Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту персональних даних підприємства рітейлу»

Студента 2 курсу, 8м групи, спеціальності 125 «Кібербепека» освітня програма «Безпека систем електронних комунікацій в економіці»

_____
підпис студента

Марчука Богдана Вячеславовича

Науковий керівник
старший викладач
кафедри інженерії програмного забезпечення та кібербезпеки

_____
підпис керівника

Бебешко Богдан Тарасович

Гарант освітньої програми
кандидат технічних наук,
доцент кафедри інженерії програмного забезпечення та кібербезпеки

_____
підпис гаранта

Савченко Тетяна Віталіївна

КИЇВ – 2023

Державний торговельно-економічний університет

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки
Освітній ступінь магістр
Спеціальність 125 «Кібербезпека»

Затверджую
Зав. кафедри інженерії програмного забезпечення та кібербезпеки
Криворучко О. В.
«16» листопада 2022 р.

Завдання
на випускну кваліфікаційну роботу студентові
Марчуку Богдану Вячеславовичу
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи «Технологія захисту персональних даних підприємства рітейлу».

Затверджена наказом ректора від «06» грудня 2022 р. № 3287

2. Строк здачі студентом закінченої роботи 15 листопада 2023 р.

3. Цільова установка та вихідні дані до роботи

Мета роботи − полягає в проведені комплексного аналізу та дослідження сучасних технологій захисту персональних даних в підприємствах рітейлу з метою розробки та впровадження ефективної системи захисту, яка забезпечить високий рівень безпеки персональних даних, відповідно до законодавчих вимог і забезпечить довіру споживачів до обробки їхніх особистих даних в рітейл-сегменті.

Об'єкт дослідження – процес оцінки сучасних технологій захисту персональних даних в підприємствах рітейлу з метою з'ясування їхньої ефективності, відповідності законодавчим вимогам та можливості забезпечення високого рівня безпеки особистих даних споживачів.

Предмет дослідження – підходи, методи та інструменти, які використовуються для оцінки та вдосконалення сучасних технологій захисту персональних даних на підприємствах рітейлу.

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В РІТЕЙЛІ

1.1. Поняття та значення персональних даних

1.2. Законодавча база щодо захисту персональних даних в рітейлі

1.3. Сучасні технології збору та обробки персональних даних в рітейлі

1.4. Основні загрози та ризики для персональних даних в рітейлі

1.5. Висновок до розділу 1

РОЗДІЛ 2. СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В РІТЕЙЛІ

2.1. Криптографічні методи захисту персональних даних

2.2. Технології обробки та зберігання персональних даних

2.3. Використання штучного інтелекту та машинного навчання в захисті персональних даних

2.4. Біометричні технології в рітейлі

2.5. Висновок до розділу 2

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ПІДПРИЄМСТВІ РІТЕЙЛУ

3.1. Розробка та впровадження конфігурації захисної системи на прикладі підприємства рітейлу

3.2. Методи аудиту та моніторингу захисту персональних даних

3.3. Розробка конкретних рішень та інструментів для забезпечення ефективності захисту персональних даних

3.4. Рекомендації щодо подальших дій підприємств рітейлу в сфері захисту персональних даних

3.5. Висновок до розділу 3

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

6. Календарний план виконання випускної кваліфікаційної роботи

№ пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів випускної кваліфікаційної роботи	
		за планом	фактично
1	2	3	4
1.	*Вибір теми випускної кваліфікаційної роботи*	*05.11.2022*	*05.11.2022*
2.	*Розробка та затвердження завдання на роботу магістра*	*16.11.2022*	*16.11.2022*
3.	*Вступ та перелік літературних джерел*	*25.02.2023*	*25.02.2023*
4.	*Розробка технічного завдання*	*18.03.2023*	*18.03.2023*
5.	*Розділ 1. Теоретичні аспекти захисту персональних даних в рітейлі*	*15.04.2023*	*15.04.2023*
6.	*Розділ 2. Сучасні технології захисту персональних даних в рітейлі*	*27.05.2023*	*27.05.2023*
7.	*Розділ 3. Практична реалізація технологій захисту персональних даних в підприємстві рітейлу*	*24.06.2023*	*24.06.2023*
8.	*Розробка конфігурації захисної системи на прикладі підприємства рітейлу*	*17.10.2023*	*17.10.2023*
9.	*Написання наукової статті*	*20.05.2023*	*20.05.2023*
10.	*Висновки та пропозиції*	*23.10.2023*	*23.10.2023*
11.	*Здача випускної кваліфікаційної роботи на кафедру (перша перевірка)*	*01.11.2023*	*01.11.2023*
12.	*Підготовка автореферату та презентації доповіді*	*04.11.2023*	*04.11.2023*
13.	*Попередній захист випускної кваліфікаційної роботи*	*09.11.2023 – 14.11.2023*	*10.11.2023*
14.	*Здача зброшурованої випускної кваліфікаційної роботи*	*15.11.2023*	*15.11.2023*
15.	*Зовнішнє рецензування випускної кваліфікаційної роботи*	*15.11.2023*	*15.11.2023*
16.	*Підготовка до публічного захисту випускної кваліфікаційної роботи*	*за розкладом роботи ЕК*	

7. Дата видачі завдання «16» листопада 2022 р.

8. Науковий керівник випускної кваліфікаційної роботи _____ Бебешко Б.Т.
(прізвище, ініціали, підпис)

9. Гарант освітньої програми _____ Савченко Т.В.
(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент _____ Марчук Б.В.
(прізвище, ініціали, підпис)

11. Відгук керівника випускної кваліфікаційної роботи

Науковий керівник випускної кваліфікаційної роботи
Бебешко Б.Т. _____
(підпис, дата)

Відмітка про попередній захист __Бебешко Б.Т._____
(ПІБ, підпис, дата)

12. Висновок про випускну кваліфікаційну роботу

Випускна кваліфікаційна робота студента _____Марчука Б.В.___
(прізвище, ініціали)
може бути допущена до захисту в екзаменаційній комісії.

Гарант освітньої програми _____Савченко Т.В._
(прізвище, ініціали, підпис)

Завідувач кафедри _____Криворучко О. В.
(підпис, прізвище, ініціали)

«_____»_____2023 р.

АНОТАЦІЯ

Відповідно до мети дослідження робота присвячена розробці та вдосконаленню технології захисту персональних даних в підприємствах рітейлу. Для розробки технології захисту персональних даних необхідно провести комплексний аналіз сучасних підходів, методів та інструментів, що використовуються у цій галузі. Робота розглядає як теоретичні аспекти, пов'язані з концепціями безпеки та вимогами до захисту персональних даних, так і практичні аспекти, включаючи вибір та впровадження конкретних заходів і технологічних рішень. Отримані результати та розроблена технологія допоможуть забезпечити безпеку та конфіденційність особистих даних споживачів, що є критично важливим для їхньої довіри та відносин з підприємствами.

Ключові слова: захист персональних даних, рітейл, криптографія, законодавство, інформаційна безпека, штучний інтелект, машинне навчання, біометрія, технології захисту

ABSTRACT

In accordance with the research purpose, this work is dedicated to the development and enhancement of personal data protection technology in retail enterprises. To develop the personal data protection technology, it is necessary to conduct a comprehensive analysis of contemporary approaches, methods, and tools used in this field. The work examines both theoretical aspects related to security concepts and requirements for personal data protection, as well as practical aspects, including the selection and implementation of specific measures and technological solutions. The obtained results and the developed technology will help ensure the security and confidentiality of consumers' personal data, which is critically important for their trust and relationships with enterprises.

Keywords: personal data protection, retail, cryptography, legislation, information security, artificial intelligence (ai), machine learning, biometrics, security technologies

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

PD – персональні дані

GDPR – загальний регламент з питань захисту даних (General Data Protection Regulation)

AI – штучний інтелект

ML – машинне навчання

BI – біометричні ідентифікатори

IoT – інтернет речей (Internet of Things)

СІБ – система інформаційної безпеки

СЗКД – система захисту критичних даних

ПЗ – програмне забезпечення

API – інтерфейс програмування застосунків (Application Programming Interface)

VPN – віртуальна приватна мережа (Virtual Private Network)

IT – інформаційні технології

IS – інформаційна безпека

PKI – інфраструктура відкритих ключів

DLP – захист від втрати даних (Data Loss Prevention)

API – інтерфейс застосунку програмування

R&D – наукові дослідження та розробки

ROI – питома вартість інвестицій

ЗМІСТ

ВСТУП

Актуальність. У сучасному цифровому світі рітейл-сегмент галузі взаємодіє з великою кількістю персональних даних споживачів, включаючи інформацію про покупки, платіжні дані, контактні дані та багато іншого. Захист цих даних стає надзвичайно важливою проблемою, яка впливає на довіру споживачів, законодавчі вимоги щодо захисту даних та конкурентоспроможність підприємств рітейлу. Дослідження має важливе значення для галузі рітейлу, оскільки допоможе підприємствам забезпечити безпеку та конфіденційність даних споживачів, підвищити рівень довіри та підтримати конкурентоспроможність на ринку. Зважаючи на швидкий розвиток цифрового бізнесу та зростання важливості захисту персональних даних, дослідження в галузі технології захисту даних в рітейлі є надзвичайно актуальним та релевантним для сучасного бізнесу та наукової спільноти.

Мета дослідження: розробка та впровадження ефективної системи захисту, яка забезпечить високий рівень безпеки персональних даних, відповідно до законодавчих вимог і забезпечить довіру споживачів до обробки їхніх особистих даних в рітейл-сегменті.

Об'єкт дослідження: процес оцінки сучасних технологій захисту персональних даних в підприємствах рітейлу з метою з'ясування їхньої ефективності, відповідності законодавчим вимогам та можливості забезпечення високого рівня безпеки особистих даних споживачів.

Предмет дослідження: підходи, методи та інструменти, які використовуються для оцінки та вдосконалення сучасних технологій захисту персональних даних на підприємствах рітейлу.

У відповідності з метою дослідження поставлені наступні завдання:

- Вивчення і оцінка існуючих технологій та методів захисту персональних даних в рітейл-сегменті.
- Ретельний аналіз законодавства щодо захисту персональних даних та визначення вимог, яким повинні відповідати підприємства рітейлу, визначення загроз і ризиків; розробка концепції технології захисту даних, вибір та аналіз технічних рішень.
- Оцінка ефективності та відповідності законодавству, підготовка рекомендацій для підприємств рітейлу щодо впровадження та підтримки розробленої технології.

Методи дослідження: аналіз літературних джерел, експертні опитування, аналіз кейсів, тестування технологій, аналіз статистичних даних, аналіз технологічних трендів.

Наукова новизна дослідження полягає в розробці комплексного та інтегрованого підходу до захисту персональних даних, спеціально адаптованого до потреб галузі рітейлу та враховуючого сучасні технологічні та кібербезпечні виклики.

Практичне значення дослідження: розроблена технологія захисту даних може допомогти підприємствам рітейлу зберігати конфіденційність та приватність персональних даних своїх клієнтів, що важливо для збереження довіри та лояльності споживачів; впровадження ефективної технології захисту даних допоможе підприємствам рітейлу зменшити витрати на відшкодування втрат, пов'язаних з можливими інцидентами з кібербезпеки. Таким чином, дослідження має практичне значення, оскільки воно спрямоване на розробку та впровадження технології, яка забезпечить безпеку та конфіденційність персональних даних в галузі рітейлу, що є критично важливим для підприємств та їх клієнтів.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В РІТЕЙЛІ

1.1. Поняття та значення персональних даних

Поняття та значення персональних даних у сучасному контексті кібербезпеки є надзвичайно важливими, оскільки вони становлять основу для розуміння ризиків та загроз, пов'язаних із зберіганням, передачею та обробкою особистої інформації в цифровому середовищі. Персональні дані визначаються як будь-яка інформація, яка дозволяє ідентифікувати конкретну особу або робить її ідентифікацію можливою [1, 2]. Це поняття включає в себе широкий спектр даних, включаючи, але не обмежуючись:

- Особиста інформація: ім'я, прізвище, дата народження, адреса, номер телефону, адреса електронної пошти і інша інформація, яка використовується для ідентифікації конкретної особи.
- Біометричні дані: відбитки пальців, схеми розпізнавання обличчя, голосу та інші біометричні параметри, які можуть бути використані для ідентифікації особи.
- Дані про фізичне становище: медична інформація, генетичні дані, інформація про здоров'я та інші параметри фізичного стану особи.
- Фінансова інформація: номери банківських рахунків, історія транзакцій, інформація про кредити та фінансовий статус.
- Соціальна інформація: дані про соціальний статус, освіту, професійну діяльність та інші параметри соціального життя [2, 4].

- Інформація про місцезнаходження: дані про географічне розташування особи, які можуть бути отримані з GPS-даних, сотової зв'язку та інших джерел.

Значення персональних даних полягає в їх важливості для приватності та безпеки особи. Ці дані мають бути належним чином захищені та оброблятися відповідно до законодавства для запобігання можливим порушенням та зловживанням.

Захист персональних даних стає надзвичайно важливим завдяки зростанню кількості цифрових атак та порушень безпеки даних. Втрата, незаконний доступ або недостатній захист цих даних може призвести до серйозних наслідків, включаючи порушення конфіденційності, шахрайство, крадіжку ідентичності та інші злочини. Тому встановлення високих стандартів захисту персональних даних та дотримання цих стандартів є надзвичайно важливим завданням для організацій та осіб, які працюють з особистою інформацією [1, 3].

Для суспільства в цілому, персональні дані мають велике значення у контексті розвитку бізнесу, наукових досліджень, медицини, соціальних послуг та багатьох інших сфер. Вони допомагають підприємствам та організаціям краще розуміти своїх клієнтів, покращувати продукти та послуги, розвивати інновації та забезпечувати більш ефективну роботу. Однак це також створює великі виклики в галузі кібербезпеки, оскільки потребує високого рівня захисту та відповідності стандартам для запобігання несанкціонованому доступу та порушенням даних.

Захист персональних даних є важливим завданням в сучасному цифровому світі, де обробка та обмін особистою інформацією зростають експоненційно. Забезпечення відповідного рівня захисту персональних даних має важливе значення для збереження приватності осіб та відвернення можливих загроз [4-6].

Рис. 1.1. Захист персональних даних

Ключові аспекти захисту персональних даних (рис. 1.1):

1. **Контроль доступу**: включає в себе визначення, хто має право доступу до даних, і контроль за цим доступом.
2. **Шифрування**: використання шифрування для захисту даних під час передачі та зберігання є ефективним засобом захисту від несанкціонованого доступу. Добре розроблені алгоритми шифрування забезпечують конфіденційність даних.
3. **Аутентифікація та авторизація**: системи повинні визначати, хто звертається до даних (аутентифікація) і які дії може виконати ця особа (авторизація). Це допомагає уникнути несанкціонованого доступу до даних.
4. **Аудит та моніторинг**: системи повинні вести журнали подій і моніторити дії користувачів для виявлення потенційних загроз та порушень безпеки даних.
5. **Фізичний захист**: забезпечення фізичної безпеки серверів і зберігання даних є важливим аспектом захисту. Захищені і контрольовані приміщення та обладнання допомагають запобігти фізичному доступу до даних.

6. **Захист від кібератак**: захист від кібератак, таких як хакерські атаки, віруси та інші загрози, вимагає використання програмного та апаратного захисту, виявлення загроз і реагування на них.
7. **Відповідність законодавству**: забезпечення дотримання законодавства щодо захисту персональних даних, такого як Загальний регламент про захист персональних даних (GDPR) в Європейському Союзі, є обов'язковим для підприємств і організацій.
8. **Освіта та навчання**: освіта та навчання персоналу щодо питань кібербезпеки та захисту даних є важливим аспектом захисту. Користувачі повинні розуміти ризики та керувати ними.
9. **Регулярні оновлення та патчі**: забезпечення актуальності програмного забезпечення та апаратури за допомогою регулярних оновлень та патчів допомагає виправити виявлені уразливості.

Загалом, захист персональних даних вимагає комплексного підходу, який поєднує технічні, організаційні та юридичні заходи [4, 5, 6]. Тільки такий підхід забезпечить ефективний захист від загроз та збереження конфіденційності особистої інформації.

1.2. Законодавча база щодо захисту персональних даних в рітейлі

Законодавча база щодо захисту персональних даних в рітейлі в різних країнах може відрізнятися, але загалом вона регулюється подібними принципами та стандартами [7-9]. Одним із ключових законодавчих актів, який впливає на захист персональних даних в цій галузі, є Загальний регламент про захист персональних даних (GDPR) в Європейському Союзі. Однак існують також інші законодавчі акти та стандарти, які регулюють захист даних в рітейл-секторі.

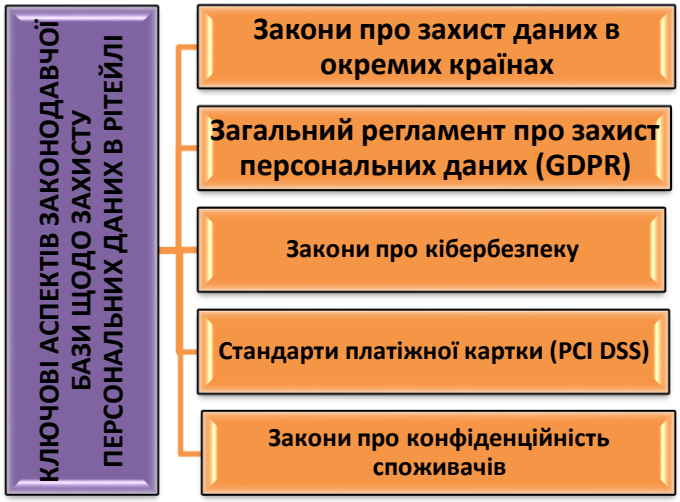

Рис. 1.2. Ключові аспекти законодавчої бази щодо захисту персональних даних в рітейлі

- Загальний регламент про захист персональних даних (GDPR): стосується збору, обробки та зберігання персональних даних у Європейському Союзі. Він встановлює строгі вимоги до захисту даних та права осіб щодо їх персональних даних.
- Закони про захист даних в окремих країнах: багато країн мають свої власні законодавчі акти, які регулюють захист персональних даних. Наприклад, в Сполучених Штатах це може бути Закон про конфіденційність і захист інформації про пацієнтів (HIPAA) та інші закони.
- Стандарти платіжної картки (PCI DSS): для роздрібних підприємств рітейлу, які обробляють платежі з кредитних карток, важливим є дотримання стандартів PCI DSS. Ці стандарти визначають вимоги до безпеки обробки платежів та захисту даних про кредитні картки.
- Закони про кібербезпеку: багато країн приймають закони, спрямовані на захист від кіберзлочинності та загроз кібербезпеці. Вони можуть

включати вимоги щодо захисту даних та повідомлення про кіберінциденти.

- Закони про конфіденційність споживачів: деякі країни мають закони, які регулюють збереження та обробку персональних даних споживачів. Ці закони зазвичай встановлюють права споживачів щодо їх даних.

Загальний принцип законодавчої бази щодо захисту персональних даних в рітейлі полягає в тому, що підприємства повинні бути обов'язково відповідальними за збереження та захист персональних даних клієнтів і споживачів [8]. Це включає в себе технічні та організаційні заходи для запобігання порушенням безпеки даних та виконання прав та обов'язків згідно з законодавством щодо захисту даних.

1.3. Сучасні технології збору та обробки персональних даних в рітейлі

Сучасні технології збору персональних даних в рітейлі розвиваються швидко і дозволяють підприємствам отримувати більше інформації про своїх клієнтів для покращення обслуговування та рекламних стратегій. Найпоширеніші сучасні технології збору персональних даних в рітейлі (рис. 1.3): Wi-Fi та Bluetooth-маяки, камери відеоспостереження, системи оптичного розпізнавання символів (OCR), RFID технології, мобільні додатки та програми лояльності, електронні каси та точки продажу (POS), системи керування запасами, онлайн-аналітика та соціальні медіа, голосові асистенти та чат-боти [2-6].

Рис. 1.3 Найпоширеніші сучасні технології збору персональних даних в рітейлі

- **Wi-Fi та Bluetooth-маяки**: багато роздрібних підприємств використовують Wi-Fi та Bluetooth-маяки для відстеження мобільних пристроїв клієнтів у магазині. Це дозволяє збирати дані про їхню присутність та рух у магазині.
- **Камери відеоспостереження**: використання камер відеоспостереження для відстеження руху клієнтів та аналізу їхньої активності у магазині. Це також може використовуватися для розпізнавання облич та аналізу настроїв покупців.
- **Системи оптичного розпізнавання символів (OCR)**: використовуються для аналізу тексту та штрих-кодів на продуктах та візуального зчитування документів, таких як посвідчення особи.
- **RFID технології**: використання RFID мікрочіпів на товарах для відстежування їх руху в магазині та оптимізації запасів.

- **Мобільні додатки та програми лояльності**: багато роздрібних підприємств надають мобільні додатки, які клієнти можуть використовувати для покупок та отримання знижок. Це дозволяє збирати дані про покупки та вирази інтересу клієнтів.
- **Електронні каси та точки продажу (POS)**: POS-системи автоматично записують дані про кожну транзакцію, збираючи інформацію про товари, ціни та споживацькі патерни.
- **Системи керування запасами**: використовуються для відстежування запасів та руху товарів в реальному часі, що допомагає оптимізувати управління запасами та поповнення.
- **Онлайн-аналітика та соціальні медіа**: моніторинг активності клієнтів в інтернеті та соціальних мережах допомагає роздрібним підприємствам зрозуміти попит та споживчі патерни.
- **Голосові асистенти та чат-боти**: використання голосових асистентів та чат-ботів для обслуговування клієнтів та збору даних про їхні запити та запити.

Ці технології допомагають роздрібним підприємствам збирати, аналізувати та використовувати дані для покращення обслуговування клієнтів, планування запасів та підвищення ефективності бізнес-процесів. Однак разом з цими можливостями виникають питання щодо захисту приватності та безпеки даних, які потребують високого рівня уваги та дотримання відповідних нормативів [4, 5].

Сучасні технології обробки персональних даних в рітейлі допомагають підприємствам створювати більш ефективні та персоналізовані стратегії обслуговування клієнтів та маркетингу.

Рис. 1.4. Технології обробки персональних даних в рітейлі

Найбільш важливі технології обробки персональних даних в цій галузі (рис. 1.4):

- ✓ **Машинне навчання та аналітика даних**: машинне навчання використовується для аналізу великих обсягів даних та виявлення патернів споживацької поведінки. Воно допомагає підприємствам створювати персоналізовані рекомендації та прогнозувати попит на товари та послуги.
- ✓ **Обробка природної мови (NLP)**: технології NLP використовуються для аналізу текстових даних, таких як відгуки клієнтів та коментарі в соціальних мережах. Це допомагає розуміти настрої та потреби клієнтів.
- ✓ **Аналітика візуального сприйняття**: використання комп'ютерного зору для аналізу фотографій та відео. Наприклад, розпізнавання облич, визначення віку та статі клієнтів, аналіз реакцій на вітрини товарів та відстеження товарів в магазинах.

- ✓ **Автоматизована обробка документів**: технології OCR (оптичного розпізнавання символів) використовуються для перетворення паперових документів у цифровий формат та обробки інформації з них.
- ✓ **Автоматизована обробка чеків та касових чеків**: системи можуть аналізувати дані з чеків та касових чеків для визначення покупок клієнтів та їхніх споживчих звичок.
- ✓ **Блокчейн технології**: блокчейн може використовуватися для створення довіреної системи обміну даними між різними сторонами, забезпечуючи високий рівень безпеки та надійності даних.
- ✓ **Цифрові гаманці та безготівкові платежі**: збір даних про платежі та фінансові транзакції клієнтів для аналізу їхньої платіжної поведінки та надання персоналізованих пропозицій.
- ✓ **Централізовані CRM системи**: системи управління відносинами з клієнтами дозволяють збирати та обробляти дані про клієнтів та їхню історію покупок.
- ✓ **Захист даних та конфіденційності**: технології шифрування та інші засоби захисту даних важливі для збереження конфіденційності та безпеки персональної інформації.

Ці технології дозволяють роздрібним підприємствам рітейлу збирати, аналізувати та використовувати дані для покращення обслуговування клієнтів, оптимізації запасів та розвитку стратегій маркетингу. Важливо забезпечувати відповідність з законодавством щодо захисту даних та дотримуватися етичних норм у використанні персональних даних клієнтів [1-7].

Сучасні технології збору та обробки персональних даних в рітейлі розвиваються швидко, щоб допомогти підприємствам вдосконалити послуги, аналізувати споживацькі патерни та підвищити конкурентоспроможність.

Найбільш важливі сучасні технологій в рітейлі [6, 7]:

1. **Аналітика даних**: великі дані (Big Data) та інструменти аналітики даних дозволяють роздрібним підприємствам аналізувати великі обсяги інформації про покупців та їх споживчі звички. Це допомагає розуміти попит на товари та послуги, планувати запаси та персонал, а також створювати персоналізовані пропозиції.
2. **Інтернет речей (IoT)**: за допомогою сенсорів та пристроїв IoT можна відстежувати рух товарів в магазинах, контролювати температуру та освітлення, а також надавати клієнтам зручність, наприклад, в інтерактивних приміщеннях.
3. **Мобільні додатки та e-commerce**: мобільні додатки для покупок, онлайн-платежі та електронна комерція роблять збір даних та обслуговування клієнтів більш зручними і ефективними. Покупці можуть зручно здійснювати покупки через мобільні пристрої, а підприємства можуть збирати дані про їх поведінку.
4. **RFID технології**: використання RFID мікрочіпів дозволяє відстежувати рух товарів в магазинах і управляти запасами більш ефективно. Також ця технологія може використовуватися для зручності покупців та для захисту від крадіжок.
5. **Оперативні системи та POS-термінали**: системи роздрібної торгівлі використовуються для обробки платежів, відстеження запасів та збору даних про клієнтів.
6. **Персоналізація та рекомендації**: системи штучного інтелекту та машинного навчання використовуються для створення персоналізованих пропозицій та рекомендацій для клієнтів на основі їхніх попередніх покупок та інших даних.
7. **Безпека даних**: захист персональних даних є надзвичайно важливим аспектом роботи в рітейлі, і технології кібербезпеки використовуються

для запобігання несанкціонованому доступу до даних та забезпечення конфіденційності клієнтів.

8. **Безготівкові платежі та цифрові гаманці**: Технології безготівкових платежів, такі як мобільні гаманці та цифрові платіжні системи, стають все популярнішими в рітейлі та вимагають збору та обробки даних платіжної інформації.

Загалом, сучасні технології дозволяють роздрібним підприємствам рітейлу збирати, аналізувати та використовувати дані для покращення обслуговування клієнтів та оптимізації бізнес-процесів. Однак це також створює виклики щодо захисту персональних даних та дотримання вимог щодо конфіденційності та безпеки даних [6, 7, 8].

1.4. Основні загрози та ризики для персональних даних в рітейлі

Захист персональних даних в рітейлі стикається з численними загрозами та ризиками, які вимагають уважного управління та захисту. Основні загрози та ризики для персональних даних в рітейлі включають наступні аспекти [2, 8]:

1. **Кіберзлочинні атаки**: рітейлери є частою мішенню для кіберзлочинців. Зловмисники можуть намагатися викрасти персональні дані клієнтів, крадуть кредитну інформацію, вимагають викуп за збиту інформацію або завдають шкоду системам зберігання даних.

2. **Фішинг та соціальна інженерія**: атаки, спрямовані на споживачів та співробітників рітейл-компаній через шахрайство та обман, можуть призвести до неправомірного доступу до даних та втрати конфіденційності.

3. **Внутрішні загрози**: інсайдери, такі як співробітники компаній рітейлу, можуть стати джерелом ризику, особливо якщо вони мають доступ

до конфіденційної інформації та намагаються її незаконно використовувати чи розголошувати.

4. **Витоки даних**: несанкціоноване розголошення персональних даних може призвести до витоків даних та порушення конфіденційності клієнтів.

5. **Неадекватний захист даних**: недостатні заходи безпеки, слабкі паролі та вразливості в програмному забезпеченні можуть призвести до несанкціонованого доступу до систем та даних.

6. **Вимоги щодо законодавства**: рітейлери повинні дотримуватися законодавства щодо захисту персональних даних, такого як GDPR в Європейському Союзі або закони про конфіденційність в інших країнах. Невиконання цих вимог може призвести до великих штрафів.

7. **Споживацькі обурення**: клієнти можуть обурюватися за незаконний або недопустимий збір та використання їхніх персональних даних, що може призвести до втрати довіри та клієнтської бази.

8. **Неавторизовані додатки та платформи**: використання неавторизованих додатків або платформ для обробки або зберігання даних може призвести до витоку інформації та порушити безпеку даних.

Для запобігання цим загрозам та ризикам роздрібні підприємства рітейлу повинні вдосконалювати свої системи безпеки, надавати перевагу шифруванню даних, надсиланню даних в безпечних мережах, надавати підготовку співробітникам щодо кібербезпеки та дотримуватися відповідного законодавства щодо захисту даних. Ретельне планування та вдосконалення систем безпеки може допомогти мінімізувати ці ризики та зберегти конфіденційність персональних даних клієнтів [4].

Загрози та ризики для персональних даних в рітейлі є вагомою проблемою, яка вимагає серйозного наукового розгляду та вдосконалення стратегій захисту. Рітейлові компанії, що працюють з великою кількістю

клієнтських даних, стикаються із здебільшого інтернет-посиленими загрозами, що включають в себе кіберзлочинні атаки, фішинг, внутрішні загрози та інші варіанти порушення безпеки та конфіденційності даних.

Перший із зазначених аспектів полягає в кіберзлочинних атаках, які, завдяки росту кількості інтернет-залежних технологій, набувають обсягів і складності, небачених раніше. Це включає в себе атаки на інфраструктуру рітейлових компаній, які можуть призвести до витоку конфіденційних даних клієнтів. Фішинг та соціальна інженерія, що є загрозами, спрямованими на людей, надзвичайно складні і підступні [2, 8, 9].

Внутрішні загрози виникають внаслідок дій інсайдерів, включаючи співробітників, які мають доступ до персональних даних клієнтів та можуть використовувати цей доступ для власної користі або навіть зловмисних цілей. Важливо розуміти, що загрози інсайдерів можуть бути такими ж серйозними, як і зовнішні атаки.

Саме ці загрози і ризики спричиняють суттєві проблеми для рітейлових підприємств та вимагають систематичного дослідження та розробки стратегій захисту даних. Налагодження надійних систем безпеки, використання шифрування та відповідних методів аутентифікації є критично важливими для забезпечення безпеки персональних даних в рітейлі. Також необхідно враховувати законодавчі вимоги щодо захисту даних та впроваджувати власні внутрішні політики та процедури, щоб забезпечити відповідність з ними та запобігти витокам даних.

1.5. Висновки до розділу 1

Теоретичні аспекти захисту персональних даних в рітейлі відіграють критичну роль у забезпеченні конфіденційності та безпеки інформації клієнтів. Для розуміння цих аспектів важливо розглянути наступні ключові поняття та принципи: персональні дані, законодавча база, принципи обробки

даних, засоби безпеки, етичні аспекти, довіра клієнтів, своєчасна реакція на порушення безпеки, освіта співробітників.

Розуміння цих теоретичних аспектів допомагає розробити та впровадити ефективні стратегії захисту персональних даних у сфері рітейлу, забезпечуючи при цьому високий рівень конфіденційності та безпеки інформації клієнтів.

Висновки до першого розділу вказують на ключові теоретичні засади та принципи, які важливі для розуміння та впровадження ефективних стратегій захисту персональних даних в рітейлових підприємствах. Основні висновки включають наступне:

1. Комплексний підхід до захисту даних: важливість комбінування різних технологічних, організаційних та правових заходів для створення комплексної системи захисту персональних даних в рітейлі.
2. Законодавча база: наявність і регулярне оновлення законодавства щодо захисту даних, такого як GDPR, вимагає від рітейлерів дотримуватися високих стандартів та нормативів збереження та обробки даних клієнтів.
3. Шифрування та безпека даних: використання сучасних методів шифрування даних та захисту інфраструктури для запобігання несанкціонованому доступу до персональних даних.
4. Співробітництво та освіта: підприємства повинні активно співпрацювати зі спеціалістами з кібербезпеки та надавати підготовку співробітникам щодо правил безпеки даних.
5. Моніторинг та виявлення порушень: важливість постійного моніторингу та вчасного виявлення можливих порушень безпеки даних для реагування на них.

6. Етичні аспекти та довіра клієнтів: підтримка довіри клієнтів шляхом етичного та відповідального використання їхніх даних, а також надання доступу та контролю над власними даними.
7. Постійне вдосконалення: сфера кібербезпеки постійно змінюється, і рітейлери повинні бути готові до апгрейда своїх стратегій та технологій для захисту даних.

Враховуючи ці теоретичні аспекти, рітейлові підприємства можуть розробити ефективні практичні стратегії захисту персональних даних, що допоможуть забезпечити конфіденційність та безпеку даних клієнтів, зберігаючи при цьому їхню довіру та сприяючи сталому розвитку бізнесу.

РОЗДІЛ 2
СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В РІТЕЙЛІ

2.1. Криптографічні методи захисту персональних даних

Криптографія відіграє критичну роль у сфері кібербезпеки та захисту персональних даних. Криптографічні методи використовуються для шифрування чутливої інформації та забезпечення конфіденційності та цілісності даних в рітейловій галузі. Як фахівець з кібербезпеки, важливо розуміти та застосовувати ці методи для забезпечення безпеки персональних даних [2].

Однією з ключових криптографічних технік є шифрування даних. Воно використовується для перетворення звичайного тексту (незашифрованого) в незрозумілий для сторонніх криптотекст за допомогою криптографічного ключа. Шифрування забезпечує конфіденційність, оскільки лише особа з правильним ключем може розшифрувати дані.

Другим важливим аспектом є геш-функції, які використовуються для створення хеш-значень чутливих даних, таких як паролі. Геш-функції перетворюють вхідні дані в фіксований рядок, який неможливо зворотно перетворити в оригінальні дані. Це забезпечує інтегрітет даних та унеможливлює відновлення початкових даних навіть в разі витоку геш-значення [5].

Крім того, асиметрична криптографія використовує пару ключів - приватний і публічний – для забезпечення безпеки комунікації та ідентифікації сторін. Ця техніка дозволяє клієнтам та рітейлерам обмінюватися інформацією без розголошення своїх приватних ключів.

Науковий підхід до використання криптографії в рітейлі передбачає аналіз загроз, вибір відповідних алгоритмів шифрування, правильне керування ключами, а також постійний моніторинг і аудит систем захисту. Важливо також розуміти сучасні тенденції в атаках та розробляти адаптивні заходи безпеки. Криптографія є фундаментальним засобом захисту персональних даних в рітейлі та вимагає постійного вдосконалення та актуалізації.

Криптографічні методи захисту персональних даних – це набір технологій та методів, які використовуються для забезпечення конфіденційності, цілісності та доступності персональних даних в інформаційних системах та під час їх передачі через мережі [4, 7]. Ці методи базуються на математичних принципах та використовуються для захисту даних від несанкціонованого доступу та незаконного використання. Криптографічні методи включають в себе такі аспекти (рис. 2.1):

Рис. 2.1. Криптографічні методи захисту персональних даних

- Шифрування: процес перетворення звичайного тексту в незрозумілий для сторонніх криптотекст за допомогою криптографічного ключа. Шифрування забезпечує конфіденційність даних, оскільки лише особа з відповідним ключем може розшифрувати дані.
- Геш-функції: математичні функції, що перетворюють вхідні дані в фіксований рядок (геш-значення). Геш-функції використовуються для перевірки цілісності даних та створення унікальних хеш-підписів.

- Асиметрична криптографія: використовує пару ключів – приватний і публічний – для забезпечення безпеки комунікації та ідентифікації сторін. Публічний ключ використовується для шифрування, тоді як приватний ключ – для розшифрування.
- Управління ключами: криптографічні системи вимагають ефективного управління ключами – від генерації та розподілу ключів до їхньої ротації та знищення.
- Підписи та аутентифікація: криптографічні підписи використовуються для підтвердження автентичності даних та ідентифікації сторін у комунікації.
- Криптографічні протоколи: криптографічні протоколи визначають спосіб взаємодії між сторонами з урахуванням захисту даних.

Отже, до сучасних криптографічних методів захисту персональних даних відносять різноманітні техніки та підходи, які використовуються для забезпечення конфіденційності, цілісності та доступності даних. Ось деякі з основних криптографічних методів, які використовуються в сучасному захисті персональних даних: симетричне шифрування, асиметричне шифрування, хеш-функції, цифрові підписи, протоколи захищеної передачі даних, квантова криптографія, формат-перетворення (format-preserving encryption), мультифакторна аутентифікація, доменна ізоляція (domain isolation) [1, 6, 7].

Рис. 2.2. Основні криптографічні методи

- Симетричне шифрування: використовує один ключ для як шифрування, так і розшифрування даних. Популярними алгоритмами симетричного шифрування є AES (Advanced Encryption Standard) та DES (Data Encryption Standard).
- Асиметричне шифрування: в асиметричному шифруванні використовуються два ключі: публічний і приватний. Публічний ключ використовується для шифрування даних, а приватний ключ - для їх розшифрування. RSA та ECC (еліптична крива криптографія) - це приклади асиметричних шифрувальних алгоритмів.
- Хеш-функції: використовуються для створення коротких, унікальних «відбитків» великих обсягів даних. Вони часто використовуються для перевірки цілісності даних та створення «цифрових підписів».
- Цифрові підписи: використовуються для перевірки автентичності та цілісності даних. Вони базуються на асиметричних криптографічних методах та дозволяють підтверджувати, що дані не були змінені після підписання.
- Протоколи захищеної передачі даних: протоколи, такі як HTTPS (TLS/SSL), використовуються для захищеної передачі даних через мережу. Вони поєднують в собі шифрування та аутентифікацію для забезпечення безпеки під час передачі інформації.
- Квантова криптографія: це новий напрямок, який використовує властивості квантової фізики для створення надійних систем шифрування. Цей підхід обіцяє високий рівень захисту від квантових обчислювачів.
- Формат-перетворення (Format-Preserving Encryption): метод дозволяє зберігати формат та структуру даних при шифруванні, що особливо корисно для деяких типів інформації, які повинні залишати свій формат (наприклад, номери кредитних карток).

- Мультифакторна аутентифікація: комбінує кілька методів аутентифікації, включаючи паролі, біометричні дані та інші фактори для підвищення рівня безпеки.
- Доменна ізоляція (Domain Isolation): даний підхід використовується для ізоляції інформаційних систем та мереж для обмеження ризику доступу до персональних даних.

Ці криптографічні методи допомагають рітейловим підприємствам забезпечити високий рівень безпеки та конфіденційності персональних даних, що є надзвичайно важливим у сучасному світі, де дані стають об'єктом зростаючого інтересу для кіберзлочинців [5].

Криптографічні методи допомагають забезпечити високий рівень безпеки персональних даних в рітейлі, зменшуючи ризик несанкціонованого доступу, витоку чи зміни даних. Вони є фундаментальним інструментом у сфері кібербезпеки та грають важливу роль у збереженні конфіденційності даних та підтримці довіри клієнтів.

2.2. Технології обробки та зберігання персональних даних

Технології обробки та зберігання персональних даних представляють собою важливий аспект в сфері інформаційної безпеки та захисту конфіденційності клієнтської інформації в рітейловому секторі. Ці технології є фундаментальними для забезпечення безпеки та ефективного управління великими обсягами персональних даних, які зберігаються та оброблюються рітейлерами. У цьому контексті важливо розглянути технологічні аспекти, що охоплюють обробку та зберігання персональних даних з відповідністю законодавству, забезпеченням безпеки, обробкою та зберіганням даних, а також оптимізацією процесів для забезпечення ефективної роботи рітейлових підприємств [1, 5, 7].

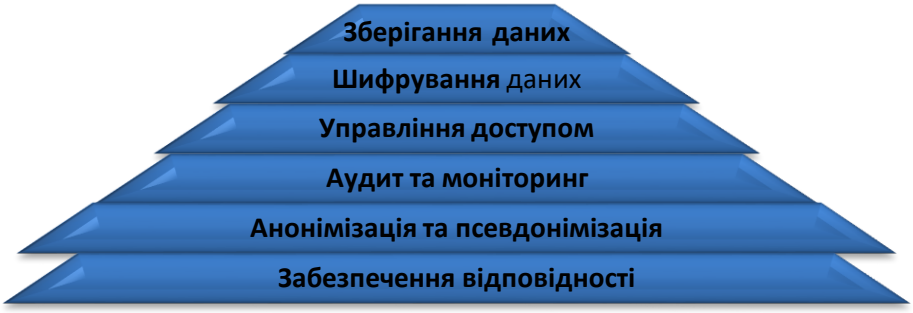

Рис. 2.2. Технології обробки та зберігання персональних даних

✓ **Зберігання даних**: технології зберігання персональних даних включають в себе використання різних видів сховищ, таких як бази даних, хмарні ресурси та фізичні сервери. Ці технології повинні забезпечити надійність, доступність та відновлення даних в разі виникнення аварій.

✓ **Шифрування даних**: використання шифрування даних на різних рівнях, включаючи транспортне та зберігання, допомагає забезпечити конфіденційність та захист даних від несанкціонованого доступу.

✓ **Управління доступом**: технології управління доступом визначають, хто має доступ до персональних даних та як він контролюється. Це може включати в себе системи ідентифікації та аутентифікації, а також ролевий доступ до даних.

✓ **Аудит та моніторинг**: системи аудиту та моніторингу допомагають виявляти незвичайну активність та потенційні порушення безпеки, що допомагає вчасно реагувати на інциденти.

✓ **Анонімізація та псевдонімізація**: технології анонімізації та псевдонімізації дозволяють зберігати корисну інформацію, не розголошуючи особистих даних.

✓ **Забезпечення відповідності**: використання технологій для відстеження відповідності з законодавством щодо захисту персональних даних, таким як GDPR, та автоматизації процесів забезпечення відповідності.

- ✓ **Оптимізація та аналітика**: використання технологій для оптимізації обробки та аналізу персональних даних для покращення рішень у сфері маркетингу та обслуговування клієнтів.

Інноваційні технології обробки та зберігання персональних даних – це передові технічні рішення та методи, спрямовані на оптимізацію обробки, зберігання та управління персональними даними з використанням сучасних інформаційних технологій та інноваційних підходів. Ці технології розробляються з метою підвищення ефективності, безпеки та якості обробки особистих даних в різних галузях, включаючи рітейл. Вони дозволяють забезпечити належний рівень конфіденційності та захисту персональних даних, що стає дедалі важливішим у світі цифрових технологій [3].

До інноваційних технологій обробки та зберігання персональних даних можна віднести такі розвинуті підходи:

- ✓ **Обробка даних в реальному часі**: використання потужних аналітичних інструментів дозволяє аналізувати та використовувати дані негайно, що корисно для персоналізації послуг та взаємодії з клієнтами.
- ✓ **Обчислення на краю (Edge Computing)**: технологія дозволяє обробляти дані на пристроях або в мережі, наближаючи обчислення до джерела даних. Це зменшує задержку та забезпечує більшу конфіденційність даних.
- ✓ **Обчислювальна гіперзберігання (Hyperconverged Storage)**: інтеграція сховищ та обчислення в єдину систему спрощує управління та зберіганням даних, забезпечуючи швидкий доступ до них.
- ✓ **Технології шифрування на рівні файлів**: використання шифрування на рівні окремих файлів забезпечує високий рівень конфіденційності даних під час їх передачі та зберігання.

- ✓ **Технології віртуалізації даних**: віртуалізація даних дозволяє управляти та переміщувати дані ефективніше, спрощуючи резервне копіювання та відновлення даних.
- ✓ **Blockchain та розподілені реєстри**: використання технологій блокчейну дозволяє створити безпечні та невід'ємні журнали обробки даних, забезпечуючи їх недоступність для змін та фальсифікації.
- ✓ **Штучний інтелект та машинне навчання**: застосування алгоритмів штучного інтелекту допомагає виявляти аномалії та загрози для даних, а також оптимізувати обробку та аналіз інформації.

Ці інноваційні технології сприяють покращенню безпеки, ефективності та якості обробки та зберігання персональних даних в рітейловій галузі, що важливо для підтримання довіри споживачів та дотримання законодавчих вимог [8].

Технології обробки та зберігання персональних даних є фундаментальними для забезпечення безпеки та ефективного управління цими даними у сфері рітейлу. Правильний вибір, налаштування та використання цих технологій дозволяють рітейлерам ефективно захищати дані клієнтів та забезпечувати дотримання вимог щодо захисту персональної інформації, сприяючи при цьому збереженню довіри споживачів та стабільному розвитку бізнесу.

2.3. Використання штучного інтелекту та машинного навчання в захисті персональних даних

Використання штучного інтелекту (ШІ) в захисті персональних даних є актуальною і важливою темою в контексті сучасних викликів у сфері кібербезпеки та обробки інформації. Штучний інтелект, зокрема машинне навчання та інші підходи, відкриває нові можливості та вдосконалює існуючі методи захисту персональних даних. Використання ШІ в цьому контексті передбачає впровадження інноваційних технологій для виявлення

загроз, відновлення безпеки та забезпечення конфіденційності даних. Ключові аспекти використання ШІ в захисті персональних даних [5, 9]:

- ✓ *Виявлення аномальної активності:* штучний інтелект може виявляти аномальну активність та несанкціонований доступ до системи на підставі аналізу великих обсягів даних. Це дозволяє реагувати на потенційні загрози швидше та ефективніше.
- ✓ *Прогнозування ризиків:* машинне навчання може використовуватися для прогнозування можливих ризиків та вразливостей у системі, допомагаючи приймати запобіжні заходи.
- ✓ *Ідентифікація аутентичності користувачів*: використання біометричних методів та інших методів ідентифікації на основі ШІ допомагає забезпечити високий рівень захисту доступу до особистих облікових записів.
- ✓ *Автоматичне шифрування та дешифрування*: ШІ може використовуватися для автоматичного шифрування та дешифрування даних під час їх обробки та передачі, що сприяє забезпеченню конфіденційності.
- ✓ *Контроль доступу та ролева автоматизація:* ШІ може допомагати у встановленні та контролі доступу до різних частин системи, а також в автоматичному призначенні ролей користувачам.
- ✓ *Захист від атак маніпулювання моделями ШІ*: використання ШІ для виявлення атак на моделі машинного навчання та покращення стійкості до таких атак.
- ✓ *Забезпечення відповідності*: ШІ може бути використаний для автоматизації процесів відстеження та відповідності з законодавством щодо захисту даних, таким як GDPR.

Використання ШІ в захисті персональних даних відкриває нові можливості для підвищення рівня безпеки та реагування на загрози в реальному часі. Відповідно до сучасних вимог до безпеки даних, інтеграція

ШІ є ключовим елементом стратегії захисту персональної інформації в рітейловому секторі, сприяючи збереженню конфіденційності даних та підвищенню довіри споживачів до обробки їхньої особистої інформації.

Використання машинного навчання (МН) в захисті персональних даних є важливим інструментом у сучасній сфері кібербезпеки та обробки інформації. Машинне навчання може допомогти виявляти та відстежувати загрози, вдосконалювати системи виявлення несанкціонованого доступу та забезпечувати конфіденційність та цілісність даних. Ключові аспекти використання машинного навчання в захисті персональних даних [7]:

- ✓ *Виявлення загроз і аномалій:* машинне навчання може бути використане для розпізнавання аномальних паттернів, які можуть свідчити про потенційні загрози. Наприклад, аналіз змін у звичайному трафіку мережі або активності користувачів може виявити незвичайні або підозрілі події.
- ✓ *Прогнозування ризику і вразливостей*: машинне навчання дозволяє аналізувати дані для виявлення можливих ризиків та вразливостей в системі. Це може сприяти прийняттю запобіжних заходів та виправленню існуючих слабкостей.
- ✓ *Ідентифікація аутентичності користувачів*: використання МН для біометричної ідентифікації, включаючи розпізнавання облич, голосу та відбитків пальців, може допомогти підвищити рівень безпеки доступу до особистих облікових записів.
- ✓ *Автоматичне шифрування та дешифрування*: машинне навчання може використовуватися для автоматичного шифрування та дешифрування даних під час їх обробки та передачі, забезпечуючи конфіденційність та цілісність даних.
- ✓ *Аналітика та прогнозування інцидентів*: машинне навчання допомагає аналізувати дані про інциденти та ризики, а також прогнозувати

можливі події, що допомагає у вчасному реагуванні та уникненні загроз.

- ✓ *Контроль доступу та ролева автоматизація*: МН може бути використане для встановлення та контролю доступу до різних частин системи та автоматичного призначення ролей користувачам, що зменшує ризик несанкціонованого доступу.
- ✓ *Захист від атак маніпулювання моделями МН*: використання МН для виявлення атак на моделі машинного навчання та покращення стійкості до таких атак.
- ✓ *Забезпечення відповідності*: МН може бути використане для автоматизації процесів відстеження та відповідності з законодавством щодо захисту даних, таким як GDPR.

Використання машинного навчання в захисті персональних даних робить можливим більш ефективне та автоматизоване виявлення загроз та покращення реагування на них. Відповідно до сучасних вимог до безпеки даних, інтеграція машинного навчання є ключовим елементом стратегії захисту персональної інформації в рітейловому секторі, сприяючи збереженню конфіденційності даних та підвищенню рівня безпеки обробки особистих інформації клієнтів [2, 4, 8].

Використання ШІ та МН в захисті персональних даних є сучасною стратегією, яка допомагає зберегти конфіденційність, цілісність та доступність цих даних у світі, де кіберзагрози стають все більш виразними та різноманітними. Інтеграція цих технологій в системи захисту персональних даних сприяє покращенню безпеки та довіри споживачів до обробки їхніх особистих інформаційних даних в рітейловому секторі та інших галузях.

2.4. Біометричні технології в рітейлі

Біометричні технології в рітейлі − це сучасний метод ідентифікації та аутентифікації користувачів, який базується на унікальних фізичних чи поведінкових рисах особи. Ця інноваційна технологія дозволяє рітейлерам підвищити рівень безпеки та зручності для клієнтів, спрощує процес аутентифікації та взаємодії зі службами рітейлу. Біометричні дані, такі як розпізнавання обличчя, відбитків пальців, голосу, рукопису тощо, використовуються для ідентифікації користувачів, а також для аналізу та відстежування їхнього поведінки та вподобань.

Ця технологія в рітейлі використовується для різних цілей, включаючи аутентифікацію покупців при безконтактних платежах, відслідковування руху та поведінки клієнтів в магазинах, а також для покращення безпеки та захисту персональних даних. Біометричні технології в рітейлі стають все більш популярними завдяки своїй ефективності та зручності, що допомагає покращити якість обслуговування та збільшити рівень захисту в цій галузі [2].

У вік цифрових інновацій та зростаючої обізнаності споживачів стосовно захисту персональних даних, біометричні технології стають важливим інструментом для рітейлових підприємств. Біометричні дані, які включають в себе розпізнавання обличчя, відбитків пальців, голосу та інших унікальних фізичних рис користувачів, стають джерелом надійного та невід'ємного ідентифікації особи. Ось докладний огляд використання біометричних технологій в рітейлі, включаючи їхні виклики та переваги. Застосування біометричних технологій в рітейлі.

1. *Аутентифікація користувачів*: біометричні технології дозволяють точно та надійно ідентифікувати користувачів при вході в онлайн-акаунти або під час платежів. Це допомагає уникнути несанкціонованого доступу та шахрайства.
2. *Відслідковування покупців*: у фізичних магазинах біометричні системи можуть служити для відслідковування руху покупців та аналізу їхнього

споживчого поведінки. Це дозволяє рітейлерам покращити обслуговування та асортимент товарів.

3. *Боротьба зі злочинністю*: використання розпізнавання обличчя може допомогти виявляти крадіїв та інших осіб, які порушують закон в магазинах. Це сприяє зменшенню крадіжок та підвищенню безпеки в магазинах.

4. *Онлайн та оффлайн безпека*: біометричні дані можуть використовуватися для захисту особистих даних споживачів як у цифровому, так і у фізичному середовищі. Це допомагає уникнути несанкціонованого доступу до приватної інформації.

Виклики використання біометричних технологій в рітейлі

1. *Приватність та захист даних*: збір та зберігання біометричних даних потребують високого рівня захисту та дотримання правил щодо приватності. Інциденти, пов'язані з витоками біометричних даних, можуть створити серйозні проблеми для рітейлерів.
2. *Ефективність та точність*: біометричні системи не завжди є ідеальними та можуть виявляти помилки у виявленні і ідентифікації осіб. Важливо постійно вдосконалювати алгоритми та забезпечувати надійність систем.

3. *Легальні аспекти*: в деяких юрисдикціях використання біометричних даних підлягає строгим правовим обмеженням. Рітейлери повинні дотримуватися всіх відповідних законів та нормативів.

Переваги використання біометричних технологій в рітейлі

1. *Надійність*: біометричні технології забезпечують високий рівень надійності ідентифікації осіб, оскільки вони ґрунтуються на унікальних фізичних рисах.
2. *Зручність*: користувачі вважають біометричні методи ідентифікації зручними, оскільки вони не вимагають запам'ятовування паролів або пін-кодів.

3. *Підвищення безпеки*: використання біометричних технологій сприяє підвищенню рівня безпеки для користувачів та рітейлерів.

Біометричні технології в рітейлі мають значний потенціал для поліпшення якості обслуговування, захисту даних та боротьби зі злочинністю. Проте їхнє впровадження вимагає ретельного розгляду всіх аспектів, включаючи приватність, безпеку та суворе дотримання відповідних правових норм. В майбутньому біометричні технології можуть стати необхідним стандартом для рітейлових підприємств, що прагнуть забезпечити максимальний рівень обслуговування та безпеки для своїх клієнтів.

2.5. Висновки до розділу 2

У розділі розглянуто широкий спектр інноваційних підходів та методів, які сприяють підвищенню рівня безпеки та конфіденційності персональних даних в сучасному рітейловому секторі. Висновки цього розділу дозволяють сформулювати ключові пункти та підсумки з використання сучасних технологій захисту даних в рітейлі:

1. Збільшення загроз та важливість захисту даних: зростання кількості цифрових даних і зростаюча кількість кіберзагроз створюють серйозні виклики для рітейлу, щодо яких необхідно приділяти особливу увагу захисту персональних даних.
2. Розширені методи шифрування: використання сучасних методів шифрування дозволяє забезпечити конфіденційність даних під час зберігання та передачі.
3. Біометричні технології та аутентифікація: використання біометричних технологій, таких як розпізнавання обличчя та відбитків пальців, спрощує процес аутентифікації та забезпечує високий рівень безпеки.
4. Машинне навчання та штучний інтелект: впровадження МН та ШІ дозволяє автоматизувати виявлення загроз, а також розробляти адаптивні системи захисту.

5. Законодавча вимоги до захисту даних: суворі законодавчі вимоги, такі як Загальний регламент з питань захисту даних (GDPR), вимагають від рітейлерів дотримання високих стандартів захисту персональних даних.
6. Постійне оновлення та навчання: збереження високого рівня безпеки вимагає постійного оновлення систем та навчання персоналу.

В цілому, використання сучасних технологій захисту даних в рітейлі допомагає підвищити рівень безпеки, покращити обслуговування клієнтів та виконати законодавчі вимоги щодо захисту персональних даних. Проте, важливо постійно слідкувати за новими загрозами та розвивати стратегії захисту для забезпечення найвищого ступеня безпеки в цьому сфері.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЙ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДПРИЄМСТВІ РІТЕЙЛУ

3.1. Розробка та впровадження конфігурації захисної системи на прикладі підприємства рітейлу

У сучасному рітейловому секторі, де обмін, зберігання та обробка великих обсягів персональних даних стають загальною практикою, захист цих даних стає надзвичайно важливим завданням. З врахуванням постійно зростаючого обсягу цифрових загроз та вимог законодавства щодо захисту даних, впровадження та конфігурація захисних систем стають необхідністю для підприємств рітейлу [7-9].

Методологія впровадження захисних систем

Процес впровадження захисних систем на підприємстві рітейлу вимагає системного підходу та дотримання наукових методів. Основні етапи цього процесу включають [2]:

1. **Аналіз вимог щодо захисту даних**: перший крок полягає в аналізі потреб і вимог щодо захисту даних на підприємстві. Цей етап передбачає визначення видів даних, їх чутливості та загроз, які можуть вплинути на їх безпеку.
2. **Вибір захисних систем та технологій**: включає вибір оптимальних захисних систем та технологій, які відповідають вимогам підприємства. Це може включати антивірусне програмне забезпечення, системи моніторингу, механізми шифрування та інші заходи безпеки.

3. **Розробка стратегії захисту даних:** передбачає розробку стратегії, яка включає в себе політику безпеки, процедури реагування на інциденти та інші аспекти захисту даних.
4. **Впровадження та конфігурація систем**: передбачає реалізацію вибраних захисних систем та їх налаштування з урахуванням потреб підприємства. Він включає в себе інсталяцію, налаштування та інтеграцію систем у існуючу інфраструктуру.
5. **Навчання персоналу**: персонал підприємства повинен бути належно навчений щодо користування та підтримки захисних систем. Це важливий аспект захисту даних.
6. **Моніторинг та аудит безпеки**: передбачає постійний моніторинг та аудит безпеки для виявлення потенційних загроз та аномалій.

Підприємства рітейлу збирають, обробляють та зберігають значний обсяг особистих даних клієнтів, таких як інформація про платіжні картки, адреси електронної пошти та інші особисті дані. З урахуванням зростаючої кількості кіберзлочинців та законодавчих вимог щодо захисту даних, підприємства рітейлу повинні вживати заходів для забезпечення безпеки цих даних [4, 8].

Крок 1: *Аналіз вимог до безпеки даних*

Перший етап полягає в аналізі вимог до безпеки даних. Підприємство повинно визначити, які дані вони обробляють, які з них є чутливими, ідентифікувати потенційні загрози та ризики для цих даних. Науковий підхід передбачає проведення аудиту безпеки для виявлення слабких місць.

Приклад: Підприємство рітейлу визначило, що обробляє платіжні дані своїх клієнтів та прагне запобігти можливим атакам на ці дані.

Крок 2*: Вибір захисних систем та технологій*

Після аналізу вимог до безпеки даних, підприємство повинно вибрати відповідні захисні системи та технології. Це може включати в себе

встановлення антивірусного програмного забезпечення, систем моніторингу безпеки, механізми шифрування даних та інші заходи безпеки.

Приклад: Підприємство встановило захисну систему для виявлення та блокування несанкціонованих спроб доступу до платіжних даних.

Крок 3: *Розробка стратегії безпеки даних*

Після вибору захисних систем підприємство повинно розробити стратегію безпеки даних. Ця стратегія включає в себе політику безпеки, процедури реагування на інциденти, механізми контролю доступу та інші аспекти безпеки даних.

Приклад: Підприємство розробило політику безпеки, яка вимагає регулярної зміни паролів для доступа до систем обробки платежів.

Крок 4*: Впровадження та конфігурація систем*

На цьому етапі підприємство впроваджує вибрані захисні системи та налаштовує їх з урахуванням конкретних потреб та вимог підприємства.

Приклад: Підприємство встановило систему двофакторної аутентифікації для доступа до систем обробки платежів.

Крок 5: *Навчання персоналу*

Персонал підприємства повинен бути навчений користуватися захисними системами та дотримуватися політики безпеки.

Приклад: Персонал пройшов навчання щодо виявлення та повідомлення про підозрілі активності в системах обробки платежів.

Крок 6: *Моніторинг та аудит безпеки*

Після впровадження захисних систем, підприємство повинно постійно моніторити безпеку даних та проводити аудит безпеки для виявлення потенційних загроз та аномалій.

Приклад: Підприємство використовує системи моніторингу безпеки для виявлення незвичайних активностей в системах обробки платежів.

Впровадження та конфігурація захисних систем на підприємстві рітейлу є необхідним для забезпечення безпеки та конфіденційності даних. Науковий підхід передбачає системний підхід до аналізу, вибору та впровадження заходів безпеки для забезпечення захисту особистих даних клієнтів і дотримання вимог законодавства. Послідовність кроків та їх ретельне виконання допомагають підприємству ефективно захищати дані та підтримувати довіру споживачів.

Розробка та впровадження конфігурації захисної системи на прикладі підприємства рітейлу

Розробка конфігурації захисної системи для підприємства роздрібної торгівлі (рітейлу) − це важливий крок для забезпечення безпеки даних, товарів і працівників, а також для запобігання крадіжкам та іншим злочинам. Ось кілька кроків, які ви могли б розглянути при розробці такої конфігурації [1-5]:

Етап 1. Оцінка загроз і ризиків:

- Провести аналіз загроз і ризиків, які можуть вплинути на підприємство рітейлу (включає крадіжки, шахрайство, кібератаки, природні катастрофи тощо).

Етап 2. Фізична безпека:

- Встановити системи відеоспостереження та контролю доступу в магазинах, складах та офісах.
- Захищати важливі активи за допомогою сейфів та сховищ.

Етап 3. Кібербезпека:

- Захистити інформаційні системи підприємства від кібератак. Це включає в себе застосування файрволів, антивірусного програмного забезпечення та систем моніторингу безпеки.
- Забезпечити безпеку в мережі Wi-Fi для клієнтів та працівників.

Етап 4. Безпека даних:

- Захистити особисті дані клієнтів від несанкціонованого доступу і витоків даних.
- Забезпечити резервне копіювання даних і розробити план відновлення після інцидентів.

Етап 5. Навчання співробітників:

- Навчати працівників правилам безпеки та встановити процедури дії в разі виявлення підозрілих обставин.
- Здійснювати перевірку на предмет злочинної діяльності при прийомі на роботу.

Етап 6. Магазинний інвентар і товари:

- Використовувати системи RFID (Radio-Frequency Identification) для відстеження товарів і запобігання крадіжкам.
- Встановити системи антикрадіжкової сигналізації та маркування товарів.

Етап 6. Відносини з правоохоронними органами:

- Співпрацювати з місцевою поліцією та іншими правоохоронними органами для розслідування крадіжок та інших правопорушень.

Етап 7. Постійна оцінка та вдосконалення:

- Постійно оцінювати ефективність захисних заходів та вносити виправлення і покращення на основі нових загроз і ризиків.

Етап 8. Поділ обов'язків:

- Призначити відповідальних осіб або команди для виконання різних аспектів безпеки.

Це загальний підхід до розробки конфігурації захисної системи для підприємства рітейлу. [9] Залежно від розміру і специфіки підприємства, можуть бути потрібні додаткові заходи безпеки та рішення. Найкраще проконсультуватися з фахівцями з безпеки, щоб створити індивідуальну конфігурацію, яка відповідає певним потребам.

Розробка захисної системи для підприємства рітейлу вимагає використання різних технологій та програмних рішень. Можна використовувати різні мови програмування для створення різних компонентів системи безпеки. Ось приклад такої конфігурації, використовуючи мову програмування Python (додаток А). Зазначений код лише загальний приклад та не включає в себе всі можливі аспекти безпеки, які можуть бути важливими для певного підприємства. Конфігурація захисної системи повинна бути ретельно розроблена з урахуванням конкретних потреб і загроз підприємства [1, 7].

Крім того, важливо пам'ятати про юридичні аспекти і вимоги до захисту особистих даних, які можуть бути обов'язковими в роздрібній торгівлі, зокрема, в рамках Загального регламенту про захист особистих даних (GDPR) або інших відповідних правових норм.

3.2. Методи аудиту та моніторингу захисту персональних даних

Забезпечення захисту персональних даних на підприємствах, особливо в сучасному цифровому середовищі, є завданням важливим та вимагає системного підходу. Методи аудиту та моніторингу захисту персональних даних є комплексом процедур та інструментів, спрямованих на виявлення, аналіз, та контроль над безпекою персональних даних. Методи аудиту та моніторингу відіграють ключову роль у виявленні порушень безпеки даних та забезпеченні їх надійного захисту [4].

1. Аудит безпеки даних

Аудит безпеки даних — це систематичне дослідження та оцінка заходів безпеки даних та процесів на підприємстві. Цей метод полягає в систематичному огляді та оцінці політик, процедур, систем та інфраструктури безпеки даних на підприємстві з метою визначення слабких місць та відповідності їх сучасним стандартам та вимогам. Аудит включає аналіз прав доступу, оцінку фізичних та логічних заходів безпеки, а також

ідентифікацію потенційних загроз та ризиків для безпеки даних. Метод включає етапи:

- **Аналіз політик та процедур безпеки**: дослідження наявних політик та процедур безпеки даних для оцінки їх відповідності сучасним стандартам та вимогам.
- **Оцінка фізичних та логічних заходів безпеки**: аналіз фізичних параметрів, таких як захищені приміщення для серверів, та логічних параметрів, таких як мережеві заходи безпеки.
- **Перевірка доступу до даних**: виявлення та аналіз прав доступу до персональних даних, включаючи облікові записи користувачів та їхні права.
- **Виявлення потенційних загроз та ризиків**: ідентифікація можливих загроз безпеці даних та оцінка ризиків для їх конфіденційності, цілісності та доступності.
- **Аналіз аудиту безпеки**: вивчення результатів аудиту для виявлення вразливостей та розробка плану заходів для усунення дефіцитів.

2. Моніторинг безпеки даних

Моніторинг безпеки даних — це постійний процес контролю та спостереження за даними та системами для вчасного виявлення аномалій та потенційних загроз безпеці. Моніторинг полягає у постійному контролі та спостереженні за активностями даних та систем з метою виявлення незвичайних або підозрілих подій. Цей метод включає в себе використання систем журналювання подій для запису активностей, виявлення вразливостей, моніторинг мережі для спостереження за мережевим трафіком та аналізу журналів подій та інцидентів. Також може використовувати автоматизовані системи виявлення загроз. Складається з елементів [3]:

- **Системи журналювання подій**: використання систем журналювання подій для запису активностей в системах та мережах для подальшого аналізу.

- **Виявлення вразливостей**: використання систем виявлення вразливостей для пошуку слабких місць в системах та програмному забезпеченні.
- **Моніторинг мережі**: спостереження за мережевим трафіком для виявлення незвичайних або підозрілих активностей.
- **Аналіз журналів подій та інцидентів**: поєднання інформації з журналів подій та інцидентів для виявлення незвичайних подій та негайної реакції на них.
- **Автоматизовані системи виявлення загроз**: використання інструментів та систем штучного інтелекту для автоматизованого виявлення загроз та реагування на них.

Методи аудиту та моніторингу є важливими компонентами захисту персональних даних на підприємствах. Науковий підхід до цих методів включає аналіз, оцінку, виявлення та реагування на загрози безпеці даних. Ці методи допомагають підприємствам зберігати конфіденційність, цілісність та доступність даних, забезпечуючи їх надійний захист у сучасному цифровому середовищі.

3.3. Розробка конкретних рішень та інструментів для забезпечення ефективності захисту персональних даних

Розробка конкретних рішень та інструментів для забезпечення ефективності захисту персональних даних − це важливий аспект забезпечення безпеки даних на підприємстві рітейлу. Для цього можуть бути розроблені такі рішення та інструменти [2]:

1. **Системи керування доступом (Access Control Systems)**: розробка та впровадження систем керування доступом дозволяє підприємству обмежувати доступ до персональних даних лише авторизованим користувачам. Це включає в себе розробку систем аутентифікації, авторизації та аудиту доступу.

2. **Інструменти моніторингу безпеки (Security Monitoring Tools)**: розробка та впровадження інструментів моніторингу безпеки дозволяє виявляти незвичайні активності та аномалії в системах обробки даних. Ці інструменти допомагають оперативно реагувати на потенційні загрози. Наприклад, розробляють інструмент для моніторингу та журналювання подій в системі. Використовують бібліотеки для журналювання подій, наприклад, **logging**, та вивчають журнали для виявлення підозрілих або нестандартних активностей (додаток Б).
3. **Інструменти шифрування даних (Data Encryption Tools)**: розробка та впровадження інструментів шифрування даних допомагає забезпечити конфіденційність даних під час їх передачі та зберігання. Шифрування даних важливе для захисту від несанкціонованого доступу. Приклад: використання бібліотеки Python, такої як **cryptography**, для шифрування даних в базі даних, на сервері та при їх передачі. Шифрування даних допоможе запобігти несанкціонованому доступу до конфіденційної інформації. Приклад використання **cryptography** для шифрування показаний в додатку Б.
4. **Системи резервного копіювання та відновлення (Backup and Recovery Systems)**: розробка систем резервного копіювання та відновлення даних допомагає забезпечити доступність даних та їх швидке відновлення в разі інциденту або аварії.
5. **Політики та процедури безпеки (Security Policies and Procedures)**: розробка конкретних політик та процедур безпеки даних допомагає створити структурований підхід до захисту даних та забезпечити відповідність з правовими вимогами.
6. **Інтеграція з системами аналізу даних (Integration with Data Analytics Systems)**: розробка інтеграції з системами аналізу даних дозволяє виявляти патерни та загрози у великих обсягах даних та вчасно реагувати на них. Інтеграція систем безпеки з системами аналізу

даних може значно підвищити ефективність захисту та допомогти в розпізнаванні аномалій та загроз. Система безпеки повинна генерувати події та журнали подій, які можуть бути інтегровані з системами аналізу даних. Використовуйте стандартизовані формати журналів, такі як Common Event Format (CEF) або Security Information and Event Management (SIEM), для легкості інтеграції. Крім того, включають системи моніторингу мережі, такі як Intrusion Detection Systems (IDS) та Intrusion Prevention Systems (IPS), які можуть реєструвати та передавати події про виявлені загрози. Використовують системи моніторингу активності користувачів та ідентифікації, такі як системи управління ідентифікацією та доступом (IAM), для слідкування за діями користувачів і виявлення аномальних активностей. Створюють дашборди та інтерактивні засоби візуалізації даних, які дозволяють спеціалістам з безпеки аналізувати та моніторити стан безпеки в режимі реального часу. Часто використовують рішення SIEM для агрегації та аналізу даних безпеки з різних джерел. Інтегруйте ваші системи безпеки з SIEM, такими як Splunk, ELK Stack, або IBM QRadar, для централізованого моніторингу та аналізу. Наприклад, розробка інтеграції з системами аналізу даних за допомогою Python та використання **REST API** для взаємодії з системою аналізу даних (на прикладі використання **Elasticsearch та Kibana**). В цьому прикладі (додаток В) дані про подію (наприклад, спроба входу користувача) надсилаються в **Elasticsearch**, який може використовуватися для аналізу даних. Після інтеграції можна використовувати інструменти, такі як **Kibana**, для візуалізації та аналізу цих даних. Залежно від конкретної системи аналізу даних і інфраструктури безпеки, спосіб інтеграції та формат передачі даних може відрізнятися. Важливо також забезпечити безпеку та конфіденційність передачі даних, зокрема, шляхом використання HTTPS, автентифікації та авторизації. Ця

інтеграція дозволяє аналізувати дані з системи безпеки в реальному часі та швидко виявляти потенційні загрози та аномалії, що допомагає забезпечити безпеку підприємства рітейлу.

7. **Виявлення вторгнень:** використання інструментів для виявлення вторгнень, які можуть виявити підозрілу активність у вашій мережі або системі. Популярні бібліотеки для виявлення вторгнень включають Snort, Suricata та PyIDS.
8. **Системи автоматизованого виявлення загроз (Automated Threat Detection Systems)**: розробка систем автоматизованого виявлення загроз дозволяє підприємствам швидко реагувати на потенційні загрози безпеці даних та автоматично застосовувати заходи безпеки. Наприклад, створення інструменту для автоматизованого аналізу вразливостей в мережі та програмному забезпеченні. Використовують бібліотеки, такі як **nmap**, для сканування портів та визначення вразливих систем.
9. **Системи ідентифікації та аутентифікації (Identity and Authentication Systems)**: розробка систем ідентифікації та аутентифікації дозволяє перевіряти ідентичність користувачів та підтверджувати їх доступ до даних. Це включає в себе системи одноразових паролів, біометричну ідентифікацію та інші методи. Наприклад, розробляють систему управління ідентифікацією та доступом з використанням бібліотеки Python, такої як **Flask**, для автентифікації користувачів і керування їх доступом до ресурсів (додаток Д).

Показані інструменти та бібліотеки можуть бути використані для розробки потужної системи безпеки для захисту персональних даних на підприємстві рітейлу. Потрібно дотримуватися найкращих практик безпеки для забезпечення найвищого рівня захисту. Ці конкретні рішення та інструменти сприяють підвищенню ефективності захисту персональних

даних на підприємстві рітейлу та забезпечують надійний захист цих даних від потенційних загроз та інцидентів.

3.4. Рекомендації щодо подальших дій підприємств рітейлу в сфері захисту персональних даних

Рекомендації щодо подальших дій підприємств рітейлу в сфері захисту персональних даних включають наступні кроки [6, 9]:

1. **Проведення аудиту безпеки даних**: потрібно розпочинати з аудиту безпеки даних, щоб оцінити поточний стан та ідентифікувати слабкі місця в системах та процесах захисту. Використовуйте цей аудит для визначення, які аспекти потребують найбільшого уваги.
2. **Оновлення політик та процедур безпеки**: переглянути та оновити політики та процедури безпеки даних на підприємстві. Вони повинні відповідати сучасним стандартам та вимогам, включаючи вимоги до захисту персональних даних.
3. **Навчання та освіта персоналу**: забезпечити навчання та освіту персоналу щодо правил та процедур безпеки даних. Це включає в себе навчання щодо виявлення підозрілих активностей та процедур повідомлення про інциденти.
4. **Використання технологій захисту даних**: розглянути використання сучасних технологій захисту даних, таких як шифрування, системи ідентифікації та аутентифікації, інструменти моніторингу безпеки та системи виявлення вразливостей.
5. **Моніторинг та аудит безпеки**: запровадити системи моніторингу та аудиту безпеки, які дозволять виявляти та реагувати на незвичайні або підозрілі активності у реальному часі.
6. **Захист від внутрішніх загроз**: приділити увагу заходам захисту від внутрішніх загроз, включаючи обмеження доступу до критичних даних та моніторинг дій власного персоналу.

7. **Реагування на інциденти**: розробити план реагування на інциденти та вправи для перевірки цього плану. Готуватися до швидкого та ефективного реагування на можливі інциденти безпеки.
8. **Відповідність із законодавством**: переконатися, що діяльність відповідає вимогам законодавства щодо захисту персональних даних, включаючи Загальний регламент з охорони даних (GDPR) та інші регіональні стандарти.
9. **Стале вдосконалення**: захист даних − це постійний процес. Постійно потрібно вдосконалювати методи та процедури, враховуючи сучасні загрози та технологічні розвитки.
10. **Співпраця та консультації**: розглянути можливість співпраці з експертами з кібербезпеки та консультантами, які допоможуть розробити та впровадити найкращі практики забезпечення безпеки даних.

Захист персональних даних є важливим завданням для підприємств рітейлу, оскільки він впливає на довіру клієнтів та відповідність законодавству. Дотримання цих рекомендацій допоможе забезпечити високий рівень безпеки та конфіденційності даних на вашому підприємстві.

3.5. Висновок до розділу 3

В сучасному цифровому світі, де обмін та обробка персональних даних стали невід'ємною частиною діяльності підприємств рітейлу, безпека цих даних стала найважливішим завданням. Ця потреба у захисті персональних даних стає ще більш актуальною в контексті росту кількості кіберзагроз та посилення законодавчих вимог до їх захисту. У цьому контексті важливим стає практичне впровадження та реалізація технологій захисту персональних даних на підприємствах рітейлу.

Практична реалізація технологій захисту персональних даних на підприємстві рітейлу передбачає послідовність дій та заходів, спрямованих на забезпечення безпеки та конфіденційності даних клієнтів та партнерів.

У розділі розглянуто практичну реалізацію технологій та заходів забезпечення безпеки персональних даних на підприємстві рітейлу. Практичні кроки, які були вжиті для захисту даних, відображають важливість інтеграції наукових та технологічних знань у повсякденну діяльність підприємства. На основі результатів проведених досліджень та аналізу ризиків, були розроблені та впроваджені практичні рішення для підвищення захисту персональних даних клієнтів та партнерів.

Перший крок у практичній реалізації заходів захисту даних - це аудит безпеки. В рамках цього аудиту проводиться аналіз поточних систем та процесів безпеки. Визначаються слабкі місця та вразливості, а також ідентифікуються потенційні загрози безпеці даних.

На основі результатів аудиту розробляються та оновлюються політики та процедури безпеки. Вони включають в себе вимоги до доступу до даних, процедури аутентифікації, шифрування даних та інші аспекти безпеки.

Важливим кроком є навчання та освіта персоналу щодо правил та процедур безпеки даних. Інформований персонал може виявити підозрілі активності та правильно реагувати на інциденти.

Практична реалізація включає в себе впровадження сучасних технологій захисту даних, таких як системи шифрування, ідентифікації та аутентифікації, інструменти моніторингу безпеки та системи виявлення загроз.

Системи моніторингу та аудиту безпеки встановлюються для постійного контролю за активностями даних та виявлення незвичайних подій. Це допомагає вчасно реагувати на загрози та вразливості. Розробляється план реагування на інциденти та проводяться вправи для перевірки цього плану. Готовність до швидкого та ефективного реагування

на можливі інциденти безпеки є важливою складовою практичної реалізації заходів захисту даних. У рамках практичної реалізації важливо переконатися, що діяльність підприємства відповідає вимогам законодавства щодо захисту персональних даних, включаючи Загальний регламент з охорони даних (GDPR) та інші регіональні стандарти. Практична реалізація технологій захисту даних є постійним процесом. Підприємство повинно постійно вдосконалювати свої методи та процедури, враховуючи сучасні загрози та технологічні розвитки. Практична реалізація технологій захисту персональних даних є важливим завданням для підприємств рітейлу, оскільки вона впливає на довіру клієнтів та відповідність законодавству. Дотримання цих кроків допоможе забезпечити високий рівень безпеки та конфіденційності даних на підприємстві рітейлу.

Важливим аспектом є вдосконалення системи керування доступом, що дозволило обмежити доступ до персональних даних лише авторизованим користувачам, а також впровадження систем моніторингу та аудиту безпеки для реагування на незвичайні події та виявлення потенційних загроз. Використання інструментів шифрування даних та систем ідентифікації сприяло забезпеченню конфіденційності та цілісності даних.

Також було надано великий акцент на навчанні та освіті персоналу, що є важливим фактором успішної реалізації заходів з захисту даних. Інформований та підготовлений персонал стає важливим ланком у системі захисту даних.

Усі ці практичні заходи спрямовані на забезпечення безпеки та конфіденційності персональних даних на підприємстві рітейлу, що в свою чергу сприяє підвищенню довіри клієнтів та забезпечує відповідність з актуальним законодавством у сфері захисту даних. В цілому, практична реалізація технологій захисту персональних даних є важливим кроком у забезпеченні безпеки та конфіденційності даних на підприємстві рітейлу.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Захист персональних даних стає дедалі важливішим завданням для підприємств рітейлу, оскільки вони обробляють великі обсяги особистої інформації клієнтів та партнерів. Сучасні технології збору та обробки даних дозволяють підприємствам рітейлу створювати персоналізовані послуги для клієнтів, але вони також створюють нові ризики для безпеки даних. Законодавча база щодо захисту персональних даних постійно розвивається, і підприємства повинні дотримуватися вимог законодавства, такого як GDPR, щоб уникнути штрафів і втрати довіри клієнтів. Важливим аспектом є вдосконалення систем захисту даних та постійний аудит безпеки для виявлення та усунення загроз.

Пропозиції:

1. Підприємства рітейлу повинні виділити ресурси на сучасні кібербезпечні технології, включаючи шифрування, моніторинг безпеки та системи виявлення загроз.
2. Регулярні аудити безпеки та моніторинг допоможуть вчасно виявляти потенційні загрози та реагувати на них.
3. Розробка та впровадження плану реагування на кіберінциденти обов'язкова для ефективного управління кризовими ситуаціями.
4. Використання зовнішнього експертного досвіду та консультації з кібербезпеки може покращити рівень захисту даних.
5. Підприємства повинні дотримуватися вимог законодавства щодо захисту персональних даних, таких як GDPR.
6. Обмін досвідом та найкращими практиками з іншими підприємствами рітейлу може сприяти загальному підвищенню рівня безпеки даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Орешич, В. В. Захист персональної інформації в кіберпросторі / Вадим Віталійович Орешич // Проблеми цивільного права та процесу : тези доп. учасників наук.-практ. конф./ МВС України, Харків. нац. ун-т внутр. справ; Харків. обл. осередок Всеукр. громад. орг. «Асоціація цивілістів України», Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2023. – С. 417-419.
2. Гнатюк С. Л. Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти: аналіт. доп. / С. Л. Гнатюк. – К. : НІСД, 2014. – 92 с.
3. Цифрова економіка : підручник / Т. І. Олешко, Н. В. Касьянова, С. Ф. Смерічевський та ін. – К. : НАУ, 2022. – 200 с.
4. Kelly D. Martin, Jisu J. Kim, Robert W. Palmatier, Lena Steinhoff, David W. Stewart, Beth A. Walker, Yonggui Wang, and Scott K. Weaven Data Privacy in Retail. Journal of Retailing. 2020 Dec; 96(4): 474–489.
5. Charles A. Sennewald, John H. Christman. Retail Crime, Security, and Loss Prevention: An Encyclopedic: Butterworth-Heinemann, Vol. 14 No. 2 2008, p.704.
6. Єсімов С. С. Захист персональних даних у контексті розвитку динамічних інформаційних систем. URL: http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsy/03_2013/13yessdis.pdf
7. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
8. Пилипчук В.Г., Брижко В.М. Реформування і розвиток системи захисту персональних даних в Україні. Інформація і право. 2017. № 3(22). С. 5
9. Захист персональних даних в сфері Інтернет речей / О. Баранов, В. Брижко // Інформація і право. – № 2(17)/2015. – 75-81.0.

ДОДАТКИ

Додаток А

Конфігурація захисної системи для підприємства рітейлу з використанням мови програмування Python

```
# Імпорт бібліотек
import cameras
import access_control
import inventory_tracking
import firewall
import encryption
import backup_recovery

# Фізична безпека: Відеоспостереження та контроль доступу
cameras.install()  # Встановити відеокамери для відеоспостереження
access_control.setup()  # Встановити систему контролю доступу

# Кібербезпека: Захист мережі та інформаційних систем
firewall.configure()  # Налаштування брандмауера для мережі
encryption.enable()  # Увімкнути шифрування даних

# Безпека даних: Захист особистих даних клієнтів
data_security = DataSecurity()
data_security.protect_customer_data()

# Співробітники: Навчання та моніторинг
employee_training = EmployeeTraining()
employee_training.train_staff()
employee_monitoring = EmployeeMonitoring()
employee_monitoring.monitor_activity()
```

Продовження додатку А

```
# Магазинний інвентар і товари: Відстеження товарів
inventory_tracking.setup()  # Встановити систему відстеження товарів

# План відновлення після інцидентів: Резервне копіювання та відновлення
backup_recovery.configure()  # Налаштування резервного копіювання та відновлення

# Постійна оцінка та вдосконалення: Моніторинг та аналіз
security_monitoring = SecurityMonitoring()
security_monitoring.monitor_security_events()
security_analysis = SecurityAnalysis()
security_analysis.analyze_weaknesses()

# Поділ обов'язків: Налаштування ролей та доступу
user_roles = UserRoles()
user_roles.configure_roles_and_permissions()

# Додаткові заходи безпеки
# Додайте інші компоненти та налаштування захисної системи, що відповідають вашим потребам.

# Запуск головного циклу системи безпеки
while True:
    # Основна логіка безпеки тут
    pass
```

Додаток Б

Використання бібліотеки Python, такої як *cryptography*, для шифрування даних в базі даних, на сервері та при їх передачі

```
from cryptography.fernet import Fernet

# Генерація ключа
key = Fernet.generate_key()

# Шифрування даних
fernet = Fernet(key)
encrypted_data = fernet.encrypt(b'My sensitive data')

# Розшифрування даних
decrypted_data = fernet.decrypt(encrypted_data)
```

Інструмент для моніторингу та журналювання подій в систем, з використанням бібліотеки *logging* для журналювання подій

```
import logging

# Налаштування журналювання
logging.basicConfig(filename='security.log', level=logging.INFO)

# Журналювання події
logging.info('User X accessed sensitive data.')
```

Інструмент для автоматизованого аналізу вразливостей в мережі та програмному забезпеченні, використовуючи бібліотеки *nmap* для сканування портів та визначення вразливих систем

```
import nmap

# Створення об'єкту nmap
nm = nmap.PortScanner()

# Сканування портів на визначеному IP-адресі
nm.scan('192.168.1.1', '1-1024')

# Виведення результатів скану
print(nm.all_hosts())
```

Додаток В

Розробка інтеграції з системами аналізу даних за допомогою Python та використання *REST API* для взаємодії з системою аналізу даних (на прикладі використання *Elasticsearch та Kibana*)

```
import requests
import json

# Приклад даного витягу даних, який ви хочете аналізувати та інтегрувати
data_to_analyze = {
    "timestamp": "2023-10-19T12:00:00",
    "event_type": "login_attempt",
    "user_id": "12345",
    "ip_address": "192.168.1.100"
}

# Відправити дані для аналізу в Elasticsearch
elasticsearch_url = "http://elasticsearch-server:9200/my_security_index/_doc"
headers = {'Content-Type': 'application/json'}

response = requests.post(elasticsearch_url, data=json.dumps(data_to_analyze),
headers=headers)

# Перевірити статус відповіді та обробити відповідь
if response.status_code == 201:
    print("Дані було успішно інтегровано в Elasticsearch.")
else:
    print("Помилка інтеграції з Elasticsearch. Статус відповіді:",
response.status_code)

# Додатковий аналіз може виконуватися в системі аналізу даних, такій як
Kibana
# Ви можете налаштувати візуалізації та дашборди для відстеження аномалій
```

Додаток Д

Система управління ідентифікацією та доступом з використанням бібліотеки Python, такої як *Flask*, для автентифікації користувачів і керування їх доступом до ресурсів

```
from flask import Flask, request, redirect, url_for

app = Flask(__name)

@app.route('/login', methods=['POST'])
def login():
    # Проведення автентифікації користувача
    if valid_login(request.form['username'], request.form['password']):
        # Встановлення сесії
        session['logged_in'] = True
        return redirect(url_for('protected_resource'))
    else:
        return 'Login failed'

@app.route('/protected_resource')
def protected_resource():
    # Перевірка доступу користувача до захищеного ресурсу
    if session.get('logged_in'):
        return 'This is a protected resource.'
    else:
        return 'Access denied'

if __name__ == '__main__':
    app.run()
```