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 в інформаційній системі підприємства на базі Microsoft Purview»

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

_____ Богдан ПЕДОСЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ПЕДОСЕНКО Богдан
(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

Педосенко Богдану Володимировичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства»

керівник кваліфікаційної роботи Марченко Віталій, д.ф., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 27 » лютого 2024 року № 36.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024

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

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблем забезпечення безпеки персональних даних.
2. Дослідження методів захисту персональних даних.
3. Розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства на основі Microsoft Purview.

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.	Аналіз проблем забезпечення безпеки персональних даних.	15.04.2024	
2.	Дослідження методів захисту персональних даних.	25.04.2024	
3.	Аналіз засобів забезпечення захисту персональних даних	10.05.2024	
4.	Аналіз функціональних можливостей Microsoft Purview	17.05.2024	
5.	Розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства на основі Microsoft Purview	21.05.2024	
6.	Оформлення результатів дослідження	25.05.2024	
7.	Підготовка доповіді до захисту		

Здобувач вищої освіти _____ Богдан ПЕДОСЕНКО
(підпис) *(ім'я, прізвище)*

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ПЕДОСЕНКО Богдана

на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства»

Актуальність: У сучасних умовах цифрової трансформації в Україні захист персональних даних в інформаційних системах підприємств набуває важливості. Зростання обсягів цифрових даних підвищує ризики їх неправомірного використання та витоку. Відповідно до українського законодавства, підприємства зобов'язані забезпечити захист особистих даних клієнтів та співробітників. Для цього необхідно впроваджувати заходи безпеки, аналізувати ризики та дотримуватися вимог нормативних актів. Недотримання цих вимог може призвести до штрафів, зупинення обробки даних, втрати довіри клієнтів та фінансових збитків.

Позитивні сторони:

Недоліки:

Висновок:

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 ПЕДОСЕНКО Богдан 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 в інформаційній системі підприємства».

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

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

Висновок кафедри про кваліфікаційну роботу

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 53 сторінки, 10 рисунків, 1 таблиця 18 джерел.

Об'єкт дослідження – процес захисту персональних даних в інформаційній системі підприємства.

Предмет дослідження – методи та засоби щодо захисту персональних даних.

Мета роботи дослідити шляхи та розробити рекомендації щодо захисту персональних даних на базі Microsoft Purview.

Методи дослідження – опрацювання літератури за даною темою, аналіз існуючих систем захисту інформації, розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства.

В умовах цифрової трансформації та зростання обсягів даних управління інформацією стає критично важливим завданням для компаній. Microsoft Purview, сучасна платформа для управління даними, пропонує інноваційні рішення для інтеграції, захисту та управління інформацією. Актуальність цієї дипломної роботи полягає у дослідженні можливостей Microsoft Purview для покращення процесів обробки та аналізу даних. Використання таких платформ сприяє підвищенню ефективності, забезпеченню відповідності нормативним вимогам та оптимізації управлінських рішень в умовах глобалізації бізнесу.

Галузь використання – кібербезпека персональних даних в інформаційній системі підприємства.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СЗ	– система захисту
ПД	– персональні дані
СЗПД	– система захисту персональних даних
ЗБПД	– загроза безпеки персональних даних
ІСПД	– інформаційна система персональних даних
ОС	– операційна система
GDPR	– General Data Protection Regulation(Загальний регламент захисту даних)
СКУД	–система контролю і управління доступом персоналу
СОС	– система охоронної сигналізації
СТН	– система телевізійного спостереження
СФЗ	– система фізичного захисту

ВСТУП

Актуальність дослідження. У сучасних умовах цифрової трансформації в Україні, питання захисту персональних даних в інформаційних системах підприємств стає дедалі більш актуальним і важливим. Зростання обсягів цифрових даних, які обробляються та зберігаються, породжує загрози їхнього неправомірного використання, крадіжки чи витоку. Відповідно до законодавства України, зокрема Закону "Про захист персональних даних" та Закону "Про захист інформації в інформаційно-телекомунікаційних системах", підприємства зобов'язані забезпечити високий рівень захисту особистих даних своїх клієнтів та співробітників.

Дослідження захисту персональних даних в інформаційній системі підприємства є необхідним кроком для ефективного впровадження заходів безпеки та відповідності законодавчим вимогам. Відповідно до вимог нормативних актів, підприємства повинні розробляти та впроваджувати проекти захисту персональних даних, що включають в себе усвідомлення важливості захисту даних, аналіз ризиків, визначення вартості та графіку реалізації проекту.

Недотримання вимог законодавства у сфері захисту персональних даних може призвести до серйозних наслідків для підприємства, включаючи адміністративні штрафи, примусову призупинення або припинення обробки даних, анулювання ліцензій, що може суттєво вплинути на фінансовий стан та репутацію компанії. Поза цими очевидними наслідками, негативний результат аудиту може також спричинити втрату довіри з боку клієнтів та партнерів, що може призвести до зниження обсягу бізнесу та збитків.

Об'єкт дослідження – процес захисту персональних даних в інформаційній системі підприємства.

Предмет дослідження – методи та засоби щодо захисту персональних даних.

Методи дослідження – опрацювання літератури за даною темою, аналіз існуючих систем захисту інформації, розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства.

Практичне значення одержаних результатів – рекомендації щодо захисту персональних даних можуть бути використані у сфері забезпечення кібербезпеки у інформаційних системах підприємтсв.

1 АНАЛІЗ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Поняття персональних даних

Сьогодні життя людини невіддільне від необхідності надання інформації про себе іншим членам суспільства та органам державної влади. Відповідно до ст. 2 Закону України «Про інформацію» від 02.10.1992, кожен має право на інформацію, що включає можливість безкоштовного отримання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод та інтересів. Використання інформаційних технологій, глобальних інформаційних систем та автоматизованих баз даних значно полегшує реалізацію цього права. Однак це також підвищує ризик несанкціонованого втручання в особисте життя та зловживань персональними даними [2].

Право на захист особистих даних є основним правом людини. Конституція України гарантує, що ніхто не може втручатися в особисте та сімейне життя, крім випадків, передбачених Конституцією. Забороняється збирати, зберігати, використовувати і поширювати конфіденційну інформацію про особу без її згоди, за винятком випадків, визначених законом, в інтересах національної безпеки, економічного добробуту та прав людини (стаття 32) [3].

Першою проблемою, з якою стикалися менеджери персональних даних під час реєстрації у національному реєстрі баз персональних даних, було визначення того, яка інформація стосується персональних даних, а яка - ні.

Відповідно до ст. 11 Закону України «Про інформацію» від 02.10.1992 р., персональні дані - це інформація або сукупність відомостей про особу, яка ідентифікує або може конкретно ідентифікувати цю особу. Конфіденційна інформація включає дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, адресу, дату та місце народження особи.

У поясненнях Міністерства юстиції "Деякі питання практичного застосування українського закону "Про захист персональних даних" від 21.12.2011.

Вказується, що українське законодавство не встановило і не може встановити переліку інформації про фізична особа, яка є персональними даними, за можливість застосування норм закону до різних ситуацій, у тому числі при обробці персональних даних у (автоматизованих) базах даних та файлах персональних даних, які можуть виникнути в майбутньому внаслідок змін у технологічній, соціальній, економічної та інших сфер суспільного життя, визнаючи існування проблеми, він не відповів на питання, яка інформація дозволяє ідентифікувати особу [6].

Конституційний Суд України, даючи офіційне тлумачення частини першої та другої статті 32 Конституції України, вважає інформацію про особисте та сімейне життя людини (особисті дані, що стосуються її) інформацією або сукупністю інформації щодо особи, яку ідентифікували або яку можна конкретно ідентифікувати, а саме: громадянство, освіта, сімейний стан, релігійні переконання, стан здоров’я, матеріальне становище, адреса, дата та місце народження, місце проживання та перебування тощо, дані про особисті майнові та позашлюбні стосунки цієї особи з іншими особами, зокрема членами сім'ї, а також інформація про події та явища, що відбулися або відбуваються в побутовій, інтимній, товариській, професійній, діловій та інших сферах особи життя, винні дані про вправу с обов'язки особи, яка займає посаду, пов'язану з виконанням функцій держави або місцевого самоврядування. Ця інформація про особу та членів її родини є конфіденційною і може бути передана лише за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [7].

Варто відзначити, що в багатьох країнах персональні дані поділяються на загальні та вразливі. До загальних належать ім'я, прізвище, по батькові, вигадка, місце проживання, тоді як вразливі дані включають відомості про расові, політичні, релігійні або інші переконання, стан здоров'я, сексуальність та судимості. Такий поділ необхідний для забезпечення спеціального режиму захисту вразливих даних.

Надання персональних даних часто пов'язане з вступом особи у певні правовідносини (професійні, цивільні, економічні тощо). Проте імплементація

закону не завжди узгоджується з іншими нормативними актами.

Основою права на використання персональних даних є згода суб'єкта на їх обробку. Відповідно до ч. 2 ст. 11 Закону України «Про інформацію» від 02.10.1992 р., збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди заборонені, за винятком випадків, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Як зазначено в п.1 ч.1 ст. 11 цього закону, основою для використання персональних даних є згода суб'єкта даних на їх обробку. Тобто законодавець надає фізичній особі право дати згоду на використання її персональних даних, а також передбачає адміністративну та кримінальну відповідальність за їх використання без цієї згоди.

Наприклад, відповідно до ст. 24 Кодексу законів про працю України при укладенні трудового договору громадянин повинен пред'явити паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, також документ про освіту (спеціальність, кваліфікацію), стані медичні та інші документи [8].

Ця проблема стає актуальною в іншому аспекті. Внаслідок посилення відповідальності за порушення закону роботодавці почали активно вимагати від співробітників згоди на використання їх персональних даних, які вже були зібрані під час прийому на роботу. Більшість співробітників підписують таку угоду автоматично, але деякі категорично відмовляються. Тому виникає питання: як роботодавцю уникнути відповідальності у разі незаконної обробки персональних даних? На сьогоднішній день можна лише сподіватися, що Державна служба України з питань захисту персональних даних під час перевірок буде враховувати такі ситуації [1].

Виходячи з вищесказаного, є кілька варіантів вирішення цієї ситуації. У випадках, коли особа повинна надати персональні дані для укладення певних правовідносин, згідно з чинним законодавством, слід виходити з того, що згода вже надана автоматично. Таким чином, немає потреби в додатковій згоді. Однак, фізична особа зберігає всі права на свої персональні дані, передбачені законом. Це

можна реалізувати, включивши в закон положення про випадки, коли згода суб'єкта даних не потрібна, наприклад, обробка персональних даних співробітника для виконання трудових обов'язків, сплати податків і зборів здійснюється без згоди співробітника.

Інший варіант полягає в наданні алгоритму дій для власника персональних даних у випадку, якщо суб'єкт даних відмовляється надати згоду на їх використання.

Ще один приклад застосування закону в сфері цивільного права. Відповідно до ч. 1 ст. 633 ЦК України. Відповідно до цієї статті, договір, де підприємець зобов’язується здійснювати продаж товарів, виконання робіт або надання послуг кожному, хто звернеться до нього (роздрібна торгівля, транспорт, послуги зв’язку, медичні послуги, готелі, банківська справа тощо), є публічним. При цьому підприємець не має права відмовити в укладенні такого договору, якщо він може надати відповідні товари або послуги. У разі необґрунтованої відмови підприємець повинен відшкодувати споживачеві збитки (ч. 4 ст. 633 ЦК України) [1]. Відмова підприємця надати послугу через відмову споживача надати згоду на використання його персональних даних буде вважатися необґрунтованою.

Тому, на мою думку, закон повинен у виняткових випадках дозволяти обробку персональних даних, необхідних для укладення та виконання договору, без згоди суб'єкта даних. Це важливо, оскільки більшість компаній мають персональну базу даних і зобов'язані її реєструвати, особливо юридичні особи, що надають послуги населенню.

Персональні дані сторін трудового договору, такі як інформація про роботодавця і працівника, мають важливе значення. При укладанні трудового договору працівник отримує інформацію про роботодавця, місце його знаходження та характер роботи, тоді як роботодавець отримує дані про вік, професію, кваліфікацію, стан здоров’я та сімейний стан працівника. Після укладання трудового договору ця інформація потрібна роботодавцю для виконання обов'язків згідно з трудовим, цивільним, сімейним, адміністративним та іншим законодавством (наприклад, утримання податків, відшкодування шкоди, сплата

аліментів), а також для надання працівникові пільг і переваг, таких як переведення на іншу роботу через хворобу, вагітність або наявність дітей.

Надаючи роботодавцю право отримувати персональні дані працівника, закон зобов'язує його вживати всіх необхідних заходів для запобігання несанкціонованому розголошенню цієї інформації. Інформація про персональні дані працівника повинна залишатися в межах роботодавця і не стати доступною третім особам без відома і згоди працівника.

Коло інформації, що відноситься до персональних даних працівника, визначається роботодавцем з урахуванням умов, визначених трудовим законодавством стосовно того чи іншого виду трудового договору і трудової діяльності, а також з урахуванням характеру виконуваної роботи. Наприклад, спеціальна інформація буде потрібна роботодавцю для укладення з працівником трудового договору на виконання роботи, що вимагає спеціальних знань або допуску до державної таємниці.

1.2 Аналіз загроз для персональних даних

Загрози безпеці персональних даних представляють собою умови або фактори, що створюють небезпеку для даних шляхом несанкціонованого доступу, модифікації, знищення, розповсюдження або інших незаконних дій. Джерела загроз можуть бути як внутрішні (співробітники організації), так і зовнішні (зловмисники, які використовують канали зв'язку, комп'ютерні мережі та Інтернет). Загрози можуть виникати також через введення в інформаційну систему шкідливих програм та вірусів.

Реалізація загроз може включати несанкціонований доступ до інформації, витоки через технічні канали, та особливі впливи на персональні дані або інформаційну систему. Програмне та апаратне забезпечення можуть допомогти вирішити проблему несанкціонованого доступу до персональних даних. Порушення режиму конфіденційності може включати незаконне копіювання або розповсюдження даних, їх модифікацію або знищення, що може призвести до

значних наслідків. Зловмисники можуть створювати ненормальні режими роботи операційного середовища або програмного забезпечення для викрадення або впливу на інформацію.

Зловмисники можуть використовувати вразливості, такі як недостатній рівень захисту, недосконаліть системного та прикладного програмного забезпечення, а також мережеві протоколи комунікації. Інші загрози можуть включати витоки через технічні канали, наприклад, через електромагнітне випромінювання та перешкоди (ПЕМВП). Ці загрози особливо актуальні для інформаційних систем вищого класу, які обробляють спеціальні категорії персональних даних.

Відповідно до вимог законодавства, для інформаційних систем розробляється спеціальна модель загроз, в якій аналізуються вразливості та загрози, визначається їх актуальність і достатність існуючих засобів захисту.

Надаючи свої персональні дані, суб’єкт очікує, що вони будуть захищені від несанкціонованого доступу, використання, розповсюдження та знищення. Для цього оператори персональних даних повинні розробити систему захисту від атак зловмисників, визначаючи, від кого і яких дій слід захищатися. Найбільш ефективними є системи захисту персональних даних, створені на основі детального аналізу загроз.

Організації, підприємства або фізичні особи, які обробляють приватні дані громадян, ризикують зіткнутися зі зловмисниками, що прагнуть отримати, змінити, знищити або передати ці дані третім особам без дозволу власника.

В рамках функціонування інформаційних систем персональних даних загрози включають всі умови та чинники, що можуть призвести до витоку або неправомірного використання даних. Це може включати промислове шпигунство, неусвідомлене поширення інформації або передачу конфіденційних відомостей стороннім співробітниками підприємства. Завданням уповноважених осіб або фахівців з кібербезпеки є виявлення "лазівок" у системі безпеки персональних даних та вжиття заходів для їх усунення. Виявлення загроз не означає, що крадіжка або втрата даних гарантовано відбудеться, але свідчить про ймовірність

виникнення небезпечних ситуацій, які слід запобігти.

Для кожного виду інформаційних систем персональних даних необхідно створювати особливу модель ризиків, враховуючи різні обставини та дії, що можуть впливати на їх функціонування. Полегшити виявлення небезпек можна шляхом їх поділу за такими ознаками:

1. **За різновидами джерел**:

- **Технічні засоби**: Викликані особливостями використовуваних технічних засобів.
- **Стихійні явища**: Пов’язані з природними катастрофами.
- **Дії персоналу або сторонніх осіб**: Можуть включати зловмисні дії співробітників чи зовнішніх зловмисників, які використовують міжнародні та внутрішні мережі.
- **Віруси та апаратні закладки**: Віруси та шкідливі програми, що інфікують систему. Відсутність чітких інструкцій по виявленню недекларованих опцій змушує операторів діяти на свій страх і ризик, тому найкраще використовувати ліцензовані програмні продукти з позитивними відгуками експертів.

2. **За способом реалізації**:

- **Спеціальний вплив**: Оцінка ризиків через специфічний вплив на систему.
- **Витік технічними каналами**: Витік інформації через технічні канали.
- **Несанкціонований доступ**: Незаконне проникнення до інформації.

3. **За типом інформаційних систем персональних даних (ІСПД)**:

- **Локальні ІС**: Загрози, пов'язані з локальними інформаційними системами.
- **Автоматизовані робочі місця**: Загрози для автоматизованих робочих місць.
- **Розподілені системи**: Загрози для розподілених систем.

4. **За типом несанкціонованих дій**:

- **Порушення конфіденційності**: Загрози, що призводять до порушення конфіденційності даних без прямого впливу на їх зміст.

5. **За уразливостями**:

- **Системне та прикладне програмне забезпечення**: Недоліки в

системному або прикладному ПЗ.

- **Мережеві протоколи**: Недоліки у протоколах мережевого обміну.
- **Технічні канали**: Недостатньо опрацьовані технічні канали та засоби інформаційного захисту.

6. **За об’єктом впливу**:

- **Автоматизовані робочі місця**: Загрози для робочих місць, оснащених автоматизованими системами.
- **Мережі зв'язку**: Загрози для мереж зв'язку.
- **Системне програмне забезпечення**: Загрози для системного ПЗ.
- **Прикладні утиліти**: Загрози для прикладних утиліт.
- **Виділені засоби роботи з інформацією**: Загрози для спеціалізованих засобів обробки інформації.

1.3 Джерела загроз персональних даних

Порушення інформаційної безпеки можуть виникати як в результаті умисних атак зловмисників, так і через недосвідченість персоналу. Для того, щоб уникнути можливих наслідків для компанії та особистої безпеки, користувачам необхідно мати базове розуміння понять інформаційної безпеки та загроз шкідливого програмного забезпечення. Такі інциденти, як втрата або витік інформації, можуть також бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали[11].

Основними джерелами загроз є окремі зловмисники («хакери»), кіберзлочинність групи і державні спецслужби, які застосовують весь арсенал доступних засобів, перерахованих і описаних вище. Щоб пробитися через захист і отримати доступ до потрібної інформації, вони використовують слабкі місця і помилки в роботі програмного забезпечення і веб-додатків, вади в конфігураціях мережевих екранів і налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів[11].

Визначення каналів і причин, що призводять до несанкціонованого доступу і неправомірним діям, має першочергове значення, і з цього потрібно починати при побудові моделі ЗБПД. Всього є три типи джерел, кожен з яких має свої особливості.

Антропогенні

Особистість (суб'єктів може бути кілька), яка має можливість здійснювати операції з конфіденційною інформацією. Доступ може бути як санкціонованим, так і несанкціонованим. У цю групу входять наступні джерела загроз персональних даних:

Зовнішні - постачальники послуг, працівники контролюючих державних органів та аварійних служб, а також хакери, представники конкуруючих організацій. Їх дії можуть бути навмисними, тобто спрямованими на отримання відомостей, або неспеціальних, наприклад, якщо витік відбувається в результаті технічного збою або непрофесійного складання проекту інформаційної системи.

Внутрішні - штатні співробітники, зокрема, працівники програмного відділу, кадрової служби, техперсонал або представники служби безпеки компанії. В процесі своєї діяльності вони можуть піддавати СЗПД небезпеки через некомпетентність і помилкових дій, застосування неврахованого софта, спотворення і знищення компонентів програм, надання доступу уповноваженою особам або ігнорування правил зберігання ПД. Причиною витоку може стати також самовільна зміна параметрів системи захисту і замовчування фактів втрати інформації, що знаходиться в обмеженому доступі (паролів, ключів і т.п.).

Стихійні

Найбільш складно прогнозовані через величезного розмаїття, причин виникнення та способів прояву. Переважно це ті чинники, на які оператор ніяким чином не здатний вплинути, наприклад : повені, цунамі, пожежі, урагани, зсуви, радіаційні катастрофи.

Техногенні

Ці джерела обумовлені застосовуваними технічними засобами і бувають двох різновидів:

внутрішні - це апаратні закладки, віруси та інші шкідливі програми, системи охорони та сигналізації, низькоякісний софт і обладнання, задіяне в процесі обробки персональних даних;

зовнішні - складові інфраструктурного призначення, наприклад, лінії телефонного та інтернет-зв'язку, системи опалення, каналізації, водопостачання, газопостачання.

Найбільш поширений спосіб нанести шкоди системі та викрадення даних – це комп’ютерний вірус.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Підходи аудиту, організації та забезпечення захисту персональних даних.

Аудит існуючої системи захисту персональних даних включає дослідження різних процесів обробки персональних даних, аналіз документації, пов'язаної з організаційно-розпорядчою діяльністю компанії, надання рекомендацій, вдосконалення існуючої системи та інші аспекти.

Аудит захисту персональних даних також може охоплювати супровід наявної системи у разі змін в законодавстві або при виникненні нових загроз. Додатково можуть здійснюватися технічні заходи щодо створення системи захисту персональних даних.

Аудит персональних даних проводиться шляхом експертно-документального аналізу, використовуючи технічну та організаційно-розпорядчу документацію. Обов'язково включається опис технічних рішень, функціональних схем та перевірка документів на відповідність вимогам законодавства.

Аудит захисту персональних даних є ключовим елементом забезпечення інформаційної безпеки в організаціях. Він дозволяє оцінити ефективність заходів захисту, виявити вразливості та розробити рекомендації щодо їх усунення.

Важливо розуміти необхідність заходів щодо захисту персональних даних. Якщо документація або навіть частина інформаційної системи персональних даних не відповідають вимогам законодавства, це може призвести до відповідальності за порушення вимог щодо захисту персональних даних.

Проблеми регулювання процесу збору персональних даних, підтримка інформаційної безпеки та інші питання, пов’язані з роботою з персональними даними, в Україні наразі є відносно вирішеними та відомими широкому колу юристів. Законодавство не є досконалим і потребує вдосконалення, але основні положення регулюються Законом України "Про захист персональних даних" від 1 червня 2010 р. № 2297-VI. Відповідно до ст. 12 цього Закону, збір персональних

даних є частиною процесу їх обробки, що передбачає дії з відбору або впорядкування інформації про особу[4].

Далі розглянемо основні підходи до аудиту захисту персональних даних, включаючи експертно-документальний аналіз, оцінку відповідності законодавству, технічний аудит, аналіз процедур обробки даних та проведення тестів на проникнення.

1. Експертно-документальний аналіз

Експертно-документальний аналіз є фундаментальним підходом до аудиту захисту персональних даних. Він включає:

1.1 **Аналіз технічної документації:**

- **Опис архітектури системи**: Вивчення схеми інформаційної системи, яка використовується для обробки персональних даних. Це дозволяє визначити ключові компоненти системи та їх взаємодію.
- **Документація на апаратне та програмне забезпечення**: Перевірка відповідності технічних засобів вимогам безпеки. Аналіз технічних рішень, що використовуються для захисту даних, таких як шифрування, брандмауери, антивірусне програмне забезпечення.

1.2 **Аналіз організаційно-розпорядчої документації:**

- **Політики безпеки**: Перевірка існування та ефективності політик безпеки, які регламентують обробку персональних даних в організації. Аналіз процедур управління доступом, зберігання даних та обробки інцидентів.
- **Інструкції та регламенти**: Вивчення інструкцій для співробітників щодо обробки персональних даних. Перевірка наявності та відповідності інструкцій вимогам законодавства та внутрішнім політикам безпеки.

1.3 **Аналіз процедур обробки даних:**

- **Оцінка процесів збору, обробки та зберігання даних**: Вивчення процедур збору, обробки, зберігання та передачі персональних даних. Виявлення можливих вразливостей та ризиків, пов'язаних з цими процесами.
- **Аналіз ланцюжків передачі даних**: Оцінка процесів передачі персональних даних між різними підрозділами та зовнішніми організаціями.

Перевірка дотримання вимог безпеки при передачі даних.

2. Оцінка відповідності законодавству

Оцінка відповідності існуючих процедур обробки персональних даних вимогам законодавства є важливим етапом аудиту. Вона включає:

2.1 **Аналіз відповідності національному законодавству:**

- **Закон України "Про захист персональних даних"**: Перевірка відповідності процедур обробки персональних даних вимогам цього закону. Оцінка наявності необхідних згод на обробку даних, правильності оформлення документів та відповідності процедур вимогам закону.

2.2 **Оцінка відповідності міжнародним стандартам:**

- **ISO/IEC 27001**: Перевірка відповідності системи управління інформаційною безпекою стандартам ISO/IEC 27001. Оцінка процедур управління ризиками, політик безпеки та заходів контролю.
- **GDPR**: Оцінка відповідності Загальному регламенту про захист даних (GDPR) для організацій, які працюють з даними громадян Європейського Союзу. Перевірка наявності процедур обробки персональних даних, які відповідають вимогам GDPR, таких як право на забуття, повідомлення про порушення безпеки даних та інші.

3. Технічний аудит

Технічний аудит передбачає оцінку технологічних аспектів системи захисту персональних даних:

3.1 **Аналіз інфраструктури безпеки:**

- **Мережеві пристрої**: Перевірка конфігурації мережевих пристроїв, таких як маршрутизатори, комутатори та брандмауери. Оцінка ефективності їх налаштувань для запобігання несанкціонованому доступу.
- **Системи виявлення та запобігання вторгнень**: Перевірка налаштувань систем виявлення та запобігання вторгнень (IDS/IPS). Оцінка їх здатності виявляти та реагувати на потенційні загрози.

3.2 **Аналіз налаштувань безпеки:**

- **Програмне забезпечення**: Перевірка конфігурацій програмного

забезпечення, використовуваного для обробки персональних даних. Оцінка налаштувань безпеки, таких як політики паролів, контроль доступу та інші заходи безпеки.

- **Системи управління доступом**: Перевірка налаштувань систем управління доступом. Оцінка ефективності контролю доступу до персональних даних та відповідності політикам безпеки.

3.3 **Оцінка вразливостей:**

- **Сканування вразливостей**: Використання спеціалізованих інструментів для сканування інформаційної системи на предмет вразливостей. Виявлення та класифікація вразливостей за рівнем ризику.
- **Тести на проникнення**: Проведення тестів на проникнення для імітації реальних атак. Оцінка здатності системи виявляти та запобігати вторгненням. Розробка рекомендацій щодо усунення виявлених вразливостей.

4. Аналіз процедур обробки даних

Аналіз процедур обробки даних дозволяє оцінити ефективність процесів управління персональними даними:

4.1 **Процеси збору даних:**

- **Методи збору даних**: Оцінка методів збору персональних даних. Перевірка дотримання вимог законодавства щодо отримання згоди суб'єктів даних та забезпечення прозорості процесів збору.

4.2 **Процеси обробки та зберігання даних:**

- **Методи обробки даних**: Оцінка процедур обробки персональних даних. Перевірка відповідності методів обробки вимогам безпеки та законодавства.
- **Зберігання даних**: Перевірка політик та процедур зберігання даних. Оцінка ефективності заходів захисту, таких як шифрування та резервне копіювання даних.

4.3 **Процеси передачі даних:**

- **Безпека передачі даних**: Оцінка процедур передачі персональних даних між підрозділами організації та зовнішніми контрагентами. Перевірка дотримання вимог безпеки при передачі даних, таких як використання шифрування та

захищених каналів зв'язку.

Далі детально розглянемо ключові аспекти організації захисту персональних даних. Організація захисту персональних даних (ПД) є ключовим компонентом системи інформаційної безпеки будь-якої компанії чи організації. Цей процес включає розробку та впровадження комплексних політик, процедур і технічних заходів для забезпечення конфіденційності, цілісності та доступності ПД.

1. Розробка політик та процедур

Організація повинна розробити і впровадити чіткі політики та процедури захисту персональних даних.

1.1 **Політики безпеки**

Політики безпеки встановлюють основні принципи та вимоги щодо захисту персональних даних. Вони визначають правила доступу, зберігання, обробки та передачі даних, а також встановлюють відповідальність за їх виконання.

1.2 **Процедури обробки даних**

Процедури обробки даних описують конкретні кроки, які слід виконати при зборі, обробці та зберіганні персональних даних. Вони включають в себе ідентифікацію ризиків, заходи безпеки та процедури реагування на порушення безпеки.

2. Регулярні аудити та оцінки ризиків

2.1 **Перевірки відповідності**

Регулярні перевірки відповідності дозволяють переконатися, що політики та процедури безпеки дотримуються на практиці. Вони включають в себе перевірку документації, аудит процесів та оцінку відповідності законодавству.

2.2 **Оцінка ризиків**

Оцінка ризиків дозволяє ідентифікувати потенційні загрози для безпеки персональних даних і розробити стратегії їх управління. Вона включає в себе аналіз потенційних загроз, визначення вразливостей та розробку заходів з мінімізації ризиків.

3. Навчання та підвищення обізнаності співробітників

3.1 **Тренінги з безпеки**

Тренінги з безпеки є важливою складовою організаційної культури безпеки. Вони надають співробітникам необхідні знання та навички для ефективного захисту персональних даних.

3.2 **Симуляції атак**

Симуляції атак допомагають підготувати персонал до реальних ситуацій загроз. Вони включають в себе проведення тренувальних сеансів, під час яких співробітники вправляються в розпізнаванні та відверненні загроз безпеці.

Ефективний захист персональних даних вимагає комплексного підходу, що включає аудити безпеки, розробку та впровадження політик, навчання співробітників та використання сучасних технічних засобів захисту. Постійний моніторинг, аналіз ризиків та вдосконалення заходів безпеки дозволяють знизити ймовірність витоків даних та забезпечити відповідність вимогам законодавства.

2.2 Засоби забезпечення захисту персональних даних

Компанії повинні впроваджувати технічні та організаційні заходи безпеки, щоб забезпечити конфіденційність і цілісність персональних даних і захистити їх від зміни, втрати, розголошення та несанкціонованого доступу.

Усі заходи захисту даних повинні забезпечувати максимально можливий захист персональних даних.Заходи безпеки повинні бути частиною системи захисту даних.

Далі ми виділимо деякі з них і пояснимо їх більш детально.

Фізична безпека

Загальні положення

Фізична безпека об’єкта означає стан захищеності життєво важливих інтересів (об’єкта) від загроз, які походять від злочинних або несанкціонованих дій фізичних осіб (порушників). Це включає захист об’єктів та обладнання для запобігання випадковим інцидентам або форс-мажорним обставинам.

Концепція безпеки

Концепція безпеки – це загальний план забезпечення безпеки об’єкта від

передбачуваних загроз.

Уразливість

Уразливість об’єкта – це ступінь невідповідності вжитих заходів захисту об’єкта прогнозованим загрозам або встановленим вимогам безпеки.

Надзвичайна ситуація

Надзвичайна ситуація на об’єкті – це стан, при якому порушуються нормальні умови життя та діяльності людей, виникає загроза їхньому життю та здоров’ю, а також завдається шкода майну та навколишньому середовищу.

Ефективність системи фізичної безпеки

Ефективність системи фізичної безпеки – це ймовірність виконання системою своєї основної функції із забезпечення захисту об’єкта від загроз, джерелами яких є злочинні або несанкціоновані дії фізичних осіб (порушників).

Система фізичного захисту

Система фізичного захисту (СФЗ) – це сукупність правових норм, організаційних заходів та інженерно-технічних рішень, спрямованих на захист життєво важливих інтересів і ресурсів підприємства (об’єкта) від загроз, джерелами яких є злочинні або несанкціоновані дії фізичних осіб – порушників (терористів, злочинців, екстремістів тощо).

Основні складові частини сучасних СФЗ

Сучасні СФЗ будуються на базі широкого застосування інженерно-технічних та програмних засобів і включають такі основні підсистеми:

- **Система контролю і управління доступом персоналу (СКУД):** Забезпечує контроль за входом та виходом осіб на об'єкт.
- **Система охоронної сигналізації (СОС):** Виявляє несанкціоновані проникнення та інші загрози.
- **Система телевізійного спостереження (СТН):** Забезпечує відеомоніторинг території та приміщень об'єкта.
- **Система оперативного зв’язку та оповіщення:** Забезпечує швидке інформування про загрози та координацію дій у разі інцидентів.
- **Забезпечувальні системи (освітлення, електроживлення, охоронне**

освітлення тощо): Підтримують роботу інших підсистем СФЗ.

Завдання СФЗ

Сучасні СФЗ також повинні захищати життєво важливі центри та системи об'єкта від ненавмисних, помилкових або некомпетентних дій персоналу, які можуть завдати шкоди, подібної до тієї, що викликається несанкціонованими діями зовнішніх порушників.

Проектування СФЗ

Через складність завдань, створення СФЗ для важливих об'єктів не може базуватися лише на принципі "розумної достатності", а вимагає комплексного наукового підходу. Це означає проектування СФЗ у дві стадії:

- **Концептуальне (системне) проектування:** Включає аналіз вразливості об'єкта, розробку принципів фізичного захисту та техніко-економічного обґрунтування створення СФЗ.
- **Робоче проектування:** Конкретизує технічні рішення та плани впровадження.

Основні етапи концептуального проектування:

1. Аналіз вразливості об'єкта та існуючої СФЗ.
2. Розробка принципів фізичного захисту об'єкта.
3. Розробка техніко-економічного обґрунтування створення СФЗ.

Логічна безпека

Загальні положення

Логічна безпека включає заходи щодо ідентифікації та автентифікації осіб або користувачів, які мають право доступу та зміни персональних даних. Цей аспект безпеки стосується використання програмних методів для підтвердження прав користувача в певній комп'ютерній мережі або системі. Логічна безпека є складовою частиною загальної комп'ютерної безпеки, яка охоплює як апаратні, так і програмні методи захисту терміналу або мережі.

Методи логічної безпеки

Імена користувачів і паролі

Аутентифікація за паролем є найбільш поширеним і знайомим типом

логічного захисту. Користувачі, які хоч раз користувалися сайтом онлайн-банкінгу або соціальних мереж, знайомі з цією концепцією. При налаштуванні аутентифікації за паролем користувачі, які намагаються увійти до мережі або на певний термінал, повинні підтвердити свої облікові дані, ввівши ім'я користувача та пароль. Основна перевага цього методу – простота: користувачам потрібно лише запам’ятати ім'я користувача та пароль для доступу до системи. Однак, недоліком є те, що комп'ютер не може перевірити, чи є користувач, який використовує конкретну комбінацію імені користувача та пароля, дійсно авторизованим. Це створює можливість для зловмисників вкрасти імена користувачів і паролі для зламу системи.

Безпека токенів

Безпека токенів використовує картки-ключі або інші фізичні пристрої для аутентифікації користувача в мережі. Після проведення картки через систему користувачу надається доступ до комп'ютера. Деякі типи токен-пристроїв містять постійно змінюваний код, який оновлюється кожну хвилину або близько того, що забезпечує додатковий захист від спроб дублювання захисних карт. Як і у випадку з паролями, існує ризик викрадення картки доступу, що може надати несанкціонований доступ до системи.

Двостороння аутентифікація

Двостороння аутентифікація передбачає обмін питаннями і відповідями між користувачем і комп'ютерною системою. Коли користувач намагається увійти в систему, комп'ютер надсилає питання, відоме як «виклик», на яке користувач повинен правильно відповісти, щоб отримати доступ. Перевага цього методу полягає в тому, що система не залежить від конкретної комбінації імені користувача та пароля. Це ускладнює доступ для несанкціонованих користувачів, оскільки недостатньо вкрасти одну конкретну комбінацію імені користувача та пароля.

Шифрування

Загальні положення

Шифрування включає впровадження та використання алгоритмів, ключів,

паролів і спеціальних заходів захисту для забезпечення цілісності та конфіденційності персональних даних у системі захисту. Це процес, за допомогою якого інформація перетворюється у форму, що недоступна для читання сторонніми особами.

Процес шифрування

Шифрування даних – давно відомий і досить зрозумілий процес. Відправник і одержувач використовують спеціальні ключі для шифрування та дешифрування. Якщо зловмисник перехопить дані під час їх передачі, він не зможе їх прочитати без відповідних ключів. Таким чином, перехоплення зашифрованої інформації стає безглуздим. Проте, хоча ідея шифрування є простою, її реалізація вимагає значних зусиль. Шифрування має два аспекти: надмірно складне шифрування може утруднити доступ для авторизованих користувачів, тоді як занадто прості ключі роблять систему вразливою. Оптимальна система шифрування має балансувати між безпекою і зручністю використання.

Типи шифрування

Симетричне шифрування

Симетричне шифрування є найбільш поширеним типом. Воно передбачає використання одного і того ж ключа для шифрування і дешифрування повідомлення як відправником, так і одержувачем. Основна перевага симетричного шифрування – швидкість, але ключ має бути надійно переданий одержувачу.

Асиметричне шифрування

Асиметричне шифрування, також відоме як криптографія з відкритим ключем, використовує пару ключів – один для шифрування (публічний ключ) і інший для дешифрування (приватний ключ). Це забезпечує високий рівень безпеки, оскільки навіть якщо публічний ключ стає відомим, без приватного ключа розшифрування неможливе.

Приклади застосування

Віртуальні приватні мережі (VPN) використовують шифрування для забезпечення безпеки інтернет-з'єднань. VPN виявляють слабкі місця в системі безпеки та маскують IP-адреси користувачів. Преміум-провайдери VPN надають

комплексний захист, гарантуючи, що з'єднання не може бути зламано. Висококласні професіонали, які займаються шифруванням даних, забезпечують настільки надійну безпеку, що зловмисники зазвичай відмовляються від своїх намірів, розуміючи складність атаки.

Важливість балансу в шифруванні

Занадто складне шифрування може уповільнити передачу даних і створити труднощі для легітимних користувачів, тоді як просте шифрування може бути легко зламано. Тому важливо забезпечити баланс між швидкістю доступу до даних та їх захищеністю. Вибір оптимальних алгоритмів та ключів є критично важливим завданням для забезпечення ефективного шифрування.

Мережевий зв'язок

Загальні положення

Мережевий зв'язок є ключовим елементом в архітектурі захисту даних. В рамках мережевої моделі даних, що є розширенням ієрархічного підходу, описуються структурні аспекти, аспекти цілісності та обробки даних у мережевих базах даних. Мережевий зв'язок у контексті захисту даних передбачає використання корпоративних служб захисту, що включає системи моніторингу, які постійно контролюють мережеву активність і блокують будь-які підозрілі дії або порушення безпеки.

Системи моніторингу мережі

Системи моніторингу мережі є невід'ємною частиною забезпечення безпеки. Вони виконують такі функції:

1. **Постійний контроль трафіку**: Моніторинг усіх вхідних і вихідних з'єднань для виявлення підозрілої активності.

2. **Виявлення аномалій**: Аналіз мережевого трафіку для виявлення незвичайних патернів, які можуть свідчити про спроби зловмисного втручання.

3. **Автоматичне блокування**: Реалізація механізмів автоматичного блокування підозрілих з'єднань для негайного реагування на загрози.

Корпоративні служби захисту даних

Корпоративні служби захисту даних використовують різноманітні технології

та підходи для забезпечення безпеки мережевих з'єднань:

1. **Брандмауери (Firewall)**: Брандмауери встановлюють межу між внутрішньою мережею організації та зовнішніми мережами, фільтруючи небезпечний трафік і захищаючи внутрішні ресурси.

2. **VPN (Віртуальні приватні мережі)**: VPN забезпечують захищене з'єднання через інтернет, шифруючи дані під час їх передачі. Це захищає дані від перехоплення зловмисниками.

3. **IDS/IPS (Системи виявлення та запобігання вторгнень)**: IDS/IPS системи аналізують мережевий трафік для виявлення і запобігання спробам вторгнення.

Ці аспекти є лише мінімальними стандартами для навчальної програми з захисту даних. Отже, організації повинні вживати додаткові заходи для досягнення вищого рівня захисту. Для цього рекомендується залучення консультантів з кібербезпеки для впровадження системи захисту персональних даних.

2.3 Порівняльний аналіз засобів захисту персональних даних

Існує багато рішень для забезпечення безпеки даних, кожне з яких має свої унікальні можливості та особливості. У цьому розділі ми детально розглянемо та порівняємо кілька провідних засобів захисту персональних даних, таких як Microsoft Purview, Symantec Data Loss Prevention (DLP), McAfee Total Protection for Data Loss Prevention та IBM Guardium

Microsoft Purview

Microsoft Purview – це комплексне рішення для управління та захисту даних, яке інтегрується в екосистему Microsoft. Основні можливості Microsoft Purview включають:

- Виявлення та класифікація даних: Використовує інтелектуальні алгоритми для автоматичного виявлення та класифікації персональних даних у різних середовищах, таких як локальні системи, хмарні сервіси та гібридні

інфраструктури. Підтримуються численні типи даних, включаючи структуровані та неструктуровані дані.

- Захист даних: Забезпечує шифрування даних у стані зберігання та під час передачі, використовуючи сучасні криптографічні методи. Інструменти для управління ключами дозволяють забезпечити високий рівень безпеки.
- Управління доступом: Надає можливість створювати та управляти ролями, політиками доступу та правами доступу до даних. Інтеграція з Azure Active Directory дозволяє централізовано управляти доступом користувачів.
- Моніторинг та аудит: Реалізує детальні засоби для моніторингу дій з даними та проведення аудитів. Логи та звіти допомагають забезпечити відповідність нормативним вимогам, таким як GDPR, HIPAA та інші.
- Інтеграція з іншими продуктами Microsoft: Тісна інтеграція з іншими рішеннями Microsoft, такими як Office 365, Dynamics 365, Azure та іншими, що забезпечує зручність використання та покращує загальну ефективність управління даними.

Symantec Data Loss Prevention (DLP)

Symantec Data Loss Prevention (DLP) – це рішення, спрямоване на запобігання втраті даних через несанкціоновану передачу або доступ. Основні функції включають:

- Ідентифікація та моніторинг: Використовує інтелектуальні алгоритми для виявлення конфіденційних даних у різних середовищах, включаючи електронну пошту, мережевий трафік, файлові системи та кінцеві точки. Підтримується широке розмаїття форматів даних.
- Запобігання втраті даних: Надає політики, які дозволяють запобігати несанкціонованій передачі конфіденційних даних за межі організації. Це включає блокування передачі через електронну пошту, веб-додатки, USB-накопичувачі та інші засоби.
- Шифрування та захист даних: Інтеграція з рішеннями для шифрування даних, забезпечуючи захист як у стані зберігання, так і під час передачі.

- Інцидент-менеджмент: Надає інструменти для управління інцидентами, пов'язаними з безпекою даних. Це включає автоматичні сповіщення, звіти та аналітику інцидентів.
- Аудит та звітність: Засоби для створення детальних звітів і логів про дії з даними, що дозволяє забезпечити відповідність нормативним вимогам.

McAfee Total Protection for Data Loss Prevention

McAfee Total Protection for Data Loss Prevention – це комплексне рішення для запобігання втраті даних, яке включає кілька важливих функцій:

- Моніторинг та аналіз: Використовує інтелектуальні алгоритми для моніторингу трафіку та виявлення загроз. Підтримується моніторинг різних типів даних і середовищ, включаючи кінцеві точки, мережі та хмарні сервіси.
- Захист кінцевих точок: Інтеграція з антивірусними та антивірусними рішеннями McAfee дозволяє забезпечити високий рівень захисту кінцевих точок від загроз.
- Управління політиками: Гнучкі інструменти для створення та управління політиками захисту даних. Можливість налаштування політик для різних груп користувачів та типів даних.
- Виявлення та класифікація: Автоматизовані засоби для виявлення та класифікації конфіденційних даних у різних середовищах, таких як електронна пошта, файлові системи та хмарні сервіси.
- Інцидент-менеджмент та звітність: Засоби для управління інцидентами та створення детальних звітів про дії з даними, що дозволяє забезпечити відповідність нормативним вимогам.

IBM Guardium

IBM Guardium – це комплексне рішення для захисту баз даних та великих обсягів даних, яке включає такі можливості:

- Моніторинг в режимі реального часу: Забезпечує безперервний моніторинг доступу до даних та дій з ними. Використовує аналітику для виявлення аномалій та потенційних загроз.

- Виявлення та запобігання загрозам: Використовує передові методи аналізу для виявлення загроз та запобігання їм. Можливість налаштування політик для автоматичного реагування на інциденти.
- Шифрування даних: Надає засоби для шифрування даних на всіх етапах: у стані зберігання, під час передачі та в процесі обробки. Підтримується інтеграція з іншими рішеннями для управління ключами.
- Відповідність нормативним вимогам: Надає інструменти для проведення аудитів та забезпечення відповідності різним регуляторним стандартам, таким як GDPR, HIPAA, PCI DSS та інші.
- Інтеграція з іншими рішеннями: Підтримується інтеграція з різноманітними рішеннями для управління безпекою та даними, що дозволяє покращити загальну ефективність захисту даних.

Таблиця 1

Порівняння засобів захисту персональних даних

Функціональність	**Microsoft Purview**	**Symantec DLP**	**McAfee Total Protection DLP**	**IBM Guardium**
Виявлення та класифікація даних	**Так**	**Так**	**Так**	**Так**
Шифрування даних	**Так**	**Так**	**Так**	**Так**
Управління доступом	**Так**	**Обмежене**	**Так**	**Так**
Моніторинг та аудит	**Так**	**Так**	**Так**	**Так**
Інцидент-менеджмент	**Так**	**Так**	**Так**	**Так**
Підтримка хмарних середовищ	**Так**	**Частково**	**Частково**	**Так**
Інтеграція з іншими рішеннями	**Висока**	**Висока**	**Висока**	**Висока**
Легкість впровадження та використання	**Висока**	**Середня**	**Середня**	**Низька**
Ціна	**$30-50 за користувача на місяць**	**$50-100 за користувача на місяць**	**$40-80 за користувача на місяць**	**$200-500 за інстанцію на місяць**
Наявність пробного періоду	**Так, 30 днів**	**Так, 30 днів**	**Так, 30 днів**	**Так, 30 днів**

Після ретельного аналізу та порівняння різних засобів захисту персональних даних, можна зробити декілька ключових висновків:

Microsoft Purview: Це потужне рішення з великою кількістю функцій та високим рівнем інтеграції з екосистемою Microsoft. Purview відмінно підходить для організацій, які використовують інші продукти Microsoft і шукають рішення для управління та захисту даних, яке легко інтегрується з їх існуючими системами.

Symantec Data Loss Prevention (DLP): Це рішення зосереджене на виявленні та запобіганні втраті даних через несанкціонований доступ або передачу. Завдяки широкому спектру функцій та спеціалізації на безпеці даних, Symantec DLP може бути відмінним вибором для організацій, які покладають основний акцент на захист конфіденційної інформації.

McAfee Total Protection for Data Loss Prevention: Це рішення від McAfee пропонує широкий спектр функцій для моніторингу та захисту даних на різних рівнях. Забезпечуючи інтеграцію з антивірусними рішеннями McAfee та іншими засобами безпеки, воно може бути ефективним вибором для комплексного захисту даних у різних середовищах.

IBM Guardium: Це рішення спеціалізується на захисті баз даних та великих обсягів даних. Його основна сильна сторона - це здатність до моніторингу в режимі реального часу та виявлення аномалій. Для організацій з великим обсягом чутливої інформації, яка зберігається в базах даних, IBM Guardium може бути важливим інструментом у забезпеченні безпеки даних.

При виборі між цими рішеннями, важливо врахувати специфічні потреби та характеристики організації, а також рівень інтеграції з існуючими системами та вартість впровадження. Щоб забезпечити найбільш ефективний захист даних, рекомендується провести докладне тестування та оцінку кожного рішення перед прийняттям остаточного рішення.

На мою думку, Microsoft Purview виділяється своєю інтегрованою екосистемою та можливістю ефективно керувати захистом даних у різних середовищах, включаючи хмарні сервіси.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА

3.1 Аналіз функціональних можливостей Microsoft Purview

У цьому розділі ми більш детально розберемо рішення Microsoft Purview.

Microsoft Purview – це комплексне рішення для управління та захисту даних, яке входить до екосистеми Microsoft. Воно поєднує в собі функції виявлення, класифікації, захисту та управління доступом до даних, забезпечуючи їхню безпеку в різних середовищах, включаючи локальні системи, хмарні сервіси та гібридні інфраструктури. Далі розглянемо детально основні функціональні можливості Microsoft Purview.

Виявлення та класифікація даних

- Інтелектуальні алгоритми: Microsoft Purview використовує сучасні технології машинного навчання та штучного інтелекту для автоматичного виявлення персональних даних у різних середовищах. Ці алгоритми можуть розпізнавати чутливі дані, такі як фінансова інформація, медичні записи та особисті дані, навіть якщо вони зберігаються в неструктурованих форматах, наприклад у текстових документах або електронних листах.

- Підтримка різних типів даних: Microsoft Purview здатний працювати з різноманітними типами даних, включаючи структуровані дані (таблиці баз даних) та неструктуровані дані (документи, електронні листи, файли). Це дозволяє організаціям контролювати широкий спектр інформації, що забезпечує більш комплексний захист даних.

- Класифікаційні теги: Після виявлення даних Purview автоматично призначає їм класифікаційні теги на основі вбудованих або настроюваних політик. Це дозволяє швидко ідентифікувати та управляти чутливою інформацією. Організації можуть створювати власні політики класифікації, щоб відповідати своїм конкретним потребам і нормативним вимогам.

Захист даних

- Шифрування: Microsoft Purview забезпечує шифрування даних як у стані зберігання, так і під час передачі. Використовуючи сучасні криптографічні методи, Purview гарантує, що дані захищені від несанкціонованого доступу. Це включає використання AES-256 для шифрування на рівні зберігання та TLS для шифрування під час передачі даних через мережу.

- Управління ключами: Інтеграція з Azure Key Vault дозволяє централізовано керувати ключами шифрування. Це забезпечує додатковий рівень безпеки, оскільки ключі шифрування зберігаються окремо від зашифрованих даних, і доступ до них контролюється за допомогою суворих політик доступу.

Управління доступом

- Ролі та політики доступу: Microsoft Purview дозволяє створювати детальні ролі та політики доступу до даних. Це означає, що можна налаштувати доступ до даних на основі ролей користувачів, функцій або відділів. Наприклад, фінансовий відділ може мати доступ до фінансових записів, але не до медичних даних.

- Azure Active Directory (AAD): Інтеграція з AAD забезпечує централізоване управління доступом користувачів до різних ресурсів. AAD надає можливості для багатофакторної автентифікації, управління ідентифікацією та доступом, а також політики умовного доступу, що додатково підвищує рівень безпеки.

Моніторинг та аудит

- Журналювання дій: Microsoft Purview забезпечує детальне журналювання всіх дій з даними, включаючи доступ, модифікації та передачу даних. Це дозволяє відслідковувати, хто і коли отримував доступ до конфіденційної інформації, що є критично важливим для виявлення потенційних порушень безпеки.

- Звіти та аналітика: Інструменти для створення звітів та аналітики дозволяють отримати детальну інформацію про стан безпеки даних. Організації можуть створювати настроювані звіти, які допомагають відслідковувати відповідність нормативним вимогам, таким як GDPR, HIPAA та інші. Ці звіти можуть бути автоматично генеровані та надані відповідальним особам для подальшого аналізу та прийняття рішень.

Інтеграція з іншими продуктами Microsoft

- Office 365 та Dynamics 365: Тісна інтеграція з популярними корпоративними додатками, такими як Office 365 та Dynamics 365, дозволяє ефективно захищати дані, що використовуються в цих середовищах. Наприклад, політики класифікації та захисту даних можуть автоматично застосовуватись до документів, створених у Word або Excel.

- Azure: Інтеграція з Azure забезпечує безшовний захист даних у хмарних середовищах. Це включає захист даних, збережених у Azure Storage, базах даних Azure SQL, а також інших службах Azure. Інтеграція з Azure Sentinel дозволяє отримувати розширені можливості для виявлення загроз та реагування на інциденти.

Додаткові можливості

- Data Map та Data Catalog: Microsoft Purview включає інструменти для створення карти даних (Data Map) та каталогу даних (Data Catalog). Це дозволяє організаціям отримати повне уявлення про свої дані, їхнє розташування та взаємозв'язки між різними наборами даних. Data Catalog допомагає користувачам легко знаходити необхідні дані та розуміти їхнє значення та контекст.

- Data Insights: Інструменти для аналізу даних (Data Insights) допомагають організаціям краще розуміти свої дані та приймати обґрунтовані рішення щодо їхнього захисту. Наприклад, можна отримати інформацію про те, які типи даних найчастіше піддаються ризику, та розробити відповідні заходи для їхнього захисту.

Переваги Microsoft Purview

- Комплексність: Поєднання всіх необхідних інструментів для виявлення, класифікації, захисту, управління доступом, моніторингу та аудиту даних в одному рішенні. Це дозволяє організаціям централізовано управляти всіма аспектами безпеки даних.

- Інтеграція: Тісна інтеграція з екосистемою Microsoft забезпечує зручність використання та управління даними. Організації, що вже використовують продукти Microsoft, можуть легко інтегрувати Purview у свою інфраструктуру.

- Гнучкість: Можливість налаштування політик та ролей відповідно до специфічних потреб організації. Це дозволяє адаптувати рішення до конкретних вимог бізнесу та нормативних стандартів.

- Відповідність нормативам: Інструменти для забезпечення відповідності різним регуляторним стандартам та проведення аудитів. Це допомагає організаціям уникнути штрафів та інших санкцій за порушення нормативних вимог.

Недоліки Microsoft Purview

- Вартість: Висока вартість рішення може бути значною для невеликих організацій або тих, хто не використовує інші продукти Microsoft. Організації повинні враховувати не тільки вартість ліцензій, але й витрати на впровадження та навчання персоналу.

- Складність впровадження: Хоча інтеграція з іншими продуктами Microsoft спрощує використання, початкове впровадження та налаштування можуть вимагати значних ресурсів та часу. Організаціям може знадобитися залучення зовнішніх консультантів або спеціалістів для успішного впровадження та налаштування Purview.

Отже, на мою думку, Microsoft Purview є потужним та комплексним рішенням для захисту персональних даних, що надає широкий спектр функціональних можливостей. Завдяки інтеграції з іншими продуктами Microsoft, воно забезпечує ефективне управління безпекою даних у різних середовищах. Вибір цього рішення залежить від специфічних потреб організації, її інфраструктури та бюджету. Для максимального ефекту рекомендується провести детальну оцінку потреб організації та протестувати Purview перед впровадженням.

3.2 Розгортання та налаштування Microsoft Purview

У цьому розділі ми детально розглянемо рішення Microsoft Purview, розгорнемо, налаштуємо, та випробуємо.

Розгортання Microsoft Purview

Створення та налаштування робочого простору

1. **Увійдіть до порталу Azure**:

- Перейдіть до порталу Azure і увійдіть у свій обліковий запис.

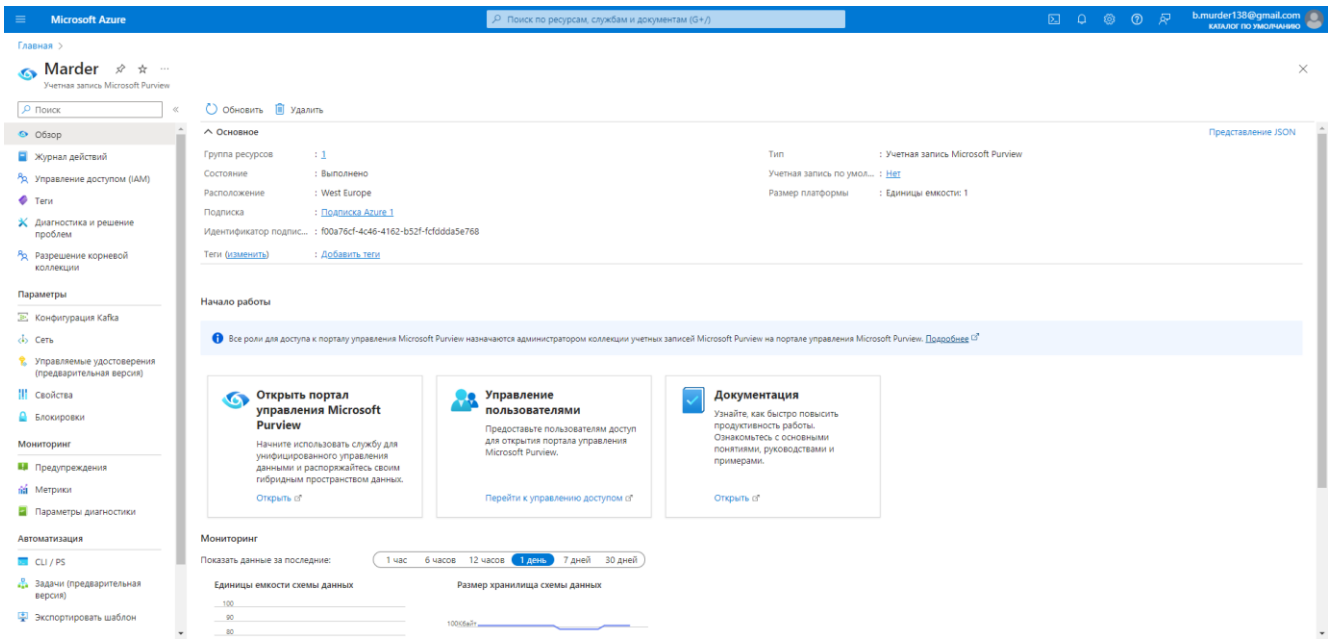

Рис. 3.1.Портал Azure

2. **Створення ресурсної групи**:

- Відкрийте меню зліва і виберіть "Resource groups".

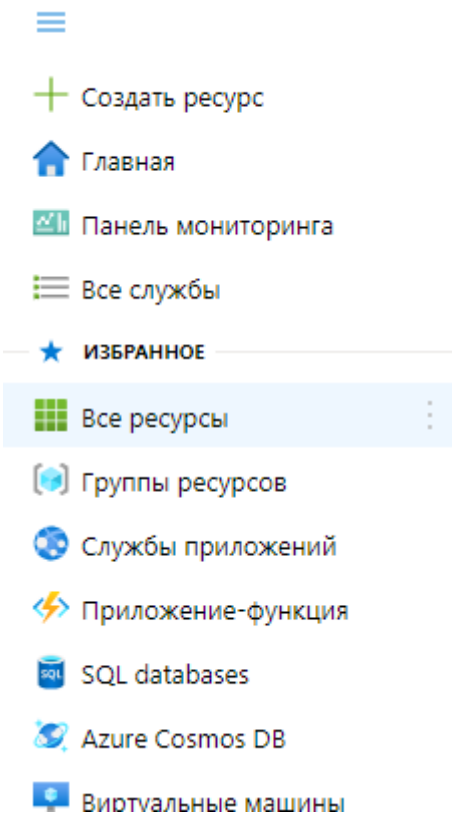

Рис. 2 – меню та служба "Resource groups"

- Натисніть "Create" і заповніть необхідну інформацію (назва ресурсної групи, регіон).

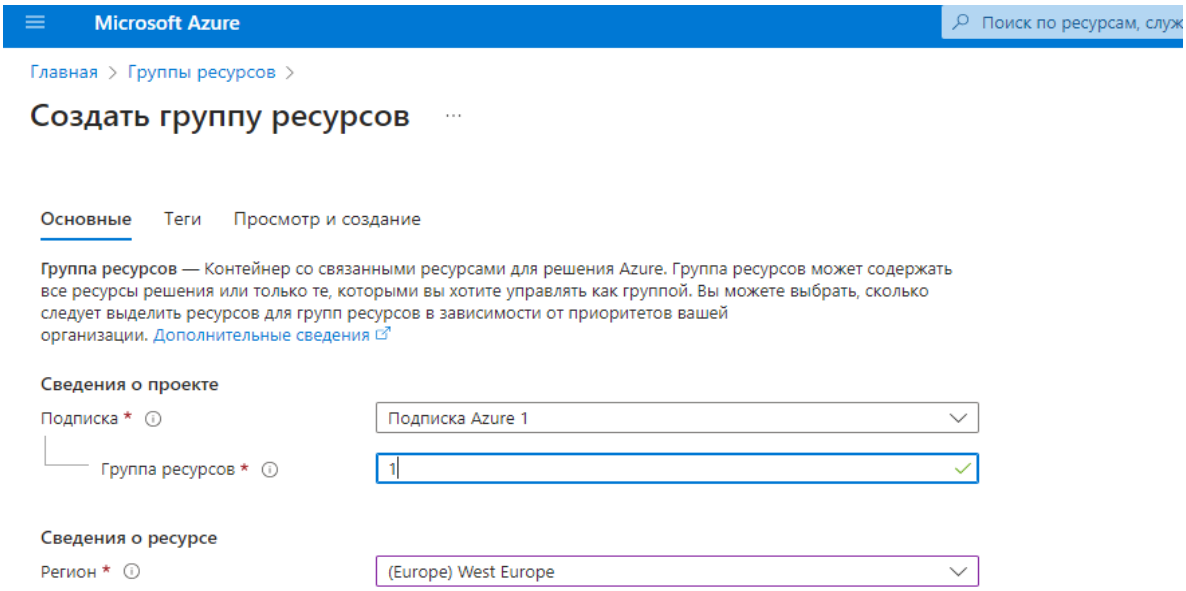

Рис. 3 – Заповнення необхідної інформації

- Натисніть "Review + create", а потім "Create".

3. **Створення облікового запису Microsoft Purview**:

- У полі пошуку зверху головної сторінки введіть "Microsoft Purview" і виберіть "Microsoft Purview Account".

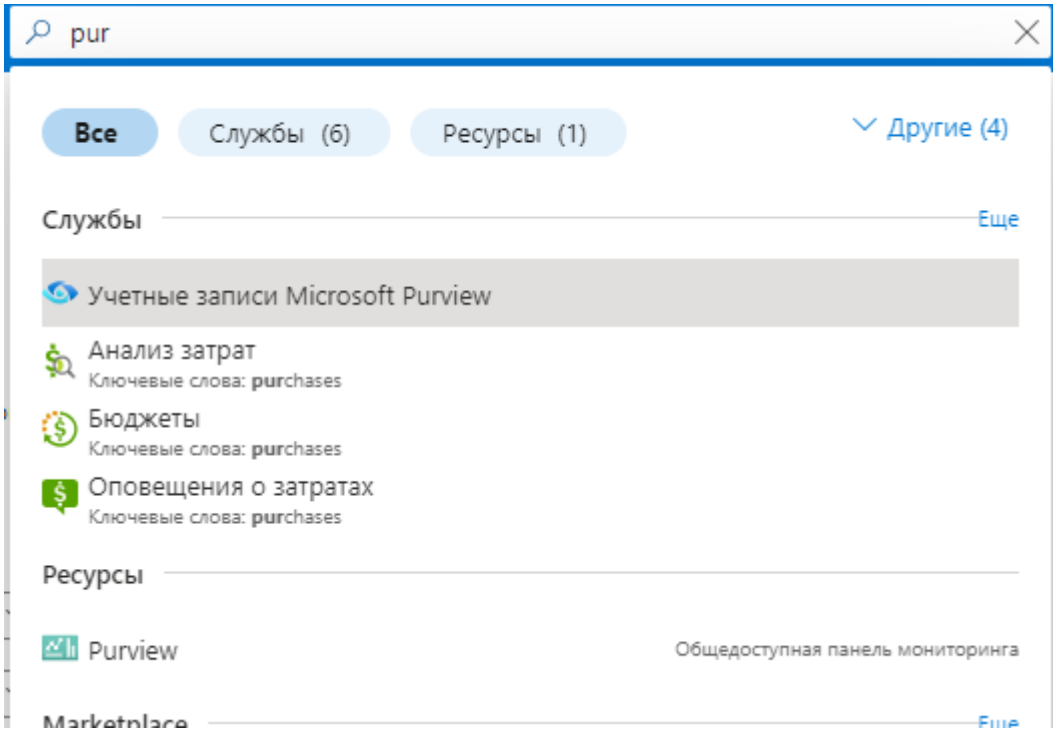

Рис. 4 – Microsoft Purview Account

- Заповніть необхідну інформацію: виберіть ресурсну групу, введіть назву облікового запису, виберіть регіон.

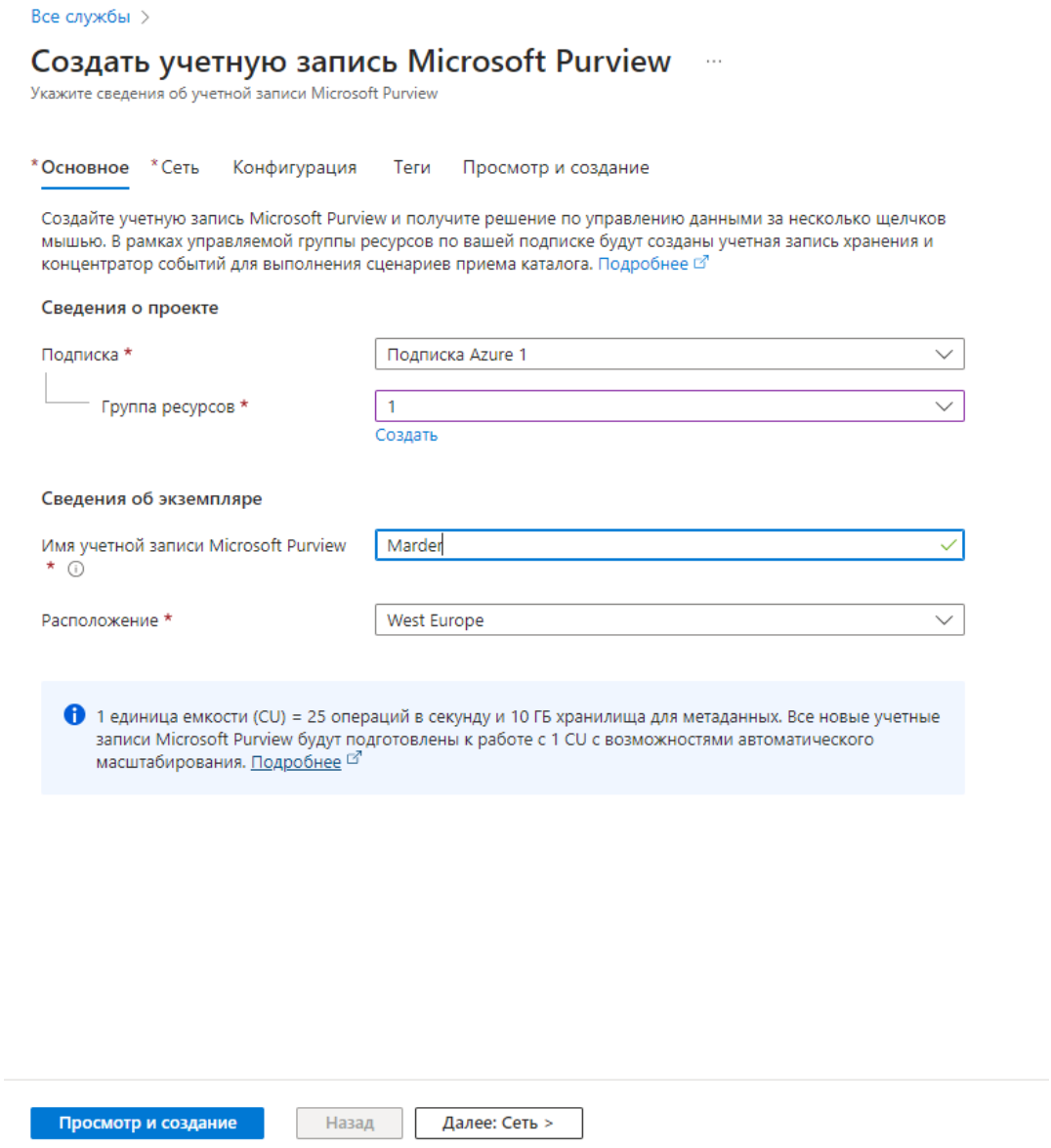

Рис. 5 – Заповнення необхідної інформації

- Натисніть "Review + create", а потім "Create".

4. **Налаштування облікового запису Microsoft Purview**:

- Перейдіть до облікового запису Microsoft Purview, який ви щойно створили.

- Натисніть на вкладку "Data Map" і додайте джерела даних, з яких ви плануєте збирати інформацію.

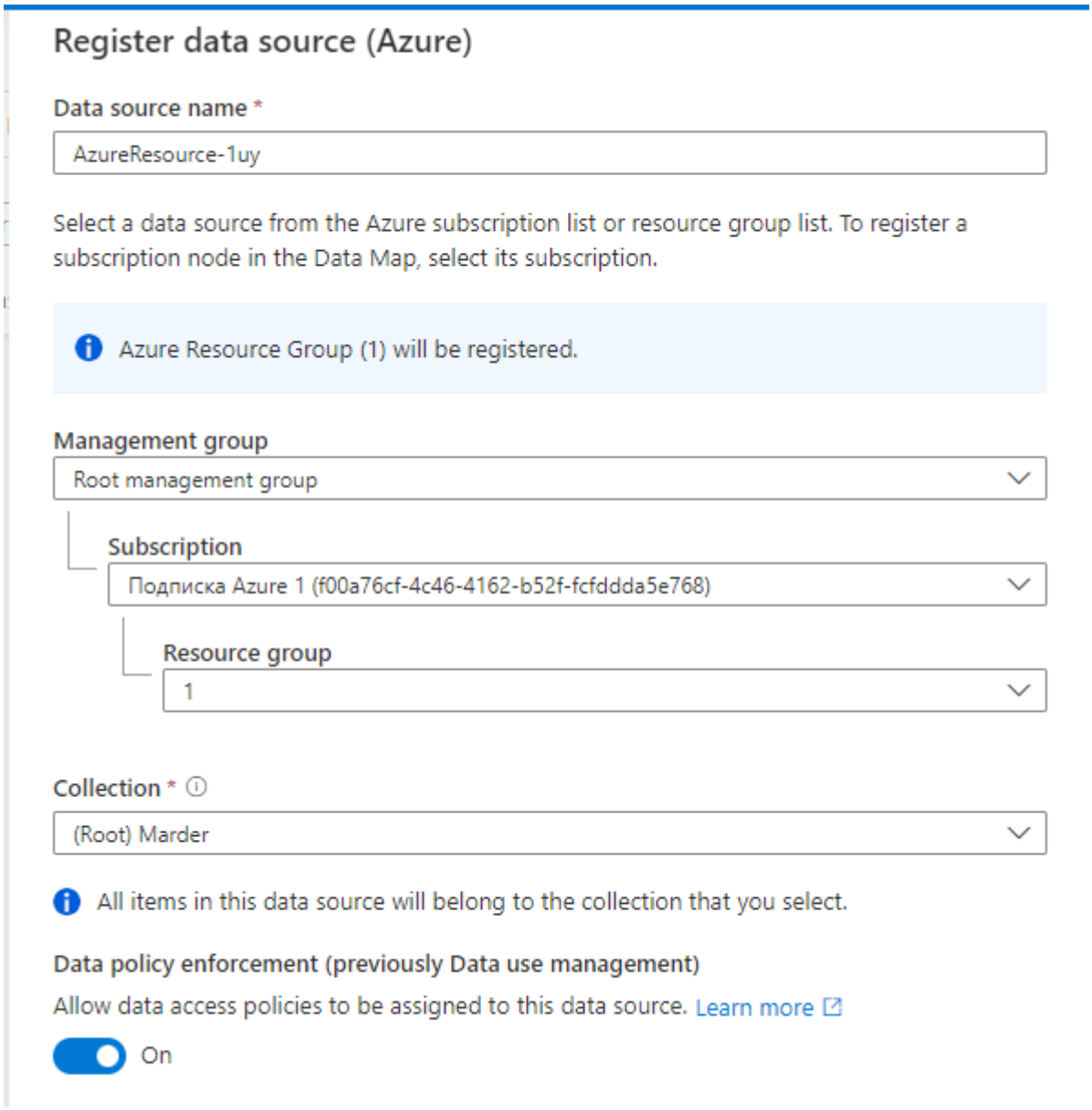

Рис. 6 – додання джерела даних

5. **Запуск робочого сканування**

1. **Вибір джерела даних**:

   - Відкрийте Microsoft Purview у вашому обліковому записі Azure.
   - Перейдіть до розділу "Data Map" і виберіть раніше зареєстроване джерело даних.

2. **Налаштування сканера**:

   - У розділі "Sources" виберіть джерело даних, яке ви хочете сканувати.
   - Натисніть "New scan" для створення нового завдання сканування.

3. **Конфігурація параметрів сканування**:

- **Назва сканування**: Введіть унікальну назву для цього завдання сканування.

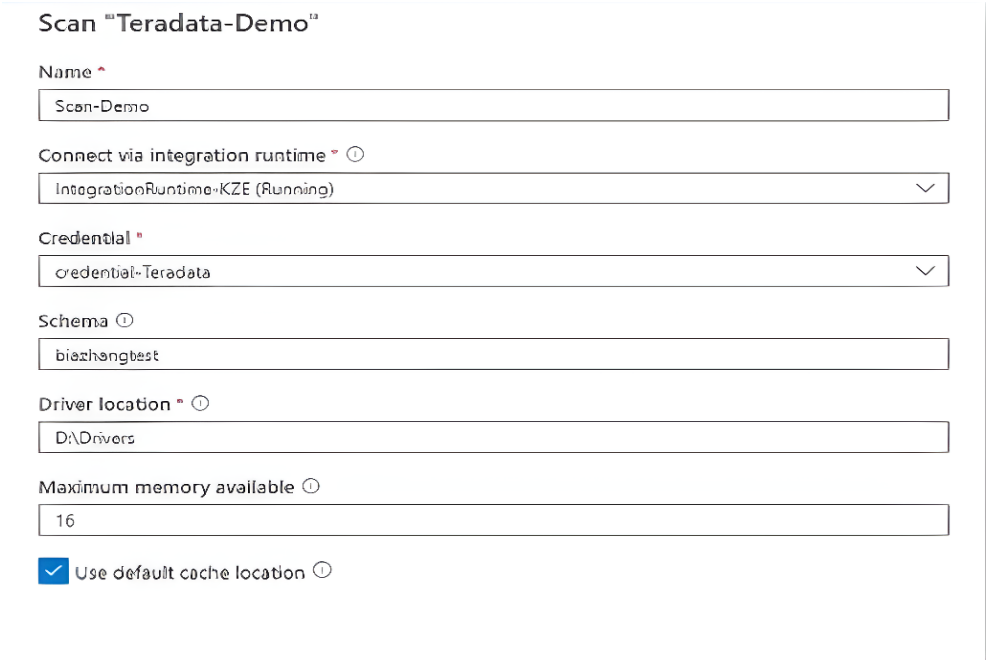

Рис. 7 – Конфігурація параметрів сканування 1

- **Інтервал сканування**: Виберіть один із доступних варіантів (наприклад, одноразове сканування або регулярні сканування з певним інтервалом)

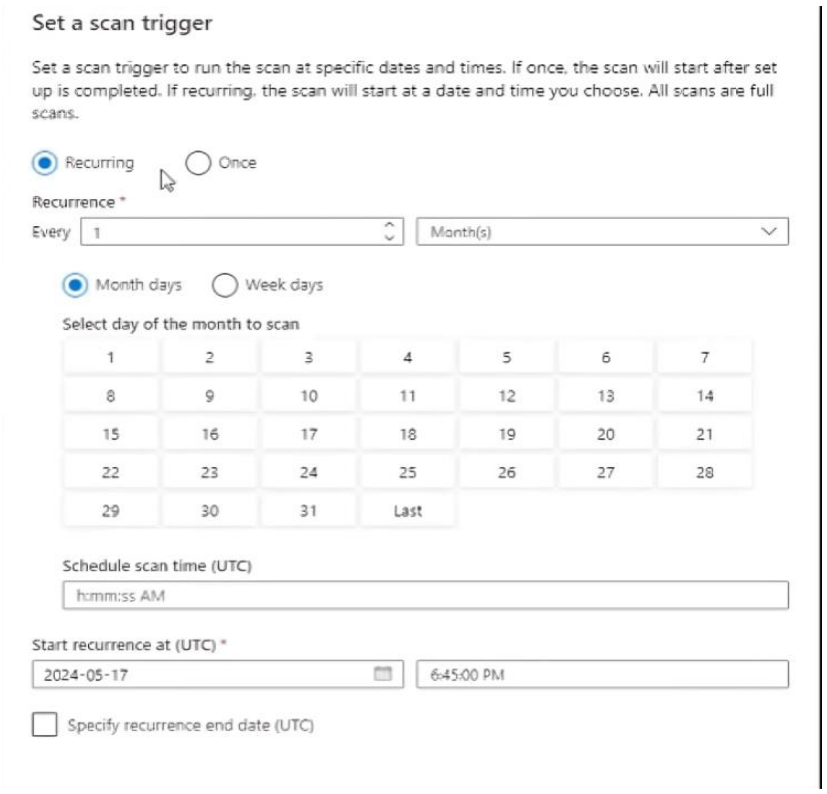

Рис. 8 – Конфігурація інтервалу сканування

4. **Запуск сканування**:

    - Після налаштування параметрів натисніть "Save and run" для запуску процесу сканування.

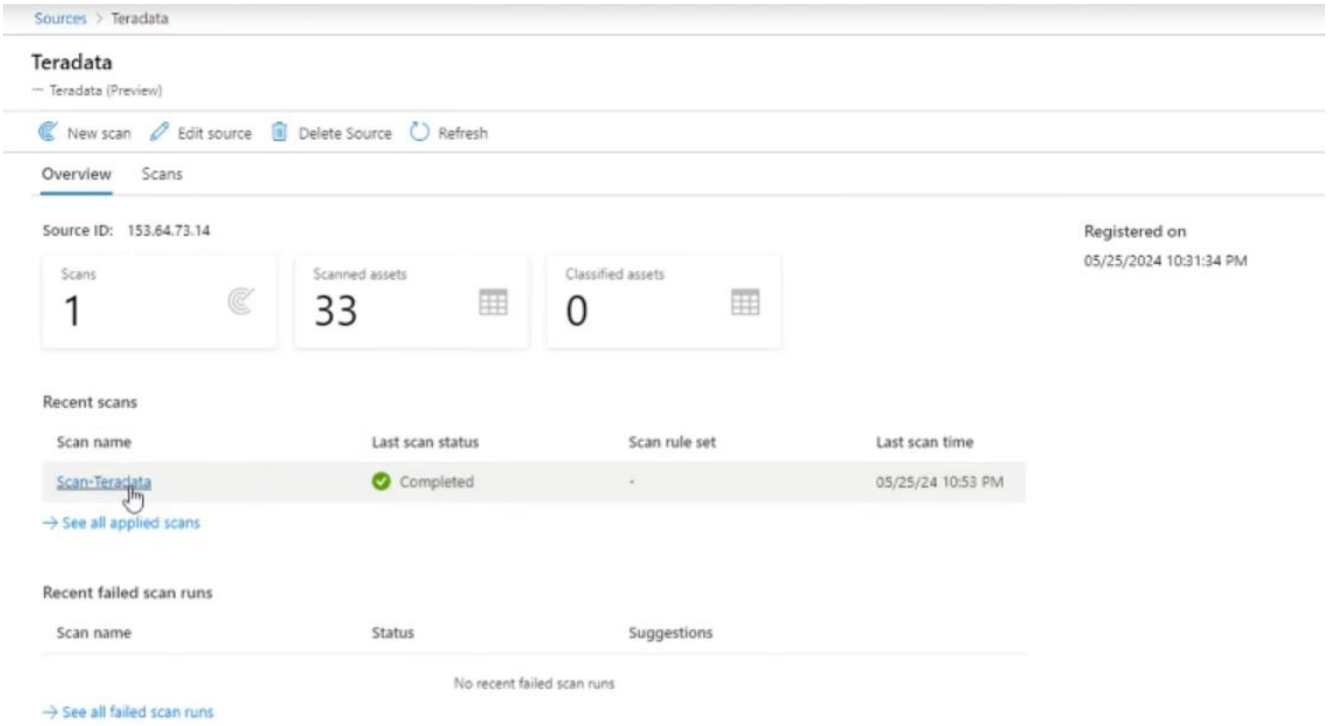

Рис. 9 – Scan history

5. **Перегляд результатів сканування**:

    - Після завершення сканування перейдіть до розділу "Scan history" в обраному джерелі даних.
    - Виберіть останнє виконане сканування для перегляду результатів.

Рис. 10 – Scan result

Розгортання та налаштування Microsoft Purview є важливими кроками для забезпечення захисту персональних даних у вашій організації. Правильне налаштування джерел даних, запуск сканування та моніторинг активності допоможуть виявити та запобігти порушенням безпеки даних.

3.3 Розробка рекомендацій щодо захисту персональних даних в інформаційній системі підприємства на основі Microsoft Purview

У цьому розділі будуть розглянуті рекомендації щодо захисту персональних даних в інформаційній системі підприємства на основі Microsoft Purview.

1. Оцінка та класифікація даних

1.1 Ідентифікація джерел даних

Першим кроком є виявлення всіх джерел даних, які можуть містити персональні дані. До таких джерел можуть належати бази даних, файлові сховища, поштові сервери, CRM-системи та інші інформаційні системи.

1.2 Використання вбудованих класифікаторів

Microsoft Purview надає вбудовані класифікатори для автоматичної ідентифікації персональних даних, таких як номери соціального страхування, фінансові дані, адреси електронної пошти тощо. Використання цих класифікаторів дозволяє швидко визначити, які дані потребують захисту.

1.3 Створення кастомних класифікаторів

Для специфічних потреб підприємства можна створити кастомні класифікатори, які допоможуть ідентифікувати дані, що не охоплені вбудованими класифікаторами.

2. Управління доступом до даних

2.1 Розмежування прав доступу

Використовуючи Microsoft Purview, підприємство може розмежовувати права доступу до персональних даних на основі ролей та обов'язків співробітників. Важливо забезпечити мінімально необхідний доступ до даних для кожного користувача.

2.2 Політики умовного доступу

Впровадження політик умовного доступу дозволяє забезпечити додатковий рівень безпеки, наприклад, обмежуючи доступ до даних лише з корпоративної мережі або з використанням багатофакторної автентифікації.

3. Захист даних

3.1 Шифрування даних

Шифрування даних є одним з найефективніших методів захисту персональних даних. Microsoft Purview дозволяє автоматично застосовувати політики шифрування до чутливих даних, як при зберіганні, так і при передачі.

3.2 Захист даних у реальному часі

Використання функцій реального часу для моніторингу та захисту даних дозволяє виявляти і реагувати на загрози негайно. Це включає моніторинг незвичайної активності, таких як масове копіювання або видалення даних.

4. Моніторинг та аудит

4.1 Журналювання дій

Впровадження журналювання дій користувачів дозволяє відслідковувати, хто і коли мав доступ до персональних даних. Це важливо для виявлення та розслідування потенційних інцидентів безпеки.

4.2 Регулярні аудити

Періодичне проведення аудитів дозволяє оцінювати ефективність існуючих політик захисту даних і виявляти можливі вразливості. Microsoft Purview надає інструменти для автоматизованого створення звітів та аналізу даних.

5. Навчання та підвищення обізнаності

5.1 Навчання співробітників

Постійне навчання співробітників щодо безпеки персональних даних та використання Microsoft Purview є критично важливим. Важливо проводити тренінги і навчання для підвищення обізнаності щодо політик безпеки.

5.2 Розробка внутрішніх політик

Створення та впровадження внутрішніх політик щодо обробки персональних даних, включаючи правила поведінки при роботі з чутливими даними, допомагає

мінімізувати ризики витоків і зловживань.

Впровадження Microsoft Purview у інформаційну систему підприємства дозволяє значно підвищити рівень захисту персональних даних завдяки комплексному підходу, що включає ідентифікацію, класифікацію, захист, моніторинг та навчання. Дотримуючись цих рекомендацій, підприємства можуть не лише забезпечити відповідність нормативним вимогам, але й створити надійний захист для своїх інформаційних активів.

ВИСНОВКИ

Дослідження показало, що Microsoft Purview є потужним та ефективним інструментом для захисту персональних даних в інформаційних системах підприємств. Він надає широкий спектр можливостей для управління даними, включаючи їх інвентаризацію, класифікацію, захист, моніторинг ризиків та управління ними.

Інвентаризація та класифікація даних: Завдяки функціям інвентаризації даних (Data Catalog) Microsoft Purview дозволяє створювати повний каталог даних, що зберігаються в системі. Це забезпечує чітке розуміння того, де знаходяться чутливі дані та який їхній обсяг. Автоматична класифікація даних (Data Classification) допомагає швидко ідентифікувати та класифікувати дані на основі попередньо визначених шаблонів. Це значно спрощує процес управління даними і дозволяє зосередитися на захисті найкритичніших даних.

Захист даних: Microsoft Information Protection (MIP), інтегрований з Purview, надає можливість шифрування даних та налаштування політик доступу. Це дозволяє забезпечити конфіденційність і цілісність даних, а також запобігти несанкціонованому доступу до них. Налаштування політик доступу дозволяє визначати, хто і які дії може виконувати з даними, забезпечуючи строгий контроль доступу до чутливих даних.

Моніторинг та управління ризиками: Функції моніторингу ризиків у Microsoft Purview дозволяють виявляти потенційні загрози безпеці даних та оперативно реагувати на них. Система сповіщень про порушення політик безпеки забезпечує своєчасне інформування про будь-які аномальні дії або потенційні загрози, що дозволяє швидко вжити відповідних заходів для їх нейтралізації.

Початкове оцінювання: Важливим кроком впровадження Microsoft Purview є проведення початкового аудиту даних та систем. Це дозволяє виявити критичні точки для захисту персональних даних і забезпечити ефективне впровадження системи захисту. Аудит допомагає виявити слабкі місця в існуючій системі безпеки та розробити стратегії їх усунення.

Навчання та підтримка: Для ефективного використання Microsoft Purview

необхідно проводити регулярне навчання персоналу щодо роботи з системою та дотримання політик захисту даних. Це підвищує обізнаність співробітників про важливість захисту даних і забезпечує правильне використання інструментів для захисту інформації. Забезпечення постійної підтримки користувачів також є критично важливим для успішного впровадження та функціонування системи.

Постійне вдосконалення: Захист даних - це безперервний процес, який вимагає регулярного оновлення політик безпеки відповідно до змін законодавства та внутрішніх вимог організації. Використання аналітики для оцінки ефективності існуючих заходів захисту та впровадження нових, більш ефективних методів, дозволяє підприємству постійно покращувати свій рівень захисту даних.

Загалом, впровадження Microsoft Purview дозволяє підприємствам значно підвищити рівень захисту персональних даних, забезпечуючи їх конфіденційність, цілісність та доступність. Це сприяє відповідності сучасним стандартам та вимогам безпеки, що є критично важливим для будь-якої організації. Використання Microsoft Purview допомагає захистити дані від несанкціонованого доступу, забезпечити їх надійне зберігання та обробку, що є ключовим елементом у забезпеченні комплексного захисту персональних даних у сучасних інформаційних системах.

ПЕРЕЛІК ПОСИЛАНЬ

1. Оніщенко О.В. Конституційне та адміністративне право / Оніщенко О.В. // Захист персональних даних. – 2012 – №1.

2. Про інформацію: Закон України від 02.10.1992 р. // Відомості Верховної Ради України. – 1992. – № 48.

3. Конституція України. Прийнята на п‘ятій сесії Верховної Ради України 28.06.1996 р. // Відомості Верховної Ради України. – 1996. – № 30.

4. Про захист персональних даних: Закон України від 01.06.2010 р. // Відомості Верховної Ради України. – 2010. – № 34. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

5. Про ратифікацію Конвенції про захист осіб у зв‘язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв‘язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 06.07.2010 р. // Відомості Верховної Ради України. – 2010. – № 46.

6. Деякі питання практичного застосування Закону України «Про захист персональних даних: Роз’яснення Мінюсту від 21.12.2011 р. / [Електронний ресурс]. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/n0076323-11#Text

7. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 р. / [Електронний ресурс]. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

8. Кодекс законів про працю України від 10.12.1971 р. // Відомості Верховної Ради УРСР від 17.12.1971.

9. Цивільний кодекс України від 16.01.2003 р. // Голос України. – 2003. – № 47.

10. Захист персональних даних [Електронний ресурс] – Режим доступу: https://tzi.com.ua/zpd.html

11. Загрози інформаційній безпеці [Електронний ресурс] – 2017. –Режим доступу:

https://www.anti-malware.ru/threats/information-security-threats

12. Захист персональних даних за правилами GDPR [Електронний ресурс] – 2020. – Режим доступу:

https://ecpl.com.ua/news/zakhyst-personal-nykh-danykh-za-pravylamy-gdpr/

13. Единое управление данными с Microsoft Purview | Microsoft Azure [Електронний ресурс] – Режим доступу:

https://azure.microsoft.com/ru-ru/products/purview/

14. Microsoft Purview – рішення для захисту даних | Захисний комплекс Microsoft [Електронний ресурс] – Режим доступу:

https://www.microsoft.com/uk-ua/security/business/microsoft-purview

15. Настройка и установка сканера защиты информации [Електронний ресурс] – Режим доступу:

https://learn.microsoft.com/ru-ru/purview/deploy-scanner-configure-install?tabs=azure-portal-only

16. Захист від втрати даних у Microsoft Purview [Електронний ресурс] – Режим доступу:

https://www.microsoft.com/uk-ua/security/business/information-protection/microsoft-purview-data-loss-prevention

17. Introducing Adaptive Protection in Microsoft Purview [Електронний ресурс] – Режим доступу:

https://www.microsoft.com/en-us/security/blog/2023/02/06/introducing-adaptive-protection-in-microsoft-purview-people-centric-data-protection-for-a-multiplatform-world/?culture=uk-ua&country=ua

18. Анализ метрик с помощью обозревателя метрик Azure Monitor [Електронний ресурс] – Режим доступу:

https://learn.microsoft.com/ru-ru/azure/azure-monitor/essentials/analyze-

metrics#apply-filters-to-charts