ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технологія забезпечення захисту персональних даних при обробці та передаванні в IT системах організації»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо- професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Анохін Д.Г.
(прізвище та ініціали)
Керівник Власенко В.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

РЕФЕРАТ

Текстова частина магістерської роботи: 48сторінок, 18 рисунків, 9 джерел.

Об'єкт дослідження – процес захисту персональних даних в інформаційних системах.

Предмет дослідження – технології захисту персональних даних.

Мета роботи – дослідити технологію щодо застосування методів та засобів захисту персональних даних при обробці та передачі в інформаційних системах організацій.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

В роботі проведено дослідження щодо захисту персональних даних інформаційної системи.. Для досягнення мети було проведено аналіз загроз щодо персональних даних. Було проведено аналіз законів та міжнародних стандартів щодо забезпечення захисту персональних даних в ІТ системі.

В результаті було проведено дослідження можливих варіантів систем, які оброблюють, зберігають та передають персональні дані з використанням криптографічного шифрування зі збереженням формату та надано рекомендації щодо основних заходів забезпечення захисту персональних даних в ІТ системі.

Галузь використання – кібербезпека інформаційних систем.

ІНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗИ, ПЕРСОНАЛЬНІ ДАНІ, ШИФРУВАННЯ, ФОРМАТ, GPDR, ЗАКОН ЗАХИСТ, МЕТОДИ ТА ЗАСОБИ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – інформаційні технології

КСЗІ – комплексна система захисту інформації

ПЗ – програмне забезпечення

ОТ – Operational Technology

GPDR – General Data Protection Regulation

NIST – National Institute of Standards and Technology

FPE – Format-preserving encryption

ВСТУП

Актуальність дослідження. Загальний регламент про захист даних (General Data Protection Regulation, GDPR) - це нова узагальнена постанова Європейського Союзу, яке замінює собою Директиву ЄС про захист Персональних даних 95/46 / EC (EU Data Protection Directive 95/46 / EC). Даний регламент уніфікує регулювання захисту персональних даних в країнах ЄС і посилює вимоги до захисту персональних даних (будь-якої інформації, що відноситься до ідентифікованого або ідентифікованому фізичній особі (суб'єкт даних), по якій прямо або побічно можна його визначити. до такої інформації належить число ім'я, дані про місце розташування, онлайн ідентифікатор або один або кілька факторів характерних для фізичної, фізіологічної, генетичної, розумової, економічної, культурної або соціальної ідентичності цієї фізичної особи).

Новий регламент націлений на підвищення рівня захисту та надання громадянам контролю над своїми даними. Невиконання правил компаніями веде до накладення великих штрафів.

Вимоги регламенту стосуються як організацій, зареєстрованих в ЄС, так і компаній, розташованих в інших країнах, за умови, що вони надають послуги громадянам Євросоюзу, або іншим способом збирають дані таких користувачів.

Підхід до захисту персональних даних в GDPR відображені в семи пунктах:

Принцип законності, справедливості і прозорості. Персональні дані повинні бути отримані законними і справедливими засобами за згодою суб'єкта даних.

Обмеження мети. Мета збору даних повинна бути вказана під час збору, і дані не повинні використовуватися ні для чого іншого, крім початкового наміру.

Мінімізація даних. Зібрані дані повинні відповідати заданій спочатку цілі. Забороняється збирати дані в більшому обсязі, ніж це потрібно для досягнення мети.

Точність. Персональна інформація повинна бути точною, повною та актуальною, наскільки це необхідно для заданих цілей. Якщо такі дані будуть вважатися неточними, вони повинні бути стерті або виправлені (на вимогу користувача).

Обмеження зберігання. Дані зберігаються в формі, яка дозволяє ідентифікувати користувача не довше, ніж це необхідно для виконання цілей обробки інформації.

Цілісність і конфіденційність. Особисті дані повинні бути захищені гарантіями безпеки від таких ризиків, як втрата або несанкціонований доступ, знищення, використання, модифікація або розкриття даних.

Підзвітність. Контролер несе відповідальність і повинен бути готовий продемонструвати дотримання заходів, зазначених вище.

Все зазначене вище повинно бути дотриманим і згідно Закону України «Про захист персональних даних».

Тому для компаній, які оброблюють, зберігають та передають персональні дані необхідно впроваджувати відповідні методи та заходи щодо захисту персональних даних в ІТ системах.

Тому тема магістерської роботи є своєчасною та актуальною.

Об'єкт дослідження – процес захисту персональних даних в інформаційних системах.

Предмет дослідження – технології захисту персональних даних

Мета роботи – дослідити технологію щодо застосування методів та засобів захисту персональних даних при обробці та передачі в інформаційних системах організацій.

Завдання магістерської роботи:

провести аналіз вимог до захисту персональних даних згідно Закону України «Про захист персональних даних» та дотримання вимог General Data Protection Regulation;

проаналізувати підходи та зміст захисту персональних даних;

визначити методи та засоби захисту робочих станцій;

розробити варіант технології забезпечення захисту персональних даних в ІТ системах;

розробити загальні рекомендації щодо захисту персональних даних в ІТ системах.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: рекомендації щодо захисту персональних даних в ІТ системах можуть бути використані у сфері забезпечення кібербезпеки і інформаційних системах.

Апробація результатів дослідження – результати дослідження оговорювались на науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Аналіз захисту персональних даних на основі нормативно-правової бази України

Останнім часом актуальним питанням є питання щодо практичного застосування положень Закону України «Про захист персональних даних» [1]. Тому надамо визначення.

Персональні дані - це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1].

Даний закон дозволяє врегулювати правовідносини, пов'язані з обробкою даних та гарантувати право на повагу до приватного і сімейного життя. Але в законі не написано, які відомості про фізичну особу персональними даними, задля можливості застосування положень Закону до різноманітних ситуацій.

Але незнання не позбавляє відповідальності, і потрібно щоб законодавство у сфері захисту інформації надавало детальні роз'яснення, усвідомлення та адаптації.

Закон України «Про захист персональних даних» поширюється на фізичних і на юридичних осіб, які виконують будь-які дії, або сукупність дій, до яких відноситься збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і розповсюдження, знищення персональних даних, у тому числі, з використанням інформаційних (автоматизованих) систем [2].

Персональні дані можна поділити на дві основні категорії: загальні та особливі.

До загальної категорії відносяться: прізвище та ім'я; дата та місце народження; громадянство; сімейний стан; псевдонім; дані, записані в посвідченні водія; економічне і фінансове становище; дані про майно; банківські дані; підпис; адреса місця проживання; диплом про освіту, професійна підготовку тощо[2].

До особливїо категорії відноситься інформація яка охоплює: расове, етнічне

та національне походження; політичні, релігійні та світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи громадських організаціях світоглядної спрямованості; стан здоров'я (медичні дані); статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності, тощо [2].

В законі написано що таке обробка даних.

Обробка персональних даних – це будь-яка дія з персональними даними починаючи від збирання і закінчуючи знищенням персональних даних. Сюда відноситься реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання, поширення (розповсюдження, реалізація, передача), знеособлення тощо (стаття 2 Закону України «Про захист персональних даних») [1-2]

Обов'язково потрібно враховувати категорію даних під час їх обробки. та застосовувати відповідні рівні безпеки. Крім того, при обробці даних, які становлять ризик для прав і свобод людини (особливої категорії даних), розпорядники персональних даних повинні повідомити Уповноваженого Верховної Ради України з прав людини про структурний підрозділ або відповідальну особу, яка організовує роботу з даними.[2]

При роботі з персональними даними необхідно розробляти внутрішні політики безпеки даних.

До них відносяться внутрішні положення (інструкції), які регулюють процедури обробки персональних даних. Вони повинні розроблятися власниками та розпорядниками персональних даних, відповідно до вимог Закону, зважаючи на:

Це внутрішні положення (інструкції), які регулюють процедури обробки персональних даних [2]. Внутрішні положення розробляють власниками та розпорядниками персональних даних, відповідно до вимог Закону, зважаючи на:

- специфіку діяльності (правові підстави);
- мету обробки, обсяг даних та їх категорії;
- інформаційні системи, мережі, програми, задіяні у процес обробки персональних даних;

- число осіб, які мають доступ до персональних даних (працюють з даними);
- форми ведення реєстру, в якому обробляються персональні дані (мануальна, електронна або змішана);
- ризики, які можуть виникнути при обробці даних, як для систем, так і осіб, чиї дані обробляються тощо [2].

Вимоги до документації, які відноситься до політики безпеки персональних даних, повинна бути повними, постійно на регулярній основі оновлюватися й містити, як мінімум, інформацію про [1-2]:

- мету, обсяг, підстави (межі повноважень) обробки персональних даних;
- конфігурацію інформаційної системи (банків даних), мережі, програми тощо;
- номенклатуру оброблюваних персональних даних (види та категорії), їхні локалізації та операції, що проводяться з ними;
- механізм здійснення заходів безпеки (у тому числі, фізичного середовища інформаційних систем);
- докладний опис критеріїв, відповідно до яких будуть доступні персональні дані;
- управління доступом та список авторизованих користувачів (у числі, рівні доступу);
- графік перевірок безпеки та звіти про інциденти безпеки;
- особу, відповідальну за політику безпеки;
- аудит безпеки (графік перевірок та звіти про інциденти безпеки);
- порядок доступу до персональних даних третіх осіб;
- строки збереження, процедури видалення або знищення даних;
- заходи з виявлення випадків несанкціонованого доступу і/або несанкціонованої обробки персональних даних та інш.

Тож визначемо ще додаткові акти, які забезпечують право людини на

захист даних:

- Конституція України (стаття 32).
- Загальна Декларація прав людини (стаття 12).
- Міжнародний Пакт про громадянські і політичні права (стаття 17)
- Конвенція про захист прав людини і основоположних свобод (стаття 8).
- Конвенція Ради Європи про захист осіб у зв'язку автоматичною обробкою персональних даних.
- Закон України «Про захист персональних даних».
- Витяг з Кодексу України про адміністративні правопорушення (стаття 188-39 «Порушення законодавства у сфері захисту персональних даних», стаття 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»).
- Витяг з Кримінального кодексу України (стаття 182 «Порушення недоторканності приватного життя»).
- Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № 1/02-14.

1.2. Аналіз змісту General Data Protection Regulation

У країнах Європейського Союзу докладається максимум зусиль щоб населення, державні служби, муніципалітети, бізнес розуміли норми закону, що регулюють обробку даних, кібербезпеку та електронну комунікацію, знали практичні аспекти впровадження та ризики, пов'язані з невиконанням цих положень.

Для цього було створено Загальний регламент щодо захисту даних Генеральний регламент про захист персональних даних General Data Protection Regulation (GDPR). GDPR спрямований перш за все на те, щоб дати громадянам

контроль над власними персональними даними і на спрощення нормативної бази для міжнародних економічних відносин шляхом уніфікації регулювання в рамках ЄС.

Дія GDPR охоплює не тільки правову сферу діяльності організації і питання дотримання вимог, але також зачіпає підрозділи, що відповідають за інформаційні технології, безпеку, управління даними та інформацією.

Правові питання і дотримання вимог

GPDR ставить нові завдання і нові вимоги перед підрозділами, які відповідають за юридичні аспекти і питання дотримання вимог. Багатьом організаціям потрібно ввести у себе посаду директора із захисту даних (Data Protection Officer, DPO), який буде грати ключову роль в питанні забезпечення дотримання вимог. За деякими оцінками, в одній тільки Європі додатково буде потрібно близько 28 тисяч директорів щодо захисту даних. При недотриманні вимог GDPR організації може загрожувати дуже серйозний штраф в розмірі до 4% від сумарного обороту.

Посилення акценту на питаннях підзвітності зажадає від організацій прийняття завчасних і надійних заходів в області управління конфіденційністю: організаціям потрібно переглянути свій підхід до формування політики в сфері конфіденційності, щоб таким чином зробити ці політики доступнішими для розуміння.

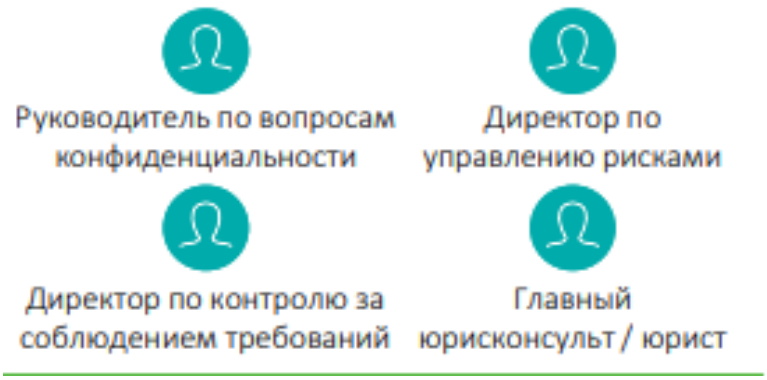

Рис.1.1. Посади згідно GPDR

Інформаційні технології та безпека.

Нові вимоги GDPR приведуть до зміни підходів до розробки та управління технологіями. Для розгортання нових систем і технологій буде вимагатися документування оцінки ризиків конфіденційності.

Випадки порушення системи безпеки повинні будуть доводитись до відома регулюючих органів протягом 72 годин. Це означає необхідність впровадження нових або вдосконалених процедур реагування на інциденти.

Тепер, коли концепція «конфіденційність за замовчуванням» (Privacy by Design) закріплена законодавчо, очікується, що протягом наступних декількох років практика проведення оцінки впливу на сферу конфіденційності стане в організаціях повсюдною. Крім того, передбачається, що організації почнуть приділяти більше уваги питанням маскування, псевдоанонімізації і шифрування даних.

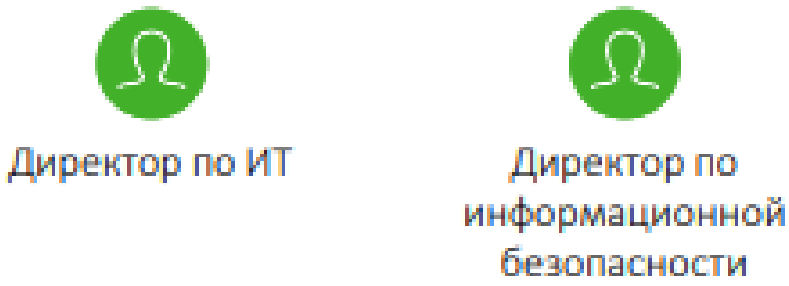

Рис.1.2. Посади відповідальні за інформаційні технології та безпеку

Управління даними та інформацією

Перед фізичними особами та командами, які відповідають за управління інформацією, постане завдання щодо забезпечення більш чіткого контролю за процесами зберігання і переміщення даних, а також відстеження послідовності перетворення даних (data lineage). Наявність більш чіткого розуміння того, як відбувається збір даних і де ці дані зберігаються, дозволить полегшити процес дотримання вимог стосовно нових прав суб'єктів даних (право на видалення даних або на їх передачу в іншу організацію).

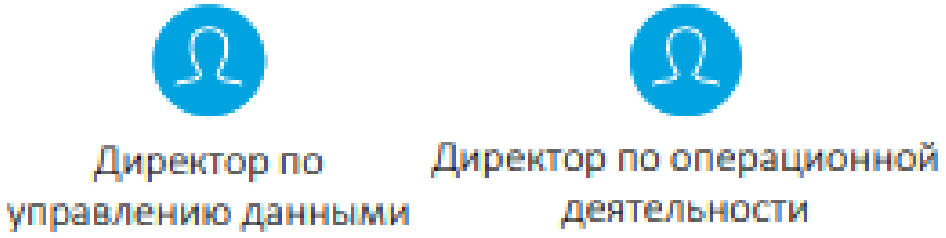

Рис. 1.3. Посади по управлінню даними та інформацією

Аспекти щодо юридичної сторони питання. Головні юрисконсульти, директора з контролю за дотриманням вимог, директора з питань конфіденційності та директора із захисту даних: необхідно переглядати стратегії управління конфіденційністю, а також процесів ресурсного забезпечення та механізмів організаційного контролю. Це вимагає ще більшого залучення зі боку рад директорів до вирішення юридичних питань:

1. Розмір штрафів може становити до 4% від сумарного річного обороту. У разі серйозних порушень величина штрафу може досягати 4% від сумарного річного обороту або 20 млн євро.

2. Проактивний підхід. Існуюча в даний момент вимога про направлення місцевим регулюючим органам щорічних повідомлень про діяльність по обробці даних буде замінено новими, істотними вимогами щодо ведення даних для контрольних перевірок («аудиторський слід») та інформації про переміщення даних.

3. Брак незалежних фахівців на ринку. Організаціям, які обробляють персональні дані у великих обсягах, буде потрібно заснувати у себе посаду кваліфікованого незалежного директора із захисту даних.

4. Прозорість і навчання є ключовими факторами. В рамках GDPR організаціям потрібно ретельно підходити до формування призначених для клієнтів політик конфіденційності і включати в ці політики більш детальну інформацію.

Технологічні аспекти

Директорам з інформаційних технологій, технічним директорам і директорам з інформаційної безпеки: потрібно переглянути підхід до використання технологій, що забезпечують інформаційну безпеку і дотримання відповідних вимог; при цьому можливе збільшення витрат. Ось основні апекти щодо технічної підтримки:

1. Повідомлення про витоки протягом 72 годин.

Тепер істотні порушення інформаційної безпеки повинні будуть доводитись до відома регулюючих органів і, в окремих випадках, до відома фізичних осіб, порушених такими порушеннями. Відповідно, організаціям необхідно в терміновому порядку переглянути свої процедури з управління інцидентами, а також подумати про впровадження процедур регулярного тестування, перевірки та оцінки існуючих наскрізних процесів управління інцидентами.

2.Профілювання стає складним питанням.

Фізичні особи отримають право відмовлятися або забороняти використання коштів для відстеження дій і профілювання, що зробить істотний вплив на компанії, які безпосередньо працюють з споживачами і використовують методи, що дозволяють краще аналізувати дані про клієнтів. Це відноситься не тільки до веб-сайтів, а й до інших цифрових засобів, наприклад, до мобільних додатків, а також до вже існуючих або тільки формуючихся технологій.

3. Шифрування як спосіб забезпечення імунітету.

У GDPR на формалізованій основі визнані переваги шифрування даних з точки зору забезпечення конфіденційності, включаючи звільнення від необхідності повідомляти фізичних осіб про порушення інформаційної безпеки в разі якщо дані пройшли шифрування. Це, однак, не означає, що організації можуть на цьому заспокоїтися і що виключення з вимог буде діяти також і в разі слабких механізмів шифрування. З урахуванням можливих ризиків організаціям потрібно посилити акцент на формуванні надійного режиму забезпечення інформаційної та кібербезпеки.

4. Загальновизнана найкраща практика стає законодавчою вимогою.

Хоча концепція конфіденційності за замовчуванням (Privacy By Design) не є чимось новим, тепер вона закріплена у вимогах GDPR. Таким чином, організаціям потрібно впровадити у себе новий підхід, відповідно до якого конфіденційність повинна стати ключовим компонентом при проектуванні, розробці та впровадженні нових технологій. Одним з проявів вимоги щодо забезпечення дотримання концепції «конфіденційність за замовчуванням» є необхідність проведення оцінки впливу на конфіденційність (Privacy Impact Assessment, PIA). Така оцінка повинна проводитися для всіх нових форм використання особистих даних, які несуть високий ризик для фізичних осіб.

Аспекти оброблюваних даних

Директора з управління даними, керівники з управління якістю даних, директора з маркетингу та керівники цифрових напрямків: діяльність зазначених керівників завжди включала в себе забезпечення ініціатив в області конфіденційності. Однак в рамках GDPR потрібно реалізація нових ініціатив, які безпосередньо пов'язані з дотриманням вимог. А саме:

1. Ідентифікація та відстеження даних.

Організаціям потрібно реалізувати у себе ініціативи, які дозволять продемонструвати, що організація знає, які дані у неї є, де вони зберігаються і у кого є спільний доступ до цих даних. Для цього буде необхідно створити і підтримувати реєстр процесів з обробки даних.

2. Нове право на запит стандартизованої копії даних.

Нове право на мобільність даних полягає в тому, що фізичні особи тепер можуть вимагати надання копії їх даних в читаємій стандартизованій формі.

3. Зміцнення права споживачів вимагати видалення власних даних.

Нове так зване «право на забуття» є ще одним свідченням того, що споживачі стають на чолі процесу, пов'язаного з використанням їх даних.

4. Концепція псевдоанонімність даних.

У GDPR включена концепція псевдоанонімність даних і розширено визначення персональних даних з більш чітким акцентом на класифікацію даних і управління ними.

Розглянемо шляхи впровадження програми готовності до GDPR, яка допоможе компанії підготуватися до впровадження GDPR оптимальним способом (рис. 1.4.)

Стратегія

Головна відправна точка, яка визначає високорівневий напрямок і ризик-апетит, на підставі яких компанія будує свої процедури з управління конфіденційністю.

Організація і Відповідальність

Ефективне впровадження стратегії з управління конфіденційністю вимагає чіткої і ультідісціплінарной організаційної структури в частині питань конфіденційності. Це включає в себе як структуру, так і ролі і позиції ключових гравців, таких як директор із захисту даних. Цей шар також включає в себе закріплення відповідальності за забезпечення відповідності регуляторним вимогам.

Політики, процеси і дані

Співпраця з бізнесом для забезпечення захисту, регулювання, управління і ефективного використання даних у відповідності зі стратегією організації. Також включає в себе технологічні питання, такі як запити на доступ до даних, зберігання даних, «право на забуття», повідомлення про витоки та інциденти, а також передача даних в інші країни і третім особам.

Оповіщення, Навчання, Підвищення обізнаності

Забезпечення всередині організації високого рівня обізнаності про питання конфіденційності дозволяє бути впевненими в тому, що співробітники знають правила і виконують їх.

Процедури по забезпеченню конфіденційності

Впровадження концепції конфіденційності в проектну методологію організації за допомогою ефективного управління на етапі розробки концепції нового або допрацьовувати продукт або сервіс (Конфіденційність за замовчуванням), а також оцінки нових або існуючих систем з допомогою оцінки впливу на конфіденційність. Також даний компонент покриває аудити і

дослідження питань сертифікації на відповідність вимогам ЄС в області конфіденційності (нова опція в GDRP).

Реєстр процедур по обробці даних

Реєстр процедур по обробці даних є фундаментальним елементом будь-якої програми по забезпеченню конфіденційності, і стане обов'язковою вимогою з впровадженням GDPR.

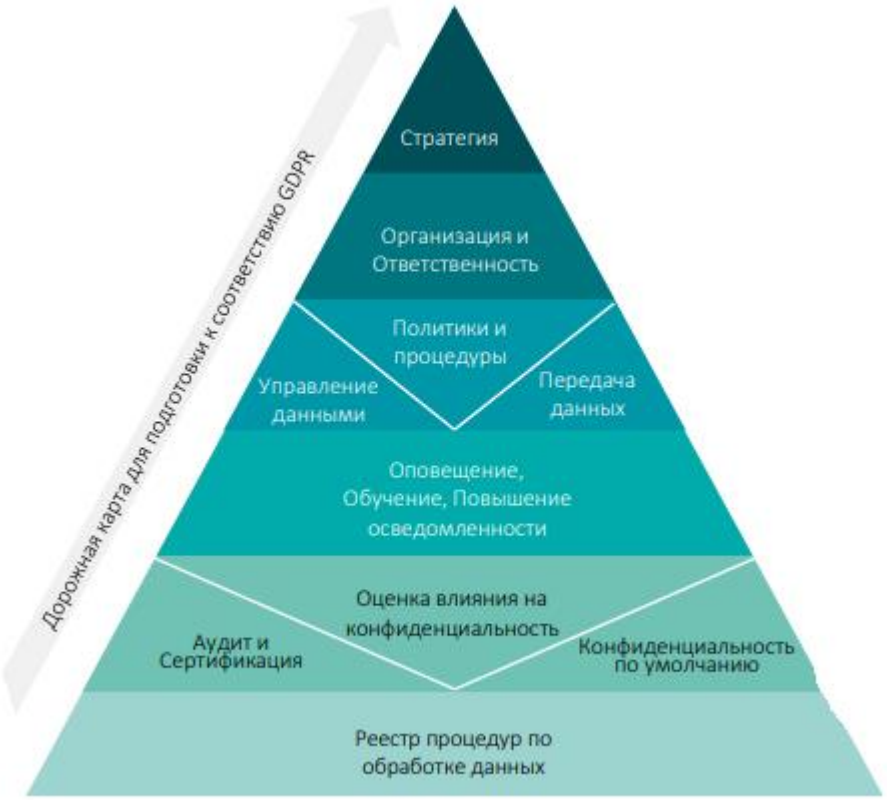

Рис.1.4. Шляхи впровадження програми готовності до GDPR

Розглянемо процес щодо реєстру процедур по обробці даних і оцінки впливу на конфіденційність. Стаття 30 GDPR вимагає своєчасної оцінки процедур по обробці конфіденційних даних, діаграма якого показано на рис 1.5.

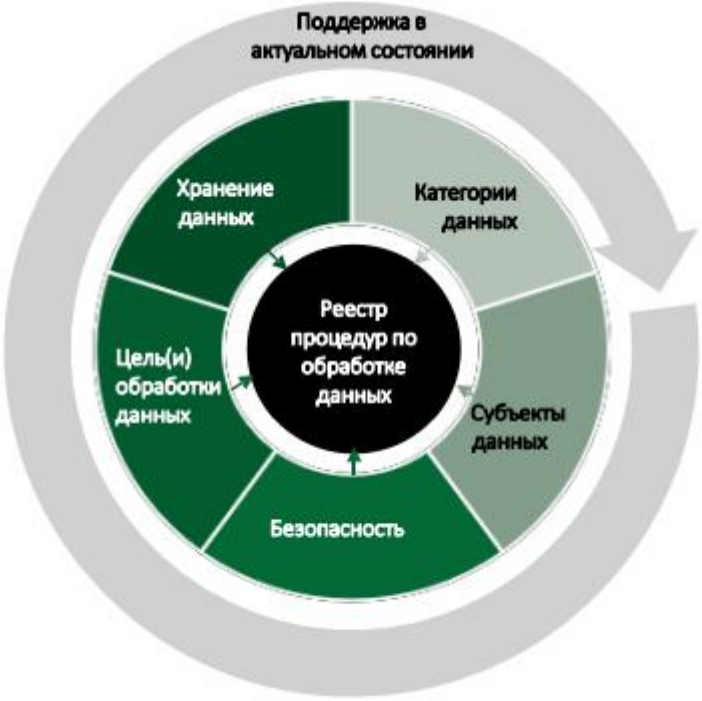

Рис 1.5. Процес реєстру процедур по обробці даних і оцінки впливу на конфіденційність

Процес оцінки впливу на конфіденційність (Data Protection Impact Assessment, DPIA) складається з трьох основних етапів:

1. Ідентифікація:

• Збір конфіденційних даних;

• Верхньорівнева оцінка ризиків;

• Пріоритизація .

2. DPIA

• Законні підстави;

• Мета обробки;

• Ведення внутрішніх реєстрів;

• Якість даних;

• Прозорість;

• Права суб'єкта даних;

• Конфіденційність відповідно до дизайну і за замовчуванням;

• Оцінка впливу на конфіденційність;

• Повідомлення про витік;

• Безпека;

• Обробка даних оператором;

• Передача даних.

3. Виправлення

• Оцінка ризику конфіденційності;

• Зниження ризику;

• Прийняття ризику;

Більшість аспектів, якими компанія, найімовірніше, вже управляє вже представлено але є й ті над якими компаніям ще приходиться працювати.

1.3. Види загроз витоку персональних даних

Впровадження інформаційних технологій, відповідні закони вимагають вирішення проблему захисту інформації при роботі з персональними даними. Про це свідчать фахівці з інформаційних систем та представники бізнесу, аналітичні звіти з питань безпеки бізнесу та інформаційної безпеки. Опитування фахівців показує, що лише не всі фахівців з інформаційної безпеки вважають свою компанію чи установу такою, яка зможе протистояти сучасним інформаційним загрозам, а саме те, що вони можуть призвести до неконтрольованого розповсюдження інформації за межі інформаційних систем, в яких вона обробляється, зберігається та передається.

Саме до неконтрольованого розповсюдження особливо чутливий такий вид інформації, як персональні дані (ПД) [5]. Тому для будь-якої компанії є важливим на сьогодні актуальними питання саме внутрішньої безпеки інформаційних систем (ІС), зокрема і питання неконтрольованого поширення даних [6, 7]. Це пов’язано зо зростаючою кількістю випадків витоку конфіденційної інформації у всіх країнах світу. При цьому, від 70 до 90 % даних, які втрачаються, є ПД.

Основними загрозами в інформаційній безпеці можна виділити дві групи загроз: внутрішні та зовнішні.

До зовнішніх загроз відносяться ті загрози, які виникають та якими управляють за межами ІС, відносно ресурсів як на які вони спрямовані. Внутрішні загрози виникають безпосередньо всередині ІС.

Використання засобів захисту від внутрішніх загроз, використовує незначна частина компаній, хоча необхідність у цих засобах об’єктивно існує. Основна причина виникнення внутрішніх загроз інформаційній безпеці є несанкціонований виток інформації за межі захищених ІС, яка має тенденцію до зростання. Для мінімізації таких загроз необхідно впровадження систем протидії внутрішнім загрозам інформаційній безпеці. Згідно даних, персональні дані за межами захищеної інформаційної системи, стають доступними практично досить необмеженій кількості користувачів. ПД можуть бути знищені, спотворені, а використані з метою нанесення шкоди особі, якої вони стосуються, з боку моральної та матеріальної сторони. Тому саме вирішенню проблеми захисту від неконтрольованого поширення персональних даних приділяється велика увага зі сторони міжнародного співтовариства та урядів багатьох держав світу [8, 9].

Велика зацікавленість з боку кібер-злочинців викликає діяльність державних структур, і комерційних підприємств. Це пов’язано з розвитком інформаційних технологій і їх проникненням у всі сфери людської діяльності. Метою кібер-злочинців є викрадення, розголошення конфіденційної інформації, підрив ділової репутації, порушення працездатності і, як можливий наслідок - доступність інформаційних ресурсів компанії.

Виток персональних даних може спіткати не тільки великі установи, але окремих користувачів. За допомогою різних засобів злочинці можуть отримати доступ до персональних даних – номерів банківських рахунків, кредитних карт, паролів, що може призвести до виходу з ладу обчислювальної системи або отримати повний доступ до комп'ютера. Скомпрометований комп'ютер зловмисник може використовувати надалі для своїх цілей для проведення атак на сервери, розсилки спаму, збору конфіденційної інформації, розповсюдження нових вірусів і троянських програм. Таким чином, постає питання про створення

такої системи інформаційної безпеки, яка забезпечить захист персональних даних з дотриманням закону України та міжнародних стандартів. \

Тож наразі визначимо основні джерела загроз:

1. Людський чинник. Це група загроз, яка пов'язана з відповідними діями людини, яка має санкціонований або несанкціонований доступ до інформації. Загрози цієї групи діляться:

а) зовнішні - це є відповідно кібер-злочинці, хакери, інтернет-шахраї, недобросовісні партнери,та інші;

б) внутрішні -це є дії персоналу компанії, а також це можуть бути користувачі домашніх ПК. Дії таких людей можуть бути розділено на умисні, так і випадкові.

2. Технічний чинник. Дані загрози пов'язані з технічними питаннями – особливістю обладнання устаткування, неліцензовані програмні і апаратні засоби обробки інформації. Все це може приводити до відмови обладнання та втрати інформації.

3. Стихійний чинник. Ця група загроз пов’язана з природними катаклізми, стихійними лихами або інші форс-мажорні обставини, які є незалежні від діяльності людини.

Розглянемо шляхи поширення загроз (людський чинник):

1) Мережа Інтернет унікальна тим, не має територіальних меж. Саме це сприяє розвитку безлічі веб-ресурсів і можливістю обміну інформацією. Сьогодні будь-яка людина при бажанні може дістати доступ до даних, які зберігаються в Інтернеті, або створити свій власний веб-ресурс. Такі особливості глобальної мережі надають можливість скоєння злочинів в Інтернеті, ускладнюючи їх виявлення і покарання.

У зв'язку з появою кредитних карт, електронних грошей і можливістю їх використання через Інтернет інтернет-шахрайство стало одним з найбільш поширених злочинів.

2) Інтранет – це внутрішня мережа, спеціально розроблена для управління інформацією усередині компанії або домашньої мережі. Інтранет є загальною

мережею для зберігання, передачі і доступу до інформації між всіма комп'ютерами мережі.

3) Електронна пошта. Наявність поштових скриньок є практично на кожному комп'ютері і використання шкідливих програмам в електронних адресних книгах для виявлення нових жертв забезпечує сприятливі умови для розповсюдження шкідливих програм. Користувач зараженого комп'ютера, сам того не підозрюючи, розсилає заражені листи адресатам, які у свою чергу відправляють нові заражені листи і т.д.

4) Крім загрози проникнення шкідливих програм існують проблема зовнішньої небажаної пошти рекламного характеру (спаму). Не будучи джерелом прямої загрози, небажана кореспонденція збільшує навантаження на поштові сервери, створює додатковий трафік, засмічує поштову скриньку користувача, веде до втрати робочого часу і тим самим наносить значні фінансові втрати. Зловмисники стали використовувати так звані спамерські технології масового розповсюдження, щоб примусити користувача відкрити лист, перейти по посиланню з листа на якийсь інтернет-ресурс. Отже, можливості фільтрації спаму важливі не лише самі по собі, але і для протидії інтернет-шахрайству і розповсюдженню шкідливих програм.

5) Носії інформації —флеш-карти, хмарні сховища — широко використовують для зберігання і поширення інформації. [10].

Таким чином основні витоки інформації приходить на зовніхні втручання, як це показано на рис. 1.6.

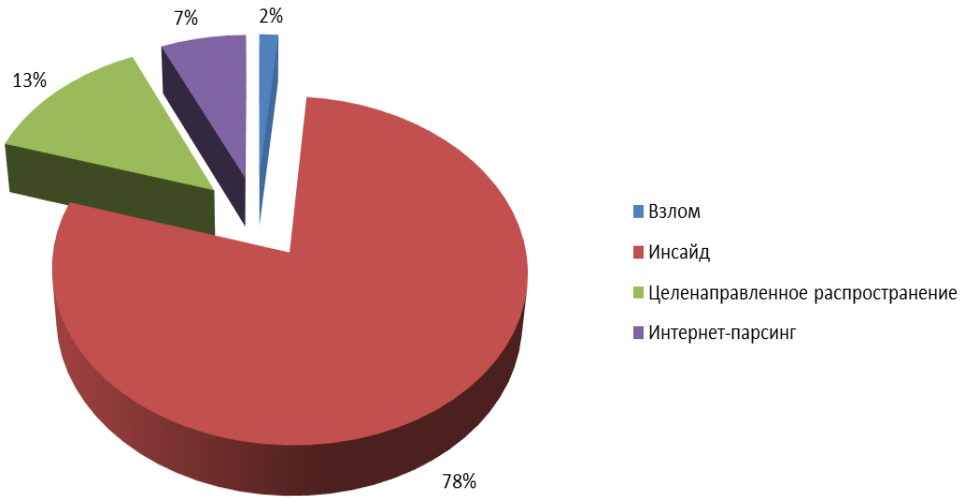

Рис. 1.6 Причини витоку інформації

Надалі показано статистику витоку персональних даних в країнах Європи з 2018 по 2020р.

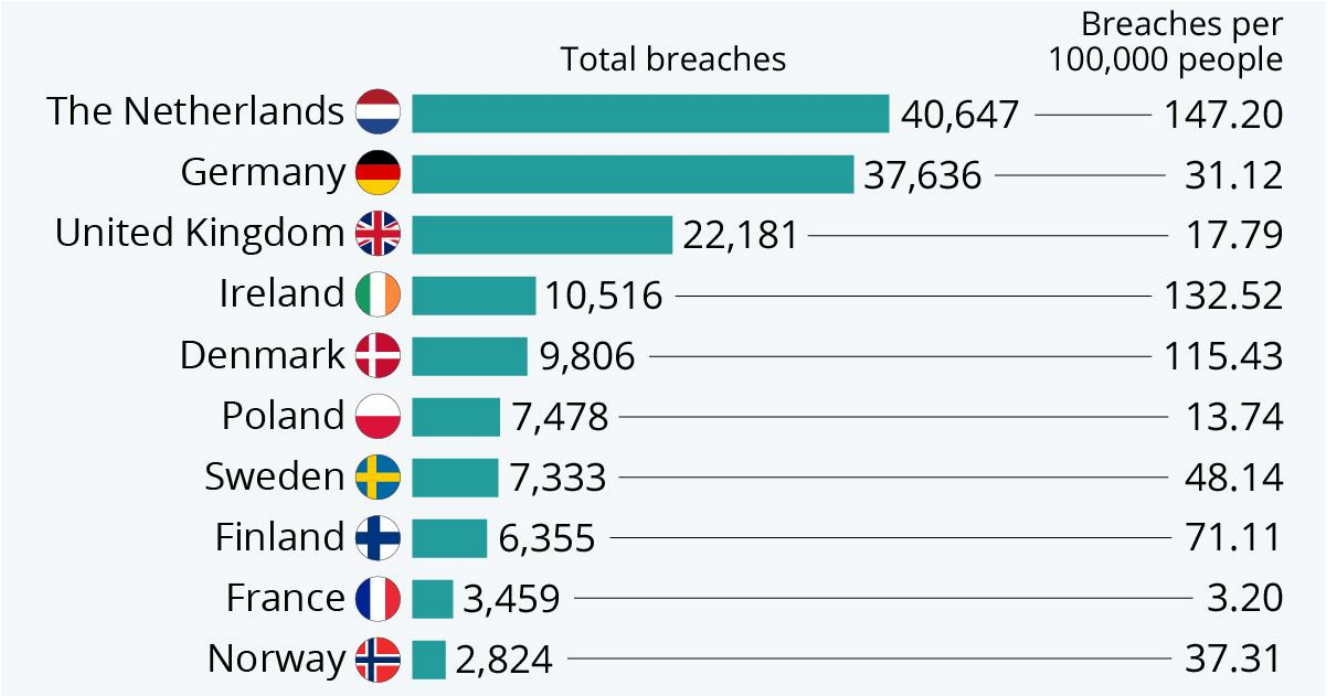

Рис 1.7. Країни з найбільшою кількістю витоків даних GDPR

Таким чином згідно з статистикою, зробимо висновок про необхідність застосування відповідних методів та засобів захисту персональної інформації в ІС компаній при обробці, зберігання та передачі даної інформації.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ ТА GDPR

2.1. Засоби псевдонімізації та шифрування персональних даних

GDPR рекомендує псевдонімізацію та шифрування як два механізми, які можна використовувати для захисту персональних даних. Існує величезна кількість інформації про те, які дані потрібно захищати, хоча існують відносно загальнодоступні відомості про те, як організація може застосовувати технології та процеси для захисту цих даних [4-5].

Тому розглянемо типові випадки використання бізнесу для застосування псевдонімізації та шифрування, який забезпечує огляд основних технологій та платформи Voltage SecureData від Micro Focus, а потім опишемо архітектури та стратегії, прийняті Micro Focus щодо захисту персональних даних за допомогою SecureData:

■ Великий європейський мобільний оператор, який використовує технології захисту даних SecureData для захисту інформації про мобільного абонента на основі даних Hadoop.

■Ввикористовує захист даних для захисту даних при їх перенесенні в хмару та використовує ту саму архітектуру для захисту конфіденційних персональних даних клієнта в середовищі Onpremises.

Псевдонімізація та шифрування:

Розглянемо різницю між цими поняттями.

GDPR пропонує використовувати механізми псевдонімізації та шифрування як прийнятний засіб захисту персональних даних. Псевдонімізація часто використовується як загальний термін, який може застосовуватися до різних методів деідентифікації даних, коли псевдонім або видумані дані можуть використовуватися в бізнес-процесах [5].

Шифрування - це приклади псевдонімізації. GDPR в своїх рекомендаціях не

прописує конкретні форми шифрування чи псевдонімізації. У IDC білому документі "Увімкнення відповідності GDPR за допомогою інноваційних підходів до шифрування та управління ключами", зроблено посилання на застарілі методи шифрування, які роблять дані невпізнанними та порушують бізнес-процеси. Однак GDPR зазначає дві важливі функції шифрування: можливість дешифрувати дані за необхідності та можливість продовжувати запустити бізнес-процеси на зашифрованих даних.

Особливості використовування кейсів для псевдонімізації та шифрування заключаються в:

■ «Захищеній аналітиці» для сховищ даних та Hadoop: Технології великих даних, включаючи платформи сховищ даних, такі як Teradata, Micro Focus® Vertica та Hadoop, дозволять організаціям отримати нові аналітичні дані та операційну ефективність.

Організації передають потокові дані, постійно аналізують та зберігають такі важливі поля даних як імена, адреси, адреси електронної пошти, геопозиціонні дані, номери телефонів та номери карток або банківських рахунків на цих платформах. Отримання рентабельності інвестицій з цих платформ вимагає відкриття даних для аналітиків даних. Однак, розширення доступу до конфіденційних даних спонукає організацію на ризик порушення даних через викрадення інсайдерами, неправильну обробку даних або безпеку інших Глобальних організацій, які збирають дані з пунктів присутності в декількох європейських країнах в центральне сховище або сховище даних, які підлягають додатковому регламенту захисту та збереженню даних. Передача даних, захищених Voltage FPE, на ці платформи дозволяє організаціям проводити аналіз неідентифікованих даних. Такий підхід зменшує ризик порушення даних та дозволяє підприємству підтримувати відповідність таким вимогам, як GDPR.

■ Міграція до хмари: організації застосовують стратегії хмарних обчислень, щоб отримати значні ринкові переваги та реалізувати економічні економії. Для конфіденційних корпоративних та клієнтських даних, таких як медичні або фінансові дані, використання нових хмарних можливостей створює унікальні

виклики, бізнес-ризики та ускладнення дотримання через архітектуру хмар. Заміна ідентифікованих даних на зашифроване значення звужує можливу експозицію конфіденційних даних і може значно зменшити обсяг аудиту та витрати на дотримання вимог.

■ Захист даних у реальних виробничих системах: організації зберігають та обробляють конфіденційні дані в деяких виробничих додатках, базах даних систем. Ці системи, як правило, відстають від засобів управління інфраструктурою та мережею, таких як брандмауери, списки контролю доступу та системи моніторингу активності баз даних гарантують, що зловмисники не мають доступу до реальних персональних даних дані, коли ці засоби контролю безпеки будуть взломані. Тільки вибрані та авторизовані програми, авторизовані користувачі мають можливість розшифрувати дані для використання в режимі реального часу. Інші програми працюють із зашифрованими даними Voltage FPE для зменшення атаки щодо отримання конфіденційних персональних даних в межах інфраструктури підприємства, знижуючи ризик організації.

■ Системи розробки та тестування: генерування даних для середовищ розробки та тестування представляє серйозні проблеми для корпоративної безпеки та управління ризиками. Коли дані копіюються з виробничих баз даних і використовуються, великі обсяги приватних даних накопичуються на незахищених серверах та робочих станціях. піддаючи підприємство непотрібному ризику. Служби забезпечення та розвитку якості послуг, що передаються сторонніми або офшорними компаніями, ще більше посилюють ці ризики. Тривожна кількість порушень даних, поряд із вимогами дотримання нормативних вимог, таких як GDPR, підкреслюють необхідність деідентифікації конфіденційних даних при переході від виробництва до випробування, середовища розробки та навчання. Передача зашифрованих даних у ці системи захищає конфіденційні дані від втрати та крадіжки [5].

2.2. Технології захисту персональних даних за допомогою шифрування та псевдонімізації

Існує ряд технічних міркувань для організацій, які прагнуть захистити персональні дані за допомогою шифрування та псевдонімізації. Збереження формату Voltage шифрування організації, які прагнуть дотримуватися GDPR, можуть зберігати та обробляти конфіденційні особисті дані в різних базах даних, додатках та системах протягом декількох років, якщо не десятиліть [4-5].

Шифрування структурованих відформатованих полів, таких як імена клієнтів, національні ідентифікаційні номери, номери паспортів, номери телефонів, місцезнаходження GPS та дати народження вимагали б значних схем бази даних та змін додатків для розміщення захищених даних у новому форматі. Потім потрібно розшифрувати дані для кожного аналізу та використання, зменшуючи загальну безпеку та нав'язуючи додаткові витрати на управління ключами. Voltage FPE є фундаментальним нововведенням, що дозволяє платформі Voltage SecureData, орієнтоватися на дані, щоб забезпечити високий рівень шифрування даних. Технічні властивості даних, зашифрованих Voltage Hyper FPE, включають:

■ Зберегти формат і структуру;

■ Зберігати логічну структуру даних, таку як контрольна сума, термін дії;

■ Зберігати часткові нечутливі значення в зашифрованих полях (часткові поля);

■ Зберігати зв’язки з іншими полями та посилену цілісність, де це необхідно;

■ Зберігати значення в даних та робити взаємозв’язки даних між записами, щоб зберегти аналітичне значення.

Ці властивості дозволяють програмам, аналітичним процесам та базам даних використовувати захищені дані для переважної більшості випадків використання, навіть у розподілених системах, платформах та інструментах. Захист застосовується на рівні поля або часткового поля, залишаючи нечутливі

частини полів доступними для додатків, одночасно захищаючи чутливі частини. Voltage FPE може, якщо це потрібно, зберігає у посиланнях цілісність у наборі даних, щоб захищені дані могли послідовно посилатися на них та об'єднуватись. Це особливо важливо, коли загальні ідентифікатори, такі як телефонні номери або ідентифікатори, використовуються як посилання на різні набори даних.

Voltage FPE відповідає стандарту AES-FF1 відповідно до стандарту FIST NIST SP-800-38G. Це забезпечує підприємствам впевненість у підтвердженнях безпеки та стандартах, що лежать в основі Voltage Hyper FPE [4-5].

В якості технології шифрування використовується відповідно стандарту структура Фейстеля.

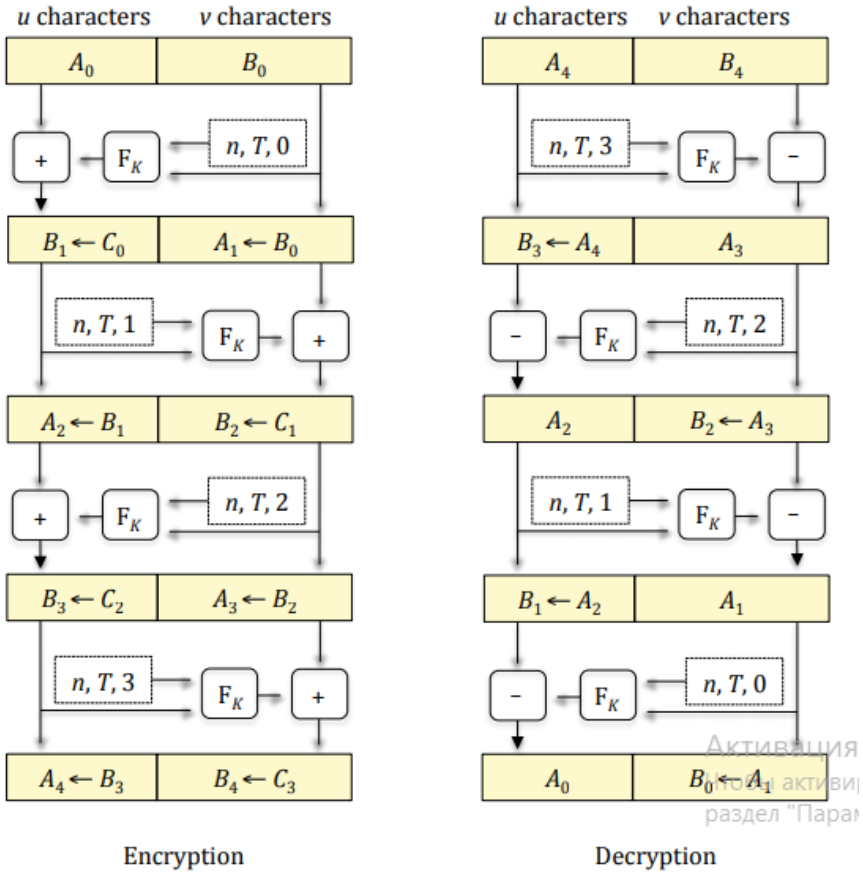

Рис.2.1. Структура Фейстела

Схеми FFX, включаючи FF1 та FF3, базуються на структурі Фейстеля. Структура Фейстела складається з декількох ітерацій, званих раундами, оборотного перетворення. Перетворення складається з трьох етапів: 1) дані

поділяються на дві частини; 2) ключова функція, яка називається раунд функція, застосовується до однієї частини даних, щоб змінити іншу частину даних; і 3) ролі двох частин поміняні на наступний раунд. Структура проілюстрована на рис.2.1 нижче, як для шифрування, так і для дешифрування. На рисунку показано чотири раунди, але насправді вказано десять раундів для FF1 та вісім раундів для FF3.

Масштабування за допомогою управління ключами

Оскільки організації захищають безліч програм і конфіденційних персональних даних за допомогою шифрування, вони стикаються збільшення проблем із масштабуванням їхніх систем управління ключами з використанням традиційної системи управління ключами шифрування, які зберігаються у внутрішній базі даних або сховищі, що спричиняє проблеми з масштабованістю, резервним копіюванням та аварійним відновленням. При роботі з шифруванням у гетерогенних системах та кількох місцях, традиційні системи управління ключами, що базуються на сховищах, вимагають постійного резервного копіювання, синхронізації та захисту, що є обтяжливим, і саме по собі підвищує ризики безпеки та відповідності.

Для безпечного отримання, якщо потрібно, без зберігання та управління базами даних синхронізація та резервне копіювання баз даних не потрібні, мінімізуючи ризик втрати ключів. Керування ключами інтегрується з існуючою інфраструктурою управління при ідентифікації, таких як зовнішні каталоги LDAP. Дозвіл на дешифрування може включати в себе ролі та групи користувачів для спрощення управління на основі політик системи управління ідентифікацією. Рольовий доступ до даних на рівні поля надає додаткам і користувачам можливість перегляду і використовувати лише ті дані, на які вони мають право доступу. Спрощена реалізація та високопродуктивна, масштабована розподілена обробка Voltage Stateless Key Management добре поєднується з сучасними архітектурами додатків.

Підтримка різних типів платформ

Клієнти, які шукають відповідність вимогам GDPR, мають конфіденційні персональні дані на різних платформах та системах, зокрема:

■ Такі платформи, як Windows, Linux, HP-UX, Solaris, AIX та інші;

■ Бази даних, такі як Oracle, DB2, Microsoft SQL Server та інші;

■ Критично важливі платформи, такі як z / OS, HPE NonStop, віртуальна операційна система Stratus (VOS), і інші;

■ Платформи зберігання даних, такі як Teradata, Micro Focus Vertica та провідні дистрибутиви Hadoop;

■ Хмарні платформи, такі як Amazon Web Services та Microsoft Azure;

■ Мобільні пристрої на базі iOS та Android.

Ці дані також передаються в різних системах за допомогою інструментів вилучення, перетворення та завантаження (ETL - through extract, transform, and load) такі як NiFi, Sqoop, Informatica, IBM DataStage та Microsoft Server Integration Services (SSIS). Сучасні організації також проводять аналіз цих даних, використовуючи широкий спектр інструментів бізнес-аналітики.

Головна перевага Voltage Hyper FPE як технології захисту на рівні поля полягає в тому, що дані можуть бути захищені за допомогою сильного шифрування, як тільки вони захоплені, а потім дані залишаються захищеними у стані спокою, в русі та під час використання. Дуже важливо, щоб організація, яка планує використовувати шифрування для дотримання вимог GDPR, розглядала рішення, що забезпечують відповідну підтримку шифрування та дешифрування на найширшій кількості платформ і систем які вони використовують.

Format Preserving Encryption або FPE - це алгоритм шифрування, zrbq використовується для збереження формату відкритого тексту, поки він залишається зашифрованим. Однак сила FPE нижче в порівнянні з AES. Однак FPE є важливим механізмом для шифрування даних зі збереженням довжини даних. FPE гарантує, що, поки дані залишаються зашифрованими, всі програми, програми бази даних працюють в захищеному режимі.

Визначимо що таке шифрування зі збереженням формату.

Якщо компанія має кілька 16-значних номерів кредитних карт, що зберігаються в базі даних, то зашифрований текст повинен бути також 16-значним

після шифрування, саме для цього використовується шифрування зі збереженням формату [FPE].

FPE шифрує відкритий текст певної довжини і створює зашифрований текст тієї ж довжини, що і відкритий текст, і використовує той же набір значень, що і відкритий текст. Використовуючи попередній приклад 16-значного номера кредитної карти з відкритим текстом 1483920193402918, зашифрований текст, створений за допомогою FPE, може дати на виході таке значення 1483666666662918.

Таким чином, використовуючи FPE, можна побачити, що зашифрований і відкритий текст мають однакову довжину і для шифрування використовуються тільки числові значення. Одним з хмарних провайдерів, який дозволяє користувачам впроваджувати FPE свого шифрування, є Google Cloud, Micro Focus та інші компанії які впроваджують методи захисту персональних даних.

Таке шифрування надає користувачам доступ до методу деідентіфікації, який називається псевдонімізація. Псевдонімізація - це метод, при якому конфіденційні дані замінюються криптографически згенерованими токенами. Існують три різни способами псевдонімізації:

- Детерміноване шифрування з використанням AES-SIV;
- Шифрування зі збереженням формату;
- криптографічне хешування.

Усі три методи використовують криптографічні ключі для перетворення даних.

Рис. 3.1 Результат при використанні FPE шифрування.

2.3. Архітектура рішення Voltage SecureData

Архітектура рішення Voltage SecureData, як правило, розгортається у два шари:

■ Рівень 1: Віртуальні прилади Voltage SecureData підтримують автентифікацію, авторизацію, управління ключами, управління політиками та інтеграцію з модулями апаратного захисту для зберігання апаратного ключа. Цей рівень забезпечує безпеку та подвійні контрольовані веб-інтерфейси для управління, моніторингу, аудиту та експлуатація розгорнутого рішення Це дозволяє централізовано управляти політикою формату даних для шифрування та токенізації даних, контролю автентифікації та авторизації, а також центральний аудит та моніторинг модулів рівня 2.

■ Рівень 2: Цей рівень включає низку гнучких і простих у використанні контрольованих політикою інтерфейсів прикладного програмування (API), інструментів командного рядка, інструментів обробки файлів, бази даних та визначених користувачем функцій, які можна використовувати для шифрування або маркування. Ці інструменти доступні на ряді платформ і працюють для

Windows, Linux, AIX, HP-UX, Solaris, різних дистрибутивів Hadoop, Teradata, Micro Focus Vertica, z / OS, HPE NonStop та Stratus VOS.

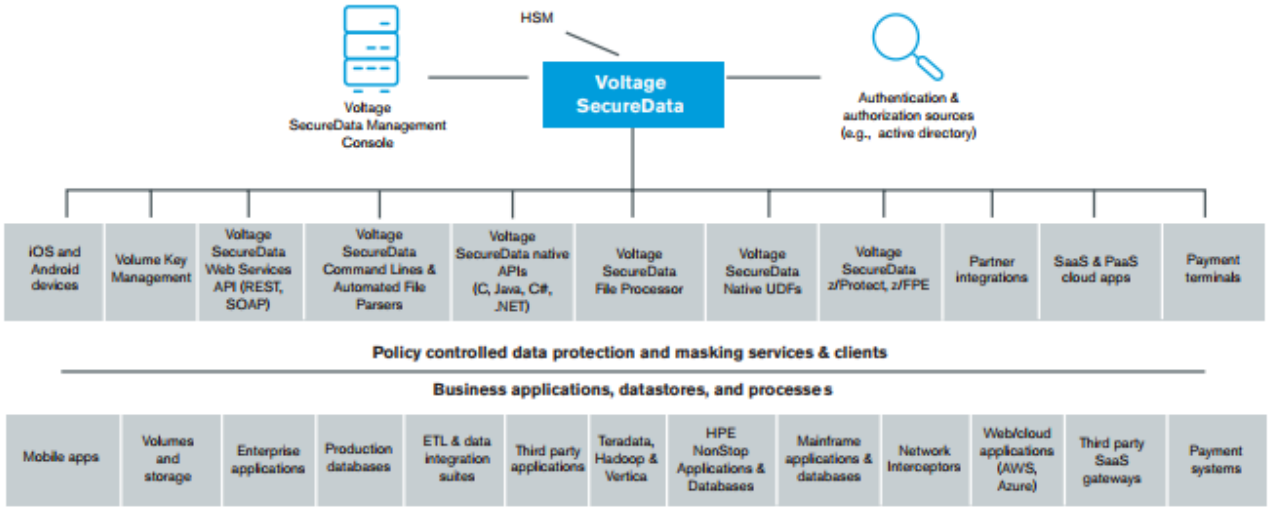

Рис. 2.2. Архітектура рішення Voltage SecureData

Voltage SecureData підтримує різні платформами та широка кількість варіантів інтеграції, що дозволяє клієнтам виконувати вибірково шифрування та дешифрування, як вимагають бізнес-процеси та додатки. За допомогою Voltage FPE, зберігається значення та логіка в даних, реалізація їх спрощена оскільки більшість додатків та процесів можуть працювати з використанням зашифрованих даних, тому реалізація рішення не вимагає змін програми або процесу у переважній більшості випадків. Це значно спрощує розгортання порівняно із традиційним шифруванням даних, де інтеграція та управління ключами є складним процесом.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІТ-СИСТЕМІ

3.1. Варіанти розгортання системи, які забезпечує захист персональних даних та GDPR

Розглянемо архітектурні приклади: збереження формату Voltage Шифрування та GDPR

Велика європейська телекомунікаційна служба використовує деідентифікацію записів дзвінків у Hadoop для "безпечного аналізу".

Даний європейський оператор збирає величезні масиви даних від своїх абонентів мобільного зв'язку в ряді європейських країн. Дані переміщуються до центрів обробки даних у Німеччині та Італії для аналізу в 140-вузловах Hadoop кластеру. Оператор планує обробляти понад 11 мільярдів записів щодня.

Основні потреби бізнесу полягають в:

■ Захисті масивних наборів даних, включаючи записи контактів, місцезнаходження, IMEI, IMSI, дані абонентів, програми, текст, дані дзвінків та інші особисті дані;

■ Дотримці місцевих законів про збереження даних з багатьох країн та GDPR;

■ Застосуванні FPE до персональних даних, підключених з різних європейських точок присутності, щоб відповідати нормам щодо збереження даних та GDPR, зберігаючи при цьому можливість аналізувати дані для виявлення шахрайства з доступом, отримання інформації про шаблон користувача та налагодження сценаріїв несправності мережі.

Рішення щодо дотримання вимог:

Оператор використовує схвалений NIST Voltage FPE як технологію для псевдонімізації персональних даних у записах викликів перед їх аналізом у Hadoop. Компоненти, розгорнуті як частина цього рішення, п:раедставлені як (рис.3.1):

1. Ключові сервери Voltage SecureData: Ці сервери використовують технологію керування ключами без Voltage з їхніх центрів обробки даних у Німеччині та Італії. Архітектура Voltage SecureData дозволяє цим серверам розміщуватися в окремих ключових юрисдикціях. Наприклад, це гарантує, що дані, що обробляються в Німеччині, захищені ключами, сформованими в Італії, тому державний орган при вилученні даних не може захопити сервери ключів, необхідні для ідентифікації цих даних.

2. Файловий процесор Voltage SecureData в зоні розгортання: Багато архітектур Hadoop розгортають зону розгортання, де вхідні дані попередньо обробляються, форматуються та нормалізуються перед потраплянням у HDFS 2.

Оператор розгортає інструмент обробки файлів Voltage SecureData на серверах у своїй зоні для виконання FPE щодо персональних даних у файлах перед зберіганням у Hadoop. Інструмент обробки файлів Voltage SecureData шифрує чутливі поля в структурованих файлах різних форматів, включаючи, але не обмежуючись XML, JSON, розділеними записами та інше.

3. API Voltage SecureData, інтегровані в Apache Spark: Оператор використовує Apache Spark для швидкої обробки даних у пам’яті, оскільки вони потрапляють у Voltage FPE як в Hadoop.

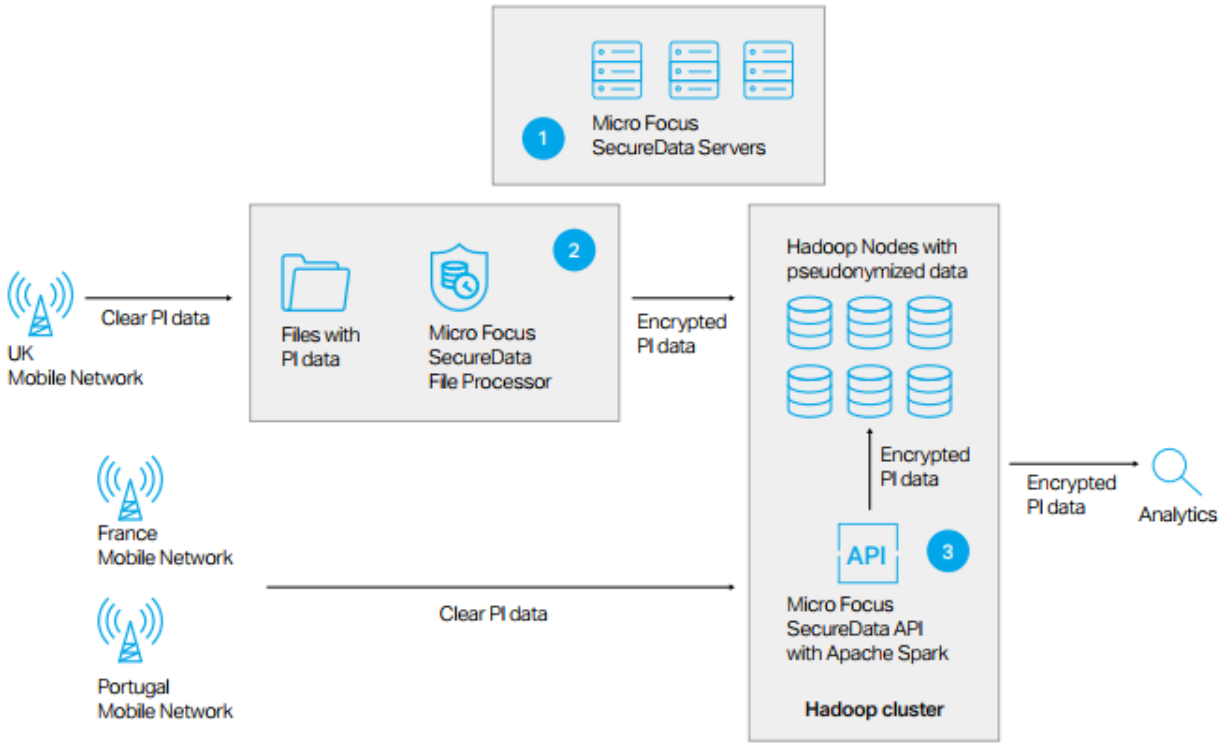

Рис 3.1. Архітектура де-ідентифікації даних у Hadoop

Використання Voltage FPE гарантує цілісність посилань і дозволяє псевдонімізованим даним зберігати свої характеристики, такі як довжина та тип даних. Оператор виконує весь їх аналіз на псевдонімізованих даних, не вимагаючи деідентифікації даних до їх початкової форми.

Визначимо переваги від такої архітектури

Розгортання Voltage SecureData забезпечило оператора зв'язку низку переваг, зокрема:

■ Захист їх найцінніших та вразливих систем, таких як данні Hadoop;

■ Порушення в системи Analytics більше не викривають особисті дані та не викликають вимог щодо сповіщення;

■ Дотримання європейських норм про зберігання даних, включаючи GDPR;

■ Єдина масштабована платформа корпоративного рівня, яка використовується для захисту конфіденційних персональних даних в інших платформах та системах. Глобальний бренд картки: Шифрування даних для переміщення в хмару

Розглянемо архітектуру на прикладі з використанням хмар:

Бренд глобальних карт переміщує низку програм до загальнодоступної хмари Azure, щоб зменшити витрати та пришвидшити час виходу на ринок, надаючи гнучкі стратегії розвитку.

Ця програма для аналізу транзакцій була написана мовою NET і використовувалась багатьма підрядниками, створюючи проблеми з безпекою та витратами, пов'язаними з наданням доступу до мережі торгової марки карток.

Переміщення даних у відкриту хмару може спричинити низку ризиків, включаючи можливість порушення даних та потенційне порушення дотримання норм, включаючи GDPR.

Потреби бізнесу для переходу в хмару:

■ Підтримка широкомасштабної гібридної інфраструктури із поєднанням застарілих, корпоративних та хмарних платформ. Підтримка операційних систем, таких як z / OS, Windows, Linux, HPE NonStop та платформ баз даних, таких як Oracle, Microsoft SQL та DB2. Підтримка платформ зберігання даних, таких як Teradata, та платформ зберігання та обробки, таких як Hadoop.

■ Швидкий захист даних від певних програм, коли вони переміщуються до хмари;

■ Масштабований захист мільярдів особистих даних у сотнях програм, що збирають, зберігають та обробляють персональні дані.

Рішення щодо забезпечення безпеки:

Global Card Brand розгорнув Voltage Hyper FPE для захисту даних під час їх переміщення в архітектуру хмари розгорнутій у рішенні показано не рис. 3.2 та заключено у:

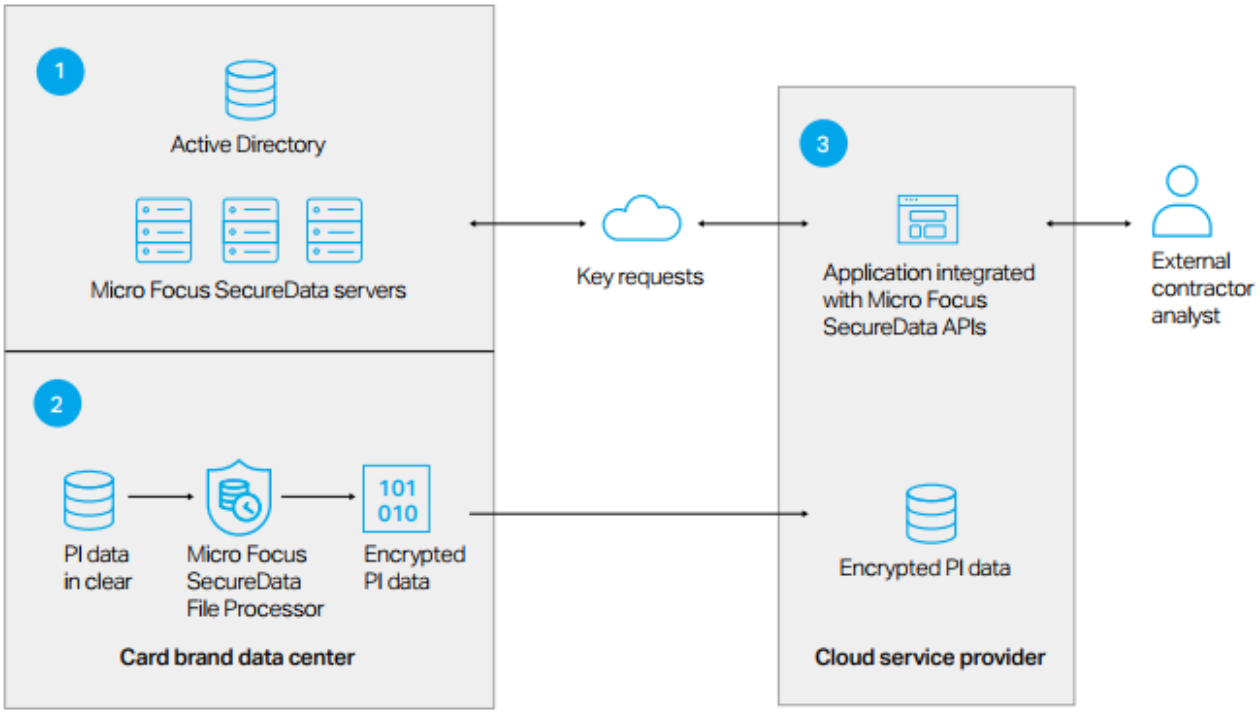

Рис.3.2. Шифрування даних в хмарній інфраструктурі

1365 / 5000

Результати перекладу

1. Сервери ключів Voltage SecureData: Глобальна інфраструктура серверів ключів напруги SecureData із збалансованим навантаженням з використанням системи керування ключами без Voltage була розгорнута в мережі торгової марки Global Card Brand. Розгортання локальних серверів дозволило забезпечити повний контроль ключів шифрування в будь-який час, що задовольняється створеною кількістю внутрішніх політик безпеки та зовнішніх вимог регулювання та дотримання вимог.

2. Міграція даних додатків до хмари: програми, які переміщуються до загальнодоступної хмари, мали значний обсяг персональних даних у базах даних. Файл-процесор Voltage SecureData та інструменти командного рядка використовувались для перетворення особистих даних із чистої форми у зашифровану форму. Ця інтеграція була виконана за допомогою пакетних сценаріїв із набором інструментів ETL.

3. Інтеграція хмарних додатків з API Voltage SecureData: Транзакція картки на основі NET додатоку аналітики було інтегровано з API Voltage SecureData для

виконання рольового дешифрування персональних даних за потреби аналітиків. API Voltage SecureData використовує зворотний зв'язок із ключовими серверами, розміщеними у внутрішній інфраструктурі системи, для завантаження ключів для дешифрування. Кожен дзвінок автентифікується за допомогою корпоративної інфраструктури Active Directory системи. Усі ключові запити та відповіді реєструються централізовано для попередження та звітування.

Розгортання Voltage SecureData забезпечило ряд переваг для Global Card Brand:

■ Миттєвий захист даних у певних програмах із можливістю масштабування;

■ Легко переміщує кілька десятків програм у хмару із значною економією засобів та коштів;

■ Відповідність внутрішнім стандартам безпеки та зовнішнім правилам, таким як GDPR.

Це розгортання Voltage SecureData було розширено до понад 130 програм в рамках інфраструктури системи. До них належать програми, розгорнуті на мейнфреймових платформах, сховищах даних та Hadoop, а також ряду розподілених операційних систем.

3.2. Розробка рекомендацій щодо забезпечення захисту даних в IT системах

Українські підприємці можуть продовжувати співпрацювати з Європейськими компаніями з дотриманням норм регламенту захисту Даних (GDPR) Євросоюзу та Закону України «Про захист персональних даних» без загрози отримати багатомільйонний штраф за порушення норм. Для цього необхідно:

1. Дотримуватись прав користувачів при роботі з персональними даними:

- Ключовою вимогою GDPR - збір персональних даних користувачів можна проводити тільки з чіткою и конкретною метою. в іншому випадки, обробка даних буде вважатися незаконною.
- Підприємці можуть збирати тільки необхідні дані.
- Необхідно отримати дозвіл користувачів в цифровому вигляді на обробку їхніх даних для конкретної мети. Як тільки мета досягнута, дані слід видалити відповідно до принципу обмеженого в часі зберігання.
- Користувачі мають право робити запити щодо своїх персональних даних, з метою дізнатися мету їх обробки. Компаніям необхідно відповісти на запит протягом 30 днів.
- Користувачі також мають право вимагати видалити їхні дані або оскаржити обробку даних в судовому порядку, отримавши компенсацію.

2. Необхідно впровадити технічні та організаційні заходи.

- Технічні заходи припускають технічну діагностику процесів збору і зберігання даних, впровадження методів та засобів псевдонімізацію та шифрування даних.

- Організаційні заходи складаються з :

- записи оброблених даних (документування інформації про компанії, процеси збору даних і користувачів);
- введення посади спеціального Data Protection Officer (DPO, директора з питань захисту даних).

ВИСНОВКИ

Дотримання вимог щодо захисту персональних даних є важливим питанням для компаній які зберігають, оброблюють та передають їх в своїх IT системах. Таким чином в магістерській роботі отримано наступні результати:

Проведено аналіз сучасних загроз, які притаманні при роботі з персональними даними.

Проведено аналіз вимог нормативної бази щодо захисту персональних даних згідно положень Закону України «Про захист персональних даних» де надано рекомендації щодо використання персональних даних.

Проведено аналіз вимог нормативної бази щодо захисту персональних даних згідно регламенту про захист персональних даних General Data Protection Regulation, який спрямований на те, щоб дати громадянам контроль над своїми персональними даними та спрощення нормативної бази для міжнародних економічних відносин шляхом уніфікації регулювання в рамках ЄС. В результаті аналізу визначено основні питання та особи, які повинні бути відповідальними за забезпечення безпеки персональних даних.

Для визначення основних підходів та змісту персональних даних визначено вдорівневу архітектуру. Дана архітектура забезпечує управління, процедури та передачу даних, яка повинна забезпечити стратегію захисту даних в IT системі.

В результаті дотримання вимог щодо шифрування даних було досліджено шифрування Voltage FPE на основі платформи Voltage SecureData, яке дозволяє працювати з персональними даними зі збереженням формату та забезпечить захист даних, який відповідає стандарту NIST SP-800-38G.

В результаті виконання роботи було запропоновано варіанти розгортання системи, які забезпечують захист персональних даних та GDPR.

Як практичне значення одержаних результатів було надано рекомендації щодо з надано рекомендації щодо роботи з персональними даними в інформаційних системах.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закону України «Про захист персональних даних» [Електронний ресурс] – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/ed_2010_06_01/T102297.html .

2. NIST SP-800-38G [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf .

3. Топ 10 питань захисту персональних даних [Електронний ресурс] – Режим доступу: https://ecpl.com.ua/news/top-10-pytan-u-sferi-zakhystu-personal-nykh-danykh/.

4.Особливості GPDR [Електронний ресурс] – Режим доступу: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/gdpr.pdf.

5. Рекомендації дотримання персональних даних від Gartner [Електронний ресурс] – Режим доступу: https://www.gartner.com/smarterwithgartner/ready-guide-to-gdpr/ .

6 Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf .

7.Безпека персональних даних від Voltage SecureData [Електронний ресурс] – Режим доступу: https://www.microfocus.com/media/data-sheet/voltage_securedata_security_ds.pdf.

8. Архітектура Voltage-Securedata [Електронний ресурс] – Режим доступу: https://ohmag.net/voltage-securedata-simplifies-data-protection-and-drives-value-for-the-enterprise/.

9. Технологій захисту персональних даних [Електронний ресурс] – Режим доступу: https://www.forbes.ru/tehnologii/370635-zashchita-personalnyh-dannyh-novyy-rynok-dlya-startapov .

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)