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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо захисту персональних даних на підприємстві»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Олександр ГАЙДАЙЧУК
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ГАЙДАЙЧУК Олександр
(прізвище, ім'я)

Керівник д.ф., доцент, МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

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

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гайдайчуку Олександру Володимировичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо захисту персональних даних на підприємстві»

керівник кваліфікаційної роботи Марченко Віталій, д.ф., доцент
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Enzuzo;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту кінцевих точок організації.
2. Аналіз методів та засобів захисту персональних даних.
3. Розроблення рекомендацій щодо захисту персональних даних на підприємстві відповідно до міжнародних стандартів.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок організації.	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз методів та засобів захисту персональних даних на підприємстві.		
4.	Практична реалізація аналізу вебсайту підприємства на відповідність вимогам GDPR на базі Enzuzo.		
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Олександр ГАЙДАЙЧУК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ГАЙДАЙЧУКА Олександра

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту персональних даних на підприємстві»

Актуальність: Захист персональних даних на підприємствах стає все більш критичним через зростання кількості кіберзагроз та обсягів оброблюваних даних. Сучасні підприємства все більше залежать від інформаційних систем, і будь-які порушення безпеки можуть призвести до значних фінансових втрат, втрати довіри клієнтів та юридичних наслідків. Відповідність міжнародним стандартам, таким як GDPR та HIPAA, є обов'язковою для збереження репутації та уникнення штрафів. Ефективні заходи та рекомендації щодо захисту даних допоможуть підприємствам забезпечити конфіденційність, цілісність та доступність інформації, що є необхідним для їх стабільної та безперервної роботи в умовах сучасних кіберзагроз. Тому тема дипломної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми захисту персональних даних на підприємстві та створено рекомендації щодо дотримання всіх вимог для якісного захисту цих даних.
2. Досліджено методи та засоби захисту кінцевих точок організації на базі FortiEDR.
3. Запропоновано варіант системи захисту персональних даних на підприємстві на базі Enzuzo та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі було використано не найкращий метод для аналізу та проведення перевірок на відповідність вимогам, так як доступ до них не був відкритим.
2. Запропонований порядок застосування методів та засобів захисту кінцевих точок бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ГАЙДАЙЧУКА Олександра** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ГАЙДАЙЧУК Олександр до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту персональних даних на підприємстві».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ГАЙДАЙЧУК Олександр*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ГАЙДАЙЧУК Олександр*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ГАЙДАЙЧУКА Олександра*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ГАЙДАЙЧУК Олександр** допускається до захисту
даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 53 сторінки, 17 рисунків, 12 джерел.

Об'єкт дослідження – система управління персональними даними на підприємстві, яка включає правові, організаційні, технологічні та методологічні аспекти захисту інформації.

Предмет дослідження – методи та процедури ідентифікації, аналізу та мінімізації ризиків, пов'язаних з обробкою персональних даних на підприємстві.

Мета роботи розробка рекомендацій щодо захисту персональних даних на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних та державних стандартів та їх порівняння, розробка рекомендацій щодо захисту персональних даних на підприємстві.

Проведене дослідження підтвердило актуальність та необхідність впровадження сучасних методів і технологій для захисту персональних даних на підприємствах. У рамках дипломної роботи було виявлено основні вразливості персональних даних, зокрема технічні, організаційні та людські фактори, які можуть спричинити витік або несанкціонований доступ до даних. Розглянуто вплив міжнародних стандартів GDPR та HIPAA на процеси обробки даних, що дозволило порівняти їх з актуальними нормами українського законодавства та визначити ключові відмінності та подібності.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, ПЕРСОНАЛЬНІ ДАНІ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДПРИЄМСТВІ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 9

ВСТУП 10

1 АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДПРИЄМСТВІ 11

1.1.Загальна характеристика персональних даних і їх значення в діяльності підприємства 11

1.2. Аналіз вразливостей персональних даних на підприємстві та методів їх витоку 14

1.3. Аналіз проблеми захисту ПД та вплив GDPR і HIPAA на процеси обробки персональних даних 17

2 ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ 23

2.1. Аналіз нормативної бази та правових аспектів захисту даних згідно GDPR та HIPAA та порівняння їх з актуальними пунктами ДСТУ 23

2.2. Огляд сучасних технологій і методик захисту персональної інформації 31

2.3. Розробка корпоративної політики захисту персональних даних та впровадження організаційних заходів 37

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ на основі Enzuzo 56

3.1. Розробка критеріїв оцінки ПЗ на відповідність вимогам GDPR 56

3.2. Застосування “Enzuzo” для перевірки інформаційних систем підприємства на дотримання вимог GDPR 70

3.3. Розробка рекомендацій щодо захисту персональних даних на підприємстві на основі Enzuzo..... 78

ВИСНОВКИ 81

ПЕРЕЛІК ПОСИЛАНЬ..... 83

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 85

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES - Advanced Encryption Standard

ABAC - Attribute-Based Access Control

EDR - Endpoint Detection and Response

ECC - Elliptic Curve Cryptography

GDPR - General Data Protection Regulation

HIPAA - Health Insurance Portability and Accountability Act

IAM - Identity and Access Management

MDM - Mobile Device Management

RBAC - Role-Based Access Control

RSA - Rivest-Shamir-Adleman

SHA-3 - Secure Hash Algorithm 3

SSO - Single Sign-On

ПД - Персональні дані

ВСТУП

Актуальність дослідження. Наразі кількість інцидентів, які спричиняють витік чи несанкціонований доступ до персональної інформації працівників різних підприємств зростає, та тенденції не вказують на потенційне зменшення їх. Таке зростання вказує на потребу у вдосконаленні існуючих методів та розробці нових рекомендацій для їх захисту.

З огляду на зростаючу кіберзагрозу, підприємства повинні не тільки дотримуватись нормативно-правової бази, але й розвивати внутрішні політики та процедури, що забезпечують надійний захист інформації про особисті дані. Це повинно включати в себе розробку комплексних систем захисту, навчання персоналу, створення ефективної системи реагування на інциденти та впровадження сучасних технологічних рішень.

Комплексний підхід до захисту даних забезпечує декілька різних факторів, а саме: відповідність сучасним вимогам законодавства а також одну із складових стійкості бізнесу в умовах зростаючих кіберризиків

Об'єкт дослідження - система управління персональними даними на підприємстві, яка включає правові, організаційні, технологічні та методологічні аспекти захисту інформації.

Предмет дослідження - методи та засоби захисту персональних даних на підприємстві.

Мета роботи - розробка рекомендацій щодо захисту персональних даних на підприємстві.

Методи дослідження - опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних та державних стандартів та їх порівняння, розробка рекомендацій щодо захисту персональних даних на підприємстві.

Практичне значення одержаних результатів: рекомендації щодо захисту персональних даних на підприємстві можуть бути використані у сфері забезпечення кібербезпеки у корпоративних інформаційних системах

1 АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПІДПРИЄМСТВІ

1.1.Загальна характеристика персональних даних і їх значення в діяльності підприємства

В наш час цифрові технології відіграють неабияку роль у ролі життєвого циклу будь-якого підприємства. Обробка будь-якого процесу в житті компанії полегшується в десятки разів завдяки його цифровізації. Проте, для того, щоб ефективно оптимізовувати процеси, досить часто доводиться збирати та зберігати протягом довгого часу персональні дані працівників, клієнтів та, потенційно, третіх осіб, дані яких можуть бути корисні при обробці тих чи інших процесів. Визначимо основні поняття, які тим чи іншим чином зачіпають цю тему.

Згідно з Законом Україні №2297–VI Про захист персональних даних, персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Це означає, що персональні дані можуть включати будь-яку інформацію, яка прямо або опосередковано може вказувати на конкретну людину.

1. Ідентифікована особа - це людина, яку можна точно визначити за допомогою певних даних. Наприклад, ім'я, прізвище, по батькові, адреса проживання, номер телефону, електронна адреса тощо. Якщо у вас є така інформація, ви можете точно сказати, про кого йде мова.

2. Особа, яка може бути конкретно ідентифікована - це людина, яку можна визначити за допомогою додаткових даних або комбінації даних. Наприклад, номер соціального страхування, ідентифікаційний код, IP-адреса, дані про місцезнаходження, або інші унікальні ідентифікатори. Навіть якщо інформація не вказує прямо на особу, вона може бути достатньою для ідентифікації в комбінації з іншими даними.

Які можуть бути приклади персоналних даних:

1. Основні ідентифікаційні дані: ім'я, дата народження, номер паспорта.
2. Контактна інформація: телефонний номер, адреса електронної пошти, домашня адреса.
3. Фінансові дані: номер банківського рахунку, кредитна історія.
4. Медичні дані: медична історія, діагнози, дані про лікування.
5. Біометричні дані: відбитки пальців, фотографії, зображення обличчя.
6. Онлайн-ідентифікаційні дані: IP-адреси, cookie-файли, ідентифікатори пристроїв.

Персональні дані відіграють критичну роль у діяльності підприємств, зокрема в аналізі ринку та споживацької поведінки. Це дозволяє підприємствам отримувати глибоке розуміння своїх клієнтів, що включає інформацію про їхні вподобання, поведінку та звички. Завдяки цьому бізнес може краще сегментувати ринок, виявляти нові можливості для зростання, адаптувати свої пропозиції та створювати більш цільові маркетингові кампанії, що підвищує ефективність маркетингу та продажів.

Детальний опис значення персональних даних:

1. Сегментація ринку:

- Розуміння демографічних характеристик: Персональні дані, такі як вік, стать, місце проживання та дохід, дозволяють підприємствам сегментувати своїх клієнтів на різні групи. Це допомагає створювати спеціалізовані продукти або послуги, які відповідають потребам кожної групи.

- Поведінковий аналіз: Аналізуючи поведінку клієнтів (наприклад, історію покупок, частоту візитів на сайт, взаємодію з рекламою), компанії можуть виявляти закономірності, які допомагають краще зрозуміти споживачів і відповідно адаптувати маркетингові стратегії (Penn LPS Online) (Termly).

2. Виявлення нових можливостей для зростання:

- Аналіз трендів: Персональні дані допомагають підприємствам відстежувати та аналізувати ринкові тренди. Це дозволяє передбачати зміни в

уподобаннях споживачів і швидко реагувати на них, впроваджуючи нові продукти чи послуги.

- Ідентифікація незадоволених потреб: За допомогою аналізу даних компанії можуть виявляти потреби, які ще не задоволені на ринку. Це відкриває нові можливості для розвитку та інновацій (Datafloq).

3. Адаптація пропозицій:

- Персоналізація маркетингових кампаній: Використовуючи персональні дані, компанії можуть створювати більш цільові та релевантні маркетингові кампанії. Наприклад, реклама може бути адаптована під індивідуальні вподобання та потреби клієнтів, що підвищує ймовірність успіху кампаній.

- Динамічне ціноутворення: Персональні дані дозволяють застосовувати динамічне ціноутворення, коли ціни можуть змінюватися в залежності від попиту, часу доби, місця розташування клієнта та інших факторів (Harvard Business Review).

4. Підвищення ефективності маркетингу та продажів:

- Оптимізація каналів продажів: Аналіз даних допомагає визначити найефективніші канали продажів і маркетингу, що дозволяє сконцентрувати зусилля та ресурси на найприбутковіших напрямках.

- Вимірювання ефективності маркетингових кампаній: Персональні дані дозволяють оцінювати успішність маркетингових кампаній у реальному часі та вносити необхідні корективи для досягнення кращих результатів (Penn LPS Online).

Отже, персональні дані відіграють невід’ємну роль в діяльності підприємства, через що вони є особливо важливим кластером інформації, яка повинна зберігатись та оброблятись підприємствами для створення ефективних рішень з точки зору сервісу, маркетингу, тощо. Ці дані можуть бути як проблемою при ризиках витоку інформації так і чудовим багажем знань для підприємства, що може значно покращити себе завдяки цьому.

1.2. Аналіз вразливостей персональних даних на підприємстві та методів їх витоку

Вразливість персональних даних (ВПД) - це слабке місце в системі, процесі або заході безпеки, яке може бути використане зловмисником для несанкціонованого доступу до, використання, розкриття, зміни або знищення персональних даних.

ВПД можуть існувати різного типу, наприклад:

Ось деякі поширені причини ВПД:

1. Технічні вразливості

1.1. Недостатньо захищені системи зберігання даних: Багато підприємств використовують застаріле або ненадійне обладнання для зберігання даних, що робить їх вразливими до кібератак.

1.2. Використання застарілого програмного забезпечення: Застаріле ПЗ часто має невиправлені вразливості, які можуть бути використані зловмисниками для доступу до конфіденційної інформації.

1.3. Відсутність шифрування при передачі даних: Якщо дані передаються в незашифрованому вигляді, вони можуть бути перехоплені та прочитані сторонніми особами.

1.4. Уразливості в мережевій інфраструктурі: Недостатньо захищені мережі можуть бути піддані атакам, таким як проникнення через незахищені порти або використання слабких паролів.

2. Організаційні вразливості

2.1. Недостатня обізнаність співробітників щодо політики безпеки: Співробітники можуть не знати про існуючі політики та процедури захисту даних, що підвищує ризик випадкових або навмисних порушень безпеки.

2.2. Відсутність регулярних аудитів та перевірок систем безпеки: Без регулярного моніторингу та оцінки безпекових практик, підприємства можуть не виявити нові вразливості або недоліки в захисті.

2.3. Неадекватні процедури управління доступом до даних: Відсутність чітких правил щодо надання та обмеження доступу до конфіденційних даних може призвести до їх несанкціонованого використання.

2.4. Відсутність планів реагування на інциденти безпеки: Без належно розроблених та впроваджених планів реагування на інциденти, підприємство може виявитися неготовим до оперативного вирішення проблем безпеки.

3. Людський фактор

3.1. Недбалість або помилки співробітників: Людський фактор залишається однією з основних причин витоків даних. Помилки можуть включати випадкове видалення даних або неправильне налаштування систем безпеки.

3.2. Відсутність навчання з інформаційної безпеки: Співробітники, які не отримали належного навчання, можуть не усвідомлювати важливості захисту даних та бути вразливими до соціальної інженерії.

3.3. Соціальна інженерія та фішингові атаки: Зловмисники можуть використовувати психологічні прийоми для отримання конфіденційної інформації, видаючи себе за довірених осіб.

Важливо зазначити, що ВПД може виникнути навіть у організаціях, які мають надійні заходи безпеки. Тому важливо постійно відстежувати та оцінювати ризики ВПД, а також вживати заходів для їх пом'якшення.

ВПД надають можливість появи інцидентів інформаційної безпеки, результатом яких буде втрата чи виток персональних даних. Серед методів витоку персональних даних визначають:

1. Технічні методи:

- Вторгнення: Зловмисники можуть отримати несанкціонований доступ до ваших систем і даних, використовуючи різні методи, такі як експлойти нульового дня, фішинг, шкідливі програми та брутфорс-атаки.
- Витік даних: Персональні дані можуть бути ненавмисно розкриті через помилку або недбалість, наприклад, через незахищені електронні листи, втрачені USB-накопичувачі або неправильно налаштовані веб-сайти.

- Внутрішні погрози: Недобросовісні або ненавчені співробітники можуть навмисно або ненавмисно розкрити або викрасти дані.
- Фізичне викрадення даних: Зловмисники можуть фізично викрасти носії даних або сервери, на яких зберігаються персональні дані.

2. Організаційні методи:

- Недостатня політика та процедури: Відсутність чітких політик і процедур щодо захисту персональних даних може призвести до помилок і вразливостей.
- Недостатнє навчання співробітників: Співробітники, які не знають про ризики кібербезпеки та не розуміють, як захищати дані, можуть стати мішенню для зловмисників.
- Недостатній контроль доступу: Надання співробітникам занадто широкого доступу до даних може збільшити ризик несанкціонованого розкриття або використання.
- Недостатні технічні заходи безпеки: Застаріле програмне забезпечення, слабкі паролі та нешифровані дані можуть полегшити зловмисникам доступ до даних.

3. Соціальні методи:

- Соціальна інженерія: Зловмисники можуть маніпулювати людьми, щоб вони розкрили конфіденційну інформацію або надали доступ до даних.
- Шантаж: Зловмисники можуть погрожувати публікацією або розкриттям персональних даних, якщо їм не буде надано щось цінне.
- Фішинг: Зловмисники можуть надсилати електронні листи або текстові повідомлення, які виглядають так, ніби вони надходять від законних джерел, щоб спонукати людей розкрити конфіденційну інформацію або перейти за посиланнями на шкідливі веб-сайти.

4. Фізичні методи:

- Підслуховування: Зловмисники можуть використовувати електронні пристрої для перехоплення телефонних розмов або онлайн-спілкування.

- Підглядання: Зловмисники можуть використовувати камери або інші пристрої для спостереження за людьми, щоб отримати доступ до персональних даних.
- Крадіжка даних: Зловмисники можуть фізично викрасти носії даних, такі як паперові документи, USB-накопичувачі або ноутбуки.

Вразливість персональних даних (ВПД) є серйозною загрозою для будь-якого підприємства. Вона може призвести до витоків даних, інцидентів інформаційної безпеки та значних фінансових втрат. Важливо пам'ятати, що захист персональних даних - це постійний процес. Зловмисники постійно розробляють нові методи атак, тому підприємствам необхідно бути на крок попереду і вживати заходів для захисту своїх даних.

1.3. Аналіз проблеми захисту ПД та вплив GDPR і HIPAA на процеси обробки персональних даних

Наразі мобільні додатки та IoT-пристрої набувають все більшого поширення, саме через це захист персональних даних (ПД) стає критично важливою проблемою для будь-якого підприємства. Ці технології генерують, зберігають та обробляють значні обсяги даних про користувачів, роблячи їх ласою здобиччю для зловмисників.

Незахищені ПД можуть нести в собі ряд ризиків, які можуть мати серйозні наслідки для підприємств. Серед ризиків, до яких можуть бути схильні незахищені ПД можна визначити такі:

- Несанкціонований доступ: Зловмисники можуть отримати доступ до ПД через кібератаки, фізичну крадіжку або людську помилку.
- Несанкціоноване використання: Зловмисники можуть використовувати ПД для шахрайства, крадіжки особистих даних, фішингу або інших злочинних цілей.

- Витік даних: ПД можуть бути ненавмисно розкриті через помилку або недбалість, наприклад, через незахищені електронні листи, втрачені USB-накопичувачі або неправильно налаштовані веб-сайти.
- Зміна або знищення даних: Зловмисники можуть змінити або знищити ПД, що може призвести до фінансових втрат або шкоди репутації.

Ці ризики є досить вагомими та можуть мати дуже серйозні наслідки, наприклад:

- Фінансові втрати: Витік даних, шахрайство або крадіжка особистих даних можуть призвести до значних фінансових втрат для підприємств.
- Юридичні санкції: Законодавство багатьох країн передбачає суворі штрафи для підприємств, які не вживають належних заходів для захисту ПД.
- Пошкодження репутації: Витік даних або незаконне використання ПД може серйозно пошкодити репутацію підприємства.
- Втрата довіри клієнтів: Користувачі можуть втратити довіру до компанії, що негативно вплине на її лояльність та прибуток.
- Переривання роботи: Кібератаки або інші інциденти інформаційної безпеки можуть призвести до перебоїв у роботі та втрати продуктивності.

У сучасному цифровому світі, де дані стали рушійною силою багатьох компаній, захист персональних даних (ПД) перетворився на критичну необхідність, а не просто на формальність.

Чому це так важливо?

Витік даних може завдати непоправної шкоди репутації компанії, призвести до значних фінансових втрат та навіть до юридичних санкцій. Зловживання ПД зловмисниками може мати руйнівні наслідки, адже вони можуть використовувати їх для шахрайства, крадіжки особистих даних або фішингу. Це не лише негативно вплине на клієнтів та партнерів, а й завдасть непоправної шкоди репутації компанії.

Втрата довіри - це те, чого будь-який бізнес прагне уникнути. Споживачі стають все більш обізнаними про питання захисту даних і очікують, що їхні ПД

будуть захищені. Недотримання жорстких законів про захист ПД, таких як GDPR в ЄС та HIPAA в США**,** може призвести до значних штрафів та інших санкцій.

Інвестування в захист ПД - це не просто витрата, а розумне вкладення, яке може допомогти захистити ваш бізнес від багатьох ризиків. Це також може допомогти вам побудувати міцні стосунки з клієнтами та партнерами, що, в свою чергу, може стати рушійною силою зростання вашого бізнесу.

Загальний регламент про захист даних (GDPR), прийнятий Європейським Союзом у 2016 році, мав значний вплив на те, як підприємства та організації в усьому світі збирають, обробляють та зберігають персональні дані (ПД). Ось деякі з ключових моментів впливу GDPR на процеси обробки ПД:

1. Підвищення рівня прозорості та контролю:

- GDPR надає фізичним особам більше прав щодо їхніх ПД, включаючи право на доступ, виправлення, видалення, обмеження обробки та перенесення даних.
- Організації зобов'язані чітко та прозоро інформувати фізичних осіб про те, як вони збирають, обробляють та використовують їхні ПД.
- Фізичні особи мають право висловити незгоду з обробкою своїх ПД.

2. Посилення вимог до згоди:

- GDPR вимагає від організацій отримувати чітку та специфічну згоду від фізичних осіб на обробку їхніх ПД.
- Згода має бути вільною, конкретною, обґрунтованою та однозначною.
- Організації повинні мати можливість довести те, що згоду було надано.

3. Впровадження принципу "проектування за замовчуванням за принципом конфіденційності та за замовчуванням за принципом захисту даних":

- Організації повинні вбудовувати принципи захисту даних та конфіденційності у свої процеси та системи обробки ПД на стадії проектування та за замовчуванням.
- Це означає, що ПД повинні бути мінімізовані, псевдонімізовані та оброблені таким чином, щоб мінімізувати ризики для прав та свобод фізичних осіб.

4. Впровадження принципу "підзвітності":

- Організації повинні нести відповідальність за дотримання принципів GDPR та вживати відповідних заходів для забезпечення їх дотримання.
- Це включає в себе призначення відповідального за захист даних, проведення оцінки впливу на захист даних та впровадження належних технічних та організаційних заходів безпеки.

5. Збільшення ризику штрафів:

- GDPR передбачає значні штрафи за невиконання його вимог, до 4% від річного світового обороту або 20 мільйонів євро, залежно від того, що більше.
- Це призвело до підвищення обізнаності та акценту на дотриманні GDPR з боку організацій у всьому світі.

Загалом, GDPR мав значний вплив на те, як підприємства та організації поводяться з ПД. Це призвело до більшої прозорості, посилення контролю з боку фізичних осіб, більш жорстких вимог до згоди та впровадження принципу "проектування за замовчуванням за принципом конфіденційності та за замовчуванням за принципом захисту даних". Організації, які не дотримуються GDPR, ризикують зіткнутися зі значними штрафами.

Закон про переносимість та підзвітність медичного страхування (HIPAA), прийнятий у Сполучених Штатах у 1996 році, мав значний вплив на те, як медичні організації та постачальники послуг поводяться з захищеною медичною інформацією (PHI). PHI - це тип ПД, який включає інформацію про здоров'я, історію хвороби та інші медичні дані особи. Ось деякі з ключових наслідків HIPAA:

1. Підвищення рівня захисту PHI:

- HIPAA встановлює жорсткі стандарти для захисту PHI, включаючи фізичні, адміністративні та технічні заходи безпеки.
- Медичні організації та постачальники послуг повинні вживати заходів для запобігання несанкціонованому доступу, розкриттю, використанню, зміні або знищенню PHI.

2. Надання пацієнтам більшого контролю над своєю PHI:

- Пацієнти мають право на доступ до своєї PHI, запитувати її копію та вносити до неї виправлення.
- Вони також мають право на обмеження того, як їхня PHI використовується та розкривається.

3. Впровадження принципу найменшого розкриття:

- Медичні організації та постачальники послуг повинні розкривати PHI лише в тому випадку, коли це дозволено законом або коли пацієнт дає явну згоду.
- Розкриття PHI повинно бути мінімізовано, щоб забезпечити захист конфіденційності пацієнтів.

4. Впровадження принципу підзвітності:

- Медичні організації та постачальники послуг повинні нести відповідальність за дотримання правил HIPAA та вживати відповідних заходів для забезпечення їх дотримання.

5. Збільшення ризику штрафів:

- HIPAA передбачає значні штрафи за невиконання його вимог, до 50 000 доларів США за кожне порушення.

Загалом, HIPAA мав значний вплив на те, як медичні організації та постачальники послуг поводяться з PHI. Це призвело до підвищення рівня захисту PHI, надання пацієнтам більшого контролю над своїми даними, впровадження принципу найменшого розкриття та підвищення підзвітності. Організації, які не дотримуються HIPAA, ризикують зіткнутися зі значними штрафами.

З вищезазначеної інформації ми можемо зробити короткий висновок, що захист персональних даних (ПД) став критично важливим питанням для будь-якого підприємства. Незахищені ПД можуть призвести до серйозних наслідків, таких як фінансові втрати, юридичні санкції, пошкодження репутації та втрата довіри клієнтів.

Тому інвестування в захист ПД - це не просто витрата, а розумне вкладення, яке може допомогти захистити ваш бізнес від багатьох ризиків. Це також може

допомогти вам побудувати міцні стосунки з клієнтами та партнерами, що, в свою чергу, може стати рушійною силою зростання вашого бізнесу.

Важливо пам'ятати про такі закони, як GDPR та HIPAA, які встановлюють жорсткі вимоги до захисту ПД. Недотримання цих законів може призвести до значних штрафів та інших санкцій.

2 ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Наразі дані стали ключовим активом для багатьох організацій, саме тому захист персональних даних (ПД) перетворився на критичну проблему. Неналежне поводження з ПД може призвести до серйозних наслідків, таких як фінансові втрати, крадіжка особистих даних та пошкодження репутації.

Захист персональних даних є не лише юридичною вимогою, але й важливою складовою підтримки довіри клієнтів та репутації організації. В умовах постійних кіберзагроз підприємства повинні впроваджувати ефективні методи та інструменти для забезпечення безпеки інформації. У цьому розділі розглянемо основні підходи та стратегії для захисту персональних даних, аналізуючи їхню ефективність та доцільність у сучасних умовах.

2.1. Аналіз нормативної бази та правових аспектів захисту даних згідно GDPR та HIPAA та порівняння їх з актуальними пунктами ДСТУ

Як уже було сказано в попередньому розділі - GDPR та HIPAA є одними з найважливіших та найпоширеніших міжнародних стандартів захисту інформації. Між ними є досить значна різниця, так як GDPR охоплює загалом безпеку даних користувачів, що є громадянами ЄС, а HIPAA - це стандарт захисту саме медичної інформації, тобто знань, що дають змогу ідентифікувати стан здоров’я конкретної людини. Для обох цих стандартів є аналог в українському законодавстві - Закон України «Про захист персональних даних».

Таблиця 2.1.

Порівняймо загальну інформацію про ці законодавчі дані:

Законодавство	HIPAA (Health Insurance Portability and Accountability Act)	GDPR (General Data Protection Regulation)	Закон України "Про захист персональних даних"
Сфера застосування	Медична інформація громадян США	Персональні дані фізичних осіб в ЄС	Персональні дані фізичних осіб в Україні
Мета	Захист конфіденційності та безпеки медичної інформації	Захист прав та свобод фізичних осіб щодо їхніх персональних даних	Захист прав та свобод фізичних осіб щодо їхніх персональних даних
Основні принципи	- Найменшого розкриття - Адміністративні, технічні та фізичні запобіжні заходи - Обмежений доступ - Підзвітність	- Законність, обґрунтованість та справедливість обробки - Обмеження мети обробки - Мінімізація даних - Точність даних - Зберігання даних протягом обмеженого періоду - Цілісність та конфіденційність даних - Підзвітність	- Законність, обґрунтованість та справедливість обробки - Обмеження мети обробки - Мінімізація даних - Точність даних - Зберігання даних протягом обмеженого періоду - Цілісність та конфіденційність даних - Підзвітність
Права суб'єкта персональних даних	- Доступ до власної медичної інформації - Виправлення помилок - Запит про обмеження обробки	- Доступ до власних персональних даних - Виправлення помилок - Видалення даних - Обмеження	- Доступ до власних персональних даних - Виправлення помилок - Видалення даних - Обмеження

	- Переносимість даних - Видалення даних	обробки - Переносимість даних - Заперечення проти обробки	обробки - Переносимість даних - Заперечення проти обробки
Обов'язки володільця персональних даних	- Розробка та впровадження політики захисту медичної інформації - Навчання персоналу - Захист медичної інформації від несанкціонованого доступу, розкриття, використання, зміни або знищення - Регулярний аудит та оновлення практики захисту даних	- Розробка та впровадження політики захисту персональних даних - Призначення відповідального за захист даних - Оцінка впливу на захист даних - Впровадження належних технічних та організаційних заходів - Навчання персоналу - Співпраця з регулюючими органами	- Розробка та впровадження політики захисту персональних даних - Призначення відповідального за захист даних - Оцінка впливу на захист даних - Впровадження належних технічних та організаційних заходів - Навчання персоналу - Співпраця з регулюючими органами
Відповідальність за порушення	Штрафи до 50 000 доларів США за кожне порушення	Штрафи до 4% від світового річного обороту або 20 мільйонів євро, залежно від того, що більше	Штрафи до 1 000 000 гривень

Як ми можемо побачити з таблиці, наведеної вище, стандарти GDPR та Закон України "Про захист персональних даних" є практично ідентичними за загальним їх описом. При цьому, HIPAA - це закон, що має відношення лише специфічно персональні дані про здоров’я, виключаючи іншу персональну інформацію про людину.

Проте, в межах даної роботи куди важливіше буде розглянути вимоги цих законів до технічного забезпечення інформаційних ресурсів, що можуть бути використані підприємством, тому розглянемо їх:

Таблиця 2.2.

Вимоги	Закон України "Про захист персональних даних"	GDPR (ЄС)	HIPAA (США)
Шифрування	Рекомендується, але не є обов’язковим. Рекомендуються шифри AES-256, RSA-2048	Стаття 32: обов'язкове шифрування при передачі та зберіганні даних. Використовуються AES-256, RSA-2048	Обов'язкове для захисту електронної інформації. Використовуються AES-256, RSA-2048
Контроль доступу	Обмеження доступу на основі ролей. Вимагає аутентифікації користувачів та розмежування доступу	Стаття 25, 32: обмеження доступу на основі потреби. Вимагає багатофакторної аутентифікації	Обов'язкове. Використовуються методи аутентифікації, авторизації та контроль доступу на основі ролей (RBAC)
Моніторинг та аудит	Рекомендується проведення регулярних аудитів безпеки та логування подій	Стаття 32: обов'язкове проведення регулярних аудитів та логування подій	Обов'язкове. Включає регулярні аудити безпеки, логування доступу та діяльності користувачів
Інформування про порушення	Обов'язкове інформування контролюючих органів та суб'єктів даних у разі витоку даних. Термін – протягом 72 годин	Стаття 33, 34: обов'язкове інформування регуляторних органів та суб'єктів даних протягом 72	Обов'язкове інформування пацієнтів та регуляторних органів. Термін – без зволікань

		годин	
Управління ризиками	Рекомендується проведення оцінки ризиків з використанням ISO/IEC 27005	Стаття 35: обов'язкове проведення оцінки впливу на захист даних (DPIA)	Обов'язкове проведення аналізу та управління ризиками. Використовується NIST SP 800-30
Документація та політики	Обов'язкове ведення документації щодо обробки персональних даних, включаючи політики безпеки	Стаття 30: обов'язкове ведення документації та політик захисту даних	Обов'язкове ведення політик і процедур захисту інформації. Включає плани безпеки, процедури реагування на інциденти
Навчання персоналу	Рекомендується регулярне навчання з інформаційної безпеки	Стаття 39: обов'язкове навчання працівників з питань захисту даних	Обов'язкове регулярне навчання співробітників з інформаційної безпеки
Фізична безпека	Рекомендується впровадження заходів фізичної безпеки, включаючи контроль доступу до серверів	Стаття 32: необхідні заходи для захисту фізичних приміщень, зокрема серверів	Обов'язкове забезпечення фізичної безпеки, включаючи контроль доступу до серверних приміщень, відеоспостереження
Планування реагування на інциденти	Рекомендується розробка планів реагування на інциденти. Включає інструкції для співробітників	Стаття 32: обов'язкове мати плани дій на випадок інцидентів, включаючи інструкції для співробітників	Обов'язкове планування реагування на інциденти. Включає детальні плани дій, інструкції для співробітників, контакти екстрених служб

Регулярні перевірки та тестування	Рекомендується періодичне тестування систем безпеки, включаючи пентестинг	Стаття 32: обов'язкове регулярне тестування заходів безпеки, включаючи пентестинг	Обов'язкове регулярне тестування систем безпеки, включаючи пентестинг та вразливостей
Анонімізація та псевдонімізація	Рекомендується використовувати для додаткового захисту. Використовуються методи анонімізації даних	Стаття 25, 32: обов'язкова псевдонімізація, коли це можливо. Використовуються методи анонімізації та псевдонімізації	Рекомендуєтьс я для додаткового захисту. Використовуються методи анонімізації даних
Відновлення після збоїв	Рекомендується мати плани відновлення, включаючи резервне копіювання даних	Стаття 32: обов'язкове забезпечення можливості відновлення даних, включаючи резервне копіювання	Обов'язкове. Включає плани відновлення після збоїв, резервне копіювання даних
Захист від шкідливого ПЗ	Рекомендується використовувати антивірусне ПЗ та інші засоби захисту від шкідливого ПЗ	Стаття 32: обов'язкове використання засобів захисту від шкідливого ПЗ	Обов'язкове. Використовуються антивірусне ПЗ, засоби захисту від шкідливого ПЗ
Регулярне оновлення ПЗ	Рекомендується оновлювати ПЗ для усунення вразливостей	Стаття 32: обов'язкове регулярне оновлення програмного забезпечення	Обов'язкове. Включає регулярне оновлення програмного забезпечення для усунення вразливостей
Обмеження	Рекомендується	Стаття 32:	Обов'язкове.

доступу до робочих місць	контролювати фізичний доступ до робочих місць, зокрема до серверних приміщень	необхідні заходи для обмеження доступу до робочих місць та серверних приміщень	Включає контроль фізичного доступу до робочих місць та серверних приміщень
Логування та звітність	Рекомендується ведення логів доступу та дій користувачів. Включає моніторинг активності	Стаття 30, 33: обов'язкове ведення логів та їх аналіз. Включає моніторинг активності	Обов'язкове. Включає ведення логів доступу та дій користувачів, моніторинг активності
Контроль за змінами	Рекомендується впровадження політики контролю за змінами, включаючи відстеження змін у ПЗ	Стаття 32: обов'язкове забезпечення контролю за змінами, включаючи відстеження змін у ПЗ	Обов'язкове. Включає політику контролю за змінами, відстеження змін у програмному забезпеченні
Ідентифікація та аутентифікація	Рекомендується використання засобів ідентифікації та аутентифікації, включаючи паролі та токени	Стаття 32: обов'язкове використання багатофакторної аутентифікації. Використовуються паролі, токени, біометричні дані	Обов'язкове. Включає використання багатофакторної аутентифікації, паролів, токенів, біометричних даних
Контроль за використанням ресурсів	Рекомендується моніторинг використання IT-ресурсів, включаючи сервери та мережеві пристрої	Стаття 32: обов'язковий моніторинг використання IT-ресурсів, включаючи сервери та мережеві пристрої	Обов'язкове. Включає моніторинг використання IT-ресурсів, серверів, мережевих пристроїв

Локація розміщення сервера	Рекомендується, але не є обов'язковим, розміщення серверів у безпечних дата-центрах з фізичним захистом, резервними копіями та захистом від стихійних лих. Сервери можуть бути розміщені як в Україні, так і в інших країнах за умови забезпечення належного рівня захисту даних.	Стаття 44: Дані можуть бути передані лише до країн, які забезпечують адекватний рівень захисту даних (наприклад, країни ЄЕЗ). Вимагається розміщення серверів у країнах з відповідним рівнем захисту даних.	Обов'язкове. Сервери повинні бути розміщені в США або в країнах, які мають адекватні заходи захисту даних, відповідно до вимог HIPAA.

На основі таблиці 2.2., яка порівнює вимоги Законів України "Про захист персональних даних", GDPR (ЕС) та HIPAA (США), видно, що ці нормативні акти мають спільну мету — забезпечення захисту персональних даних, але відрізняються деталями та суворістю вимог. В Україні багато заходів, таких як шифрування та моніторинг, є рекомендованими, а не обов'язковими. Натомість, GDPR і HIPAA встановлюють строгі обов'язкові вимоги до шифрування, контролю доступу, моніторингу, аудиту та інформування про порушення, забезпечуючи більш високий рівень захисту даних. Особливо важливою є вимога щодо розміщення серверів: GDPR дозволяє зберігання даних тільки в країнах з адекватним рівнем захисту, тоді як HIPAA вимагає розміщення серверів у США або в країнах з відповідними заходами захисту. Таким чином, GDPR і HIPAA мають більш жорсткі вимоги порівняно із законодавством України, що сприяє підвищенню рівня безпеки даних та захисту прав суб'єктів даних.

2.2. Огляд сучасних технологій і методик захисту персональної інформації

Так як дані щодня стають ще більш цінним активом - захист персональних даних (ПД) набуває все більшої ваги. Підприємства, які збирають, обробляють та зберігають ПД, несуть відповідальність за їх захист від несанкціонованого доступу, розкриття, зміни або знищення.

Сучасні технології та методики захисту ПД пропонують широкий спектр інструментів та методів, які можуть допомогти підприємствам виконати цю відповідальність.

Технології та методики захисту ПД:

1. Шифрування
2. Управління ідентичністю та доступом (IAM)
3. Захист від шкідливого програмного забезпечення

Розглянемо кожну з технологій більш детально та оберемо найсучасніші рішення, які варто використовувати для захисту персональної інформації

Шифрування

Шифрування – це спосіб захисту інформації, який перетворює дані у вигляд, який не можна зрозуміти без спеціального ключа. Це потрібно для того, щоб гарантувати конфіденційність і безпеку даних під час їх зберігання або передачі.

Початкові, незашифровані дані називаються plaintext. Щоб їх зашифрувати, використовують спеціальний математичний процес, який називається алгоритмом шифрування. Для цього процесу потрібен ключ шифрування – унікальний набір даних, який робить можливим перетворення початкової інформації у зашифровану. Результат цього процесу – зашифровані дані або ciphertext. Без відповідного ключа ці дані неможливо зрозуміти.

Існують два основні типи шифрування: симетричне і асиметричне. У симетричному шифруванні один і той самий ключ використовується для шифрування і розшифрування даних. Це швидкий метод, але виникає проблема з

безпечним обміном ключа між сторонами. Приклади симетричного шифрування включають AES (Advanced Encryption Standard).

Асиметричне шифрування використовує пару ключів: публічний і приватний. Публічний ключ можна передавати відкрито, тоді як приватний тримається в секреті. Це забезпечує високий рівень безпеки, оскільки навіть якщо публічний ключ стає відомим, дані залишаються захищеними. RSA (Rivest-Shamir-Adleman) є прикладом асиметричного шифрування.

Процес шифрування виглядає так: спочатку дані змішуються з ключем і обробляються за допомогою алгоритму шифрування, в результаті чого виходить ciphertext. Для розшифрування потрібно змішати ciphertext з ключем розшифрування і знову обробити даними алгоритмом, що дозволить відновити початкові дані.

Шифрування використовується для захисту даних під час їх передачі через інтернет, для захисту інформації, що зберігається на різних носіях, і для аутентифікації користувачів або систем шляхом перевірки паролів або інших даних.

Для захисту персональних даних (ПД) рекомендується використовувати такі сучасні алгоритми шифрування:

1. AES (Advanced Encryption Standard)

Чому вибрати AES

Високий рівень безпеки: AES вважається одним з найнадійніших алгоритмів симетричного шифрування і використовується урядовими установами США для захисту конфіденційних даних.

Швидкість: AES працює швидше порівняно з багатьма іншими алгоритмами, що робить його ефективним для шифрування великих обсягів даних.

Гнучкість: AES підтримує різні розміри ключів (128, 192, 256 біт), що дозволяє збільшити рівень безпеки в залежності від потреби.

Стандартизація: AES є міжнародним стандартом (FIPS 197), що забезпечує його сумісність з багатьма системами та додатками.

2. RSA (Rivest-Shamir-Adleman)

Чому вибрати RSA:

Асиметричне шифрування: RSA використовує два ключі (публічний і приватний), що забезпечує високий рівень безпеки при передачі даних. Публічний ключ використовується для шифрування, а приватний — для розшифрування.

Захист ключів: RSA дозволяє безпечно обмінюватися симетричними ключами (наприклад, для AES) через незахищені канали.

Довговічність: RSA з довжиною ключа 2048 біт і більше вважається безпечним для захисту даних протягом найближчих років.

3. ECC (Elliptic Curve Cryptography)

Чому вибрати ECC:

Висока безпека при меншій довжині ключа: ECC забезпечує високий рівень безпеки при меншій довжині ключа порівняно з RSA. Наприклад, ECC з ключем 256 біт еквівалентний RSA з ключем 3072 біт.

Ефективність: ECC споживає менше ресурсів і швидше виконується, що робить його ідеальним для мобільних пристроїв і інших обмежених середовищ.

Сучасність: Багато нових криптографічних протоколів, таких як TLS 1.3, активно використовують ECC.

4. SHA-3 (Secure Hash Algorithm 3)

Чому вибрати SHA-3:

Криптографічна стійкість: SHA-3 пропонує високу стійкість до різних видів криптоаналітичних атак, таких як колізії та попередні образи.

Гнучкість: SHA-3 підтримує різні довжини хешу (224, 256, 384, 512 біт), що дозволяє адаптувати алгоритм до конкретних потреб.

Стандартизація: SHA-3 є стандартом (FIPS 202), що забезпечує його сумісність з багатьма системами та додатками.

Управління ідентичністю та доступом (IAM)

Управління ідентичністю та доступом (IAM) – це комплекс процесів, технологій і політик, що забезпечують керування цифровими ідентичностями і

контролювання доступу користувачів до інформаційних ресурсів в організації. У контексті захисту персональних даних IAM є критично важливим інструментом, який допомагає забезпечити, що тільки авторизовані особи можуть отримати доступ до конфіденційної інформації, і що їхні дії відстежуються і контролюються.

Як працює IAM:

Аутентифікація - процес перевірки ідентичності користувача. Для цього можуть використовуватися паролі, біометричні дані (наприклад, відбитки пальців або розпізнавання обличчя), смарт-карти або інші засоби. Мета аутентифікації – переконатися, що користувач є тим, за кого себе видає.

Авторизація - після успішної аутентифікації визначається, які ресурси і дані користувач може використовувати і які дії він може виконувати. Авторизація визначає рівень доступу користувача до різних частин системи. Наприклад, одні користувачі можуть мати доступ лише для читання, тоді як інші можуть редагувати або видаляти дані.

Розмежування повноважень - це принцип, за яким кожен користувач отримує лише ті права, які необхідні для виконання його роботи. Це допомагає мінімізувати ризики несанкціонованого доступу до чутливої інформації. Наприклад, менеджер може мати доступ до фінансових звітів, а працівник відділу кадрів – до персональних даних співробітників.

Управління ідентичністю та доступом надзвичайно важливе через те, що воно забезпечує захист конфіденційності, запобігання витоку даних, відповіднсіть законодавству та підвищення безпеки систем.

Розглянемо найефективніші рішення для контролю доступу, які ми маємо наразі:

Рішення	Опис
Системи управління доступом на основі ролей (RBAC)	RBAC дозволяє адмініструвати доступ, призначаючи користувачам ролі з певними наборами дозволів. Це знижує ризики, пов’язані з надмірними привілеями, оскільки користувачі отримують лише ті права, які

	необхідні для їх роботи.
Контроль доступу на основі атрибутів (ABAC)	ABAC використовує атрибути (наприклад, місце роботи, час доби, рівень безпеки) для визначення правил доступу. Це дозволяє гнучко та динамічно керувати доступом до ресурсів залежно від різних умов.
Багатофакторна аутентифікація (MFA)	MFA включає кілька методів перевірки особистості, таких як паролі, SMS-коди, біометричні дані або апаратні токени. Це значно знижує ймовірність несанкціонованого доступу навіть у разі компрометації одного з методів аутентифікації.
Єдина точка доступу (я, SSO)	SSO дозволяє користувачам входити до системи один раз і отримувати доступ до декількох додатків без повторного введення паролів. Це підвищує зручність користувачів і зменшує ризики, пов’язані з використанням кількох паролів.
Контроль доступу на основі ризиків	Цей підхід аналізує поведінкові фактори та контекст доступу, щоб оцінити ризик кожного запиту на доступ. Наприклад, якщо користувач намагається увійти з незвичного місця або пристрою, система може запросити додаткову аутентифікацію.
Шифрування даних	Шифрування захищає дані як під час зберігання, так і під час передачі. Використання сучасних алгоритмів шифрування, таких як AES для симетричного шифрування та RSA для асиметричного шифрування, є критично важливим для захисту конфіденційної інформації.
Технології виявлення та реагування (EDR)	EDR-системи (Endpoint Detection and Response) забезпечують моніторинг кінцевих точок на предмет шкідливої активності, що дозволяє швидко реагувати на загрози та потенційні інциденти безпеки.
Управління мобільними пристроями (MDM)	MDM рішення допомагають захистити дані на мобільних пристроях, забезпечуючи можливість віддаленого блокування або видалення даних у разі втрати або крадіжки пристрою.
Журнали аудиту та моніторинг	Ведення журналів аудиту та постійний моніторинг активності користувачів допомагають виявляти та реагувати на аномальну або підозрілу активність у

	реальному часі.
Технології нульової довіри (Zero Trust)	Zero Trust підхід передбачає, що жодна система чи користувач не може бути автоматично довіреною, навіть якщо вони знаходяться у внутрішній мережі. Це означає постійну перевірку кожного запиту на доступ до ресурсів.

Захист від шкідливого програмного забезпечення

Захист від шкідливого програмного забезпечення (антивірусний захист) – це комплекс заходів і технологій, спрямованих на виявлення, запобігання і видалення шкідливого програмного забезпечення (malware) з комп'ютерних систем. Цей тип захисту є важливою складовою забезпечення безпеки персональних даних, оскільки шкідливе програмне забезпечення може бути використано для крадіжки, маніпуляції або знищення конфіденційної інформації.

Серед основних видів шкідливого ПЗ виділяють: віруси, трояни, черви, шпигунське ПЗ, руткіти, вимагачі.

Технології та методики захисту включають в себе:

- Антивірусне програмне забезпечення (Програми, що сканують файли і системи на наявність шкідливого ПЗ, видаляють або ізолюють його. Сучасні антивіруси використовують бази даних відомих шкідливих програм, а також евристичний аналіз для виявлення нових загроз.)

- Фаєрволи (Програмні або апаратні засоби, що контролюють вхідний і вихідний мережевий трафік, запобігаючи несанкціонованому доступу до системи.)

- Системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS) (IDS моніторять мережевий трафік і системні активності для виявлення підозрілої діяльності, тоді як IPS автоматично вживають заходів для запобігання виявленим загрозам.)

- Регулярне оновлення програмного забезпечення (Оновлення операційних систем, додатків і антивірусних програм забезпечують захист від нових вразливостей і загроз.)

- Шифрування даних (Захист даних за допомогою шифрування унеможливлює їх використання навіть у разі, якщо вони потраплять до рук зловмисників.)

- Резервне копіювання (Регулярне створення резервних копій даних дозволяє відновити інформацію у випадку атаки шкідливого ПЗ, наприклад, вимагачів.)

2.3. Розробка корпоративної політики захисту персональних даних та впровадження організаційних заходів

Розробка корпоративної політики захисту персональних даних включає кілька ключових етапів, які повинні бути ретельно сплановані та реалізовані. Перш за все, необхідно визначити, які саме дані потребують захисту, та провести аналіз ризиків, пов'язаних з їх обробкою. Це дозволить виявити потенційні загрози та визначити слабкі місця в існуючій системі захисту.

Створимо корпоративну політику захисту персональних даних для умовного підприємства “Х”:

В першу чергу, створимо загальні положення даної політики:

1. Загальні положення

1.1. Мета політики

Метою цієї політики є забезпечення належного рівня захисту персональних даних, які обробляються на підприємстві "Х". Це включає дотримання вимог чинного законодавства України щодо захисту персональних даних, а також відповідність міжнародним стандартам, таким як GDPR (Загальний регламент захисту даних ЄС). Політика спрямована на:

Захист прав та свобод фізичних осіб при обробці їхніх персональних даних.

Запобігання несанкціонованому доступу, втраті, знищенню або пошкодженню персональних даних.

Підтримання довіри клієнтів, партнерів та співробітників до безпечної обробки їхніх персональних даних.

1.2. Область застосування

Ця політика поширюється на всі підрозділи підприємства "Х" без винятку і охоплює всіх співробітників, які мають доступ до персональних даних. Область застосування включає:

Всі види персональних даних, що збираються, зберігаються, обробляються та передаються підприємством "Х".

Всі системи та процеси, за допомогою яких обробляються персональні дані.

Всі співробітники, незалежно від їх ролі або рівня доступу до персональних даних.

Всі треті сторони, що взаємодіють з підприємством "Х" і мають доступ до персональних даних, відповідно до умов укладених договорів та угод.

1.3. Визначення термінів

Для цілей цієї політики застосовуються наступні визначення:

Персональні дані: будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи (суб'єкта даних). До таких даних можуть належати: ім'я, адреса, електронна пошта, номер телефону, ідентифікаційний номер, дані про місцезнаходження, інтернет-ідентифікатори, або інші фактори, специфічні для фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї особи.

Обробка даних: будь-яка операція або сукупність операцій, що здійснюються з персональними даними, незалежно від того, автоматизовані вони чи ні. Це включає збір, запис, організацію, структурування, зберігання, адаптацію або зміну, вилучення, ознайомлення, використання, розкриття шляхом передачі, розповсюдження або надання доступу, вирівнювання або поєднання, обмеження, видалення або знищення даних.

Суб'єкт даних: фізична особа, до якої належать персональні дані, що обробляються підприємством "Х".

Контролер даних: юридична або фізична особа, орган державної влади, установа або інший орган, який самостійно або спільно з іншими визначає цілі та засоби обробки персональних даних.

Обробник даних: фізична або юридична особа, орган державної влади, установа або інший орган, який обробляє персональні дані від імені контролера даних.

Згода: будь-яке добровільне, конкретне, інформоване та однозначне волевиявлення суб'єкта даних, яким він або вона, шляхом заяви або чіткого ствердного діяння, погоджується на обробку персональних даних, що стосуються його або її.

Ця політика встановлює загальні правила та принципи обробки персональних даних, які повинні дотримуватись всі співробітники підприємства "Х" для забезпечення належного захисту даних та дотримання прав суб'єктів даних.

Наступним кроком для створення корпоративної політики щодо захисту персональних даних буде визначення принципів обробки персональних даних:

2. Принципи обробки персональних даних

2.1. Законність

Обробка персональних даних на підприємстві "Х" здійснюється виключно на законних підставах. Це означає, що перед початком обробки даних підприємство повинно забезпечити наявність однієї з наступних правових підстав:

Згода суб'єкта даних: суб'єкт даних добровільно, свідомо і однозначно надає згоду на обробку своїх персональних даних для визначених цілей.

Виконання договору: обробка даних необхідна для виконання договору, учасником якого є суб'єкт даних, або для вжиття заходів на запит суб'єкта даних до укладення договору.

Законодавча вимога: обробка даних необхідна для виконання юридичного обов'язку, що покладений на підприємство "Х".

Захист життєвих інтересів: обробка даних необхідна для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи.

Виконання завдання в суспільних інтересах або здійснення офіційних повноважень: обробка даних необхідна для виконання завдання, що здійснюється

в суспільних інтересах, або при здійсненні офіційних повноважень, наданих підприємству "Х".

Законні інтереси: обробка даних необхідна для цілей законних інтересів, які переслідує підприємство "Х" або третя сторона, за умови, що такі інтереси не переважають над інтересами або основними правами і свободами суб'єкта даних.

2.2. Справедливість і прозорість

Підприємство "Х" зобов'язується забезпечити справедливу та прозору обробку персональних даних. Це включає наступні заходи:

Інформування суб'єктів даних про цілі, правові підстави, обсяги та способи обробки їх персональних даних.

Надання суб'єктам даних інформації про їх права та способи реалізації цих прав.

Забезпечення доступності та зрозумілості інформації про політику захисту персональних даних підприємства "Х".

2.3. Обмеження метою

Персональні дані збираються з чітко визначеними, законними цілями і не можуть оброблятися у спосіб, несумісний з цими цілями. Основні цілі обробки персональних даних на підприємстві "Х" можуть включати:

Виконання договірних зобов'язань перед клієнтами, постачальниками та співробітниками.

Виконання законодавчих вимог та регуляторних зобов'язань.

Управління трудовими відносинами та забезпечення кадрових процесів.

Підтримка та покращення якості послуг, що надаються клієнтам.

Захист прав та інтересів підприємства "Х".

2.4. Мінімізація даних

Підприємство "Х" збирає лише ті персональні дані, які є необхідними для досягнення визначених цілей. Це означає:

Оцінка потреби у кожному виді персональних даних перед їх збором.

Використання методів анонімізації та псевдонімізації даних, коли це можливо.

Регулярний перегляд обсягу персональних даних, що зберігаються, з метою видалення зайвих даних.

2.5. Точність

Персональні дані повинні бути точними та, за необхідності, оновлюватися. Для досягнення цього принципу підприємство "Х":

Впроваджує процедури для регулярного оновлення персональних даних.

Забезпечує можливість суб'єктам даних перевіряти та виправляти свої персональні дані.

Вживає заходів для виправлення неточних або неповних даних.

2.6. Обмеження зберігання

Персональні дані зберігаються не довше, ніж це необхідно для досягнення цілей їх обробки. Це включає:

Встановлення строків зберігання для різних видів персональних даних.

Проведення регулярних перевірок на відповідність строків зберігання визначеним періодам.

Безпечне видалення або анонімізація даних, які більше не потрібні.

2.7. Цілісність та конфіденційність

Персональні дані обробляються таким чином, щоб забезпечити їх належний захист, включаючи захист від несанкціонованого або незаконного доступу, випадкової втрати, знищення або пошкодження. Для цього підприємство "Х":

Використовує сучасні технологічні рішення для захисту даних, такі як шифрування, контроль доступу та моніторинг безпеки.

Впроваджує організаційні заходи, включаючи навчання персоналу, розробку внутрішніх політик та процедур.

Регулярно проводить оцінку ризиків та аудити безпеки даних для виявлення та усунення потенційних загроз.

Наступним кроком в розробці даної політики буде створення пункта “Права суб’єктів даних”:

3. Права суб'єктів даних

Підприємство "Х" забезпечує реалізацію прав суб'єктів даних відповідно до вимог чинного законодавства. Кожен суб'єкт даних має наступні права:

3.1. Право на доступ

Суб'єкти даних мають право отримати інформацію про обробку своїх персональних даних. Це право включає можливість:

Отримання підтвердження, чи обробляються персональні дані суб'єкта.

Отримання копії персональних даних, що обробляються.

Отримання наступної інформації:

Цілі обробки даних.

Категорії персональних даних, що обробляються.

Одержувачі або категорії одержувачів даних, яким персональні дані були або будуть розкриті.

Строк зберігання даних або критерії його визначення.

Інформація про права суб'єкта даних, включаючи право на виправлення, видалення, обмеження обробки та заперечення.

Джерело отримання даних, якщо вони не були надані самим суб'єктом даних.

Інформація про автоматизоване прийняття рішень, включаючи профілювання, та значення і наслідки такої обробки для суб'єкта даних.

3.2. Право на виправлення

Суб'єкти даних мають право вимагати виправлення неточних або неповних персональних даних. Підприємство "Х" зобов'язане:

Виправити неточні персональні дані без невиправданої затримки.

Доповнити неповні персональні дані, враховуючи цілі обробки, шляхом надання додаткової заяви суб'єкта даних.

3.3. Право на видалення (право "бути забутим")

Суб'єкти даних мають право вимагати видалення своїх персональних даних за певних умов, зокрема, якщо:

Персональні дані більше не потрібні для цілей, для яких вони були зібрані або оброблені.

Суб'єкт даних відкликає згоду, на підставі якої здійснювалася обробка, і немає іншої законної підстави для обробки.

Суб'єкт даних заперечує проти обробки і немає переважних законних підстав для обробки.

Персональні дані оброблялися незаконно.

Персональні дані повинні бути видалені для виконання юридичного обов'язку.

3.4. Право на обмеження обробки

Суб'єкти даних мають право вимагати обмеження обробки своїх персональних даних за певних умов, зокрема, якщо:

Суб'єкт даних оскаржує точність персональних даних, на період, що дозволяє підприємству "X" перевірити точність даних.

Обробка незаконна, і суб'єкт даних заперечує проти видалення даних, натомість вимагаючи обмеження їх використання.

Підприємству "X" більше не потрібні персональні дані для цілей обробки, але вони потрібні суб'єкту даних для встановлення, здійснення або захисту правових вимог.

Суб'єкт даних заперечив проти обробки, на період перевірки того, чи переважають законні підстави підприємства "X" над підставами суб'єкта даних.

3.5. Право на перенесення даних

Суб'єкти даних мають право отримати свої персональні дані у структурованому, загальноприйнятому форматі, що читається машиною, та передати їх іншому контролеру. Це право застосовується, якщо:

Обробка здійснюється на підставі згоди суб'єкта даних або договору.

Обробка здійснюється автоматизованими засобами.

Суб'єкти даних також мають право вимагати передачу своїх персональних даних безпосередньо від одного контролера до іншого, якщо це технічно можливо.

3.6. Право на заперечення

Суб'єкти даних мають право заперечувати проти обробки своїх персональних даних у будь-який час, зокрема, якщо:

Обробка здійснюється для виконання завдання, що здійснюється в суспільних інтересах або при здійсненні офіційних повноважень, наданих підприємству "Х".

Обробка необхідна для цілей законних інтересів підприємства "Х" або третьої сторони, за винятком випадків, коли такі інтереси переважають над інтересами або основними правами і свободами суб'єкта даних.

У разі заперечення, підприємство "Х" припиняє обробку персональних даних, якщо не зможе довести наявність вагомих законних підстав для обробки, які переважають над інтересами, правами і свободами суб'єкта даних, або для встановлення, здійснення або захисту правових вимог.

3.7. Право на автоматизоване прийняття рішень, включаючи профілювання

Суб'єкти даних мають право не бути підданими рішенню, заснованому виключно на автоматизованій обробці, включаючи профілювання, яке має правові наслідки для суб'єкта даних або аналогічним чином істотно впливає на нього, за винятком випадків, коли таке рішення:

Є необхідним для укладення або виконання договору між суб'єктом даних та підприємством "Х".

Дозволено законодавством, що застосовується до підприємства "Х", яке також передбачає відповідні заходи для захисту прав, свобод та законних інтересів суб'єкта даних.

Ґрунтується на явній згоді суб'єкта даних.

Підприємство "Х" забезпечує, щоб суб'єкт даних мав можливість оскаржити рішення, прийняте на основі автоматизованої обробки, отримати людське втручання з боку підприємства, висловити свою точку зору та оскаржити рішення.

Ця політика зобов'язує підприємство "Х" дотримуватися всіх вищевказаних прав суб'єктів даних, забезпечувати їх реалізацію та оперативно реагувати на запити суб'єктів даних у встановлені законодавством терміни.

Наступним кроком створимо інструкції по обов’язкам співробітників:

4. Обов'язки співробітників

4.1. Відповідність політиці

Співробітники підприємства "Х" зобов'язані обробляти персональні дані відповідно до цієї політики та інших внутрішніх нормативних документів. Це включає:

Ознайомлення з політикою захисту персональних даних та регулярне оновлення своїх знань щодо змін у політиці та законодавстві.

Дотримання всіх процедур та інструкцій, визначених у політиці.

Виконання обробки персональних даних лише в межах своїх посадових обов'язків та повноважень.

Забезпечення належного рівня захисту персональних даних на всіх етапах їх обробки.

4.2. Дотримання конфіденційності

Кожен співробітник зобов'язаний дотримуватися конфіденційності персональних даних і не розголошувати їх третім особам без відповідного дозволу. Це означає:

Використання персональних даних лише для цілей, визначених політикою захисту персональних даних та у межах своїх посадових обов'язків.

Захист інформації від несанкціонованого доступу, розкриття, копіювання або використання.

Забезпечення, що доступ до персональних даних мають лише ті співробітники, які мають відповідні повноваження та необхідність в обробці цих даних для виконання своїх посадових обов'язків.

Використання технічних засобів захисту інформації, таких як паролі, шифрування та інші методи безпеки.

4.3. Повідомлення про інциденти

Співробітники повинні негайно повідомляти про будь-які інциденти, пов'язані з порушенням безпеки персональних даних. Це включає:

Виявлення інцидентів: співробітники повинні бути навчені розпізнавати інциденти, пов'язані з безпекою персональних даних, такі як несанкціонований доступ, витік даних, втрата або пошкодження даних.

Негайне повідомлення: співробітники зобов'язані негайно повідомити відповідальну особу за захист персональних даних або інші визначені контактні особи про будь-який інцидент, який вони виявили або підозрюють.

Надання детальної інформації: під час повідомлення про інцидент співробітник повинен надати якомога більше деталей про інцидент, включаючи обставини, які призвели до інциденту, характер персональних даних, що піддалися ризику, та будь-які заходи, які вже були вжиті для усунення інциденту.

Співпраця в розслідуванні: співробітники повинні активно співпрацювати з відповідальними особами та командами, які проводять розслідування інциденту, надавати всю необхідну інформацію та підтримку.

4.4. Використання безпечних методів обробки даних

Співробітники зобов'язані використовувати безпечні методи обробки персональних даних, включаючи:

Використання захищених паролями комп'ютерів та інших пристроїв, які мають доступ до персональних даних.

Регулярне оновлення паролів та використання складних комбінацій для запобігання несанкціонованому доступу.

Встановлення на комп'ютери та інші пристрої антивірусного програмного забезпечення та його регулярне оновлення.

Застосування методів шифрування для захисту персональних даних, особливо при передачі даних через мережі.

4.5. Навчання та підвищення кваліфікації

Співробітники повинні регулярно проходити навчання з питань захисту персональних даних, включаючи:

Обов'язкові вступні тренінги для нових співробітників, що включають огляд політики захисту персональних даних та основних принципів обробки даних.

Регулярні оновлюючі тренінги для всіх співробітників, що включають оновлення інформації про нові загрози, методи захисту та зміни у законодавстві.

Спеціалізовані тренінги для співробітників, які мають підвищений доступ до персональних даних або відповідають за їх захист.

4.6. Виконання внутрішніх аудитів

Співробітники повинні брати участь у внутрішніх аудитах та перевірках відповідності політиці захисту персональних даних. Це включає:

Надання необхідної інформації та документації аудиторам.

Співпраця з аудиторами під час перевірок та аудитів.

Виконання рекомендацій та виправлення виявлених порушень чи недоліків у процесах обробки персональних даних.

4.7. Захист персональних даних під час передачі

При передачі персональних даних, співробітники зобов'язані дотримуватися вимог щодо безпеки передачі даних, включаючи:

Використання зашифрованих каналів зв'язку для передачі персональних даних через Інтернет.

Забезпечення, що одержувачі персональних даних мають відповідні повноваження та зобов'язання щодо захисту даних.

Використання захищених методів передачі даних у межах підприємства, таких як захищені мережі та засоби внутрішньої комунікації.

4.8. Ведення реєстрів обробки персональних даних

Співробітники, відповідальні за обробку персональних даних, повинні вести та підтримувати актуальні реєстри обробки даних, включаючи:

Ведення записів про всі операції з обробки персональних даних.

Оновлення реєстрів при зміні методів або цілей обробки даних.

Забезпечення доступності реєстрів для внутрішніх та зовнішніх аудитів, а також для запитів суб'єктів даних.

Ця політика встановлює обов'язки співробітників підприємства "Х" щодо захисту персональних даних і вимагає від них дотримання високих стандартів безпеки та конфіденційності. За порушення цих обов'язків співробітники несуть відповідальність відповідно до внутрішніх нормативних документів та чинного законодавства.

Визначимо технічні заходи політики:

5. Технічні заходи

5.1. Використання шифрування

Для захисту персональних даних, що передаються через відкриті мережі, підприємство "Х" використовує сучасні методи шифрування. Це включає:

Шифрування під час передачі: всі персональні дані, що передаються через Інтернет або інші відкриті мережі, повинні бути зашифровані за допомогою протоколів SSL/TLS або аналогічних.

Шифрування під час зберігання: персональні дані, що зберігаються на серверах, базах даних або інших пристроях, повинні бути зашифровані. Використовуються сучасні алгоритми шифрування, такі як AES (Advanced Encryption Standard).

Управління ключами шифрування: підприємство розробляє та впроваджує політику управління ключами шифрування, включаючи генерацію, зберігання, обробку та знищення ключів.

5.2. Контроль доступу

Для забезпечення належного рівня захисту персональних даних підприємство "Х" впроваджує систему контролю доступу, яка включає:

Аутентифікація: доступ до систем, що обробляють персональні дані, надається лише авторизованим користувачам. Використовуються багатофакторна аутентифікація (MFA) та надійні методи перевірки особи.

Авторизація: права доступу до персональних даних надаються відповідно до ролей і обов'язків співробітників. Впроваджуються принципи мінімальних привілеїв та необхідності знання.

Моніторинг доступу: всі спроби доступу до персональних даних журналюються та регулярно аналізуються для виявлення підозрілої активності або порушень.

Регулярний перегляд прав доступу: права доступу співробітників регулярно переглядаються та оновлюються у відповідності до їх поточних посадових обов'язків.

5.3. Системи моніторингу

Для виявлення та попередження несанкціонованого доступу до персональних даних підприємство "X" впроваджує системи моніторингу, які включають:

Системи виявлення вторгнень (IDS): впровадження IDS для моніторингу мережевого трафіку та виявлення підозрілих дій.

Системи запобігання вторгненням (IPS): IPS, що працюють разом з IDS, для активного блокування або запобігання підозрілим діям в режимі реального часу.

Моніторинг подій безпеки (SIEM): впровадження систем управління інформацією та подіями безпеки для збору, аналізу та кореляції логів з різних джерел.

Регулярні перевірки та аудит: регулярне проведення внутрішніх і зовнішніх аудитів для перевірки ефективності систем моніторингу та відповідності вимогам безпеки.

5.4. Резервне копіювання

Для запобігання втраті персональних даних підприємство "X" впроваджує систему резервного копіювання, яка включає:

Регулярне резервне копіювання: всі важливі персональні дані регулярно копіюються на захищені резервні носії. Частота резервного копіювання визначається відповідно до важливості даних та бізнес-процесів.

Зберігання резервних копій: резервні копії зберігаються у захищених місцях, відокремлених від основних систем, для забезпечення їх доступності у разі аварії або інциденту.

Відновлення даних: регулярне тестування процедур відновлення даних з резервних копій для забезпечення їх ефективності та надійності.

Контроль доступу до резервних копій: доступ до резервних копій має бути обмежений лише авторизованими особами, які відповідають за резервне копіювання та відновлення даних.

5.5. Безпека мережі

Підприємство "X" впроваджує заходи для забезпечення безпеки мережі, що включає:

Мережеві брандмауери: встановлення та налаштування брандмауерів для захисту від несанкціонованого доступу до внутрішніх мереж та систем.

Віртуальні приватні мережі (VPN): використання VPN для захищеного доступу до внутрішніх мереж підприємства з віддалених локацій.

Розмежування мереж: створення сегментів мережі для розмежування внутрішніх ресурсів та підвищення рівня безпеки.

5.6. Управління уразливостями

Для мінімізації ризиків, пов'язаних з уразливостями програмного та апаратного забезпечення, підприємство "X" здійснює:

Регулярне оновлення програмного забезпечення: встановлення оновлень та патчів для усунення відомих уразливостей.

Аналіз уразливостей: регулярне проведення сканування та оцінки уразливостей в системах та мережах.

Планування виправлень: розробка та реалізація планів виправлень для усунення виявлених уразливостей у визначені строки.

5.7. Захист кінцевих точок

Підприємство "X" впроваджує заходи для захисту кінцевих точок, що включають:

Антивірусне програмне забезпечення: встановлення та регулярне оновлення антивірусного програмного забезпечення на всіх кінцевих точках.

Захист від шкідливого програмного забезпечення (Endpoint Protection): використання рішень для захисту від шкідливого програмного забезпечення та інших загроз.

Контроль доступу до пристроїв: обмеження використання зовнішніх пристроїв зберігання даних, таких як USB-накопичувачі.

5.8. Захист електронної пошти

Для запобігання несанкціонованому доступу та витоку персональних даних через електронну пошту підприємство "Х" використовує:

Шифрування електронних листів: шифрування електронних листів, що містять конфіденційну інформацію.

Фільтрація спаму: впровадження системи фільтрації спаму для зменшення ризиків фішингових атак.

Контроль вкладень: перевірка та обмеження вкладень в електронних листах для запобігання поширенню шкідливого програмного забезпечення.

Всі зазначені технічні заходи спрямовані на забезпечення високого рівня захисту персональних даних та мінімізацію ризиків їх несанкціонованого доступу, втрати або пошкодження. Підприємство "Х" регулярно переглядає та оновлює ці заходи відповідно до змін у технологіях та вимогах безпеки.

Останнім блоком нашої політики буде “Реагування на інциденти”

6. Реагування на інциденти

6.1. Визначення процедур

Для забезпечення швидкого та ефективного реагування на інциденти, пов'язані з безпекою персональних даних, підприємство "Х" розробляє та впроваджує чіткі процедури, які включають:

Виявлення інцидентів: встановлення механізмів та інструментів для виявлення інцидентів безпеки, включаючи системи моніторингу та виявлення вторгнень (IDS/IPS), а також аналіз логів та інших даних.

Оцінка інцидентів: визначення критеріїв для оцінки серйозності інциденту, враховуючи потенційні ризики та наслідки для персональних даних і безпеки підприємства.

Повідомлення про інциденти: встановлення процедур для негайного повідомлення відповідальної особи або групи, яка займається питаннями безпеки інформації, про виявлені інциденти.

Реагування на інциденти: визначення кроків для оперативного реагування на інциденти, включаючи ізоляцію уражених систем, відновлення даних та запобігання подальшому поширенню загрози.

6.2. Повідомлення про інциденти

Всі інциденти, пов'язані з порушенням безпеки персональних даних, повинні негайно повідомлятися відповідальній особі. Процедура повідомлення включає:

Канали повідомлення: встановлення конкретних каналів для повідомлення про інциденти, таких як спеціальні телефони, електронна пошта або внутрішні системи повідомлення.

Формат повідомлення: визначення стандартного формату для подання інформації про інцидент, що включає опис інциденту, час і місце виявлення, залучені системи та персональні дані, потенційні ризики та вжиті заходи.

Відповідальні особи: визначення конкретних співробітників або груп, відповідальних за отримання повідомлень про інциденти та їх подальше розслідування.

6.3. Розслідування та аналіз

Після кожного інциденту проводиться детальне розслідування для визначення причин та вжиття заходів щодо запобігання їх повторенню. Процес розслідування включає:

Формування групи розслідування: створення команди з відповідних фахівців, яка буде займатися розслідуванням інциденту.

Збір даних: збір усіх необхідних даних для аналізу інциденту, включаючи лог-файли, журнали доступу, мережеві трафіки та інші релевантні дані.

Аналіз причин: визначення основних причин інциденту, включаючи технічні, організаційні та людські фактори.

Вжиття заходів: розробка та впровадження коригувальних дій для усунення виявлених недоліків та запобігання подібним інцидентам у майбутньому.

Документування інциденту: детальне документування інциденту, включаючи його причини, наслідки, вжиті заходи та рекомендації для запобігання повторенню.

Комунікація з зацікавленими сторонами: інформування керівництва підприємства, відповідних регуляторів (якщо це вимагається законодавством), та, за необхідності, суб'єктів даних про інцидент і вжиті заходи.

6.4. Відновлення після інциденту

Після інциденту підприємство "Х" забезпечує швидке та ефективне відновлення нормальної роботи систем і процесів, що включає:

Відновлення даних: використання резервних копій для відновлення втрачених або пошкоджених даних.

Відновлення систем: перевірка та відновлення уражених систем до стану, в якому вони були до інциденту, включаючи перевстановлення програмного забезпечення та оновлення конфігурацій.

Перевірка безпеки: проведення детального аналізу безпеки відновлених систем для забезпечення відсутності подальших загроз або уразливостей.

Комунікація з користувачами: інформування користувачів про завершення відновлювальних робіт та повернення до нормального режиму роботи.

6.5. Оцінка ефективності заходів реагування

Після завершення всіх дій, пов'язаних з інцидентом, підприємство "Х" проводить оцінку ефективності вжитих заходів реагування. Це включає:

Аналіз ефективності реагування: оцінка швидкості та ефективності дій, вжитих під час інциденту.

Виявлення недоліків: виявлення слабких місць у процедурах реагування та захисту даних.

Розробка рекомендацій: розробка рекомендацій для покращення процедур реагування на інциденти та підвищення рівня безпеки.

Оновлення політик та процедур: внесення змін до політик та процедур на основі отриманих висновків та рекомендацій.

6.6. Навчання та підвищення обізнаності

Для забезпечення готовності співробітників до реагування на інциденти, підприємство "X" проводить регулярне навчання та підвищення обізнаності, що включає:

Навчальні тренінги: регулярні тренінги для співробітників щодо процедур виявлення, повідомлення та реагування на інциденти.

Симуляції інцидентів: проведення симуляцій інцидентів для перевірки готовності співробітників та ефективності процедур реагування.

Оновлення знань: регулярне оновлення знань співробітників про нові загрози та методи захисту.

У цьому розділі ми докладно розглянули теоретичні аспекти та практичні підходи, необхідні для забезпечення надійного захисту ідентифікованих персональних даних на підприємстві. Було висвітлено основні принципи обробки персональних даних, які забезпечують законність, справедливість, прозорість, обмеження метою, мінімізацію даних, точність, обмеження зберігання, цілісність та конфіденційність.

Ми детально розглянули права суб'єктів даних, зокрема їхнє право на доступ, виправлення, видалення, обмеження обробки, перенесення даних, заперечення проти обробки та право на автоматизоване прийняття рішень. Підприємство зобов'язане забезпечувати реалізацію цих прав і надавати суб'єктам даних можливість контролювати свої персональні дані.

Також було розглянуто обов'язки співробітників щодо дотримання політики захисту персональних даних, забезпечення конфіденційності, негайного повідомлення про інциденти, використання безпечних методів обробки даних,

участі у внутрішніх аудитах, захисту даних під час передачі та ведення реєстрів обробки персональних даних.

Особливу увагу приділено технічним заходам захисту, таким як використання шифрування, контроль доступу, системи моніторингу, резервне копіювання, безпека мережі, управління уразливостями, захист кінцевих точок та електронної пошти. Ці заходи дозволяють мінімізувати ризики несанкціонованого доступу, втрати або пошкодження персональних даних.

Розділ також детально висвітлює процеси реагування на інциденти, що включають визначення процедур виявлення та повідомлення про інциденти, проведення розслідувань, відновлення після інциденту, оцінку ефективності заходів реагування та проведення навчання для підвищення обізнаності співробітників.

Таким чином, ми визначили оптимальні шляхи та практичні рекомендації для забезпечення надійного захисту персональних даних на підприємстві. Запропоновані методи та заходи спрямовані на створення комплексної системи захисту даних, яка відповідає вимогам законодавства та сучасним стандартам безпеки, що дозволить ефективно захищати інформацію та підтримувати довіру клієнтів, партнерів і співробітників.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ОСНОВІ ENZUZO

3.1. Розробка критеріїв оцінки ПЗ на відповідність вимогам GDPR

Вибір програмного забезпечення (ПЗ), яке відповідає вимогам GDPR, є критичним завданням для забезпечення належного рівня захисту персональних даних. У цьому підрозділі будуть розроблені критерії оцінки ПЗ на відповідність вимогам GDPR.

Загалом ми можемо виділити 6 основних пунктів, які можна визначити як критерії для оцінки ПЗ на відповідність вимогам GDPR, а саме:

1. Законність обробки даних
2. Принципи обробки даних
3. Права суб'єктів даних
4. Безпека обробки даних
5. Відповідальність та звітність
6. Взаємодія з третіми сторонами

Досягнувши вимог по кожному з цих пунктів ми можемо визначити, що наше ПЗ відповідає вимогам GDPR. Розглянемо детальніше кожен з них.

1. Законність обробки даних

Законні підстави для обробки даних

Програмне забезпечення має забезпечувати можливість обробки даних виключно на основі однієї з законних підстав, передбачених статтею 6 GDPR. Ці підстави включають:

- Згода суб'єкта даних: ПЗ повинно забезпечувати можливість збору явної та добровільної згоди від суб'єктів даних. Це означає, що користувачі повинні мати змогу надати, відкликати та змінити свою згоду через інтерфейс програми. Згода повинна бути документована, і ПЗ має зберігати історію згод для аудиту.

- Виконання контракту: ПЗ повинно обробляти персональні дані, коли це необхідно для виконання контракту, де суб'єкт даних є стороною. ПЗ повинно забезпечувати можливість чітко визначати, які дані потрібні для виконання контракту і обробляти лише ці дані.

- Виконання юридичних зобов'язань: ПЗ має забезпечувати можливість обробки даних для дотримання юридичних зобов'язань підприємства. Це включає зберігання та обробку даних згідно з вимогами законодавства, таких як податкове законодавство чи регуляторні вимоги.

- Захист життєво важливих інтересів: ПЗ повинно дозволяти обробку даних для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи. Це може включати ситуації надзвичайного стану, коли необхідно обробляти персональні дані для забезпечення безпеки та здоров'я.

- Виконання завдань в інтересах суспільства або здійснення офіційних повноважень: ПЗ повинно підтримувати обробку даних для виконання завдань, що здійснюються в інтересах суспільства або офіційними органами влади. Це може включати обробку даних у сфері охорони здоров'я, освіти, громадської безпеки тощо.

- Законний інтерес підприємства: ПЗ має забезпечувати можливість обробки даних на основі законного інтересу підприємства, за умови, що такі інтереси не переважують права та свободи суб'єктів даних. Приклади можуть включати обробку даних для захисту від шахрайства, забезпечення безпеки IT-систем або маркетингових досліджень.

Згода суб'єктів даних

Згідно з статтею 7 GDPR, програмне забезпечення повинно забезпечувати такі можливості для роботи зі згодою суб'єктів даних:

- Отримання згоди: ПЗ має включати функціонал для отримання згоди суб'єктів даних. Це може бути реалізовано через діалогові вікна, форми або інші інтерфейсні елементи, де користувачі можуть надавати свою згоду. Згода повинна бути явно надана (наприклад, через чекбокси, кнопки підтвердження тощо).

- Відкликання згоди: ПЗ повинно забезпечувати можливість суб'єктам даних легко відкликати свою згоду в будь-який час. Це може бути реалізовано через інтерфейс користувача, де суб'єкт даних може побачити свої активні згоди та відкликати їх за необхідності.

- Оновлення згоди: ПЗ має забезпечувати можливість оновлення згоди, якщо змінюються умови обробки даних. Це може включати відправку запитів на оновлення згоди з новими умовами та забезпечення зручного способу надання або відмови від оновленої згоди.

- Журнал згод: ПЗ повинно зберігати детальну історію наданих, відкликаних та оновлених згод. Ця інформація має бути доступна для аудиту та забезпечення відповідності вимогам GDPR. Журнал повинен містити дату та час надання або відкликання згоди, а також деталі про умови, на які надавалась згода.

Ці можливості дозволяють забезпечити повну відповідність вимогам GDPR щодо законності обробки даних та згоди суб'єктів даних, що є основою для захисту персональної інформації в сучасних умовах.

2. Принципи обробки даних

У контексті дотримання вимог GDPR, ПЗ повинно відповідати ключовим принципам обробки даних, щоб забезпечити належний захист персональної інформації. Розглянемо кожен принцип детальніше.

Прозорість

Прозорість обробки даних є основним принципом, закріпленим у статті 12 GDPR. ПЗ має забезпечувати:

- Повідомлення про конфіденційність: ПЗ повинно надавати суб'єктам даних чіткі та доступні повідомлення про конфіденційність, які пояснюють, які дані збираються, з якою метою, як довго вони зберігатимуться, хто має доступ до цих даних і які права мають суб'єкти даних.

- Легкий доступ до інформації: Інтерфейс користувача повинен забезпечувати легкий доступ до політики конфіденційності та іншої важливої

інформації про обробку даних. Це може бути реалізовано через посилання на головній сторінці, в налаштуваннях або через спливаючі вікна при зборі даних.

- Зрозуміла мова: Інформація повинна бути представлена простою і зрозумілою мовою, без використання юридичних або технічних термінів, щоб суб'єкти даних могли легко зрозуміти, як їхні дані обробляються.

- Оновлення інформації: ПЗ повинно своєчасно інформувати користувачів про будь-які зміни в політиці конфіденційності або умовах обробки даних, забезпечуючи їх згодою з цими змінами.

Мінімізація даних

Мінімізація даних, як зазначено у статті 5 GDPR, передбачає:

- Обмеження обсягу даних: ПЗ повинно збирати і обробляти лише ті дані, які є необхідними для досягнення визначених цілей. Наприклад, якщо для надання послуги необхідні лише ім'я та електронна адреса, інші дані (наприклад, дата народження або номер телефону) не повинні збиратися без необхідності.

- Функціонал для регулярного перегляду: ПЗ має включати інструменти для регулярного перегляду та оцінки обсягу даних, які обробляються, з метою видалення непотрібних даних. Це може бути реалізовано через автоматичні скрипти, які перевіряють та очищують базу даних від зайвих записів.

- Анонімізація даних: У випадках, коли зберігання персональних даних більше не є необхідним, але дані потрібні для аналітичних цілей, ПЗ повинно забезпечувати можливість їх анонімізації, щоб зберегти корисну інформацію без ризику ідентифікації суб'єктів даних.

Точність

Забезпечення точності даних відповідно до статті 5 GDPR включає:

- Можливість коригування даних: ПЗ повинно дозволяти суб'єктам даних самостійно коригувати неточні або застарілі дані через інтерфейс користувача. Наприклад, користувачі повинні мати можливість оновлювати свою контактну інформацію або інші персональні дані.

- Автоматичне оновлення даних: ПЗ має підтримувати механізми автоматичного оновлення даних на основі нової інформації. Це може включати синхронізацію з іншими системами або автоматичне застосування змін, внесених суб'єктами даних.

- Періодичні перевірки: ПЗ повинно виконувати періодичні перевірки даних для виявлення та виправлення неточностей. Це може бути реалізовано через регулярні аудити баз даних та інформування користувачів про необхідність оновлення їхніх даних.

Обмеження зберігання

Відповідно до статті 5 GDPR, обмеження зберігання даних означає:

- Автоматичне видалення даних: ПЗ повинно забезпечувати автоматичне видалення або анонімізацію даних після досягнення мети їх обробки. Це може включати налаштування політик зберігання даних, які визначають, як довго дані повинні зберігатися, та автоматичні процедури видалення даних після закінчення цього періоду.

- Політики зберігання даних: ПЗ повинно мати гнучкі налаштування для визначення політик зберігання даних, які враховують різні вимоги для різних типів даних. Наприклад, фінансові дані можуть зберігатися довше, ніж контактні дані.

- Регулярні перевірки: ПЗ має виконувати регулярні перевірки відповідності даних політикам зберігання та забезпечувати, що дані, які більше не потрібні, видаляються або анонімізуються.

Ці принципи обробки даних є основоположними для забезпечення відповідності вимогам GDPR та захисту персональних даних на підприємстві. Забезпечення прозорості, мінімізації, точності та обмеження зберігання даних допомагає знизити ризики та підвищити довіру суб'єктів даних до підприємства.

3. Права суб'єктів даних

Відповідно до вимог GDPR, підприємства зобов'язані забезпечити суб'єктам даних певні права щодо обробки їх персональних даних. Програмне забезпечення

(ПЗ), яке використовується для обробки даних, має включати функціональні можливості, які забезпечують реалізацію цих прав.

Право на доступ (стаття 15)

Суб'єкти даних мають право знати, чи обробляються їхні персональні дані, а також отримувати доступ до таких даних та інформації про їх обробку. ПЗ повинно забезпечувати наступне:

- Інтерфейс для запитів: Суб'єкти даних повинні мати можливість подати запит на доступ до своїх даних через зручний інтерфейс. Це може бути форма запиту на веб-сайті або мобільному додатку.
- Автоматичне створення звітів: ПЗ має автоматично генерувати звіти, які містять повний перелік даних, що обробляються, включаючи мету обробки, категорії даних, одержувачів даних, строки зберігання, джерела даних, а також інформацію про автоматизоване прийняття рішень, якщо таке має місце.
- Формати звітів: Звіти повинні бути надані у зручному для читання форматі, наприклад, PDF або CSV, щоб суб'єкти даних могли легко ознайомитися з інформацією.

Право на виправлення (стаття 16)

Суб'єкти даних мають право вимагати виправлення неточних або неповних персональних даних. ПЗ повинно забезпечувати:

- Можливість оновлення даних: Інтерфейс користувача повинен дозволяти суб'єктам даних легко оновлювати свою інформацію. Це може бути реалізовано через особистий кабінет або профіль користувача, де можна редагувати дані.
- Автоматичне застосування змін: Після внесення змін суб'єктами даних, ПЗ повинно автоматично оновлювати відповідні записи в базі даних, забезпечуючи актуальність даних.

Право на стирання ("право бути забутим") (стаття 17)

Суб'єкти даних мають право вимагати видалення їхніх персональних даних у певних випадках. ПЗ повинно забезпечувати:

- Інтерфейс для подання запитів: Суб'єкти даних повинні мати можливість подати запит на видалення своїх даних через зручний інтерфейс, наприклад, через форму на веб-сайті або мобільному додатку.

- Автоматичне видалення даних: ПЗ повинно забезпечувати автоматичне видалення даних на запит суб'єктів даних, включаючи всі копії та резервні копії даних, де це можливо.

- Підтвердження виконання: Після видалення даних ПЗ повинно надавати суб'єктам даних підтвердження про успішне виконання запиту.

Право на обмеження обробки (стаття 18)

Суб'єкти даних мають право вимагати тимчасового обмеження обробки своїх даних. ПЗ повинно забезпечувати:

- Можливість блокування даних: Інтерфейс користувача повинен дозволяти суб'єктам даних подати запит на обмеження обробки їхніх даних. Після цього дані повинні бути заблоковані і не використовуватися для обробки, крім зберігання.

- Позначення заблокованих даних: ПЗ повинно мати механізм для позначення даних, обробка яких обмежена, наприклад, встановлення статусу "заморожені" дані, які не можуть бути використані до зняття обмеження.

Право на переносимість даних (стаття 20)

Суб'єкти даних мають право отримати свої персональні дані в структурованому, загальноприйнятому та машиночитабельному форматі та передати ці дані іншому контролеру. ПЗ повинно забезпечувати:

- Експорт даних: ПЗ має включати функцію експорту даних у форматах, таких як CSV, XML або JSON, щоб суб'єкти даних могли легко отримати свої дані.

- Інтерфейс для подання запитів: Суб'єкти даних повинні мати можливість подати запит на отримання своїх даних через зручний інтерфейс, наприклад, через особистий кабінет на веб-сайті.

- Безпечна передача даних: ПЗ повинно забезпечувати безпечну передачу даних, використовуючи сучасні методи шифрування та аутентифікації, щоб запобігти несанкціонованому доступу під час передачі.

Забезпечення цих прав допомагає підприємствам дотримуватися вимог GDPR та підвищує довіру суб'єктів даних, забезпечуючи прозорість і контроль над обробкою їхніх персональних даних.

4. Безпека обробки даних

Захист персональних даних є основним принципом GDPR, що вимагає від підприємств впровадження відповідних технічних та організаційних заходів для запобігання несанкціонованому доступу, втраті чи пошкодженню даних. У цьому розділі детально розглянуто ключові заходи, які повинні бути реалізовані в програмному забезпеченні (ПЗ) для забезпечення відповідності вимогам статті 32 GDPR.

Технічні та організаційні заходи

ПЗ повинно включати наступні технічні та організаційні заходи для захисту даних:

- Контроль доступу: ПЗ має забезпечувати багаторівневу систему контролю доступу, яка включає аутентифікацію користувачів (наприклад, використання паролів, двофакторна аутентифікація), авторизацію (надання прав доступу відповідно до ролі користувача) та аудит доступу (ведення журналу всіх спроб доступу до даних).

- Шифрування даних: ПЗ повинно використовувати сучасні методи шифрування для захисту даних під час передачі (наприклад, TLS/SSL) та зберігання (AES, RSA). Це допомагає запобігти несанкціонованому доступу до даних навіть у разі перехоплення або фізичного доступу до носіїв інформації.

- Моніторинг та виявлення загроз: ПЗ повинно включати інструменти для моніторингу системи та виявлення потенційних загроз, таких як несанкціоновані спроби доступу, аномальна активність та інші інциденти безпеки. Це може бути реалізовано через систему виявлення вторгнень (IDS) та моніторинг журналів подій.

- Регулярні перевірки безпеки: ПЗ повинно підлягати регулярним перевіркам безпеки, включаючи внутрішні та зовнішні аудити, тестування на

проникнення (пен-тести) та оцінку вразливостей. Це допомагає виявити та усунути потенційні слабкі місця у системі.

- Політики безпеки: Організація повинна мати чітко визначені політики та процедури безпеки, які регулюють обробку персональних даних. Це включає політики щодо управління доступом, інцидент-менеджменту, резервного копіювання та відновлення даних.

Псевдонімізація та шифрування

Псевдонімізація та шифрування даних є важливими методами захисту, передбаченими статтею 32 GDPR:

- Псевдонімізація: ПЗ повинно підтримувати псевдонімізацію даних, що передбачає заміну ідентифікуючих даних з відповідними псевдонімами. Це дозволяє зменшити ризик ідентифікації суб'єктів даних у випадку компрометації інформації. Псевдонімізація може бути реалізована через генерацію унікальних ідентифікаторів для користувачів, які використовуються замість їх реальних імен.

- Шифрування: Як згадувалось раніше, шифрування є ключовим заходом захисту даних під час передачі та зберігання. ПЗ повинно забезпечувати можливість шифрування всіх критичних даних та конфіденційної інформації, а також використання відповідних криптографічних алгоритмів та ключів.

Резервне копіювання та відновлення

Резервне копіювання та відновлення даних є необхідними для забезпечення безперервності бізнесу та мінімізації втрат даних у разі інцидентів:

- Регулярне резервне копіювання: ПЗ повинно забезпечувати автоматичне та регулярне створення резервних копій даних. Це може бути реалізовано через налаштування періодичних завдань резервного копіювання, які зберігають копії даних на безпечних носіях або у хмарних сховищах.

- Захист резервних копій: Резервні копії даних повинні бути захищені так само, як і основні дані. Це включає шифрування резервних копій та обмеження доступу до них.

- План відновлення: ПЗ повинно мати чітко визначений план відновлення даних після інцидентів. Це включає процедури швидкого відновлення даних з резервних копій, тестування процесів відновлення та забезпечення їх ефективності у разі реальних інцидентів.

- Документування та звітність: Всі процеси резервного копіювання та відновлення повинні бути документовані та підлягати регулярному перегляду. Це допомагає забезпечити відповідність політикам безпеки та вимогам GDPR.

Впровадження цих заходів у програмне забезпечення дозволяє підприємствам забезпечити належний рівень захисту персональних даних, мінімізувати ризики та забезпечити відповідність вимогам GDPR.

5. Відповідальність та звітність

Відповідальність і звітність є основоположними аспектами забезпечення дотримання вимог GDPR. Програмне забезпечення (ПЗ) повинно включати інструменти та функціональні можливості для документування обробки даних, проведення оцінок впливу на захист даних та сповіщення про порушення. Розглянемо кожен із цих аспектів детальніше.

Документування обробки

Відповідно до статті 30 GDPR, контролери та обробники даних зобов'язані вести журнали обробки персональних даних. ПЗ повинно забезпечувати:

- Ведення журналів обробки даних: ПЗ повинно мати функціонал для автоматичного ведення журналів усіх операцій з обробки персональних даних. Журнали повинні включати інформацію про те, які дані обробляються, ким і коли, з якою метою, та будь-які зміни або оновлення даних.

- Детальний облік операцій: Журнали повинні містити детальний облік всіх операцій, таких як створення, доступ, оновлення, видалення та передача даних. Це допомагає забезпечити прозорість і підзвітність у процесах обробки даних.

- Автоматичне створення звітів: ПЗ повинно мати можливість автоматичного створення звітів для внутрішнього та зовнішнього аудиту. Це

включає генерацію регулярних звітів про обробку даних, а також звітів на запит для зовнішніх аудиторів або регуляторних органів.

- Аудитна слідовість: ПЗ має забезпечувати можливість відстеження будь-яких змін у даних та операціях з ними. Це включає ведення журналів аудиту, які фіксують всі зміни, внесені до даних, та дозволяють відновити хронологію подій.

Оцінка впливу на захист даних (DPIA)

Оцінка впливу на захист даних (Data Protection Impact Assessment, DPIA) є обов'язковою для нових або значно змінених процесів обробки даних, які можуть мати високий ризик для прав і свобод суб'єктів даних (стаття 35 GDPR). ПЗ повинно забезпечувати:

- Інструменти для аналізу ризиків: ПЗ повинно включати інструменти для аналізу ризиків, пов'язаних з обробкою даних. Це може бути реалізовано через інтегровані шаблони для оцінки ризиків, які допомагають ідентифікувати потенційні загрози та вразливості.

- Процес оцінки впливу: ПЗ має підтримувати проведення повного циклу DPIA, включаючи ідентифікацію та аналіз ризиків, оцінку їх впливу на захист даних, розробку заходів для зниження ризиків та документування результатів оцінки.

- Шаблони та керівництва: ПЗ повинно надавати користувачам шаблони та керівництва для проведення DPIA, щоб забезпечити відповідність процесів вимогам GDPR. Це може включати чек-листи, інструкції та приклади заповнення оцінок.

- Моніторинг та оновлення: ПЗ має забезпечувати регулярний моніторинг та оновлення оцінок DPIA відповідно до змін у процесах обробки даних або нових загроз. Це включає автоматичні нагадування про необхідність перегляду та оновлення оцінок.

Сповіщення про порушення

Згідно з статтею 33 GDPR, контролери повинні сповіщати компетентні органи про порушення захисту персональних даних протягом 72 годин після його виявлення. ПЗ повинно забезпечувати:

- Виявлення порушень: ПЗ повинно мати механізми для автоматичного виявлення порушень захисту даних. Це може включати інструменти моніторингу безпеки, які виявляють аномалії та потенційні інциденти безпеки.
- Автоматичні сповіщення: ПЗ має забезпечувати автоматичні сповіщення відповідальних осіб у разі виявлення порушення. Це може бути реалізовано через систему сповіщень, яка негайно інформує про інциденти через електронну пошту, SMS або внутрішні повідомлення.
- Створення звітів про інциденти: ПЗ повинно мати можливість автоматичного створення звітів про інциденти, які включають детальну інформацію про порушення, такі як тип порушення, обсяг даних, які постраждали, можливі наслідки та вжиті заходи для їх усунення.
- Документування порушень: ПЗ має вести журнал всіх інцидентів безпеки та порушень захисту даних. Це допомагає забезпечити прозорість та підзвітність у процесах реагування на інциденти та дозволяє проводити аналіз для запобігання майбутнім порушенням.
- Комунікація з суб'єктами даних: У разі серйозних порушень, які можуть мати значні наслідки для суб'єктів даних, ПЗ повинно забезпечувати можливість швидкого та ефективного інформування суб'єктів даних про інцидент і про вжиті заходи для захисту їхніх даних.

Ці заходи допомагають підприємствам забезпечити відповідальність та підзвітність у процесах обробки персональних даних, мінімізувати ризики порушень та забезпечити відповідність вимогам GDPR.

6. Взаємодія з третіми сторонами

У контексті дотримання вимог GDPR, взаємодія з третіми сторонами є критичним аспектом, який вимагає ретельного управління та контролю. Програмне забезпечення (ПЗ) повинно включати функціональні можливості, що забезпечують

ефективну взаємодію з обробниками даних та відповідність вимогам щодо міжнародної передачі даних.

Контракти з обробниками

Згідно зі статтею 28 GDPR, контролер даних зобов'язаний укладати договори з обробниками даних, які забезпечують дотримання вимог захисту даних. ПЗ повинно забезпечувати наступне:

- Управління контрактами: ПЗ повинно включати інструменти для управління контрактами з обробниками даних. Це може бути реалізовано через систему управління контрактами (CMS), яка дозволяє створювати, зберігати та керувати договорами. ПЗ повинно забезпечувати можливість легкої перевірки умов договорів та їх відповідності вимогам GDPR.

- Стандартизовані шаблони договорів: ПЗ має надавати стандартизовані шаблони договорів, які включають всі необхідні положення щодо захисту даних відповідно до GDPR. Це допомагає забезпечити, що всі договори з обробниками містять необхідні умови, такі як обов'язки обробника, заходи безпеки, умови субпідрядників, аудит та інспекції, повідомлення про порушення та видалення даних.

- Моніторинг дотримання умов договорів: ПЗ повинно включати інструменти для моніторингу дотримання умов договорів. Це може бути реалізовано через систему сповіщень та нагадувань, яка інформує про терміни перегляду договорів, дотримання умов захисту даних та результати аудитів.

- Аудит та звітність: ПЗ має забезпечувати можливість проведення регулярних аудитів обробників даних та створення звітів про результати аудитів. Це допомагає контролерам переконатися, що обробники дотримуються умов договорів та вимог GDPR.

Міжнародна передача даних

Відповідно до статей 44-50 GDPR, міжнародна передача даних повинна відповідати певним вимогам для забезпечення належного рівня захисту даних. ПЗ повинно забезпечувати:

- Контроль за передачею даних: ПЗ має включати інструменти для контролю за міжнародною передачею даних. Це може бути реалізовано через систему відстеження переданих даних, яка фіксує, які дані передаються, кому, коли та з якою метою.

- Механізми передачі: ПЗ повинно підтримувати різні механізми міжнародної передачі даних, передбачені GDPR, такі як стандартні договірні положення (SCC), корпоративні правила (BCR), схеми сертифікації, кодекси поведінки та інші дозволені механізми передачі даних до країн, що не забезпечують належний рівень захисту даних.

- Шифрування та анонімізація: ПЗ має забезпечувати можливість шифрування даних під час передачі, щоб запобігти несанкціонованому доступу. Також може бути корисним впровадження анонімізації або псевдонімізації даних перед їх передачею, що знижує ризик ідентифікації суб'єктів даних.

- Документування передач: ПЗ повинно забезпечувати ведення журналів всіх міжнародних передач даних, включаючи інформацію про мету передачі, приймаючі сторони, обсяги даних та використані механізми захисту. Це допомагає забезпечити прозорість та підзвітність у процесах передачі даних.

- Оцінка впливу на захист даних: У випадку міжнародної передачі даних до країн, які не забезпечують належний рівень захисту, ПЗ повинно підтримувати проведення оцінки впливу на захист даних (DPIA) для ідентифікації та зниження ризиків, пов'язаних з передачею даних.

Розробка цих критеріїв оцінки допоможе підприємствам вибрати та впровадити програмне забезпечення, яке відповідає вимогам GDPR та забезпечує належний захист персональних даних під час взаємодії з третіми сторонами. Це включає ефективне управління контрактами з обробниками даних, контроль за міжнародною передачею даних та впровадження необхідних заходів безпеки.

3.2. Застосування “Enzuzo” для перевірки інформаційних систем підприємства на дотримання вимог GDPR

Enzuzo — це програмна платформа для забезпечення відповідності вимогам захисту даних, яка допомагає підприємствам легко керувати зобов'язаннями щодо конфіденційності відповідно до GDPR, CCPA та інших регуляторних стандартів.

Для прикладу застосування використаємо некомерційний вебсайт, створений за допомогою платформи Bubble.io. При створенні аккаунта підключимо вебсайт, який матимемо аналізувати, у нашому випадку він буде знаходитись за посиланням https://alextest-62204.bubbleapps.io/. Далі встановлюємо платформу як “Інша платформа” так як Bubble.io не вказаний серед запропонованих. Після успішної реєстрації бачимо наступне модальне вікно:

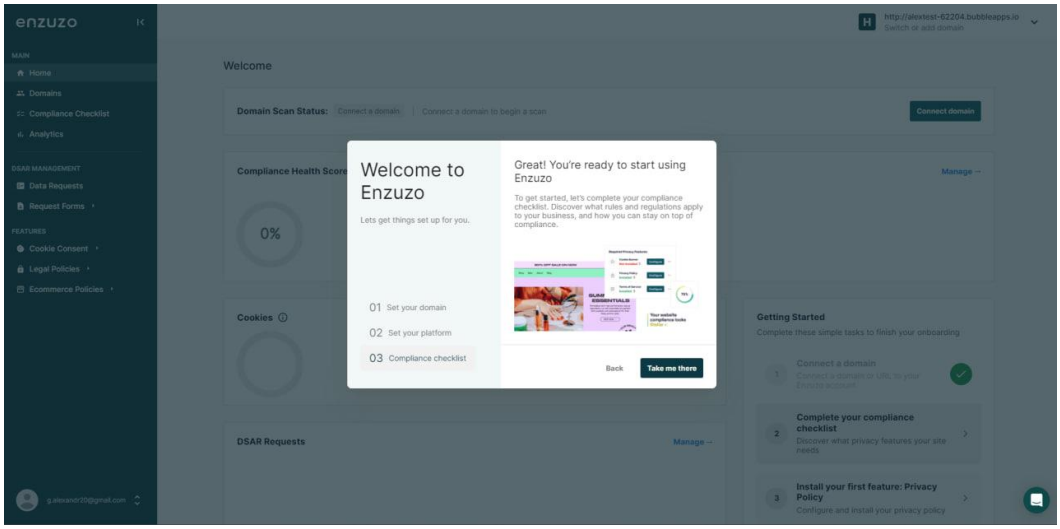

Рис. 3.1. Успішна реєстрація

Одразу після цього процесу платформа Enzuzo переносить нас до блоку “Compilance Checklist”, на якому нам потрібно буде визначити такі параметри як “Buisness Type”, “Website”, “Geography” та “DSAR”. Для того, щоб сфокусуватись лише на GDPR обираємо ті країни, у законодавстві яких діє GDPR.

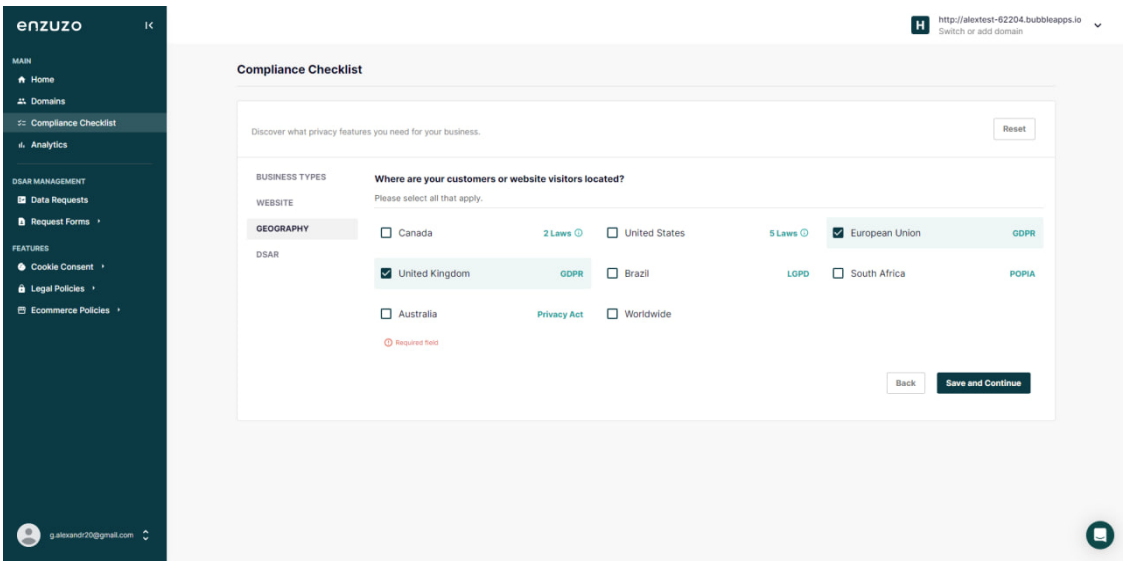

Рис. 2 - Вибір країн

Після успішної реєстрації ми бачимо результат сканування нашого вебсайту на відповідність вимог GDPR і бачимо, що в результаті сканування наш вебсайт потребує уваги:

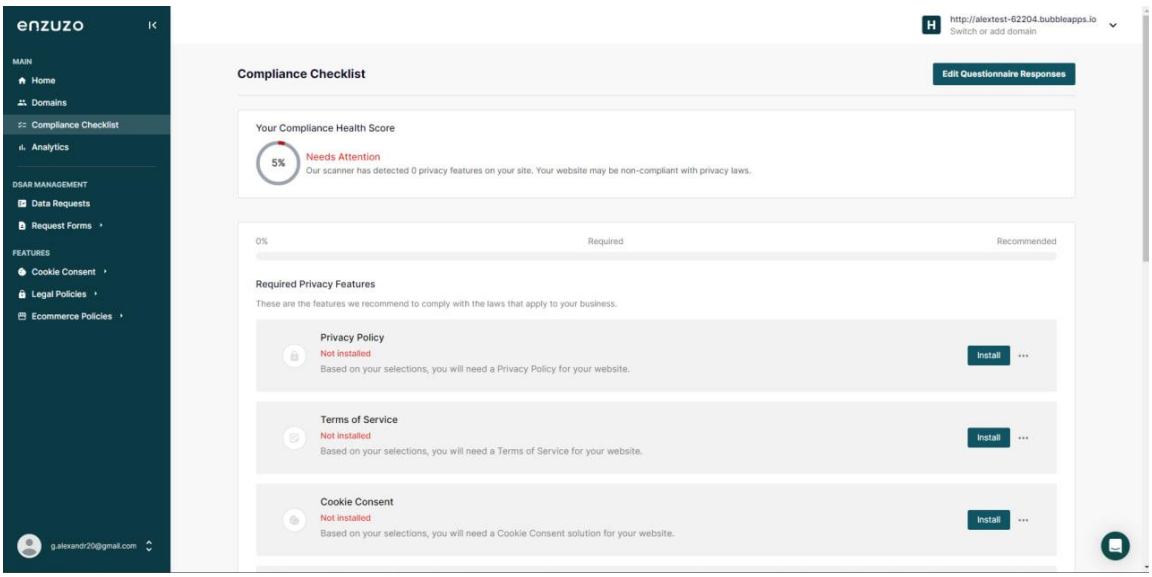

Рис. 3 - Перше сканування вебсайту

Перейдемо до основних пунктів, які вимагають уваги та виправимо їх.

В першу чергу нам потрібно встановити базові сторінки, що будуть вказувати нормативну базу користування вебсайтом, такі як Privacy Policy, Terms of Service та Subscription Services Agreement, а також встановити Cookie Banner

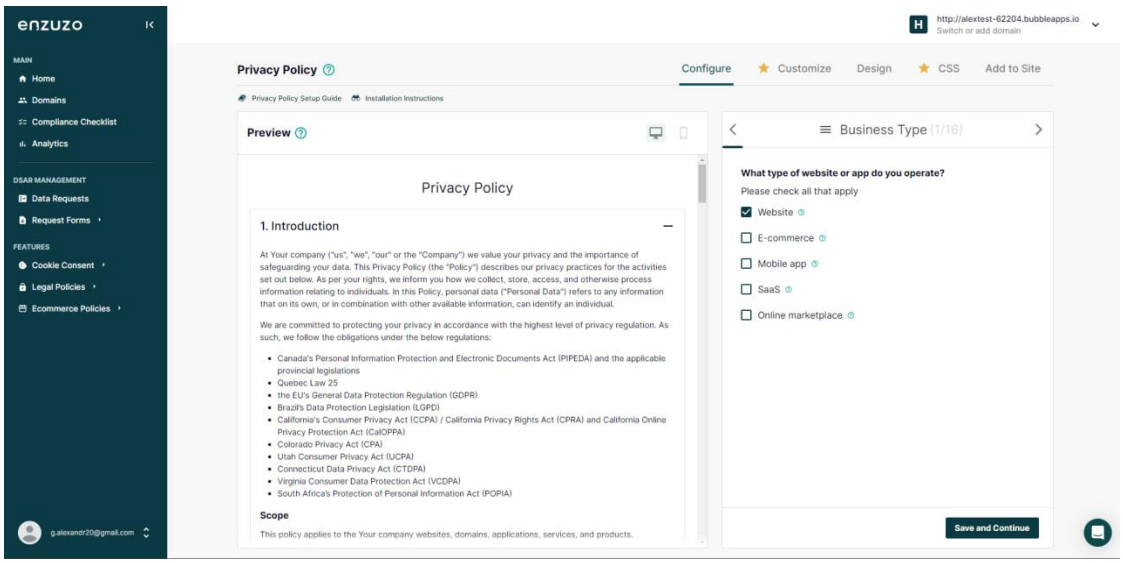

Рис. 4 - Створення Privacy Policy

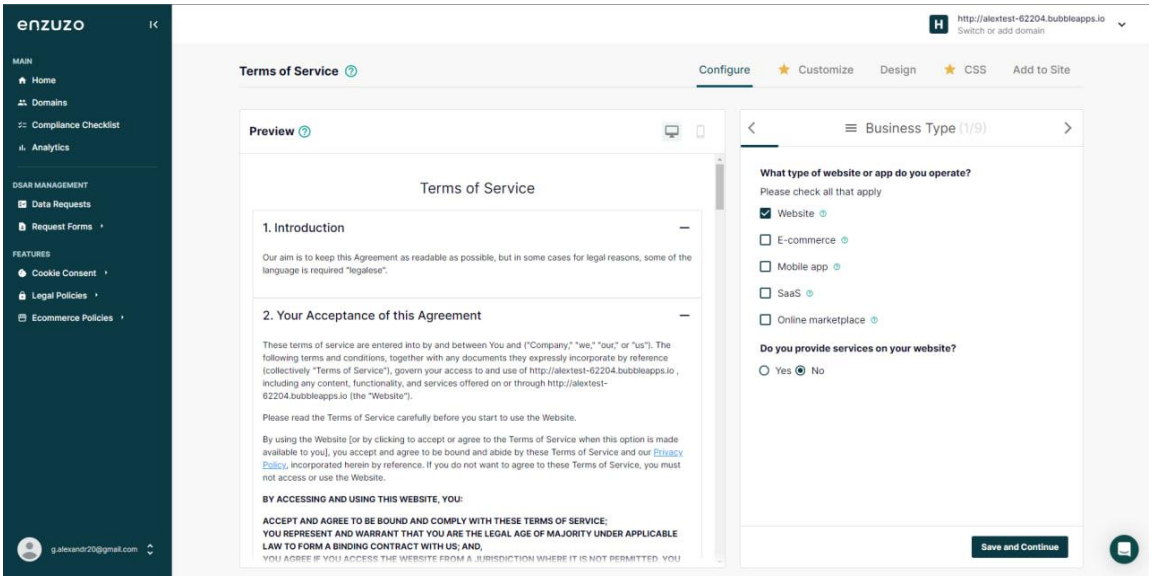

Рис. 5 - Створення Terms of Service

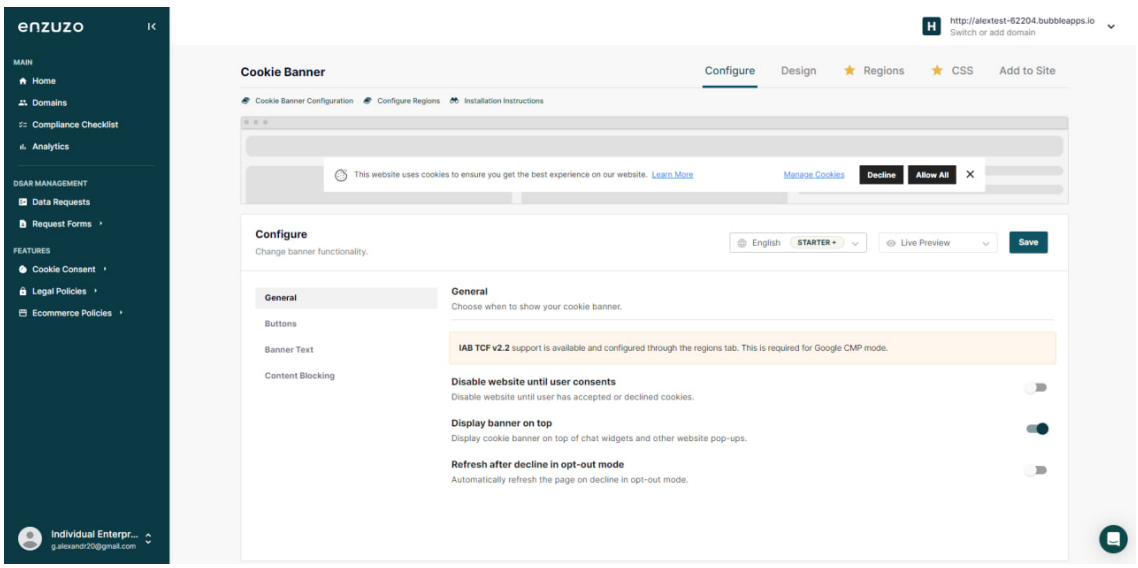

Рис. 6 - Створення Cookie Banner

Далі встановлюємо блоки, що ми отримали в код вебсайту:

Для Cookie Banner:

<script src="https://app.enzuzo.com/apps/enzuzo/static/js/__enzuzo-cookiebar.js?uuid=8a5210ae-1815-11ef-b7ca-ef1bbd61b100"></script>

Для Privacy Policy:

<script id="__enzuzo-root-script" src="https://app.enzuzo.com/scripts/privacy/8a5210ae-1815-11ef-b7ca-ef1bbd61b100"></script>

Для Terms of Service:

<script id="__enzuzo-root-script" src="https://app.enzuzo.com/scripts/tos/8a5210ae-1815-11ef-b7ca-ef1bbd61b100"></script>

Для Subscription Services Agreement:

<script id="__enzuzo-root-script" src="https://app.enzuzo.com/scripts/ssa/8a5210ae-1815-11ef-b7ca-ef1bbd61b100"></script>

Після цього ми бачимо елементи, що з’явились на сторінках нашого вебсайту, наприклад Privacy Policy та Cookie Banner:

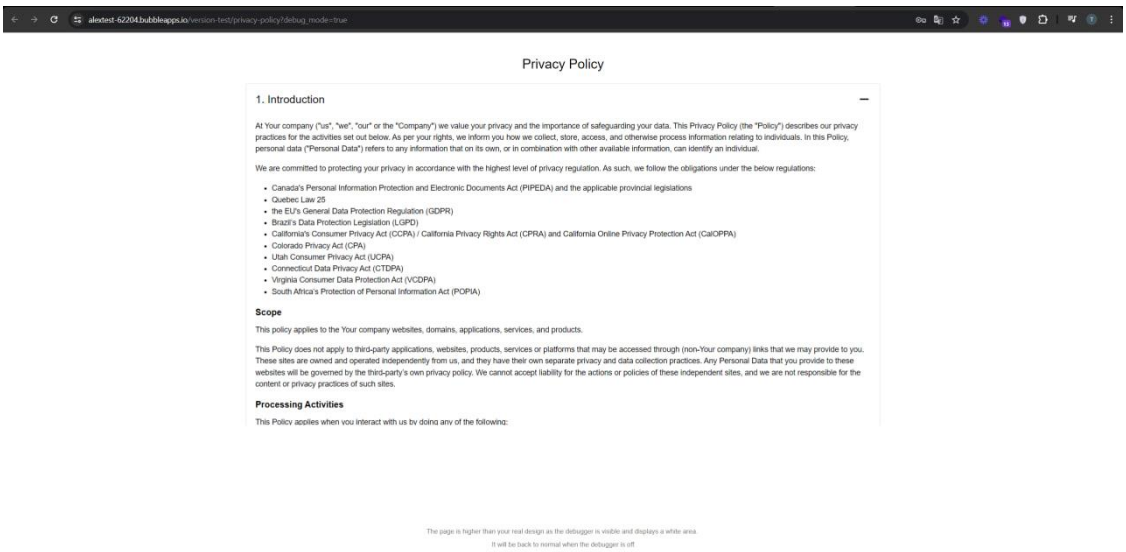

Рис. 7 - Успішно додані Privacy Policy

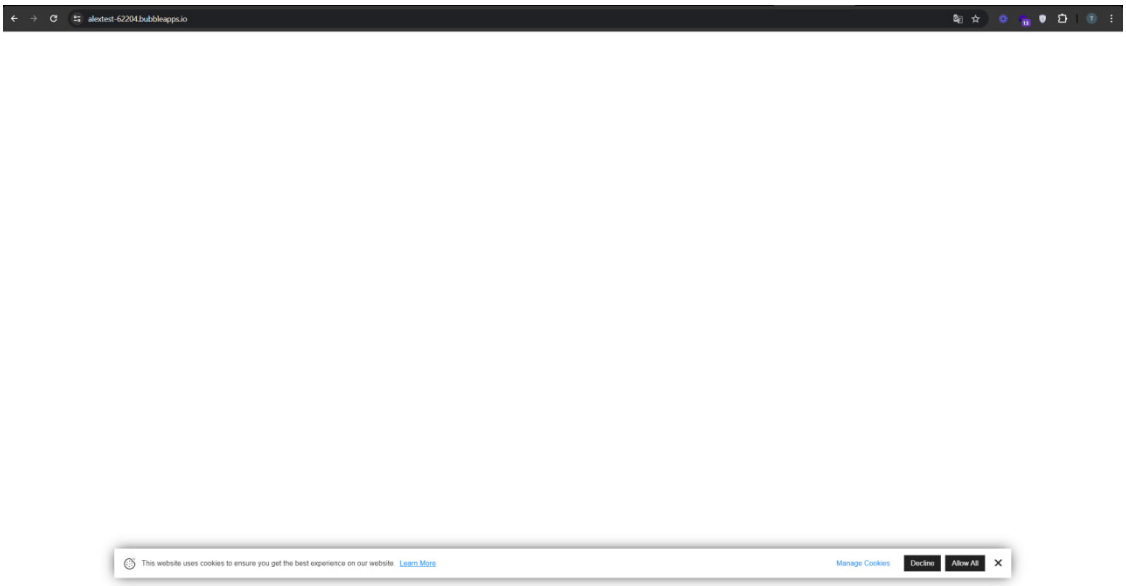

Рис. 8 - Успішно доданий Cookie Banner

Давайте переглянемо, яким чином буде виглядати результат сканування нашого вебсайту після того, як ми додали ці елементи на вебсайт:

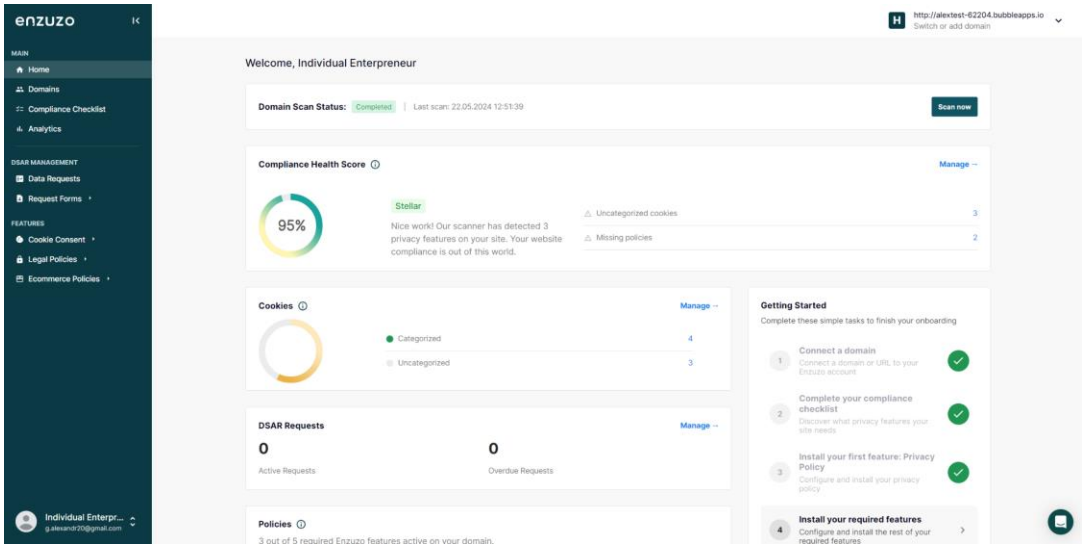

Рис. 9 - Результат сканування після встановлення сторінок з нормативною базою

Візьмемо до уваги, що це сканування і на початку, і на кінці проводилось на прикладі абсолютно пустого сайту, який збирає лише базову інформацію про користувача в Cookies, без запитів на ім’я, прізвище, тощо.

Для виконання вимог GDPR зробимо наступні кроки:

1. Встановлення шифрування даних у стані спокою за алгоритмом RDS AES-256

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
from Crypto.Random import get_random_bytes

def encrypt_message(message, key):
    # Генерація випадкового 16-байтового ініціалізаційного вектора (IV)
    iv = get_random_bytes(16)

    # Створення об'єкта шифрування AES у режимі CBC
    cipher = AES.new(key, AES.MODE_CBC, iv)

    # Додавання паддінгу до повідомлення до кратності 16 байтам
    padded_message = pad(message.encode(), AES.block_size)

    # Шифрування повідомлення
    encrypted_message = cipher.encrypt(padded_message)

    # Повернення ініціалізаційного вектора та зашифрованого повідомлення
    return iv + encrypted_message

# Приклад використання
message = "Це секретне повідомлення"
key = get_random_bytes(32)  # 256-бітний ключ

encrypted_message = encrypt_message(message, key)
print(f"Зашифроване повідомлення: {encrypted_message.hex()}")
```

2. Встановлення TLS для захисту даних при передачі по API

Серверний скрипт:

```
from flask import Flask, request, jsonify
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
from Crypto.Random import get_random_bytes
import base64

app = Flask(__name__)

key = get_random_bytes(32)  # 256-бітний ключ

@app.route('/decrypt', methods=['POST'])
def decrypt_message():
    try:
        data = request.json
        iv = base64.b64decode(data['iv'])
        encrypted_message = base64.b64decode(data['message'])

        cipher = AES.new(key, AES.MODE_CBC, iv)
        decrypted_message = unpad(cipher.decrypt(encrypted_message), AES.block_size)

        return jsonify({'message': decrypted_message.decode()}), 200
    except Exception as e:
        return str(e), 400

if __name__ == '__main__':
    app.run(ssl_context=('cert.pem', 'key.pem'))
```

Генерація самопідписаних сертифікатів SSL:

openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes

Клієнтський скрипт для передачі по API:

```
import requests
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
from Crypto.Random import get_random_bytes
import base64

def encrypt_message(message, key):
    iv = get_random_bytes(16)
    cipher = AES.new(key, AES.MODE_CBC, iv)
    padded_message = pad(message.encode(), AES.block_size)
    encrypted_message = cipher.encrypt(padded_message)
    return iv, encrypted_message

# Ключ повинен бути однаковим на клієнті та сервері
key = b'your_32_byte_key_here_your_32_byte_key_here'

message = "Це секретне повідомлення"
iv, encrypted_message = encrypt_message(message, key)

iv_base64 = base64.b64encode(iv).decode('utf-8')
encrypted_message_base64 = base64.b64encode(encrypted_message).decode('utf-8')

data = {
```

```
    'iv': iv_base64,
    'message': encrypted_message_base64
}

response = requests.post('https://localhost:5000/decrypt', json=data, verify='cert.pem')
print(response.json())
```

Завдяки цим діям ми встановили належний захист при передачі та зберіганні даних, а також попередили користувача про всі можливі наслідки завдяки нормативно-правовим сторінкам вебсайту.

3.3. Розробка рекомендацій щодо захисту персональних даних на підприємстві на основі Enzuzo

Для забезпечення належного захисту персональних даних на підприємстві, важливо розробити комплексний підхід, який охоплює всі аспекти обробки, зберігання та передачі інформації. В якості основи для розробки таких рекомендацій використовується платформа Enzuzo, яка пропонує інструменти для управління конфіденційністю та захисту даних. Нижче наведено основні рекомендації, розбиті на ключові пункти:

Впровадження політики конфіденційності

- Створення та оновлення політики конфіденційності: Використання шаблонів Enzuzo для розробки політики конфіденційності, яка відповідає вимогам законодавства. Політика повинна бути зрозумілою та доступною для всіх співробітників і клієнтів.

- Регулярне оновлення: Проводити регулярний перегляд і оновлення політики конфіденційності відповідно до змін у законодавстві та внутрішніх процесах підприємства.

Оцінка ризиків та аудит

- Регулярні аудити: Проведення регулярних аудитів систем обробки персональних даних для виявлення потенційних вразливостей. Використання інструментів Enzuzo для автоматизації процесу оцінки ризиків.

- Оцінка впливу на захист даних (DPIA): Використання Enzuzo для проведення оцінки впливу на захист даних під час впровадження нових систем або процесів, що обробляють персональні дані.

Управління доступом та автентифікація

- Контроль доступу: Впровадження багаторівневої системи контролю доступу до персональних даних. Визначення та обмеження прав доступу на основі ролей і обов’язків співробітників.

- Багатофакторна автентифікація (MFA): Використання багатофакторної автентифікації для доступу до критично важливих систем і даних.

Навчання та підвищення обізнаності співробітників

- Регулярне навчання: Проведення регулярних тренінгів для співробітників щодо правил обробки персональних даних та методів захисту інформації.

- Тестування знань: Використання Enzuzo для організації тестування знань співробітників щодо політик конфіденційності та безпеки даних.

Обробка запитів суб'єктів даних

- Автоматизація процесу обробки запитів: Використання інструментів Enzuzo для автоматизації процесу обробки запитів суб'єктів даних на доступ, виправлення або видалення їхніх персональних даних.

- Прозорість і комунікація: Забезпечення прозорого процесу обробки запитів та ефективного спілкування з суб'єктами даних.

Захист даних під час передачі

- Шифрування даних: Використання передових методів шифрування для захисту даних під час передачі між системами, таких як AES-256, RSA-2048.

- Безпечні канали передачі: Впровадження захищених каналів передачі даних, таких як SSL/TLS для всіх комунікацій, що містять персональні дані.

Інцидент-менеджмент

- План реагування на інциденти: Розробка та впровадження плану реагування на інциденти, пов'язані з порушеннями безпеки персональних даних.

- Моніторинг і виявлення: Використання інструментів Enzuzo для моніторингу систем та виявлення потенційних інцидентів безпеки в режимі реального часу.

Відповідність законодавству

- Моніторинг змін у законодавстві: Постійне відстеження змін у законодавстві щодо захисту персональних даних та забезпечення відповідності внутрішніх політик цим вимогам.

- Документування процесів: Збереження всіх документів та записів, пов'язаних з обробкою персональних даних, для підтвердження відповідності вимогам законодавства.

Захист даних у хмарних сервісах

- Вибір надійних провайдерів: Використання перевірених та сертифікованих хмарних провайдерів, які забезпечують високий рівень безпеки даних.

- Управління конфігураціями: Постійний моніторинг і управління конфігураціями хмарних сервісів для мінімізації ризиків витоку даних.

Застосування наведених рекомендацій дозволить підприємству значно підвищити рівень захисту персональних даних, зменшити ризики витоку інформації та забезпечити відповідність вимогам законодавства у сфері захисту даних. Платформа Enzuzo надає необхідні інструменти та підтримку для реалізації цих заходів ефективно та зручно.

ВИСНОВКИ

Проведене дослідження підтвердило актуальність та необхідність впровадження сучасних методів і технологій для захисту персональних даних на підприємствах. У рамках дипломної роботи було виявлено основні вразливості персональних даних, зокрема технічні, організаційні та людські фактори, які можуть спричинити витік або несанкціонований доступ до даних. Розглянуто вплив міжнародних стандартів GDPR та HIPAA на процеси обробки даних, що дозволило порівняти їх з актуальними нормами українського законодавства та визначити ключові відмінності та подібності.

Проведено аналіз нормативної бази та правових аспектів захисту даних, зокрема вимог GDPR та HIPAA, що дало можливість виявити ефективні практики та підходи до захисту інформації. Огляд сучасних технологій і методик захисту персональної інформації показав необхідність використання шифрування, багатофакторної аутентифікації та управління ідентичністю для забезпечення високого рівня безпеки даних на підприємствах.

Запропоновані рекомендації включають створення та впровадження корпоративної політики захисту персональних даних, яка охоплює правові, організаційні та технічні аспекти. Особлива увага приділена технічним заходам захисту, таким як шифрування, контроль доступу, системи моніторингу та резервне копіювання, що дозволяє мінімізувати ризики несанкціонованого доступу, втрати або пошкодження даних.

Розроблені рекомендації можуть бути використані у сфері забезпечення кібербезпеки у корпоративних інформаційних системах, що дозволяє підвищити рівень захисту персональних даних та відповідність законодавчим вимогам. У цілому, дослідження підтвердило, що інтеграція сучасних технологій та методик захисту персональних даних є критично важливою для забезпечення безпеки інформації на підприємствах. Впровадження запропонованих рекомендацій дозволить мінімізувати ризики витоку даних, підвищити довіру клієнтів та

забезпечити відповідність вимогам міжнародних стандартів та українського законодавства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Загальний регламент захисту даних (GDPR) Європейського Союзу. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 25.04.2024).

2. Закон про переносимість та підзвітність медичного страхування (HIPAA) Сполучених Штатів. URL: https://www.hhs.gov/hipaa/index.html (дата звернення: 25.04.2024).

3. Закон України «Про захист персональних даних», №2297–VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 25.04.2024).

4. NIST SP 800-30: Guide for Conducting Risk Assessments. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 25.04.2024).

5. ISO/IEC 27005: Інформаційна безпека. Управління ризиками інформаційної безпеки. URL: https://www.iso.org/standard/75281.html (дата звернення: 25.04.2024).

6. FIPS 197: Advanced Encryption Standard (AES). URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (дата звернення: 25.04.2024).

7. FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (дата звернення: 25.04.2024).

8. Datafloq. Ресурси для аналізу ринкових трендів та виявлення незадоволених потреб. URL: https://datafloq.com/ (дата звернення: 25.04.2024).

9. Penn LPS Online. Поведінковий аналіз та сегментація ринку. URL: https://lpsonline.sas.upenn.edu/ (дата звернення: 25.04.2024).

10. Termly. Принципи прозорості та доступності політики конфіденційності. URL: https://termly.io/ (дата звернення: 25.04.2024).

11. Harvard Business Review. Динамічне ціноутворення та оптимізація каналів продажів. URL: https://hbr.org/ (дата звернення: 25.04.2024).

12. Enzuzo. Рішення для перевірки інформаційних систем підприємства на дотримання вимог GDPR. URL: https://www.enzuzo.com/ (дата звернення: 25.04.2024).

13. RSA (Rivest-Shamir-Adleman). Асиметричне шифрування. URL: https://en.wikipedia.org/wiki/RSA_(cryptosystem) (дата звернення: 25.04.2024).

14. AES (Advanced Encryption Standard). Симетричне шифрування. URL: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard (дата звернення: 25.04.2024).

15. Управління ідентичністю та доступом (IAM) та методики багатофакторної аутентифікації (MFA). URL: https://en.wikipedia.org/wiki/Identity_management (дата звернення: 25.04.2024).

16. Системи виявлення та реагування (EDR) для моніторингу кінцевих точок. URL: https://en.wikipedia.org/wiki/Endpoint_detection_and_response (дата звернення: 25.04.2024).

17. Управління мобільними пристроями (MDM) для захисту даних. URL: https://en.wikipedia.org/wiki/Mobile_device_management (дата звернення: 25.04.2024).

18. Zero Trust. Технології нульової довіри для постійної перевірки запитів на доступ. URL: https://en.wikipedia.org/wiki/Zero_trust_security_model (дата звернення: 25.04.2024).

19. Системи управління контрактами (CMS) для контролю взаємодії з третіми сторонами. URL: https://en.wikipedia.org/wiki/Contract_management_software (дата звернення: 25.04.2024).

20. Політики контролю за змінами, включаючи відстеження змін у ПЗ. URL: https://en.wikipedia.org/wiki/Change_management_(ITSM) (дата звернення: 25.04.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)