЗапропJt запропонований підхід до навчання, що включає планування, проведення тренінгів, оцінку ефективності та регулярне оновлення, підвищує обізнаність працівників і формує культуру кібербезпеки.

Використання симуляцій фішингових атак і практичних завдань, таких як налаштування 2FA, є особливо ефективним для підготовки до реальних загроз [14].

Аудит і тестування систем захисту дозволяють виявляти вразливості та оцінювати ефективність заходів безпеки. Запропонований підхід, який включає планування, проведення аудиту, тестування (наприклад, penetration testing) і вдосконалення, забезпечує відповідність регуляторним вимогам і зниження ризиків [23]. В Україні аудит і тестування є особливо актуальними для захисту державних реєстрів, але потребують автоматизованих інструментів, таких як Nessus, для підвищення ефективності [28].

Реагування на інциденти зловживань даними є невід'ємною частиною стратегії безпеки. Запропонований алгоритм, що охоплює виявлення, обмеження, аналіз, усунення наслідків і вдосконалення, дозволяє мінімізувати збитки та запобігати повторним порушенням [15]. Інтеграція з SIEM і DLP-системами, такими як Splunk і Microsoft Purview, підвищує швидкість і точність реагування [21]. В Україні цей процес ускладнений через високий рівень кіберзагроз, але співпраця з кіберполіцією та автоматизація сприяють його ефективності [15].

Практичні аспекти впровадження захисту персональних даних формують комплексний підхід, який поєднує організаційні, технічні та правові заходи. В Україні їхнє впровадження сприяє підвищенню кібербезпеки, зниженню ризиків зловживань і відповідності законодавчим стандартам, але потребує подолання фінансових, технічних і кадрових обмежень. Отримані результати можуть бути використані організаціями для вдосконалення систем безпеки та підвищення довіри клієнтів, що є важливим для розвитку цифрової економіки.

ВИСНОВКИ

Бакалаврська робота присвячена дослідженню інструментів аналізу та захисту від зловживань персональними даними, що є актуальною проблемою в умовах стрімкої цифровізації та зростання кіберзагроз. Проведений аналіз дозволив досягти поставленої мети – дослідити сучасні інструменти, оцінити їхню ефективність і розробити практичні рекомендації для запобігання зловживанням, з урахуванням специфіки українського контексту. Основні результати роботи підсумовуються наступним чином.

У першому розділі було проаналізовано зловживання персональними даними, їхні типи, джерела загроз і методи аналізу ризиків. Встановлено, що персональні дані включають ідентифікаційні, фінансові, медичні та поведінкові категорії, кожна з яких має свої вразливості [1]. Зловживання, такі як крадіжка даних, шахрайство та несанкціоноване використання, є поширеними загрозами, які посилюються в Україні через воєнний стан і низький рівень кіберграмотності [14]. Джерела загроз поділяються на зовнішні (хакерські атаки, фішинг), внутрішні (помилки працівників) і технологічні (вразливості ПЗ) [7]. Методи аналізу ризиків, такі як якісний, кількісний і сценарний аналіз, дозволяють оцінити ймовірність і наслідки інцидентів [8]. Інструменти моніторингу, такі як DLP (Microsoft Purview), SIEM (Splunk) і OSINT (Maltego), забезпечують своєчасне виявлення зловживань, але їхнє впровадження в Україні обмежене фінансовими та кадровими ресурсами [19].

Другий розділ був присвячений інструментам захисту персональних даних, які формують комплексний підхід до безпеки. Класифікація інструментів за функціональністю (шифрування, IAM, DLP, моніторинг), сферою застосування і рівнем автоматизації показала їхню різноманітність і адаптивність [10]. Технології шифрування, такі як AES, RSA і гомоморфне шифрування, забезпечують конфіденційність даних, але потребують належного управління ключами [3]. Системи управління доступом (IAM), наприклад, Azure Active Directory, дозволяють обмежувати доступ і впроваджувати 2FA, що є особливо актуальним для України [13]. DLP-системи, такі як Symantec DLP, ефективно

запобігають витокам шляхом моніторингу та блокування передачі даних, але їхнє використання ускладнене високою вартістю [11]. В Україні хмарні інструменти набувають популярності, але локальні рішення залишаються поширеними через вимоги до локалізації даних [20].

Третій розділ зосереджений на практичних аспектах впровадження захисту даних, що включають розробку політики, навчання персоналу, аудит, тестування та реагування на інциденти. Запропонований алгоритм створення політики захисту даних забезпечує відповідність Закону України «Про захист персональних даних» і GDPR, але потребує автоматизації для спрощення реалізації [12]. Навчання персоналу знижує ризики внутрішніх загроз, які є значною проблемою в Україні, через використання симуляцій і практичних завдань [18]. Аудит і тестування систем, включаючи penetration testing і сканування вразливостей, дозволяють виявляти слабкі місця, але потребують регулярності та використання інструментів, таких як Nessus [28]. Реагування на інциденти, підкріплене SIEM і DLP-системами, мінімізує збитки та запобігає повторним порушенням, що є критично важливим у період підвищених кіберризиків [15].

Наукова новизна роботи полягає в систематизації інструментів аналізу та захисту персональних даних із урахуванням українських реалій, а також у розробці практичних підходів до їхнього впровадження. Практична значущість зумовлена можливістю застосування рекомендацій у державних і комерційних організаціях для підвищення рівня кібербезпеки, зниження ризиків зловживань і відповідності законодавчим вимогам. Зокрема, використання хмарних інструментів (Microsoft Purview, Azure Active Directory) і автоматизованих підходів до навчання та аудиту може значно спростити захист даних для організацій із обмеженими ресурсами [21].

Водночас впровадження запропонованих заходів в Україні стикається з викликами, такими як брак кваліфікованих фахівців, обмежені бюджети та застаріла інфраструктура. Для їх подолання рекомендуються поетапне впровадження автоматизованих рішень, співпраця з правоохоронними органами

(кіберполіція, CERT-UA) і підвищення кіберграмотності через регулярне навчання [15]. У майбутньому дослідження може бути розширене шляхом аналізу нових технологій, таких як блокчейн або квантове шифрування, а також оцінки їхньої ефективності в українських умовах.

Захист персональних даних вимагає комплексного підходу, який поєднує аналіз загроз, використання сучасних інструментів і практичні заходи. Впровадження запропонованих рекомендацій сприятиме підвищенню безпеки даних, зниженню ризиків зловживань і сталому розвитку цифрової інфраструктури в Україні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Big data privacy: a technological perspective and review // Journal of Big Data. – 2016. – Режим доступу: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-016-0059-y.
2. Practical Approaches to Big Data Privacy Over Time // Harvard University Privacy Tools Project. – 2019. – Режим доступу: https://privacytools.seas.harvard.edu/publications/practical-approaches-big-data-privacy-over-time.
3. Protecting Information with Cybersecurity // PMC. – 2018. – Режим доступу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7122347/.
4. Maintaining the Privacy and Security of Research Participants' Data // NN/g. – 2022. – Режим доступу: https://www.nngroup.com/articles/privacy-and-security/.
5. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches // PMC. – 2022. – Режим доступу: https://pmc.ncbi.nlm.nih.gov/articles/PMC8800549/.
6. Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World // SSRN. – 2022. – Режим доступу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4005750.
7. Practical approaches to big data privacy over time // International Data Privacy Law. – 2018. – Режим доступу: https://academic.oup.com/idpl/article/8/1/29/4930711.
8. A systematic overview on methods to protect sensitive data provided for various analyses // International Journal of Information Security. – 2022. – Режим доступу: https://link.springer.com/article/10.1007/s10207-022-00607-5.
9. PERSONAL DATA PROTECTION Research Papers // Academia.edu. – Режим доступу: https://www.academia.edu/Documents/in/PERSONAL_DATA_PROTECTION.
10. Journal of Data Protection and Privacy // Henry Stewart Publications. – Режим доступу: https://www.henrystewartpublications.com/jdpp.

11. Інструменти для аналізу даних // Бібліотека СумДУ. – Режим доступу: https://library.sumdu.edu.ua/uk/doslidnyku/prohramne-zabezpechennia/analiz-danykh-ta-vizualizatsiia/instrumenty-dlia-analizu-danykh.html.
12. Політика конфіденційності та захисту персональних даних // Ukrinform. – Режим доступу: https://www.ukrinform.ua/info/policy.html.
13. Захист персональних даних // WikiLegalAid. – Режим доступу: https://legalaid.wiki/index.php/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85.
14. Інтернет-шахрайство: в МВС розповіли про сучасні фінансові злочини, хакерські атаки та методи протидії // Міністерство внутрішніх справ України. – Режим доступу: https://mvs.gov.ua/news/internet-saxraistvo-v-mvs-rozpovili-pro-metodi-protidiyi.
15. Захист персональних даних у сфері охорони здоров'я: Ірина Сенюта розповіла про дієві інструменти в роботі адвоката // ADVOKAT POST. – Режим доступу: https://advokatpost.com/zakhyst-personalnykh-danykh-u-sferi-okhorony-zdorov-ia-iryna-seniuta-rozpovila-pro-diievi-instrumenty-v-roboti-advokata/.
16. Про порядок обробки і захисту персональних даних користувачів сайту // Oplatforma. – Режим доступу: https://oplatforma.com.ua/politika-konfidentsiynosti.
17. Прості правила для захисту персональних даних // Vodafone. – Режим доступу: https://www.vodafone.ua/shop/ua/blog/prosti-pravila-dlja-zahistu-personal-nih-danih.html.
18. Обов'язкове інформування, контроль та великі штрафи: як новий законопроєкт змінить правила захисту персональних даних // Ukrinform. – Режим доступу: https://www.ukrinform.ua/rubric-polytics/3826649-obovazkove-informuvanna-kontrol-ta-veliki-strafi-ak-novij-zakonoproekt-zminue-pravila-zahistu-personalnih-danih.html.

19. Топ 16 платних та безплатних інструментів для OSINT // IT Education Center Blog. – Режим доступу: https://itedu.center/ua/blog/war/top-16-platnix-ta-bezplatnix-instrumentiv-dlya-osint/.
20. ПРООН та Мінцифри презентують онлайн-інструмент для бізнесу із захисту персональних даних // UNDP Ukraine. – Режим доступу: https://www.undp.org/uk/ukraine/press-releases/proon-ta-mintsyfry-prezentuyut-onlayn-instrument-dlya-biznesu-iz-zakhystu-personalnykh-danykh.
21. Захист і контроль інформації | Захисний комплекс Microsoft // Microsoft. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/solutions/information-protection.
22. ЗАКОН УКРАЇНИ №2297–VI // Офіційне інтернет-представництво Президента України. – Режим доступу: https://www.president.gov.ua/documents/2297vi-11567.
23. Посібник із захисту персональних даних // Ombudsman. – Режим доступу: https://ombudsman.gov.ua/storage/app/media/uploaded-files/Handbook_Pers_Data_Protect_2021.pdf.
24. Про захист персональних даних | від 01.06.2010 № 2297-VI // Законодавство України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17.
25. Роз’яснення до Порядку здійснення Уповноваженим контролю за додержанням // Законодавство України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0002715-14.
26. 14 НАЙКРАЩИХ інструментів для аналізу даних (2025) // Guru99. – Режим доступу: https://www.guru99.com/uk/best-data-analytics-tools.html.
27. ТОП 10 інструментів для Аналітиків Даних // Web Academy Media. – Режим доступу: https://web-academy.ua/blog/junior/top-10-analytics-tools.
28. 36 кращих інструментів для візуалізації даних // Toplead. – Режим доступу: https://toplead.com.ua/ua/blog/id/38-luchshih-instrumentov-dlja-vizualizacii-dannyh-160/.
29. 9 найкращих інструментів ШІ для аналітиків даних (квітень 2025 р.) // Unite.AI. – Режим доступу: https://www.unite.ai/uk/ai-tools-data-analysts/.

ДОДАТКИ

ДОДАТОК А. ПРИКЛАД ПОЛІТИКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Опис: Додаток містить шаблон політики захисту персональних даних, адаптований до вимог Закону України «Про захист персональних даних» №2297-VI та GDPR. Шаблон включає основні розділи, описані в підрозділі 3.1, і може бути використаний організаціями для розробки власної політики.

Зміст:

1. Мета та сфера застосування
— Мета: Забезпечення конфіденційності, цілісності та доступності персональних даних.
— Сфера: Усі системи, що обробляють персональні дані (CRM, бази даних, хмарні сервіси).
2. Класифікація даних
— Категорії: Ідентифікаційні (ПІБ, ІПН), фінансові (банківські рахунки), медичні, поведінкові.
— Чутливість: Висока (медичні, фінансові), середня (контактні), низька (публічні).
3. Правила обробки
— Збір: Лише за згодою суб’єкта даних.
— Зберігання: Використання шифрування AES-256 [3].
— Передача: Через захищені канали (TLS, VPN).
— Знищення: Відповідно до встановлених процедур після закінчення терміну зберігання.
4. Ролі та відповідальність
— Керівництво: Затвердження політики.
— Адміністратори: Налаштування IAM і DLP-систем (наприклад, Microsoft Purview) [21].
— Працівники: Дотримання правил, проходження навчання [18].
5. Реагування на інциденти

— Виявлення: Використання SIEM (Splunk) [9].

— Повідомлення: Протягом 72 годин до Уповноваженого з прав людини [23].

— Усунення: Відновлення даних із резервних копій, оновлення паролів.

6. Аудит і перегляд

— Періодичність: Щорічно або після інцидентів.

— Інструменти: Nessus для сканування вразливостей [28].

ДОДАТОК Б. СЦЕНАРІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Опис: Додаток містить приклад сценарію тестування на проникнення (penetration testing), описаного в підрозділі 3.3, для перевірки стійкості системи до зовнішніх атак. Сценарій імітує атаку на вебдодаток, який містить персональні дані.

Зміст:

1. Мета

— Виявлення вразливостей у вебдодатку (наприклад, SQL-ін’єкції, XSS).

— Оцінка ефективності брандмауера та IAM-системи (Azure Active Directory) [21].

2. Інструменти

— Metasploit: Для експлуатації вразливостей [19].

— Burp Suite: Для аналізу HTTP-запитів.

— Nessus: Для сканування вразливостей [28].

3. Етапи тестування

— Збір інформації: Використання OSINT (Maltego) для аналізу відкритих даних про сервер [19].

— Сканування: Виявлення відкритих портів і застарілого ПЗ за допомогою Nessus.

— Експлуатація: Спроба SQL-ін’єкції для доступу до бази даних із персональними даними.

— Аналіз доступу: Перевірка, чи може атакуючий обійти 2FA в Azure Active Directory [14].

4. Очікувані результати

— Виявлення вразливостей (наприклад, незахищений API).

— Рекомендації: Впровадження TDE для бази даних, оновлення ПЗ, посилення 2FA [3].

5. Документація

— Звіт із описом вразливостей, рівнем критичності та діями для їх усунення.
— Подання звіту для аудиту відповідно до вимог Уповноваженого з прав людини [23].

ДОДАТОК В. ПРИКЛАД ПРОГРАМИ НАВЧАННЯ ПЕРСОНАЛУ

Опис: Додаток містить приклад програми навчання персоналу з питань безпеки даних, розробленої відповідно до підходу, описаного в підрозділі 3.2. Програма адаптована до українських реалій і враховує локальні загрози.

Зміст:

1. Мета

— Підвищення кіберграмотності працівників.

— Навчання розпізнаванню фішингу, безпечному використанню паролів і реагуванню на інциденти [18].

2. Аудиторія

— Усі працівники: Базовий курс із кібербезпеки.

— Адміністратори: Поглиблений курс із налаштування IAM і DLP [21].

3. Формат

— Онлайн-курс: Платформа KnowBe4 або локальний курс від IT Education Center [26].

— Симуляція фішингу: Імітація атак для перевірки реакції працівників [14].

— Практичні заняття: Налаштування 2FA (Google Authenticator), шифрування файлів (VeraCrypt) [3].

4. Зміст

— Модуль 1: Основи кібербезпеки (фішинг, ransomware, соціальна інженерія).

— Модуль 2: Правові аспекти (Закон України «Про захист персональних даних», GDPR) [12].

— Модуль 3: Практичні інструменти (VPN, антивіруси, парольні менеджери) [14].

— Модуль 4: Реагування на інциденти (повідомлення, ізоляція) [15].

5. Оцінка

— Тест: 20 питань про типи загроз і правила безпеки.

— Практичне завдання: Розпізнавання фішингового листа.

— Аналіз через DLP: Моніторинг порушень після навчання [21].

6. Періодичність

— Щорічно для всіх працівників.

— Щоквартально для адміністраторів із оновленнями щодо нових загроз [18]

ДОДАТОК Г. РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ ІНСТРУМЕНТІВ ЗАХИСТУ ДАНИХ

Опис: Додаток містить рекомендації щодо вибору інструментів захисту персональних даних залежно від типу організації, бюджету та рівня загроз. Рекомендації базуються на аналізі, проведеному в розділі 2.

Зміст:

1. Малі організації (бюджет до 5000 USD)

— Шифрування: VeraCrypt (безкоштовне, AES-256) [3].

— IAM: Google Workspace із базовою 2FA [14].

— DLP: Безкоштовні функції Microsoft 365 для базового моніторингу [21].

— Моніторинг: OpenVAS для сканування вразливостей [28].

— Рекомендація: Фокус на хмарних і безкоштовних рішеннях для зниження витрат.

2. Середні організації (бюджет до 50,000 USD)

— Шифрування: Microsoft SQL Server Always Encrypted [21].

— IAM: Azure Active Directory із підтримкою 2FA і RBAC [13].

— DLP: Forcepoint DLP для моніторингу передачі даних [11].

— Моніторинг: Splunk для аналізу логів [9].

— Рекомендація: Інтеграція хмарних і локальних рішень для гнучкості.

3. Великі організації та держустанови (бюджет понад 50,000 USD)

— Шифрування: Oracle TDE для баз даних, гомоморфне шифрування для хмар [10].

— IAM: Okta або SailPoint для управління привілейованим доступом [21].

— DLP: Symantec DLP із машинним навчанням [11].

— Моніторинг: IBM QRadar із UEBA для аналізу поведінки [9].

— Рекомендація: Комплексний підхід із використанням автоматизованих систем і регулярним аудитом [23].

4. Специфічні вимоги для України

— Локалізація даних відповідно до законодавства [22].

— Захист від локальних загроз (кібератаки, пов’язані з воєнним станом) за допомогою OSINT і співпраці з кіберполіцією [15].

— Використання 2FA (YubiKey, Google Authenticator) для всіх працівників [14].