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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо захисту конфіденційної інформації на основі Data Security Manager Fortanix»

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

_____ Дмитро КИРІЄНКО
(підпис)

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

Керівник ЧУМАК Надія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент д.е.н., проф.ЛЕГОМІНОВА Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard

BYOK – Bring Your Own Key

CSE – Client-Side Encryption

DRA – data risk assessment ()

DSM – Data Security Manage

DSPM – Data security posture management

EDR – Endpoint Detection and Response

EPP – Endpoint Protection Platform

GDPR – General Data Protection Regulation

HSM – апаратний модуль безпеки

PHI – Protected health information

PII – Personally identifiable information

RBAC – Role Based Access Control

SIEM – Security Information and Event Management

ВСТУП

Актуальність дослідження.

Кожна організація має справу з конфіденційною інформацією, яка потребує захисту. Коли ці дані потрапляють у чужі руки, наслідки виходять за рамки негайного фінансового впливу та стосуються довгострокової шкоди репутації та санкцій регуляторних органів.

Захист конфіденційної інформації є фундаментальною відповідальністю кожної організації. Впроваджуючи найкращі практики, включаючи надійні протоколи безпеки даних, навчання співробітників, програмне забезпечення для шифрування та обмеження доступу, компанії можуть значно знизити ризик витоку даних та захистити свою репутацію й фінансове благополуччя. Регулярний перегляд та оновлення заходів безпеки, проведення аудитів та пильність щодо нових загроз забезпечать постійний захист даних та збережуть довіру клієнтів у дедалі цифровому світі.

Зі зростанням поширених загроз, таких як фішингові атаки та шкідливе програмне забезпечення, розуміння того, як ефективно реагувати на порушення безпеки, є надзвичайно важливим. Впровадження методів та засобів, як ефективні рішення для захисту конфіденційної інформації є головним аспектом для організацій, які хочуть зменшити ризики несанкціонованого отримання інформації.

Організаціям важливо звернути увагу на те, що конфіденційна інформація може бути у різних станах. Це стани коли інформація оброблюється, передається та зберігається.

Отже, важливим є захистити конфіденційну інформацію протягом усього свого життєвого циклу. Тому дана робота буде присвячена дослідженню методів та засобів захисту конфіденційної інформації та розробці рекомендацій, які дозволять сфокусуватися фахівцям над проблемою захисту інформації.

Об'єкт дослідження – захист конфіденційної інформації організації.

Предмет дослідження – методи та засоби захисту конфіденційної інформації

організації на основі Data Security Manager Fortanix.

Мета роботи розробити варіант застосування методів та засобів захисту конфіденційної інформації організації на основі Data Security Manager Fortanix та рекомендації щодо їх застосування.

Наукові завдання:

дослідити сутність проблеми захисту конфіденційної інформації;

проаналізувати основні захисту конфіденційної інформації;

проаналізувати існуючі рішення захисту конфіденційної інформації;

проаналізувати методи та засоби захисту конфіденційної інформації організації на основі Data Security Manager Fortanix;

запропонувати варіант застосування методів та засобів захисту конфіденційної інформації організації на основі Data Security Manager Fortanix;

розробити рекомендацій щодо застосування методи та засоби захисту конфіденційної інформації організації.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методи та засоби захисту конфіденційної інформації організації на основі Data Security Manager Fortanix, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ

1.1. Аналіз проблеми захисту конфіденційної інформації

Поняття конфіденційність входить до моделі розробки системи кібербезпеки і має назву «Тріада кібербезпеки». Це модель, яка використовується для представлення трьох основних принципів кібербезпеки: конфіденційності, цілісності та доступності [1].

Рис. 1.1. Тріда кібербезпеки CIA [1]

Конфіденційність обмежує доступ до конфіденційної інформації компанії, цілісність гарантує, що дані та обладнання компанії залишаються надійними та точними, а доступність забезпечує своєчасний доступ до даних та обладнання компанії. Іноді до тріади кібербезпеки додають інші атрибути, такі як конфіденційність і безпека, але це загальновизнані основні принципи, і це те, на що потрібно звернути увагу всім, хто працює в організаціях.

Конфіденційність

У тріаді CIA конфіденційність стосується обмежень, встановлених для доступу до інформації, подібно до того, що ми зазвичай розуміємо як конфіденційність. Ці заходи призначені для захисту конфіденційних даних від спроб несанкціонованого доступу, а також від розголошення (навмисного чи випадкового) особам без необхідного дозволу. Правильно розуміючи різний вплив потенційних порушень даних на бізнес, можна відповідним чином визначити конфіденційність і вжити заходів для збереження найбільш конфіденційних даних із найвищим пріоритетом.

Цілісність

Цілісність означає точність, послідовність і достовірність даних організації протягом усього життєвого циклу, від створення до знищення, з надійним аудиторським слідом, якщо це необхідно. Основне занепокоєння щодо цілісності даних полягає в забезпеченні того, щоб вони не змінювалися протягом життєвого циклу особами без авторизації, тому структура CIA прагне встановити пріоритет для належного зберігання даних, щоб вони могли вийти з організації точно так, як вони ввійшли, за винятком випадків узгоджених, відповідних і каталогізованих змін, внесених всередині.

Доступність

Вирішальний елемент для аудиту та відповідності, доступність говорить про те, що дані та інформація легко, надійно та постійно доступні для тих сторін, які мають право переглядати та/або змінювати їх. Незалежно від того, чи є дані конфіденційними та зберігаються в суворій цілісності, якщо до них неможливо отримати доступ за бажанням, можуть виникнути прогалини в безпеці. Щоб забезпечити доступність, пов’язане апаратне забезпечення та інфраструктура повинні підтримуватися як пріоритет, маючи на увазі практичні випадки використання.

Конфіденційна інформація у сучасному інформаційному суспільстві є одним з головних і найцінніших активів організацій.

Комерційні секрети, ноу-хау, бази даних клієнтів, маркетингові стратегії – все це є основою конкурентної переваги та успішного розвитку бізнесу. Ось чому

захист інформації та інтелектуальної власності є надзвичайно важливим для будь-якої організації, незалежно від її розміру чи галузі.

Витік комерційної таємниці може призвести до катастрофічних наслідків, включаючи втрату прибутку, збиток репутації, зниження конкурентоспроможності та навіть банкрутство. Ризики витоку інформації зростають із розвитком технологій, зростанням кількості кібератак та нечесної конкуренції.

В інформаційній безпеці конфіденційність, цілісність і доступність є найважливішими. Незалежно від того, чи вирішить організація використовувати структуру тріади CIA як засіб для досягнення надійних і безпечних практик інформаційної безпеки, це міркування, які всі підприємства повинні мати на передньому плані, щоб гарантувати, що дані обробляються делікатно, безпечно та відповідно до відповідних нормативних і нормативних вимог.

Тріада CIA також є корисною лінзою, через яку можна розглядати поточну оптимізацію кібербезпеки, класифікуючи постійні службові завдання за відповідними областями, щоб зробити завдання керованим і ефективним.

Її також можна використовувати під час впровадження нових технологій і рішень, спонукаючи до аналізу того, де нові інвестиції в ці три основні сфери інформаційної безпеки додають користь, а також чи зможуть нові інструменти працювати злагоджено з існуючими продуктами для підтримки безпеки даних організації.

Розуміння того, що вважається конфіденційною, є першим кроком до захисту конфіденційної інформації. Конфіденційна інформація зазвичай включає:

Персональна інформація (PII) , така як імена, номери соціального страхування, адреси, облікові дані для входу та дані геолокації.

Захищена медична інформація (PHI) , така як медичні записи , рецепти, історії лікування та дані страхування.

Юридична документація , включаючи повідомлення клієнтів, угоди про врегулювання, судові документи та протоколи розслідувань.

Конфіденційні бізнес-дані , такі як фінансові записи, комерційні таємниці та внутрішні стратегічні документи.

Згідно з останнім звітом Cybersecurity Insiders про інсайдерські загрози за 2024 рік [3], 83% організацій повідомили про принаймні одну інсайдерську атаку за останній рік. Ще більш дивовижним, ніж ця статистика, є те, що організації, які зазнали 11-20 інсайдерських атак, у 2023 році зросли в п’ять разів у порівнянні з кількістю атак, здійснених ними, — лише з 4% до 21% за останні 12 місяців.

Кількість випадків внутрішньої загрози значно зросла з року в рік: 48% респондентів повідомили, що стикаються з набагато більш поширеною проблемою лише за останні 12 місяців. Переглядаючи причини цієї ескалації, Cybersecurity Insiders змогли звузити чотири основні проблеми, які є винуватцями [3]:

Складні IT-середовища: підтримка моделей віддаленої та гібридної роботи, на додаток до широкомасштабного впровадження хмарних технологій сучасними компаніями, створила складніші операційні структури, якими важче керувати та контролювати [3].

Неадекватні заходи безпеки: багатьом підприємствам важко бути в курсі найновіших найкращих практик безпеки та досі покладаються на застарілі протоколи для захисту своїх цифрових активів [3].

Відсутність навчання та обізнаності співробітників: не всі внутрішні загрози є зловмисними. Насправді більшість працівників просто недостатньо навчені, щоб усвідомлювати ризики, які вони можуть створити для бізнесу, водночас відіграючи активну роль у запобіганні внутрішнім загрозам [3].

Слабка політика забезпечення: хоча 93% респондентів у звіті сказали, що сувора видимість і контроль є для них важливим фактором, лише 36% насправді мали ефективне рішення для уніфікованої видимості та контролю доступу [3].

Розглянемо основні ризики та вектори атак, які можуть призвести до витоку інформації [2].

Відповідно до статистики користувачі інформаційної системи організації можуть стати саме тими, хто буде інсайдерами щодо витоку конфіденційної інформації. Відповідно до досліджень, третина (33%) колишніх співробітників організацій стверджують, що вони все ще мають доступ до файлів з попередньої роботи [2]. Це показує, що все ще існують організації, які діють поверхнево.

Насправді, не було б дивно, якби ті самі компанії, які залишили доступ до колишніх співробітників, також інвестували великі суми грошей у гарні рішення кібербезпеки. Існує чотири ідентифікатори співробітників, які можуть бути внутрішньою загрозою, тобто здійснити внутрішню атаку на компанію, в якій вони працюють.

Насправді, коли ми говоримо про кібербезпеку, ми часто думаємо про те, як захистити компанію від зовнішніх загроз . Однак іноді буває, що ворог знаходиться вдома і, знаючи, як рухатися, діє спокійно, доки пошкодження не стане настільки серйозним, що стає очевидним. Як і коли злодії проникають у квартиру, сигналізація не дзвонить, якщо у них є ключі та відомі коди. Те саме стосується брандмауерів у системах кібербезпеки , які не активуються без порушення.

Крім того, може статися так, що співробітник, який допустив вторгнення, навіть не підозрює про те, що він зробив. Така неуважність пов’язана з відсутністю належної підготовки, а ресурс не розуміє ризиків певних дій в Інтернеті. Працюючи з відповідною інформацією, такою як патенти, стратегічні дані та персональні дані, дуже важливо навчати всіх співробітників тому, як з ними поводитися, навіть тих, хто має, здавалося б, безпечну роботу.

І снують такі випадки, коли, наприклад, непомітні співробітники вводяться в оману фішингом або шахрайством, через листи, які надходять до їхніх електронних скриньок. З іншого боку, більш серйозною є помста у формі кібератаки, під час якої звільнений ресурс у відповідь знищує інформацію або завдає незворотної шкоди системам. Отже, щоб захистити себе, необхідновиявляти характерні риси «працівників у масках».

На рисунку 1.2 показано чотири ідентифікатори ресурсів, які можуть становити ризик для компанії.

Інсайдер, що не помічає.

Забутий інсайдер не визнає цінності своїх даних і не розуміє важливості захисту паролем. Тому вони мають доступ до цінних бізнес-даних, але не знають, які обов’язки це створює. Ресурси, які керують цінними даними у фірмі, пройшли відповідне навчання, щоб не допускати помилок. Проблема виникає через те, що

працівники миттєво отримують доступ до даних, щоб знайти потрібну інформацію в іншому бізнес-контексті.

Приклад. Хтось керує базою даних, яка містить усі конфіденційні дані клієнтів. Той хто їх створив і знав цінність інформації, які там містяться. З іншого боку, комусь з працівників потрібен доступ до цієї бази даних лише для отримання адреси доставки, оскільки він працює у відділі логістики. Це хтось з працівників матиме ті самі доступи, що й той хто керує базою даних, щоб увійти в базу даних, і без належної підготовки міг би випадково записати їх на свій мобільний телефон. Якщо він втратить свій мобільний телефон, доступи можуть потрапити в чужі руки. Але ризики зростають, коли ми говоримо про звичайні дії, такі як платформи веб-пошти. Частота використання електронної пошти та те, що вона пов’язана з усією робочою діяльністю, робить її легкою мішенню як для внутрішніх, так і для зовнішніх кібератак.

Як це буває і в приватному житті, збитки від несвідомої поведінки можуть бути як легкими, так і дуже серйозними. Все залежить від того, наскільки добре компанія захищає свої цінні дані . Співробітники, які не звертають уваги, часто потрапляють у соціальну інженерію, тобто потрапляють у пастку, коли хтось запитує інформацію для входу в компанію через фальшиве повідомлення чи електронну пошту.

Загалом, коли у вас є інформація, якою з міркувань конфіденційності не можна керувати всередині, доцільно навчити не лише тих, хто повинен буде керувати нею, але й тих, хто повинен буде нею користуватися. Важливо також поінформувати своїх співробітників про ризики, пов’язані з IT-безпекою, з першого дня роботи в компанії, щоб забезпечити контроль колег.

Рис. 1.2. типи внутрішніх інсайдерів в організації

Недбалий інсайдер

Недбалими інсайдерами можуть бути ті, хто не пройшов відповідного навчання обробці даних, з одного боку, і ті, хто свідомо обходить контроль, щоб прискорити роботу, з іншого. Деякі процедури захисту даних вимагають кроків, які здаються непотрібними, але натомість служать для того, щоб двері не залишалися відкритими. Вибір не дотримуватися протоколів безпеки може призвести до набагато серйознішої шкоди, ніж ефективність, створена упущенням. Одна оцінка показала, що середня вартість, спричинена одним недбалим інсайдером, перевищує 300 000 доларів США.

Наприклад. Дівчина працює менеджером із соціальних мереж і використовує платформи для публікації та керування публікаціями в кількох профілях компанії. У рамках своєї повсякденної роботи дівчина вважає непотрібним щодня входити в систему (це забирає багато часу), тому вона зберігає свої облікові дані та вимикає двофакторну автентифікацію. З іншого боку, введення коду безпеки служить для ідентифікації особи, яка має доступ до платформи, запобігаючи небажаним вторгненням. Досить лише мить відволіктися, і будь-який інший співробітник може опублікувати повідомлення від імені компанії, зруйнувавши репутацію організації (а не працівника).

Недбалий інсайдер може дозволити іншим отримати доступ до даних компанії, просто не вийшовши з систем компанії. Або він може писати паролі в публічних електронних щоденниках, щоб скоротити час пошуку. Або він може використовувати неавторизовані пристрої та програми, які мінімізують робочий час, але піддають ризику IT-систему.

Насправді, недбалого інсайдера, порівняно з тим, хто не помічає, можна легше викрити, оскільки обхід протоколів безпеки викликає тривоги. Відстежуючи діяльність, що відбувається в компанії, можна вчасно помітити попередження та поговорити про це з постраждалим співробітником.

Зловмисний інсайдер

Зловмисник діє з помсти або перешкоджає колегам, які можуть вкрасти їхню роботу чи підвищення. У цьому випадку відплата є лише особистою, і є як розуміння, так і усвідомлення шкоди, яку вони завдають компанії. Зловмисний співробітник уже знає паролі та знає, як отримати доступ до відповідних даних, що дає йому можливість помститися.

Наприклад. Працівник є частиною дослідницької групи, яка працює над розробкою наступного мобільного телефону для відомого виробника телефонів. До його вух дійшли чутки, що його бос незадоволений і хоче звільнити його після закінчення цього проекту. Працівник негайно починає співбесіду, і з ним зв'язуються конкуренти. Однак під час інтерв'ю він промовчує дещо про проект, над яким працює.

Компанія грає брудно і гарантує майбутньому працівнику роботу та значне збільшення річної зарплати в обмін на конфіденційні дані проекту. Працівник погоджується і повертається в компанію. Після проекту, як і очікувалося, Працівник звільняють, але через кілька днів маркетингової кампанії з просування нового стільникового телефону компанія-конкурент виводить на ринок стільниковий телефон із такою ж продуктивністю. Завдяки пропозиціям Працівника, конкурент реалізував продукт вдвічі швидше, оскільки вони перейшли безпосередньо до фази проектування, пропускаючи фазу дослідження та розробки.

Ризики зі зловмисним інсайдером дуже високі, оскільки це свідома дія. Намір

полягає в завданні шкоди компанії через видалення, крадіжку або публікацію даних.

Коли звільняють співробітника, який працює з конфіденційними даними, багато великих компаній негайно повідомляють про це. Тобто в момент, коли людина отримує лист про звільнення, вона має піти. Залишити робочу станцію негайно потрібно саме для того, щоб тим часом не завдати шкоди. Загалом, коли звільнення відбувається без згоди обох сторін, завжди доцільно змінити доступи та заборонити доступ відповідної особи.

Професійний інсайдер

Тут розпізнавання стає більш складним, оскільки професійний інсайдер знає правила гри, знає, як рухатися, і знає, як пройти непоміченим.

Більше того, ставка втілення в життя такого детального та складного плану має бути дуже високою. Інсайдер, у цьому випадку, повинен буде уникати засобів контролю, призначених для захисту даних від внутрішніх і зовнішніх вторгнень . Зазвичай професійний інсайдер не діє швидко, але з часом нарощує позицію. Можливо, їх наймають або співпрацюють як сторонніх осіб. Вони намагаються завоювати довіру начальства та колег, а потім намагаються втілити план у життя. Відшкодування від цього не завжди є лише особистим, як у випадку зловмисного інсайдера. Часто дані чи інформація, які підлягають вилученню чи знищенню, надходять на замовлення компаній-конкурентів або злочинців, які працюють у темній мережі.

Професіонал може завдати значної шкоди, яку не завжди можна виправити. Прикладом може бути крадіжка патенту. Компанія, яка бажає імітувати продукт або послугу, що охоплюється інтелектуальною власністю, може надіслати інсайдера до конкурентів. Професіонал повинен мати доступ до вмісту патенту, щоб дозволити клієнту відтворити його з незначними змінами, щоб уникнути ризику плагіату.

Зазвичай найчастіші причини погроз з боку професіоналів стосуються крадіжки даних для продажу клієнту. Цю дію непросто викрити, оскільки особа може скопіювати інформацію, щоб не запускати тривоги чи змінювати параметри

безпеки.

Шанси виявити професійного інсайдера до того, як він вчинить злочин або завдасть значної шкоди компанії, низькі. Добре розроблений план нелегко зупинити. Тим не менш, чим більше вкладає організація в захист цінних даних, тим більше шансів зупинити атаку.

Отже, організаціям необхідно визначити підходи, щодо вирішення проблеми захисту конфіденційної інформації.

1.2. Аналіз підходів захисту конфіденційної інформації в організаціях

Епоха оцифрування дозволила організаціям зберігати дані своїх клієнтів без будь-яких часових обмежень. Декілька веб-сайтів, витягують усі види інформації з пристрою без нашого дозволу. Це призводить до набуття чинності суворих законів про захист даних через 7 принципів GDPR. Кожна країна розробила закони про захист даних на основі Загального регламенту захисту даних (GDPR) Європейського Союзу.

Європейський Союз запровадив GDPR у 2018 році. Закон GDPR покликаний захистити персональні дані громадян. Організації, які задовольняють потреби громадян ЄС, вимагають схвалення клієнтів перед тим, як збирати їхні дані. Крім того, компанії повинні бути прозорими зі своїми клієнтами під час використання їхніх даних. Регламент базується на наборі принципів, якими керується організація щодо законодавства про захист даних.

Раніше Закон про захист даних 1988 року базувався на восьми принципах. Еволюція інформаційних технологій призвела до уточнення цих восьми принципів і скорочення їх числа до 7. Давайте глибше зрозуміємо ці принципи та визначимо їхнє значення.

Рис.1.3. Сім принципів GDPR

Законність, справедливість і прозорість

Цей принцип GDPR наголошує на законному зборі інформації, її використанні згідно з обіцянками та дотриманні прозорості. Законність також вказує на те, що дані отримані за згодою або через договір тощо. Справедливість стверджує, що зібрані дані мають оброблятися згідно з обіцянками клієнту. Прозорість життєво важлива для людей, оскільки вона допомагає їм зрозуміти свої права на захист даних і надати відповідну згоду.

Обмеження мети

Організації, які збирають персональні дані, повинні чітко повідомити, як ці дані обробляються разом із метою. Отримавши згоду, компанії не можуть змінити мету, для якої були зібрані дані. Цей принцип GDPR демонструє, що організація може обробляти зібрані дані лише з метою, розкритою клієнтам. Якщо зібрані дані потрібні для іншої мети, компанії повинні отримати схвалення окремих осіб.

Мінімізація даних

Цей принцип GDPR визначає, що зібрані дані мають бути достатніми та відповідними. Закон вимагає від підприємств обґрунтування зібраних даних разом із необхідною документацією. Організаціям, які збирають дані про громадян ЄС, дозволяється збирати лише первинні дані громадян для досягнення зазначених цілей. Якщо якась організація помічає перевищення ліміту збору даних, це вважається порушенням регламенту. Крім того, закон заохочує бізнес виконувати свої вимоги без збору персональних даних.

Точність

Принцип точності GDPR вимагає від компаній підтримувати актуальну інформацію про осіб. Володіння нерелевантною інформацією про осіб надалі вважається порушенням положення. Такі дані мають бути видалені з бази даних організації. Підприємства, яким часто потрібні особисті дані окремих осіб, можуть додати цей пункт до своєї політики щодо даних. Крім того, навіть клієнти можуть накласти свої права на виправлення та отримати попередні дані, видалені з бази даних.

Обмеження зберігання

Цей принцип GDPR обмежує термін зберігання персональних даних організацій. Дані, зібрані за згодою фізичних осіб, мають термін дії. Після закінчення терміну організації втрачають право зберігати дані фізичних осіб. Крім того, рекомендується повідомити осіб про цю дату обмеження. Компанії повинні мати належну систему видалення даних, щоб стерти зібрані дані. Невиконання цього вважається порушенням, за яке організації можуть сплатити величезні штрафи.

Чесність і конфіденційність

Кожна організація, яка дотримується принципів GDPR, зобов’язана захищати дані, зібрані від окремих осіб. Оскільки кількість кібератак почастішала, організації несуть відповідальність за порушення даних. Отже, підприємства зобов’язані захищати особисті дані фізичних осіб за допомогою надійної системи інформаційної безпеки. Адекватні заходи кібербезпеки є обов’язковими для організацій, які мають справу з конфіденційною інформацією окремих осіб.

Відповідальність

Цей принцип GDPR вимагає від організацій надійності та підзвітності під час збору персональних даних фізичних осіб. Щоб уникнути порушень, підприємства повинні документувати кожен крок під час обробки зібраних даних, щоб запобігти порушенням. Ця практика дозволяє організаціям виправдовувати свою практику, коли їх звинувачують у недотриманні.

Підприємства, які не дотримуються правил, визначених GDPR, повинні сплачувати значні прийнятні суми за порушення. Штраф може коливатися від 17,5 мільйонів євро до 4% річного доходу разом з іншими штрафами. У зв'язку з цим організації повинні дотримуватись положення та впроваджувати принципи під час угод із громадянами ЄС.

Отже, загальний регламент захисту даних (GDPR) — це закон, який надає людям більше контролю над своїми особистими даними та вимагає від компаній бути більш прозорими та відкритими щодо того, як вони їх використовують. Складність регулювання змусила організації наймати професіоналів, які добре знають GDPR. Ці спеціалісти мають сертифікат GDPR Certified Data Protection Officer . Отримання сертифікації GDPR CDPO допомагає людям отримати глибоке розуміння практики та принципів GDPR. Практики можна надалі впроваджувати в організаціях під час збору персональних даних фізичних осіб.

Щодо основних підходів захисту конфіденційних даних, організації можуть використовувати різноманітні стратегії та методи для захисту своєї конфіденційної інформації від несанкціонованого доступу, розголошення, зміни або знищення. Ефективний захист даних повинен передбачати багаторівневий підхід, який зможе поєднувати технологічні рішення, організаційні політики та навчання співробітників.

Розглянемо основні підходи та їх значення для захисту конфіденційної інформації (рис.1.4).

Шифрування.

Одним з найбільш ефективних методів захисту конфіденційних даних є шифрування. Шифрування передбачає перетворення даних у нечитабельний

формат, який може бути розшифрований лише за допомогою спеціального ключа. Шифрування слід застосовувати як до даних, що зберігаються (у стані спокою), так і до даних, що передаються мережами (під час передачі). Існують різні алгоритми шифрування, такі як AES-256, а також розробляються квантово-стійкі алгоритми для захисту від майбутніх загроз. Важливо зазначити, що, хоча шифрування є потужним інструментом, воно не є панацеєю і може мати обмеження, особливо з огляду на розвиток криптографічних атак та використання хмарних сховищ. Тому шифрування має бути частиною комплексного підходу до захисту даних.

Контроль доступу.

Впровадження сучасних механізмів контролю доступу є критично важливим для забезпечення того, щоб лише авторизований персонал мав доступ до конфіденційних даних. Це включає використання багаторівневої аутентифікації (MFA), яка вимагає від користувачів надання двох або більше методів підтвердження особи для отримання доступу. Рольова модель контролю доступу (RBAC) дозволяє обмежувати доступ на основі функціональних обов'язків співробітників. Більш гнучким підходом є політика контролю доступу на основі атрибутів (PBAC), яка враховує контекст доступу, такий як ідентичність користувача, його місцезнаходження та рівень чутливості даних. Слабкі або недостатні паролі є частою причиною витоків даних, тому впровадження централізованого управління паролями та MFA є важливим елементом захисту.

Рис.1.4. Підходи до захисту конфіденційної інформації

Резервне копіювання.

Регулярне створення резервних копій критично важливих даних та їхнє безпечне зберігання в окремому віддаленому місці є важливим для забезпечення

можливості відновлення у разі кібератак, системних збоїв або людських помилок. Рекомендується шифрувати резервні копії для додаткового захисту. Не менш важливим є регулярне тестування процедур відновлення, щоб переконатися в їхній ефективності.

Маскування даних.

Для захисту конфіденційної інформації в неробочих середовищах, таких як розробка та тестування, використовуються методи маскування даних. Вони передбачають заміну оригінальних даних на фіктивні, але реалістичні значення. Існують статичне маскування, яке застосовується до даних у базі даних, та динамічне маскування, яке маскує дані в режимі реального часу для неавторизованих користувачів. На відміну від шифрування, маскування даних повністю видаляє оригінальні дані, що може бути корисним у певних сценаріях використання.

Захист кінцевих точок.

Забезпечення безпеки всіх кінцевих пристроїв, включаючи ноутбуки, мобільні телефони та пристрої Інтернету речей (IoT), є важливим для запобігання несанкціонованому доступу та поширення шкідливого програмного забезпечення. Для цього використовуються рішення EDR (Endpoint Detection and Response) або XDR (Extended Detection and Response), які забезпечують комплексний моніторинг та реагування на загрози, спрямовані на кінцеві точки.

Навчання співробітників.

Оскільки людський фактор є однією з основних причин витоків даних, регулярне навчання співробітників з питань кібербезпеки є критично важливим. Програми навчання повинні охоплювати такі теми, як розпізнавання фішингових атак, використання надійних паролів, важливість конфіденційності даних та правильне поводження з чутливою інформацією.

Безперервний моніторинг.

Використання інструментів безперервного моніторингу дозволяє організаціям виявляти та оперативно реагувати на підозрілу активність у режимі реального часу. Впровадження систем SIEM (Security Information and Event

Management) допомагає збирати та аналізувати журнали подій безпеки з різних джерел для виявлення потенційних загроз.

Класифікація даних.

Організація даних за категоріями на основі їхнього рівня чутливості (наприклад, низький, середній, високий ризик) дозволяє застосовувати відповідні заходи безпеки для кожної категорії. Наявність чіткої політики класифікації даних допомагає визначити, як слід обробляти та передавати різні типи інформації.

Крім перелічених методів, організації також можуть використовувати мінімізацію даних (збір лише необхідного обсягу даних), проводити регулярні оцінки ризиків та оцінки впливу на захист даних (DPIA), розробляти та впроваджувати плани реагування на інциденти, а також впроваджувати архітектуру нульової довіри.

Ефективна стратегія захисту даних повинна бути комплексною, поєднувати кілька рівнів контролю та враховувати специфічні ризики та нормативні вимоги, що застосовуються до діяльності організації.

Вплив нормативних вимог.

Захист конфіденційних даних також обумовлений різними нормативними вимогами, такими як Загальний регламент щодо захисту даних (GDPR), Закон про переносимось та підзвітність медичного страхування (HIPAA) Дотримання цих вимог є обов'язковим для уникнення значних штрафів та збереження довіри клієнтів. Нормативні акти часто визначають конкретні заходи безпеки, які організації повинні впроваджувати для захисту персональних даних.

1.3. Аналіз існуючих засобів захисту конфіденційної інформації в організаціях

На ринку існують різні рішення для захисту конфіденційних даних, які можуть бути розглянуті як альтернативи. До трьох таких рішень належать Fortanix DSM, Thales CipherTrust Data Security Platform, HashiCorp Vault та AWS Key Management Service (KMS).

Fortanix Data Security Manager (DSM) є уніфікованою платформою, розробленою для забезпечення шифрування даних та управління ключами на підприємствах, що використовують гібридні та мультихмарні середовища. Рішення спрямоване на мінімізацію ризиків витоку даних та забезпечення повного контролю над доступом до інформації.

Архітектура та основні функції: Fortanix DSM використовує апаратні модулі безпеки (HSM), сертифіковані за стандартом FIPS 140-2 Level 3, для надійного захисту криптографічних ключів. Платформа підтримує як модель розгортання "програмне забезпечення як послуга" (SaaS), так і встановлення локально, що забезпечує гнучкість у виборі оптимального варіанту для кожної організації. Однією з ключових особливостей DSM є інтеграція з технологією Confidential Computing, яка забезпечує захист даних не лише під час зберігання та передачі, але й під час їхньої обробки.

Thales CipherTrust Data Security Platform: Thales CipherTrust є уніфікованою платформою, призначеною для виявлення, захисту та контролю конфіденційних даних в організації. Платформа пропонує широкий спектр функцій, включаючи шифрування даних у стані спокою та під час передачі, токенізацію та маскування даних. Централізоване управління ключами забезпечується за допомогою CipherTrust Manager, який підтримує мультихмарність. Рішення також надає можливості аудиту та допомагає організаціям відповідати різним нормативним вимогам, таким як GDPR, HIPAA та PCI DSS. Thales CipherTrust є комплексним рішенням, що охоплює широкий спектр потреб у захисті даних.

HashiCorp Vault: HashiCorp Vault є системою управління секретами та шифруванням, що базується на ідентифікації. Vault забезпечує безпечне зберігання секретів, генерування динамічних секретів, шифрування даних та управління криптографічними ключами. Контроль доступу здійснюється на основі гранульованих політик (ACL). Рішення веде детальний аудит усіх операцій та підтримує мультихмарність, а також різні методи аутентифікації. HashiCorp Vault вирізняється своєю гнучкістю та потужними можливостями контролю доступу, що робить його придатним для складних інфраструктур.

AWS Key Management Service (KMS): AWS KMS є керованою сервісом від Amazon Web Services, який дозволяє легко створювати та контролювати криптографічні ключі, що використовуються для захисту даних. KMS забезпечує шифрування даних, що зберігаються в сервісах AWS, а також даних у власних додатках користувачів. Сервіс пропонує централізоване управління ключами та політиками доступу, а також аудит використання ключів за допомогою AWS CloudTrail. AWS KMS тісно інтегрований з багатьма іншими сервісами AWS. Це рішення є зручним та інтегрованим варіантом для організацій, які активно використовують інфраструктуру AWS.

Таблиця 1.2.

Порівняльна таблиця рішень для захисту конфіденційної інформації

Критерій	**Fortanix DSM**	**Thales CipherTrust Data Security Platform**	**HashiCorp Vault**	**AWS Key Management Service (KMS)**
Методи шифрування	Шифрування файлів, БД, токенізація, Confidential Computing	Шифрування файлів, БД, токенізація, маскування	Безпечне зберігання, шифрування як послуга, токенізація	Шифрування сервісів AWS та додатків, симетричні/асиметричні ключі
Управління ключами	Централізоване, HSM (FIPS 140-2 L3), мультихмарність, BYOK	Централізоване, HSM, мультихмарність, BYOK/HYOK	Централізоване, підтримка HSM, хмарно-агностичне	Централізоване, HSM AWS, інтеграція з сервісами AWS
Контроль доступу	RBAC, політики доступу, кворуми	RBAC, гранульований контроль доступу	RBAC, гранульовані політики (ACL)	Політика ключів, політики IAM
Можливості аудиту	Детальні журнали, інтеграція з зовнішніми системами	Комплексні можливості аудиту	Детальний аудит усіх операцій	Аудит через AWS CloudTrail
Відповідність вимогам	FIPS 140-2 L3, GDPR, HIPAA, PCI DSS	GDPR, HIPAA, PCI DSS та інші	FIPS 140-2 L1, підтримка різних стандартів	SOC, PCI, FedRAMP, HIPAA та інші

Проведений порівняльний аналіз показує, що всі розглянуті рішення є потужними інструментами для захисту конфіденційних даних в організаціях. Однак кожне з них має свої сильні сторони та особливості, які можуть зробити його більш придатним для певних потреб.

Fortanix DSM вирізняється своєю інтеграцією з технологією Confidential Computing, що забезпечує додатковий рівень захисту даних під час їхньої обробки. Рішення також пропонує потужні можливості управління ключами в гібридних та мультихмарних середовищах, що є значною перевагою для організацій, які використовують кілька хмарних платформ.

2 МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІ

2.1. Архітектура платформи Fortanix DSM

Цифровізація та хмарні технології спричинили розповсюдження даних для підприємств будь-якого розміру. Прийняття мультихмарної та гібридної IT-інфраструктури створило накопичувачі даних, які розмежували право власності між корпоративними та хмарними провайдерами.

Доступ до даних на основі API привніс ще один рівень складності в поєднанні з динамічними політиками та розсіяними привілеями. Витоки даних, які ми спостерігаємо сьогодні у великих банках, роздрібних торговцях, закладах охорони здоров'я, технологічних компаніях, постачальниках публічних хмарних технологій і навіть уряді, є симптомом складності, яка існує сьогодні.

Fortanix Data Security Manager(DSM) — це потужне рішення, призначене для захисту конфіденційних даних у різних середовищах. Висока доступність є корисним аспектом DSM, який гарантує, що служби захисту даних залишаються надійними та доступними навіть у разі збоїв або збоїв [5].

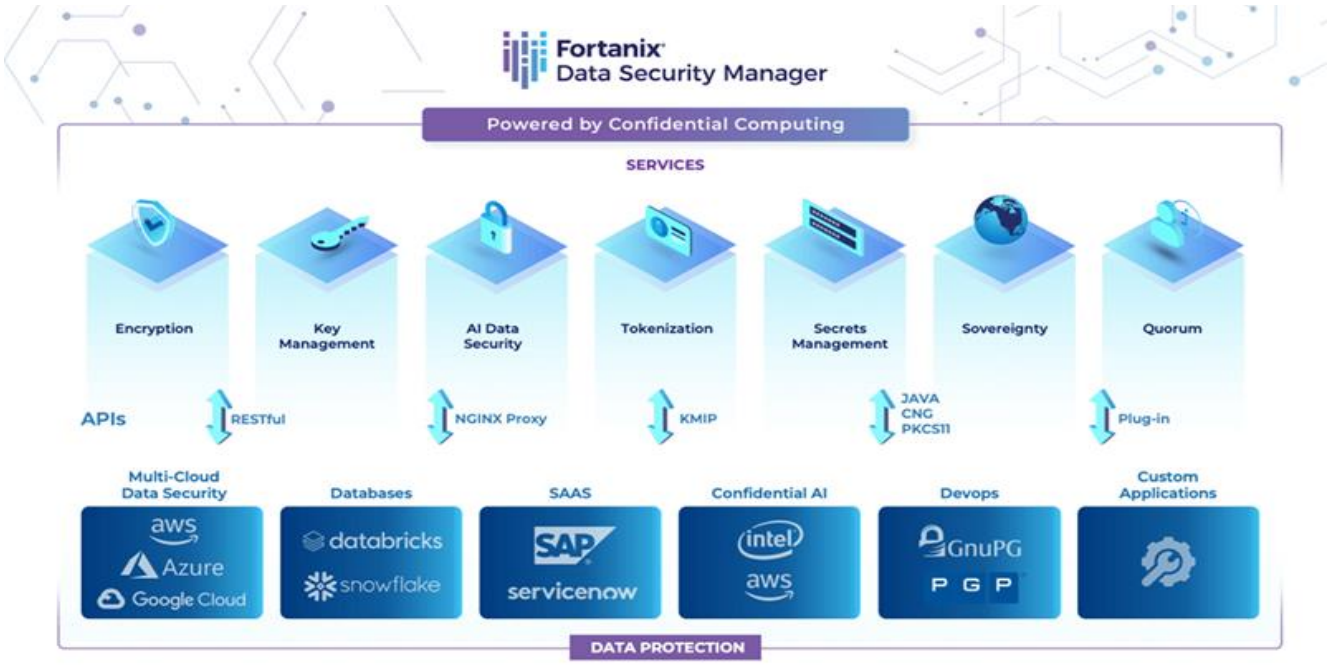

Рис. 2.1. Захист конфіденційних даних на платформі Fortnix DSM

Fortanix уже надає розгорнуті рішення або активно інвестує в найближче майбутнє за допомогою своєї платформи Data Security Manager (DSM), як це показано на рис 2.1. Можна виділити кілька важливих сфер де надаються сервіси від Fortnix:

Керування станом безпеки даних (DSPM) – згідно з Gartner, "Керування станом безпеки даних (DSPM) забезпечує видимість того, де знаходяться конфіденційні дані, хто має доступ до цих даних, як вони використовувалися та який рівень безпеки сховища даних або програми. Для цього потрібен аналіз потоку даних, щоб визначити конфіденційність даних. DSPM формує основу оцінки ризику даних (DRA) для оцінки впровадження політик управління безпекою даних (DSG)" [7].

Платформа безпеки даних – це широка область, яка насправді представляє цікаву тенденцію. Згідно зі звітом Hype Cycle [7], «платформи безпеки даних (DSP) агрегують вимоги до захисту даних для різних типів даних, сховищ та екосистем, починаючи з виявлення та класифікації даних».

DSM Fortanix отримала широке поширення завдяки цьому уніфікованому підходу до платформи, який є простим для різних підприємств, які прагнуть захистити свої конфіденційні дані.

Конфіденційні обчислення – згідно з визначенням Gartner, "конфіденційні обчислення – це механізм безпеки, який виконує код в апаратному довіреному середовищі виконання (TEE), яке також називається анклавом. Анклави ізолюють і захищають код і дані від хост-системи (а також від власників хост-системи), а також можуть забезпечувати цілісність коду та атестацію". – Серед інших варіантів використання конфіденційні обчислення дозволяють компаніям використовувати дані в хмарі більш надійним способом.

Ця технологія згадується як нова технологія у звіті Gartner Hype Cycle for Data Security. І Fortanix є лідером у цій галузі.

Останнім часом спостерігається поширена зацікавленість до цієї технології, оскільки постачальники публічних хмар, постачальники мікросхем та інших постачальників програмного забезпечення починають підтримувати цю

технологію. Для суворо регульованих галузей це усуває одну з перешкод для впровадження хмари, зберігаючи цілісність і конфіденційність даних.

Блокчейн для безпеки даних – на відміну від традиційних методів захисту даних, методи з підтримкою блокчейну забезпечують спосіб децентралізації безпеки, одночасно збільшуючи систему стримувань і противаг. Менше покладаються на централізованих арбітрів, і вони породили кілька варіантів використання, особливо з децентралізованими фінансами (DeFi), які працюють на так званій інфраструктурі Web3.0. Gartner оцінює вигоду як високу, тоді як зрілість все ще перебуває на високому рівні.

Мультихмарне керування ключами як послуга (KMaaS) – це стосується керування ключами в одній або кількох публічних чи приватних платформах хмарних служб, які зазвичай розгортаються як пропозиція SaaS і використовують апаратний модуль безпеки (HSM).

Управління ключами в кількох CSP з одночасною підтримкою ініціативи Bring Your Own Key (BYOK) для забезпечення узгодженої політики доступу до даних із розповсюдженням ключів, володінням, нормативними вимогами, захистом даних і конфіденційністю – все це стає дедалі важливішим у гібридному та багатохмарному світі. Fortanix має дуже диференційоване рішення для цього простору. Застосування правил Shrems-II і GDPR також змусило постачальників публічних хмар із власними системами керування ключами шукати зовнішні рішення для керування ключами на зразок Fortanix. Google і Fortanix, наприклад, підтримують рішення для зовнішнього керування ключами (EKM) на Google Cloud Platform.

*Безпечні багатосторонні обчислення (*SMPC) – це окреслює співпрацю між різними організаціями, що дозволяє кожній організації обмінюватися інформацією про захищені дані без шкоди для конфіденційності.

Fortanix спрощує та захищає процес обміну особистими даними, не відкриваючи їх для інших сторін і не порушуючи норм конфіденційності. Кілька сторін передають зашифровані дані в надійне середовище виконання, яке називається анклавом, де дані об’єднуються, аналізуються, а потім результати

виводяться в зашифрованому форматі назад кожній стороні разом із результатами аналітики.

Дані залишаються зашифрованими протягом усього процесу, захищаючи конфіденційність даних під час їх передачі, під час обчислення та під час зберігання.

Шифрування зі збереженням формату – шифрування зі збереженням формату, також відоме як токенізація, останнім часом стає все більш популярним і актуальним для захисту даних у стані спокою та під час використання для різноманітних випадків використання, причому вимоги до конфіденційності та відповідності є на вершині харчового ланцюжка. Це вважається важливою технікою анонімізації. Fortanix має тут сильну пропозицію

Конфіденційність за проектом (PbD) – це основний напрямок, пов'язаний із запровадженням культури конфіденційності, пов'язаної з технологіями. Fortanix продовжує інвестувати в цю сферу.

Управління корпоративними ключами (EKM) – завдяки криптографії та токенізації, які стають основними для захисту даних, запобігання витоку даних і забезпечення конфіденційності, керування корпоративними ключами використовує програмне або апаратне забезпечення для кількох рішень симетричного шифрування, полегшуючи розповсюдження ключів, зберігання ключів і підтримку узгодженого керування життєвим циклом ключів.

Fortanix має зріле рішення EKM із понад 100 інтеграціями в свою платформу Data Security Manager (DSM) .

Це робить впровадження керування ключами на підприємстві відносно простішим порівняно з традиційними рішеннями на ринку. Посібник користувача тут є чудовим прикладом рішення для керування життєвим циклом ключів.

Для досягнення цієї мети Fortanix DSM використовує кілька концепцій високої доступності, включаючи віртуальну IP-адресу та балансування навантаження. Використовуючи ці концепції високої доступності, Fortanix DSM забезпечує надійну та безперебійну безпеку даних навіть у складних умовах. Fortanix Data Security Manager™ (DSM) дозволяє користувачам і програмам

безпечно створювати, керувати та зберігати криптографічні ключі. Він використовує технологію Intel® Software Guard Extensions (Intel® SGX) у процесорах Intel® Xeon® для збереження ключів і даних в анклавах Intel® SGX, захищаючи їх від шкідливих програм, операційної системи, гіпервізорів і постачальників послуг. Цей підхід на основі програмного забезпечення забезпечує безпеку рівня HSM без необхідності фізичних апаратних модулів безпеки (HSM), підтримуючи розгортання в загальнодоступній хмарі, локальній або гібридній інфраструктурі [5-7].

Fortanix DSM використовує Intel® SGX для запуску таких критичних функцій додатків, як аутентифікація та контроль доступу в захищених анклавах, забезпечуючи чудову безпеку порівняно з традиційними HSM. Його сертифіковане апаратне забезпечення FIPS 140-2 рівня 3, створене із готових компонентів, знижує початкові та експлуатаційні витрати [5, 6].

Система горизонтально масштабується, тобто її потужність зростає в міру додавання більшої кількості вузлів, і вона розроблена для високої доступності з вбудованим резервуванням і аварійним відновленням. Вона використовує розподілену зашифровану систему зберігання з Cassandra, що включає протоколи Paxos і Raft для захисту від втрати та пошкодження даних [5-7].

Fortanix DSM генерує або отримує різні ключі та використовує їх для захисту даних у різних точках системи (рис.2.2). Fortanix DSM завжди зберігає ключі клієнтів у зашифрованому вигляді, незалежно від того, чи знаходяться вони на диску, у мережі чи в пам’яті вузла Fortanix DSM. Нижче наведено загальний огляд ієрархії ключів у Fortanix DSM:

Ключі від платформи

Кластерні ключі

Ключі для захисту даних у стані спокою

Ключі для захисту даних під час передавання

Ключі для захисту даних, що використовуються (застосовно лише під час використання розгортань на основі SGX).

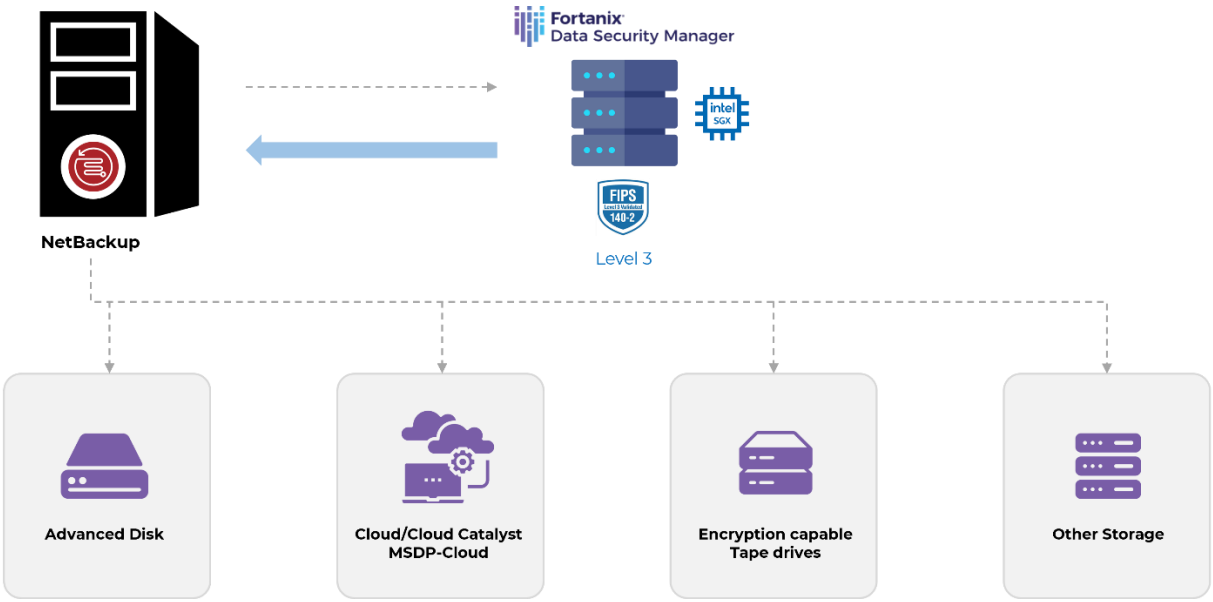

Рис.2.2. Архітектура Fortnix DCM

2.2. Функції Fortnix DCM SaaS

DSM SaaS надає всі перевірені можливості локального рішення Fortanix і є першою та єдиною багатохмарною службою безпеки даних, сертифікованою за суворим стандартом безпеки FIPS 140-2 рівня 3. DSM SaaS дозволяє організаціям вибрати нову модель на основі послуг, яка спрощує розгортання безпеки даних, полегшує керування та, перш за все, більш економічно ефективну безпеку даних на основі SaaS для світу, орієнтованого на хмару.

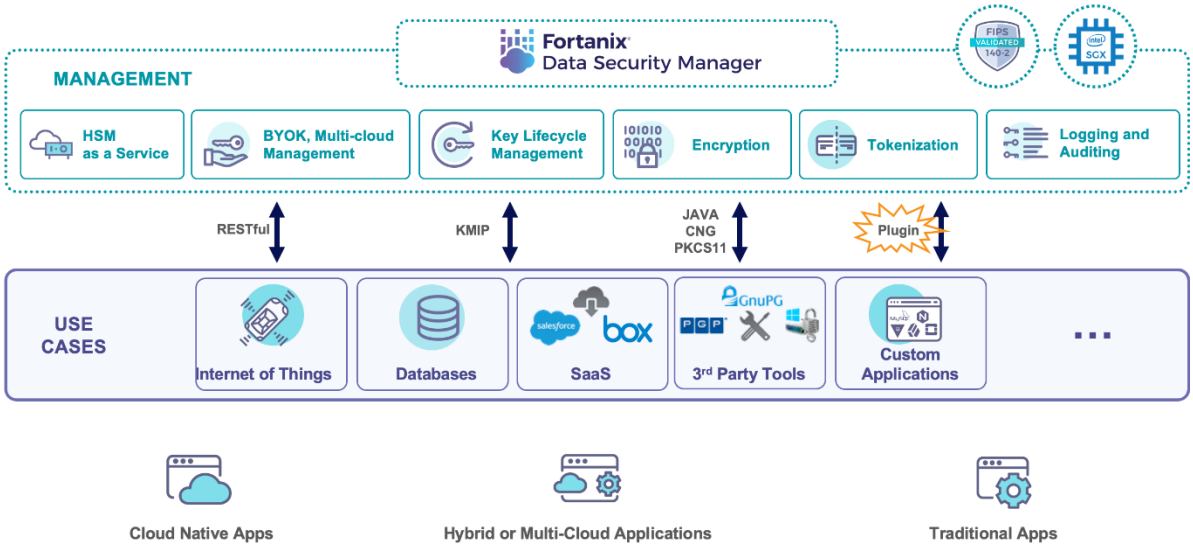

Рис.2.3. Функції Fortnix DCM SaaS

Ось основні моменти:

Комплексна безпека даних: зручне для хмари шифрування, керування ключами та секретами з єдиної інтегрованої платформи забезпечує комплексну безпеку даних. Доповнений такими функціями, як:

Токенізація

Автоматизоване керування хмарними ключами

Керування застарілими HSM

Прозоре шифрування та дешифрування даних, створених програмою, у масштабі.

HSM as a service

Застарілі системи HSM складні у використанні та складні в управлінні. Сьогодні великі підприємства часто мають 2-3 різні HSM, рішення для керування ключами та шифрування, кожне з яких вирішує лише частину проблеми за високою ціною з дорогим обслуговуванням і додатковими витратами на кожну нову програму. Крім того, ці системи не інтегруються з публічною хмарою/гібридною інфраструктурою, що вимагає від клієнтів підтримувати окремі рішення для локальних додатків і публічної хмари. Сучасні і без того перевантажені команди програм, адміністратори баз даних, аналітики даних і адміністратори безпеки не мають часу чи терпіння використовувати застарілу технологію [9].

Fortanix забезпечує інтегрований HSM FIPS 140-2 рівня 3, а також керує застарілими HSM, роблячи їхні ключі керованими та доступними через Fortanix (рис. 2.4).

Переваги

Низька вартість із захистом інвестицій

Fortanix дозволяє клієнтам зменшити вартість і складність інфраструктури HSM шляхом об’єднання всіх HSM в єдине економічно ефективне рішення. Згодом клієнти зможуть перенести ключі та замінити обладнання HSM на сучасне масштабоване рішення.

Прискорення хмарної міграції

Переміщуйтеся між локальною та загальнодоступною хмарою за допомогою єдиного набору криптографічних служб і елементів керування. Fortanix HSM Gateway, розширення для Fortanix Data Security Manager (DSM), підключається до застарілих HSM, які ви вже маєте. Fortanix HSM Gateway надає узгоджений набір уніфікованих API і служб для всіх ваших локальних, гібридних і хмарних програм. Ключі залишаються в безпеці в існуючому HSM, тоді як додатки та бази даних (локальні або хмарні) отримують єдине джерело криптографічних служб, а групи безпеки отримують єдине джерело для керування та аудиту [9].

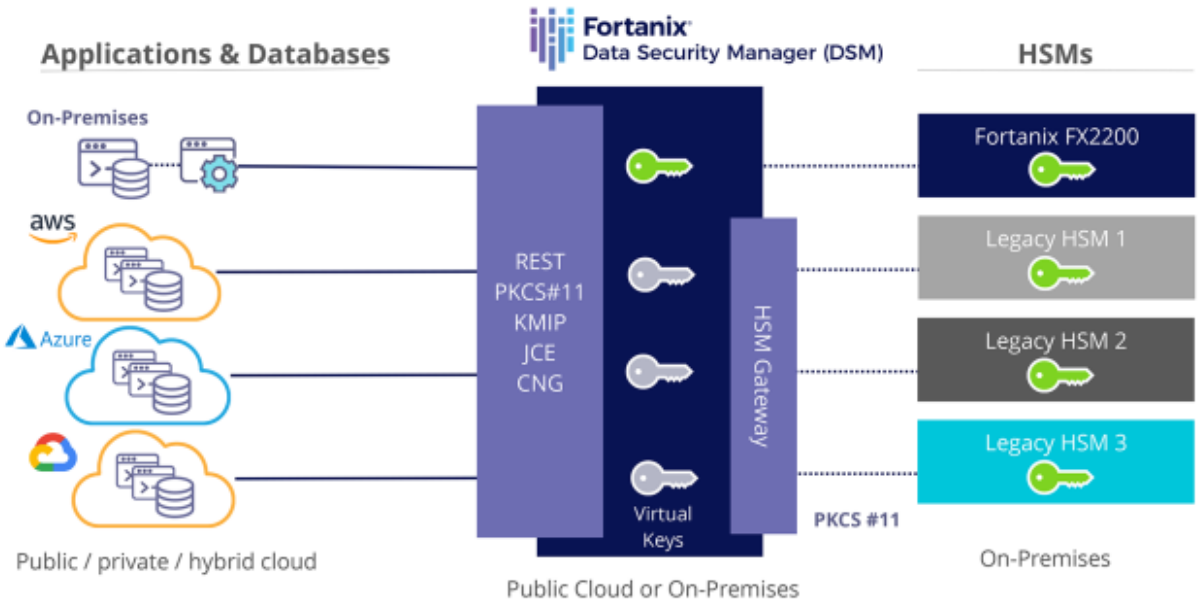

Рис.2.4. HSM as a service

Просте у використанні єдине рішення

Fortanix надає сучасні багатокористувацькі та інтуїтивно зрозумілі інтерфейси «єдиного джерела» для спрощеного адміністрування та посиленого контролю, включаючи розширене журналювання та аудит усієї інфраструктури.

BYOK

За допомогою Fortanix Data Security Manager клієнти можуть генерувати власні ключі та переносити їх у хмарні програми/робочі навантаження, незалежно від того, чи це Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft

Azure або Salesforce. За допомогою Bring Your Own Key (BYOK) Fortanix дозволяє клієнтам приносити або імпортувати власний головний ключ, який хмарний постачальник зберігає у своїй системі керування ключами (KMS) і використовує його для шифрування всіх ключів шифрування даних (DEK), що використовуються в хмарі [11].

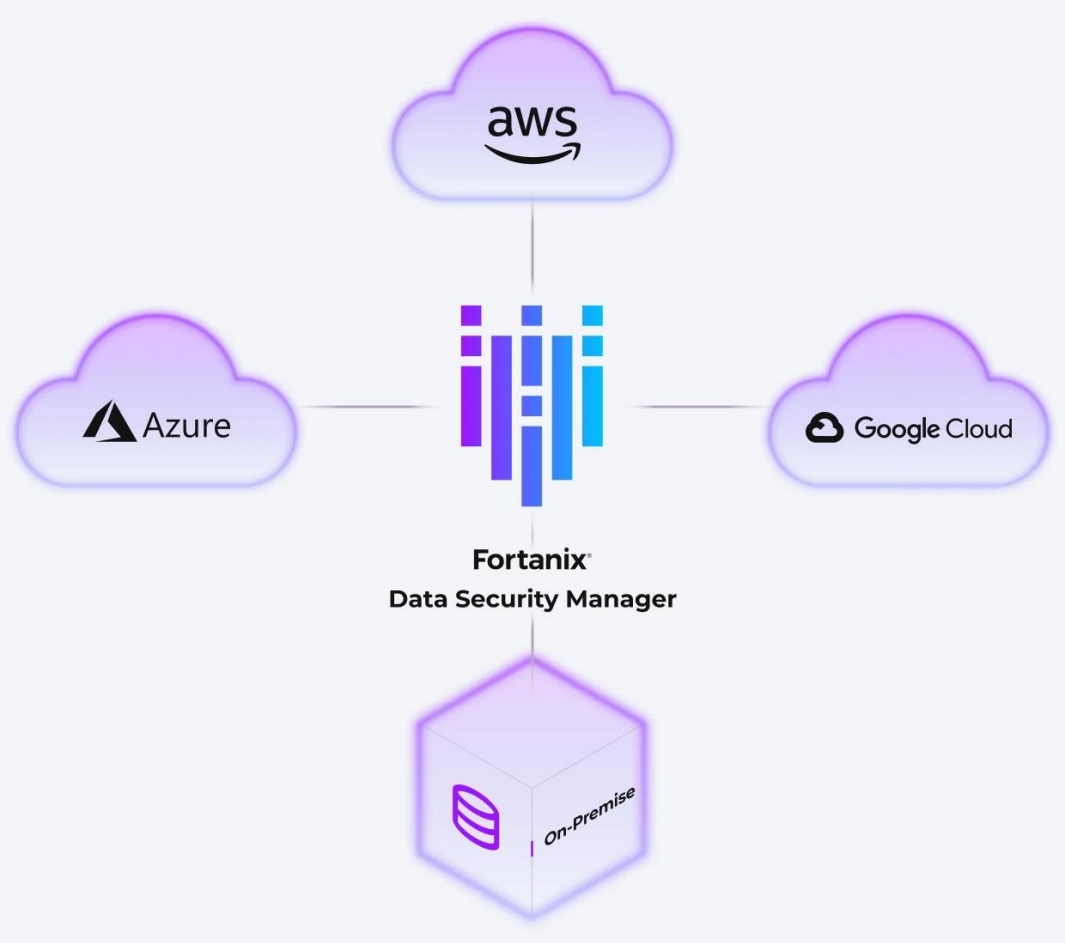

Рис. 2.5. Функція BYOK

Це дає організаціям більший контроль; головні ключі можна вимкнути або видалити, щоб хмарний постачальник більше не міг розшифрувати дані. Ця функція блокування дозволяє клієнтам відповідати найсуворішим вимогам конфіденційності.

Key lifecycle management

Fortanix пропонує використовувати сім кроків для життєвого циклу ключів.

Розглянемо суть кожного з кроків.

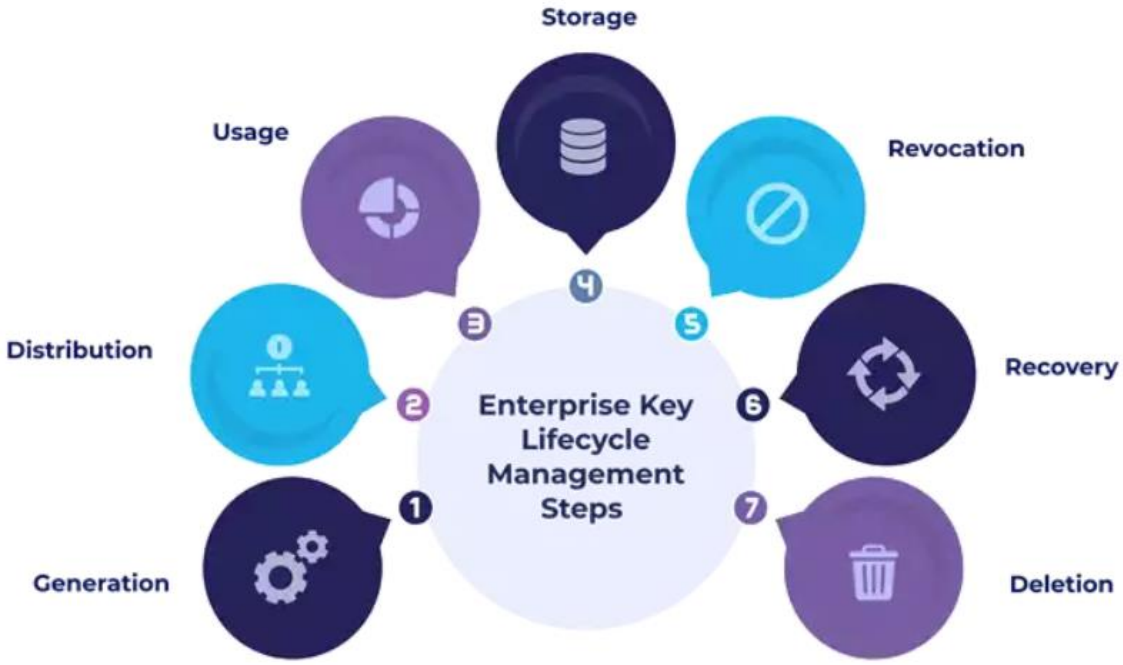

Рис. 2.6. Життєвий цикл ключів

Крок 1 – Генерація

Надійні криптографічні ключі є основою ефективної стратегії безпеки. Ключі повинні бути створені за допомогою сильних алгоритмів і ентропії.. Цей перший крок є основою для всього процесу безпеки.

Крок 2 – Розподіл

Після створення надійних ключів наступним завданням є безпечне призначення їх різним командам і системам. Для цього необхідно захистити ключі під час передачі. Щоб забезпечити безпеку ключів під час передачі, необхідно зашифрувати їх і забезпечити їх переміщення через захищені канали.

Крок 3 – Використання

Ці ключі використовуються для шифрування, дешифрування та виконання інших завдань безпеки даних. Необхідно запровадити суворий контроль доступу за допомогою ключів. Лише авторизований персонал повинен мати доступ до «сховища», де зберігаються їхні ключі. Необхідно налаштувати системи відстеження та журнал аудиту для ретельного моніторингу ключових взаємодій.

Крок 4 – Зберігання

Потрібо високобезпечне рішення для захисту ключів шифрування під час бездіяльності. Норми в його галузі диктують використання апаратних модулів безпеки (HSM), які забезпечують найвищий рівень безпеки. Щоб жодні зловмисники не могли отримати доступ, Необхідно ввести регулярну процедуру періодичної заміни та оновлення ключів.

Крок 5 – Скасування

Коли ключі більше не потрібні або досягли кінця свого призначеного терміну служби, їх потрібно зробити непридатними. Необхідно впровадити протокол, який відключав ці ключі, роблячи їх марними для супротивників. Ця практика забезпечить оперативне усунення ризиків, пов’язаних зі зламаними ключами, без порушення безпеки.

Крок 6 - Відновлення

Навіть при використанні найбезпечніших сховищ люди можуть втратити ключі, які захищають доступ до критично важливих даних. Розуміючи важливість плану резервного копіювання, необхідно створити процедуру відновлення ключів у надзвичайних ситуаціях, забезпечуючи постійний доступ до даних.

Крок 7 - Видалення

Коли ключі виконали своє призначення та застаріли, необхідно їх надійно видалити. Треба стерти ці ключі, щоб їх неможливо було відновити. Цей етап допоможе виконати одну з найважливіших вимог щодо захисту даних.

LOGGING AND AUDITING

Захищені від втручання журнали аудиту фіксують кожну операцію та легко інтегруються в SIEM.

TOKENIZATION

Анонімізує дані, зберігаючи їх цілісність і структуру, маркуючи конфіденційні набори даних, як-от PAN, PHI та PII.

ШИФРУВАННЯ ФАЙЛОВОЇ СИСТЕМИ

Допускає вийти за рамки повного шифрування диска та захищає окремі файлові системи, які активно використовуються на призначеному хості [10].

Дозволяє керувати криптографічними ключами для баз даних, таких як Oracle, SQL Server і MongoDB, захищаючи їх на HSM, перевірених FIPS.

Fortanix — це єдина платформа, яка дозволяє виявляти ключі шифрування, оцінювати рівень криптографічної безпеки та усувати потенційні вразливості в локальних і багатохмарних середовищах в одному місці.

Знаходить ключі та служби даних у всій організації, класифікуючи їх за типом і ризиком.

Визначає ключі та служби, які знаходяться під загрозою, і забезпечує відповідність нормам.

Виявляє квантово-вразливі ключі та служби під загрозою.

При виявленні вразливості визначає пріоритетність ризиків і дотримування дієвих кроків з усунення.

2.3. Зв'язок між обліковими записами, групами, програмами, ключами, користувачами та плагінами Fortanix DSM

Fortanix DSM розроблений, щоб дозволити компаніям задовольняти ключові потреби управління всіма своїми програмами, незалежно від того, чи працюють вони в публічній, приватній чи гібридній хмарі.

Як вже було сказано в попередньому розділі дозволяє керувати життєвим циклом об'єктів безпеки (ключів, сертифікатів тощо) та використовувати їх для виконання криптографічних операцій. Основні операції, які підтримуються Fortanix DSM:

Створення симетричних та асиметричних ключів

Імпорт власних ключів

Ключ імпорту/експорту

Отримання нових ключів з існуючих ключів

Токенізація ключів

Контроль доступу на основі ролей для визначення того, які користувачі, групи чи програми мають доступ до яких ключів та які операції з цими ключами

Статистика використання ключів

Повний журнал аудиту використання ключів

Шифрування та дешифрування з використанням симетричних та асиметричних ключів

Підпис та перевірка операцій

Створення та оновлення плагінів.

На рисунку 2.7 показано зв'язок між обліковими записами, групами, програмами, ключами, користувачами та плагінами Fortanix DSM KMS. Надамо визначення кожного з учасників Fortanix DSM KMS.

Обліковий запис Fortanix DSM – це контейнер верхнього рівня для об’єктів безпеки, якими керує Fortanix DSM. Обліковий запис зазвичай пов’язаний з організацією, а не з окремою особою. Об’єкти безпеки, групи та програми належать лише до одного облікового запису. Різні облікові записи повністю ізольовані один від одного.

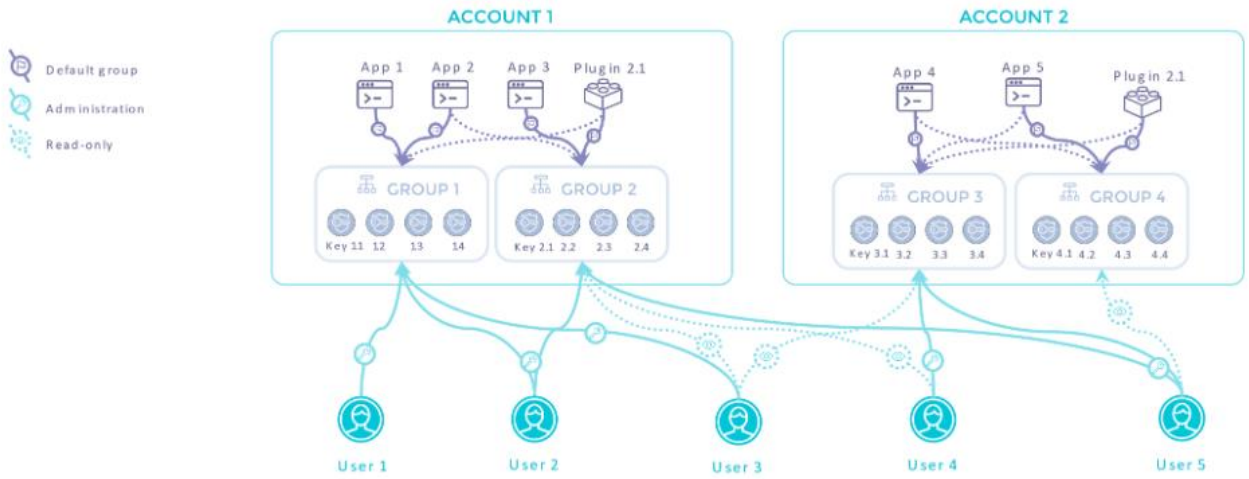

Рис.3.1. Зв'язок між обліковими записами, групами, програмами, ключами, користувачами та плагінами Fortanix DSM

Група — це сукупність пов’язаних об’єктів безпеки. Політики доступу встановлюються на рівні групи, тому всі об’єкти безпеки в групі мають однакову політику доступу. До групи можна призначити будь-яку кількість користувачів та/або програм.

Програма (додаток) — це служба або інші клієнти, що не є людьми, що використовують Fortanix DSM. Програми можуть автентифікуватися у Fortanix DSM за допомогою ключа API (секретного токена) або сертифіката клієнта TLS.

Залежно від дозволів, програми можуть: створювати об'єкти безпеки, змінити властивості об'єктів безпеки, виконувати криптографічні операції з використанням об'єктів безпеки.

Програми не можуть виконувати операції керування, такі як додавання або змінення користувачів і груп.

Програму можна призначити одній або кільком групам. Програма, призначена групі, має дозвіл на роботу з усіма об’єктами безпеки в цій групі.

Об'єкт безпеки – це будь-які дані, що зберігаються у Fortanix DSM (наприклад, ключ, сертифікат, секрет тощо). Для асиметричних пар ключів як закритий, так і відкритий ключі зберігаються в одному об'єкті безпеки. Також можливо, щоб об'єкт безпеки містив відкритий ключ без пов'язаного з ним закритого ключа.

Користувачі та програми, призначені групі, мають дозвіл на перегляд об’єкта безпеки та виконання операцій з ним. Користувачі та програми, не призначені групі об’єкта безпеки, не можуть переглядати цей об’єкт безпеки або виконувати з ним операції.

Функція копіювання ключа копіює об'єкт безпеки зі стандартної групи Fortanix DSM до іншої стандартної групи. Ця функція має такі переваги:

Зберігає єдине джерело ключового матеріалу під час використання/імпорту цього ключа в різних групах Fortanix DSM, де програмам у відповідних групах може знадобитися використовувати один ключ для досягнення певних бізнес-цілей.

Зберігає зв'язок різних копій одного й того ж ключового матеріалу з вихідним ключем для цілей аудиту та відстеження.

Користувачі пов’язані з адресами електронної пошти. Користувач може бути учасником одного або кількох облікових записів. Наприклад, співробітник може належати до облікового запису для корпоративного виробничого середовища,

облікового запису для корпоративного тестового середовища та облікового запису, що використовується для особистого тестування та розробки.

Залежно від дозволів, користувачі можуть:

виконувати операції управління, такі як додавання або змінення користувачів чи груп;

створювати об'єкти безпеки;

змінити властивості об'єктів безпеки;

перегляд журналів керування ключами Fortanix DSM та криптографічної активності.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ОРГАНІЗАЦІЇ НА ПРИКЛАДІ FORTANIX DSM

3.1. Варіант розгортання та налаштування хмарного Fortanix DSM

Розглянемо порядок перших кроків для початку використання Fortanix Data Security Manager(DSM) [12]. Цей порядок містить важливу інформацію для користувачів, щоб вони могли виконувати такі дії у Fortanix DSM:

1. Реєстрація.
2. Налаштування облікового запису.
3. Створення групи.
4. Додавання програми та призначення її до групи(груп).
5. Додавання користувачів та призначення їх до групи(груп).

Реєстрація. Щоб розпочати роботу з хмарним сервісом Fortanix Data Security Manager (DSM), вам потрібно зареєструвати обліковий запис за адресою <URL_вашого_сервісу_DSM>. Наприкладhttps://eu.smartkey.io.

Налаштування облікового запису. Відкрийте сторінку <Your_DSM_Service_URL> у веббраузері та введіть свої облікові дані для входу у Fortanix DSM (Рис.3.1).

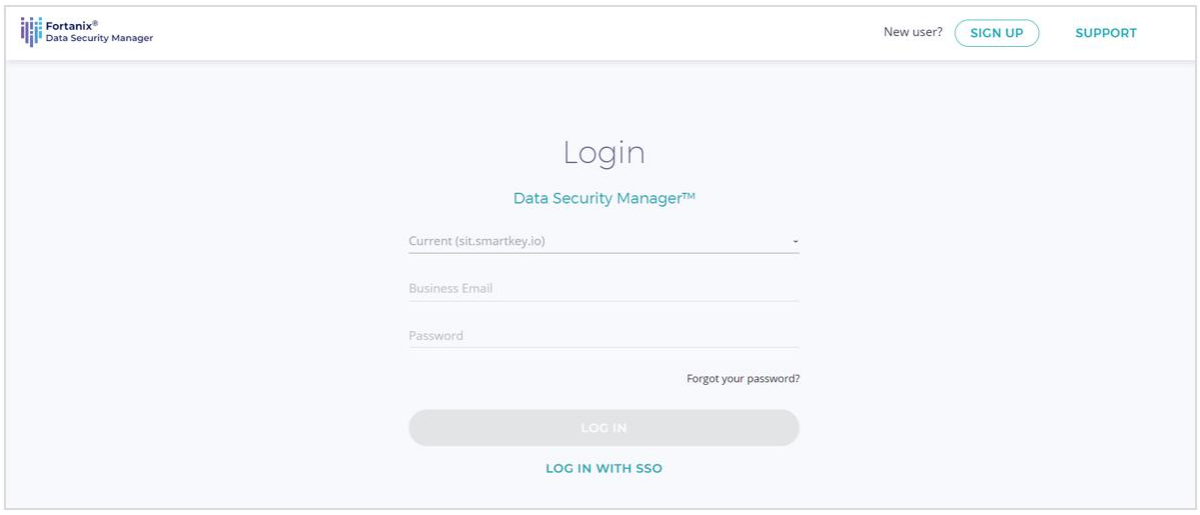

Рис.3.1. Реєстрація облікового запису

У цьому інтерфейсі можна створити новий обліковий запис або відповісти на запрошення приєднатися до існуючого облікового запису. Якщо це щойно створений обліковий запис, необхідно виконати наступні дії, щоб додати свою першу групу та програму у Fortanix DSM.

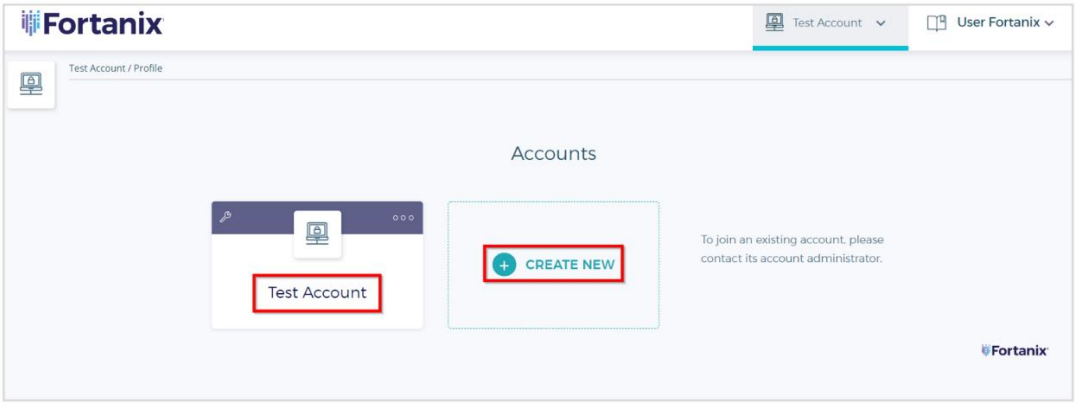

Рис.3.2. Створення/використання існуючого облікового запису

Необхідно зауважити, що Fortanix DSM тепер дозволяє створювати налаштування реплікації облікових записів, що дозволяє періодично реплікувати дані з вихідного облікового запису до цільового облікового запису для резервного копіювання, міграції або відновлення після відмови.

Після входу в обліковий запис ми побачимо *головну* сторінку DSM, яка надає повний огляд системи. У розділі цієї сторінки відображаються картки з детальною інформацією про кількість груп, програм, об’єктів безпеки, користувачів і плагінів в обліковому записі (рис.3.3).

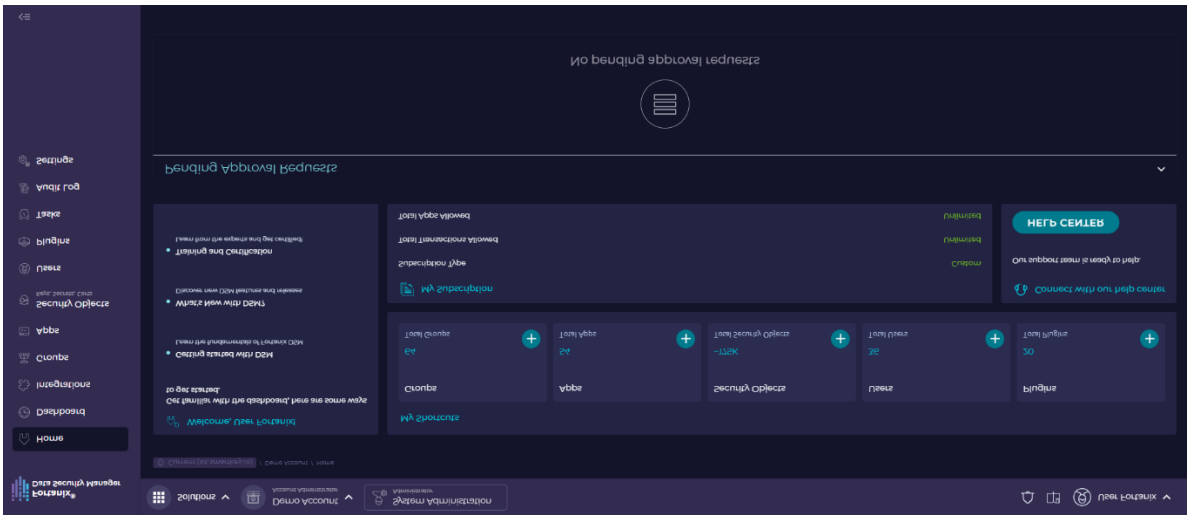

Рис.3.3. Головне меню DSM

З цього меню можна перейти до панелі інструментів DSM, де у верхньому розділі виділено найактивніші програми з точки зору активності та кількості виконуваних ними операцій тощо.

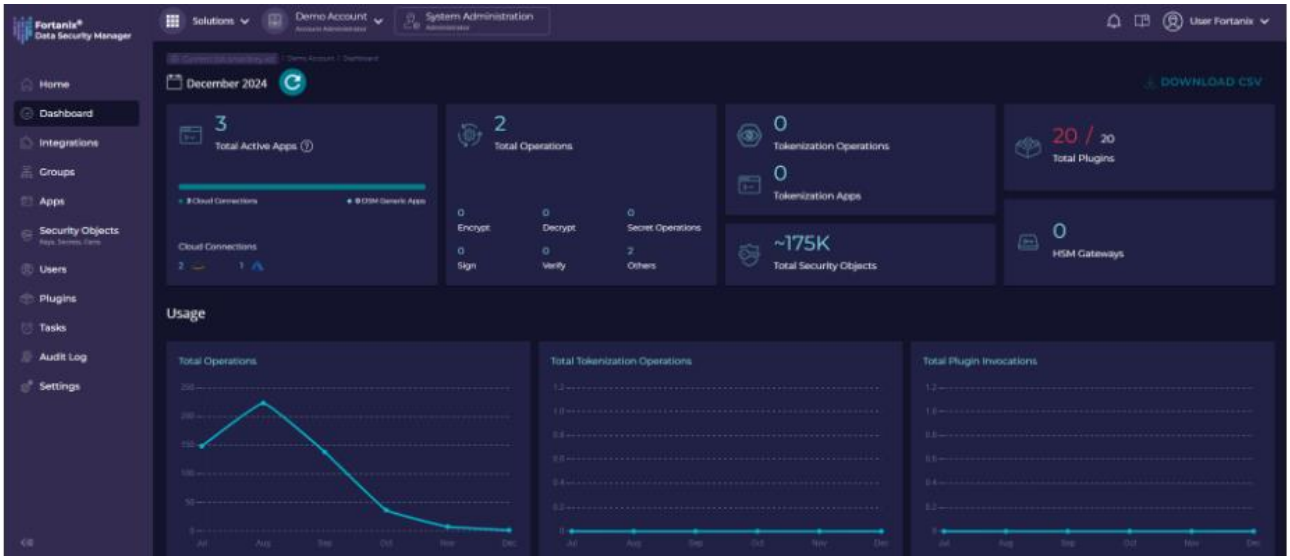

Рис.3.4. Вигляд панелі інструментів

Інтерфейс користувача Fortanix DSM тепер містить випадаючий список «*Рішення*» на верхній панелі навігації. Це меню забезпечує легку навігацію до таких інших продуктів і рішень Fortanix:

- Ключова інформація
- Управління ідентифікацією та доступом

Натискання будь-якого з варіантів у випадаючому меню *«Рішення»* перенаправить вас на сторінку входу до *Fortanix Armor* . Якщо ви вже ввійшли в систему, вас буде перенаправлено на сторінку *«Рішення Fortanix Armor»* (Рис.3.5).

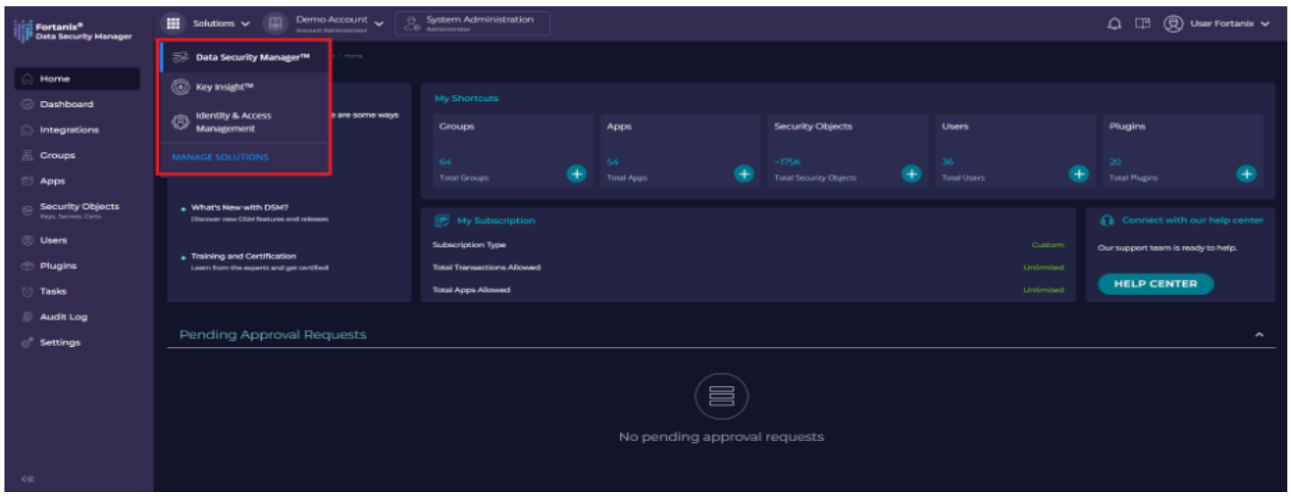

Рис.3.5. Меню рішень

Порядок створення групи

Виконайте такі кроки, щоб створити першу групу у Fortanix DSM (Рис.3.6):

1. Клацніть пункт меню «Групи» на лівій панелі навігації DSM і натисніть кнопку «+» , щоб додати нову групу.

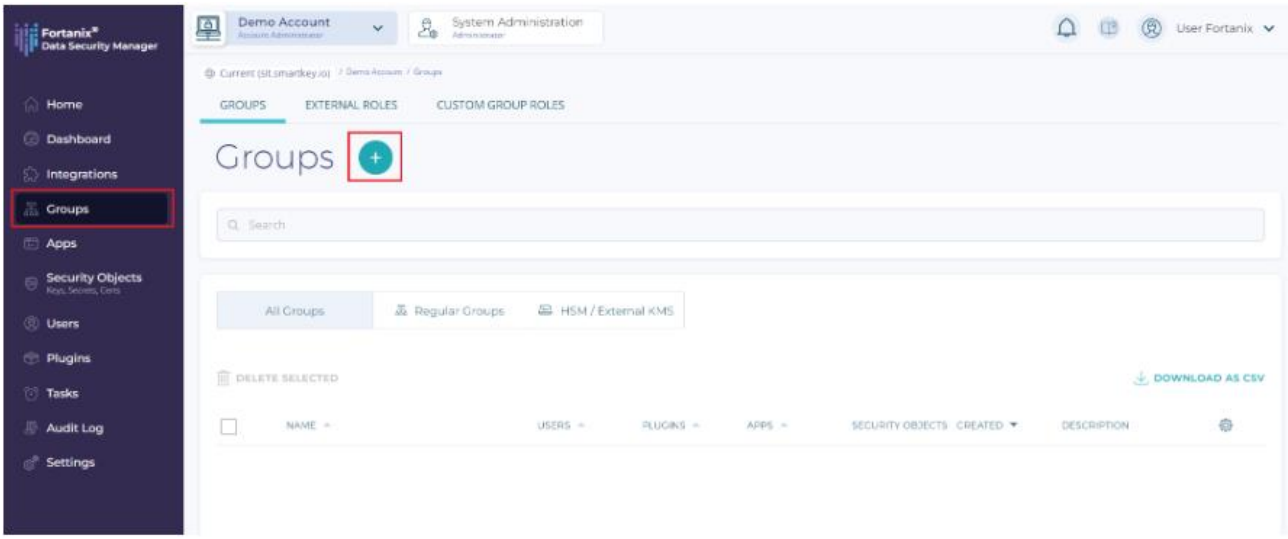

Рис.3.6. Додавання груп

2. На сторінці додавання нової групи введіть такі дані:

Назва - Введіть назву для вашої групи.

Опис (необов’язково) - Введіть короткий опис групи.

Додати політику кворуму групи: Укажіть політику кворуму для групи. Цей параметр визначає кількість схвалень, необхідних для операцій, що стосуються безпеки, в межах групи. Налаштуйте цю політику відповідно до ваших вимог безпеки. Налаштувати як групу HSM/Зовнішню KMS: Виберіть цей параметр, щоб налаштувати групу як групу HSM (модуль безпеки обладнання) або групу служби зовнішнього керування ключами (KMS). Це актуально, якщо ви плануєте використовувати зовнішні пристрої або служби для керування ключами. Налаштувати ключ шифрування ключа (KEK) з існуючої групи : виберіть цей параметр, щоб налаштувати ключ шифрування ключа (KEK) для групи, використовуючи існуючу групу як посилання. Це корисно під час встановлення криптографічних механізмів у групі. Для отримання додаткової інформації див.User's Guide: Group Key Encryption Keyдокументація.

Натисніть кнопку ЗБЕРЕГТИ , щоб створити нову групу.

Нову групу успішно додано до Fortanix DSM.

Додавання програми та призначення її до групи. Програма у Fortanix DSM використовує платформу для створення, зберігання та використання об'єктів безпеки, таких як криптографічні ключі, сертифікати або довільні секрети. Приклади таких програм включають веб-сервери, сервери інфраструктури відкритих ключів (PKI), сховища ключів та інші. Програма може взаємодіяти з Fortanix DSM через різні інтерфейси, такі як API передачі репрезентативного стану (REST) або використовуючи стандарти криптографії з відкритим ключем (PKCS)#11, розширення криптографії Java (JCE) або API криптографії наступного покоління (CNG).

Необхідно виконати такі кроки, щоб створити першу програму у Fortanix DSM (рис.3.7):

1. Клацніть пункт меню «Програми» на лівій панелі навігації DSM і натисніть кнопку «+», щоб додати нову групу.

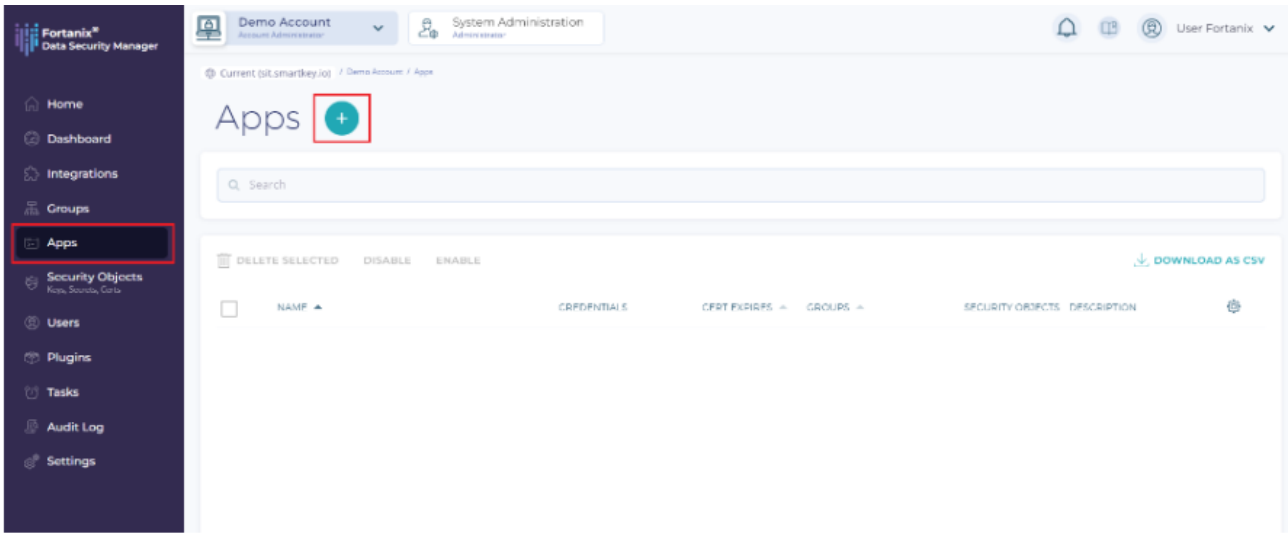

Рис.3.7. Додавання програми

2. На сторінці додавання нової програми введіть такі дані:

Назва програми - Введіть назву вашої програми.

Інтерфейс (необов'язково) - Виберіть потрібний тип інтерфейсу з випадаючого меню, наприклад, REST API, PKCS#11, JCE, CNG та KMIP.

ДОДАТИ ОПИС (необов’язково) - Введіть короткий опис програми.

Метод автентифікації - Виберіть потрібний метод автентифікації зі списку доступних опцій в інтерфейсі користувача. Щоб отримати докладнішу інформацію про ці методи автентифікації, див.User's Guide: Authenticationдокументація.

Встановити розмір секретного ключа програми - виберіть потрібний розмір секретного ключа програми в байтах зі спадного меню.

OAuth - увімкніть OAuth, щоб авторизувати програму для виконання крипто-операцій та операцій керування ключами від імені користувача в групах, де користувач має роль адміністратора.

Призначення нової програми групам : Виберіть одну або кілька назв груп у випадаючому меню, щоб пов’язати цю програму з цією(-ими) групою(-ами).

Натисніть кнопку «Зберегти» , щоб додати нову програму.

Нову програму успішно додано до Fortanix DSM.

Зіставлення групи з програмою. Щоб пов’язати нову або існуючу програму з певною групою, можна вибрати один із наведених нижче способів.

Спосіб 1 – Використання пункту меню «Програми» .

Спосіб 2 – Використання кнопки НОВА ПРОГРАМА .

Спосіб 3 – Використання кнопки «ДОДАТИ ПРОГРАМУ» .

Спосіб 1 – Використання пункту меню «Програми»

Виконайте такі кроки:

Перейдіть до меню «Програми» та виберіть потрібну програму зі списку.

У детальному перегляді потрібної програми знайдіть розділ «Групи» та натисніть кнопку «РЕДАГУВАТИ ГРУПИ» (рис.3.8).

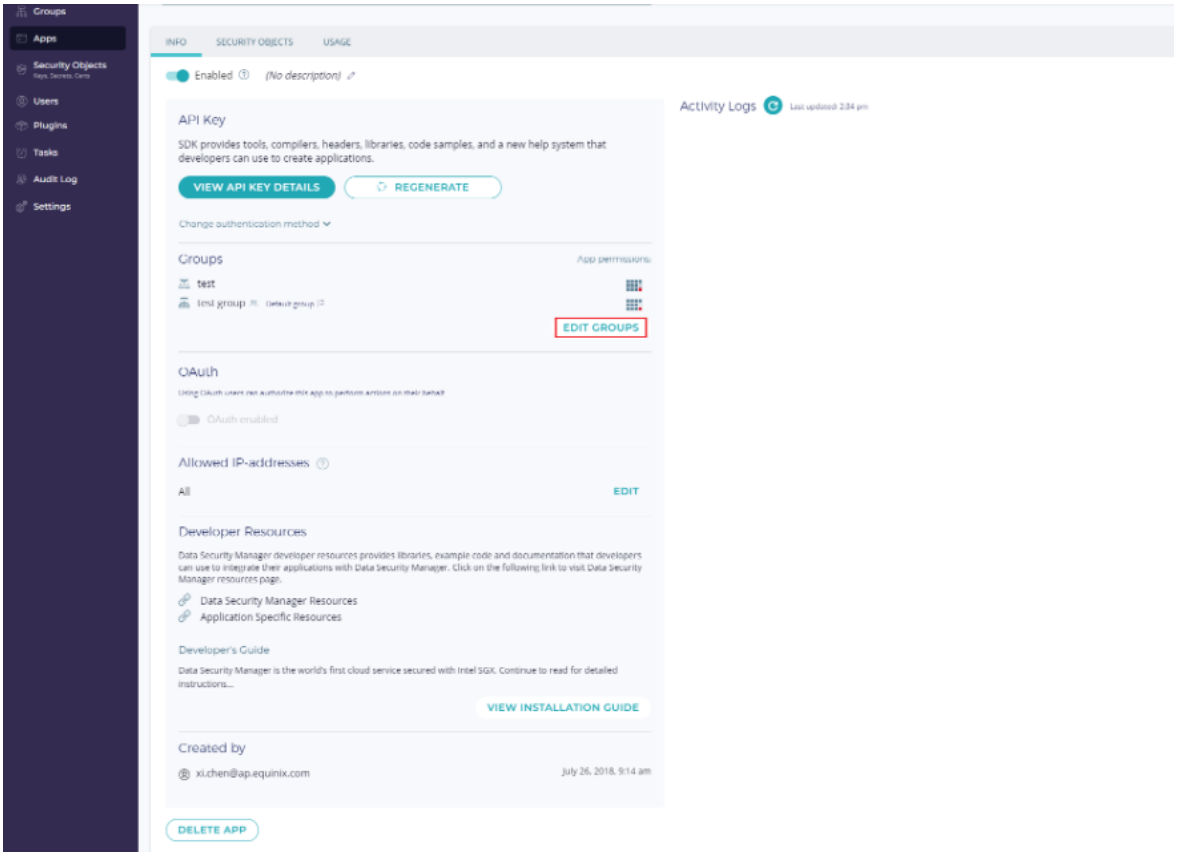

Рис.3.8. Редагування групи для програми

У діалоговому вікні «Зв’язок груп» виберіть існуючу групу з випадаючого меню або натисніть кнопку « СТВОРИТИ НОВУ ГРУПУ» , щоб додати нову групу.

Натисніть кнопку ЗБЕРЕГТИ ЗМІНИ , щоб зберегти оновлення програми.

Спосіб 2 – Використання кнопки НОВА ПРОГРАМА

Виконайте такі кроки:

Перейдіть до вкладки меню «Групи» та виберіть потрібну групу зі списку.

На вкладці «Інформація» натисніть кнопку «НОВА ПРОГРАМА» .

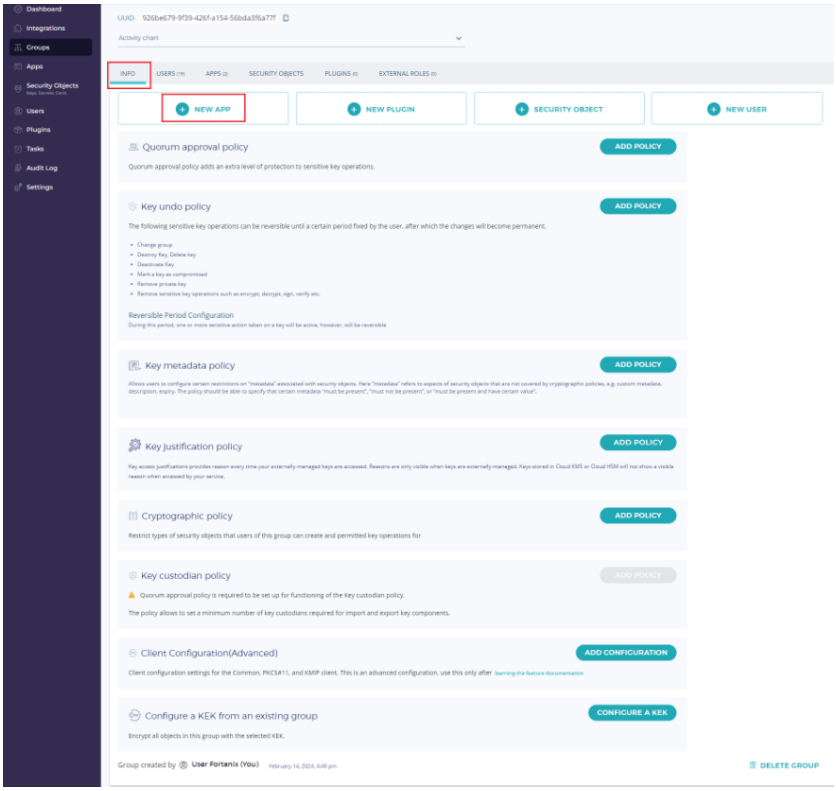

Рис.3.9. Додавання програми до групи

Це перенаправить вас на сторінку додавання нових програм.

Спосіб 3 – Використання кнопки «ДОДАТИ ПРОГРАМУ»

Виконайте такі кроки:

Перейдіть до вкладки меню «Групи» та виберіть потрібну групу зі списку.

У детальному перегляді групи, на вкладці ПРОГРАМИ , натисніть кнопку ДОДАТИ ПРОГРАМУ.

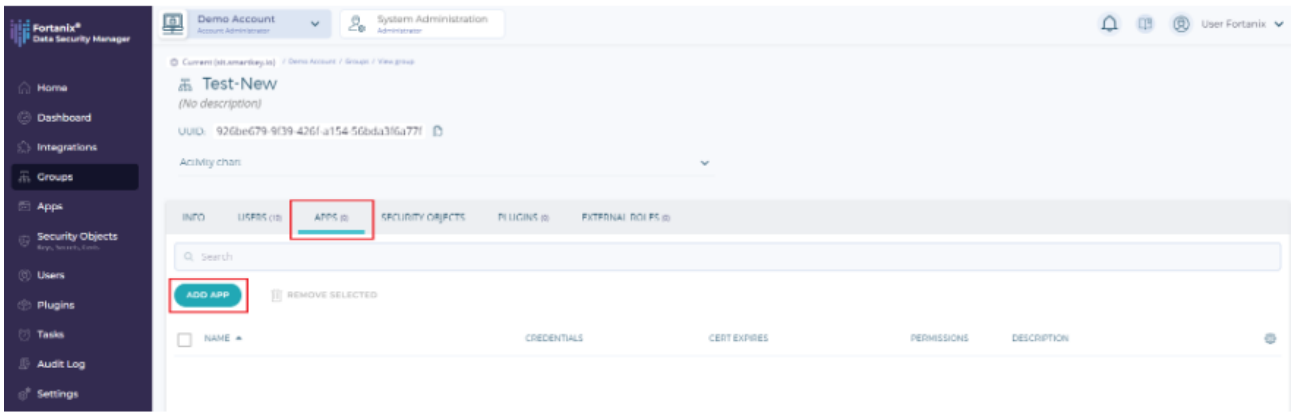

Рис.3.10. Додавання програми до вкладки «Програми»

У діалоговому вікні «Пошук програм для додавання» виберіть одну або кілька існуючих програм, які потрібно пов’язати з цією групою.

Натисніть кнопку ЗБЕРЕГТИ ЗМІНИ, щоб зберегти зміни.

Отже, в результаті ми отримали порядок налаштування Fortanix DSM, щоб була можливість виконувати відповідні дії у системі для різних груп та програм, які використовуються в організаціях.

3.2. Варіант налаштування користувацьких ролей Fortanix DSM

Для подальшої роботи необхідно знати основні кроки для створення іменованих користувацьких ролей, які дозволяють детально контролювати дії користувачів в облікових записах і групах Fortanix DSM.

Функцію налаштування ролей користувачів має ввімкнути системний адміністратор за допомогою налаштувань системного адміністратора після успішного завершення оновлення програмного забезпечення.

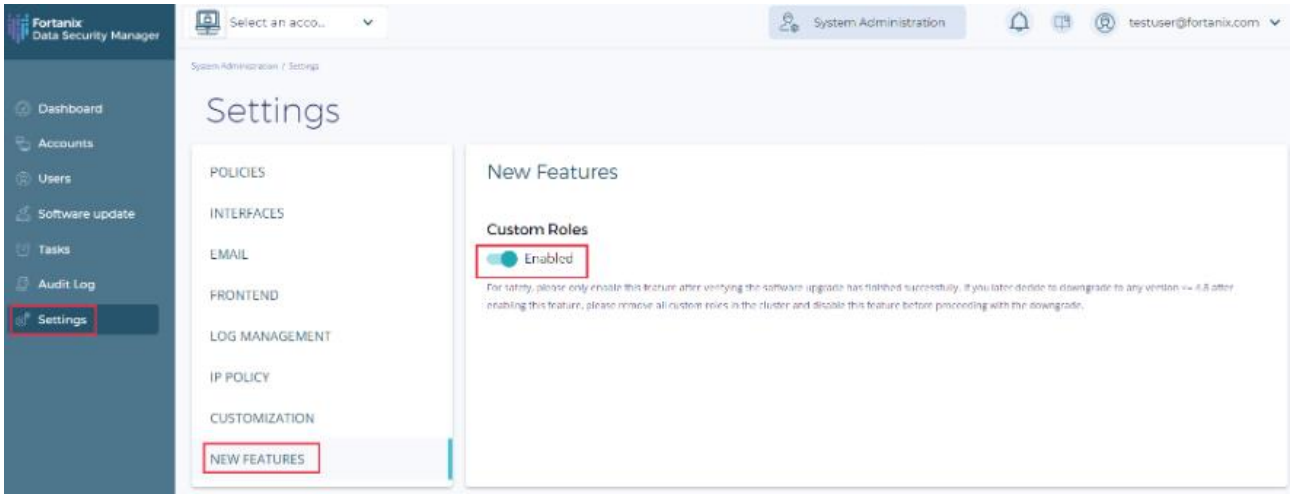

Рис. 3.11. Увімкнення користувацьких ролей

Налаштовані ролі користувачів дозволяють детально контролювати, що можуть робити користувачі в облікових записах і групах Fortanix DSM. Існує два типи налаштовуваних ролей користувачів: *роль налаштованого облікового запису* та *роль налаштованої групи*.

До появи власних ролей користувачів, Fortanix DSM мав лише п’ять вбудованих ролей для користувачів. Це адміністратор облікового запису, учасник облікового запису, аудитор облікового запису, адміністратор групи та аудитор групи. Тепер вони називаються «системними ролями».

Адміністратор облікового запису може створити довільну кількість ролей користувацького облікового запису з налаштованими дозволами облікового запису.

Користувач із роллю «Налаштована група» може мати визначений користувачем набір дозволів, які застосовуватимуться до операцій, запрошених цим користувачем над об’єктами в групі.

Роль користувацького облікового запису має такі властивості:

– дозволи - набір дозволів на рівні облікового запису, призначених користувачеві.

– ексклюзивний - це значення можна встановити на «true» або «false». Якщо роль користувацького облікового запису позначена як «ексклюзивна», тобто її значення встановлено на «true», то її не можна призначити разом з будь-якою іншою роллю.

– роль для всіх груп (необов’язково) - це унікальний ідентифікатор ролі користувацької групи. Якщо це вказано в ролі користувацького облікового запису, це означає, що користувач також матиме вибрану роль групи для всіх груп у Fortanix DSM.

Роль користувацької групи має такі властивості: дозволи: набір дозволів на рівні групи, призначених користувачеві та ексклюзивний.

«Системні ролі» Fortanix DSM визначаються через користувацькі ролі користувачів наступним чином:

- Адміністратор облікового запису:
  - дозволи: усі дозволи облікового запису.
  - ексклюзив: *правда*
  - роль для всіх груп: *Адміністратор групи*
- Учасник облікового запису:

- дозволи: читання та зміна більшості об'єктів в обліковому записі, але не має прав адміністратора в обліковому записі.
- ексклюзив: *правда*
- роль для всіх груп: *немає*

- Аудитор обліку:
  - дозволи: дозволи на читання (наприклад, отримання журналів аудиту тощо) на рівні облікового запису, але не можуть нічого змінювати.
  - ексклюзив: *правда*
  - роль для всіх груп: *Аудитор групи*
- Адміністратор групи:
  - дозволи: усі дозволи групи.
  - ексклюзив: *правда*
- Груповий аудитор:
  - дозволи: дозволи на читання в групі.
  - ексклюзив: *правда*.

Розглянемо порядок творення ролі власного облікового запису, для цього необхідно на головному меню зробити наступні дії.

Щоб створити роль користувацького облікового запису:

1. Клацніть вкладку «*Користувачі*» в головному меню Fortanix DSM.
2. Виберіть вкладку *РОЛІ ОБЛІКОВИХ ЗАПИСІВ (CUSTOM RAILS***)** і натисніть кнопку Додати (Add), щоб додати нову роль.
3. У формі «Додати нову роль користувацького облікового запису»:

a. Введіть назву ролі користувацького облікового запису в полі «*Назва користувацької ролі*».

b. Виберіть «*Ексклюзивна роль*», щоб ця роль користувацького облікового запису залишалася ексклюзивною, тобто її не можна було б призначити разом з будь-якою іншою роллю користувацького облікового запису. Вимкніть її, щоб дозволити додавання додаткових ролей користувацького облікового запису користувачеві на додаток до поточної ролі.

c. Можна налаштувати такі дозволи для ролі користувацького облікового запису:

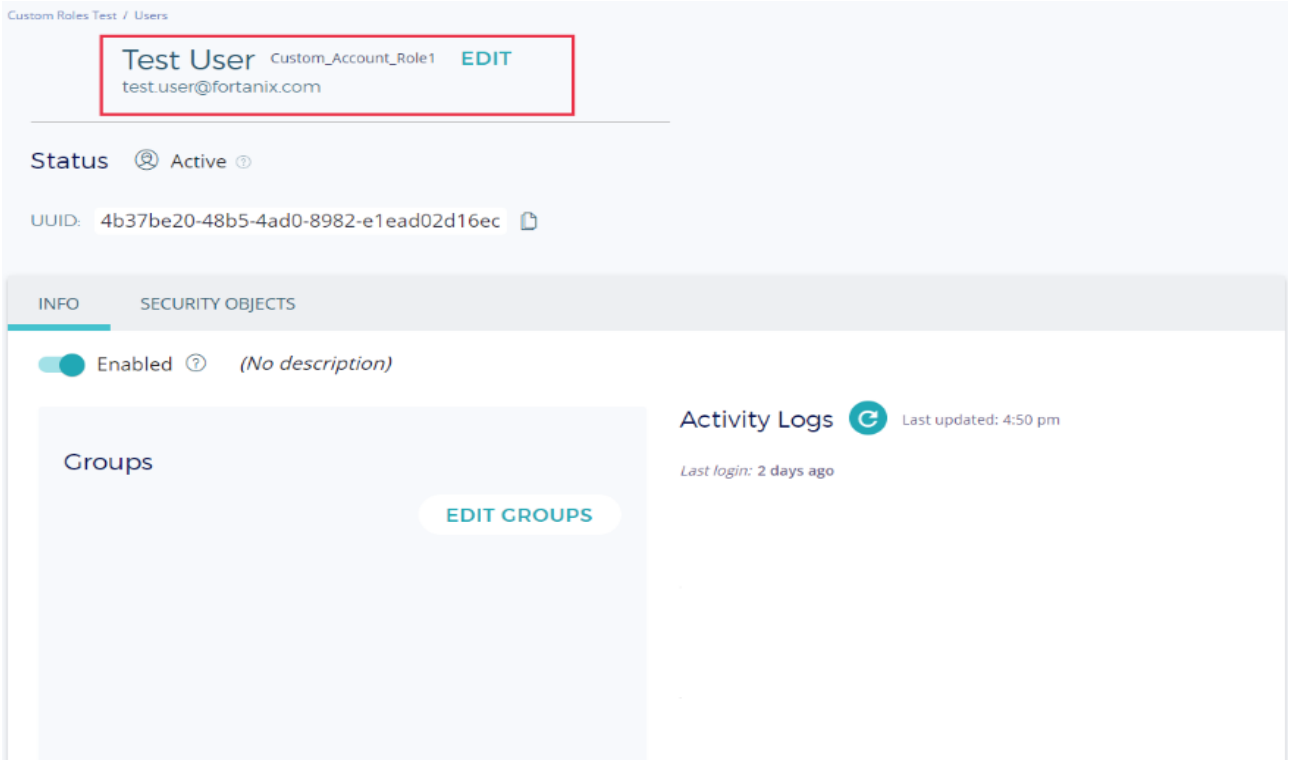

Рис.3.12. Створення та редагування ролі

- *Обліковий запис*
  - Керування журналами. Користувач із цим дозволом може оновлювати налаштування керування журналами в конфігурації облікового запису.
  - Керування автентифікацією. Користувач із цим дозволом може оновлювати налаштування автентифікації в конфігурації облікового запису.
    - Керування CSE робочого простору. Користувач із цим дозволом має право створювати, оновлювати та видаляти налаштування API шифрування на стороні клієнта Google Workspace CSE в конфігурації облікового запису.
    - Керування конфігураціями клієнта облікового запису : Користувач із цим дозволом має право на створення, оновлення та видалення параметрів конфігурації клієнта для клієнтів PKCS#11, KMIP та Common у конфігурації облікового запису

- Політика затвердження створення облікового запису : Користувач із цим дозволом має право створювати політику затвердження кворуму для облікового запису.
  - Встановити термін дії запиту на затвердження. Користувач із цим дозволом може оновлювати час закінчення терміну дії запиту на затвердження кворуму.
  - Оновити атрибути користувацьких метаданих облікового запису. Користувач із цим дозволом може оновлювати атрибути користувацьких метаданих облікового запису.
  - Керування підпискою облікового запису. Користувач із цим дозволом може керувати підпискою облікового запису (стосується лише облікових записів SaaS).
- Керування профілем облікового запису. Користувач із цим дозволом може керувати налаштуваннями профілю облікового запису та мати такі можливості як оновлення назву облікового запису, завантаження власного логотип для облікового запису, оновлювати налаштування країни, опису, організації, телефону та сповіщень.
  - Видалити обліковий запис : Користувач із цим дозволом може видалити обліковий запис.

- *Адміністративні програми*
  - Створення адміністративних програм : Користувач із цим дозволом може створювати адміністративну програму облікового запису.
  - Оновлення адміністративних програм : Користувач із цим дозволом може оновлювати адміністративну програму облікового запису.
  - Видалення адміністративних програм : Користувач із цим дозволом може видаляти адміністративну програму облікового запису.
  - Отримання секретів адміністративної програми : Користувач із цим дозволом може отримувати облікові дані адміністративної програми облікового запису.

- Керування адміністративними програмами : Користувач із цим дозволом може створювати, оновлювати та видаляти адміністративні програми облікового запису, отримувати адміністративну програму облікового запису та отримувати всі адміністративні програми облікового запису.

- *Користувацькі ролі*
  - Створення власних ролей : Користувач із цим дозволом може створювати власну роль облікового запису для користувача.
  - Оновити користувацькі ролі : Користувач із цим дозволом може оновлювати користувацьку роль облікового запису для користувача.
  - Видалення користувацьких ролей : Користувач із цим дозволом може видалити користувацьку роль облікового запису для користувача.
  - Керування власними ролями : Користувач із цим дозволом може створювати, оновлювати та видаляти власну роль облікового запису для користувача.
- *Користувачі*
  - Запрошення користувачів до облікового запису : Користувач із цим дозволом може запрошувати користувачів до облікового запису.
  - Видалення користувачів з облікового запису : Користувач із цим дозволом може видаляти користувачів з облікового запису.
  - Оновити роль облікового запису користувача : Користувач із цим дозволом може оновлювати роль облікового запису іншого користувача. Коли користувач призначає нову роль іншому користувачеві, головний користувач сам повинен мати цю роль, щоб призначити нову роль.
  - Оновити стан увімкнення облікового запису користувача : користувач із цим дозволом може вмикати або вимикати користувача в обліковому записі або обліковому записі клієнта.
  - Керування користувачами облікового запису
- *Зовнішні ролі*
  - Створення зовнішніх ролей : Користувач із цим дозволом може створювати зовнішню роль облікового запису.

- Синхронізація зовнішніх ролей : Користувач із цим дозволом може синхронізувати зовнішні ролі облікового запису.
- Видалення зовнішніх ролей : Користувач із цим дозволом може видалити зовнішню роль облікового запису.
- Керування зовнішніми ролями.

- *Політики об'єктів безпеки*
  - Створення політик об’єктів безпеки облікового запису. Користувач із цим дозволом може створювати різні політики рівня облікового запису.security objectполітики, включаючиCryptographic policy, політика ключових метаданих та політика історії ключів.
  - Оновлення політик об’єктів безпеки облікового запису : Користувач із цим дозволом може оновлювати різні політики об’єктів безпеки на рівні облікового запису, включаючи криптографічну політику, політику метаданих ключів та політику історії ключів.
  - Видалення політик об’єктів безпеки облікового запису : Користувач із цим дозволом може видаляти різні політики об’єктів безпеки на рівні облікового запису, включаючи криптографічну політику, політику метаданих ключів та політику історії ключів.
  - Керування політиками об’єктів безпеки облікового запису : Користувач із цим дозволом може створювати, оновлювати та видаляти різні політики об’єктів безпеки на рівні облікового запису, включаючи криптографічну політику, політику метаданих ключів та політику історії ключів.

- *Дочірні облікові записи*
  - Створення дочірніх облікових записів : Користувач із цим дозволом може створювати обліковий запис орендаря.
  - Оновлення дочірніх облікових записів : Користувач із цим дозволом може оновлювати обліковий запис орендаря.
  - Видалення дочірніх облікових записів : Користувач із цим дозволом може видалити обліковий запис орендаря.

- Створення дочірніх облікових записів : Користувач із цим дозволом може додавати користувачів до облікового запису орендаря.
- Отримання дочірніх облікових записів : Користувач із цим дозволом має право отримувати всі облікові записи орендарів.
- Отримати користувачів дочірнього облікового запису : Користувач із цим дозволом може отримувати всіх користувачів з облікового запису клієнта.
- Керування дочірніми обліковими записами : Користувач із цим дозволом може виконувати всі операції в обліковому записі орендаря.

3.3. Розробка рекомендацій щодо захисту конфіденційно інформації організації

Кожна організація має на меті захистити свою конфіденційну інформацію. Тому фахівцям з кібербезпеки необхідно створювати такі умови, щоб відповідну інформацію могли отримати тільки ті люди, яким це дозволено.

Використання Fortanix для забезпечення безпеки конфіденційних даних, є сучасним підходом для захисту конфіденційної інформації. Захист відбувається для всіх розподілених даних, даних які передаються та дані які зберігаються. Використання такого рішення вимагає від фахівців проводити наступні, рекомендовані дії.

1. Обов’язково проводити ідентифікацію та класифікацію даних. В організації обов’язково необхідно знати про свої дані. Проводьте інвентаризацію даних, щоб зрозуміти, яка конфіденційна інформація існує в організації, де вона зберігається (сервери, хмари, бази даних, кінцеві точки) та хто має до неї доступ. Для класифікації даних, необхідно обов’язково розділіть дані за рівнем чутливості (наприклад, публічні, внутрішні, конфіденційні, суворо конфіденційні). Це допоможе застосовувати відповідні заходи захисту.

2. Створити систему контролю доступу за принципам найменших привілеїв. Таким чином буду надано співробітникам та системам лише той мінімальний

рівень доступу, який необхідний для виконання їхніх робочих функцій. Використовувати ролі для керування правами доступу замість надання індивідуальних дозволів. Це спростить роботу.

Обов’язково періодично перевіряти та оновлювати права доступу, особливо при зміні посад або звільненні співробітників.

Використовувати багатофакторну автентифікацію (MFA) для доступу до критично важливих систем та даних, особливо для віддаленого доступу та адміністративних облікових записів.

3. Впровадити шифрування даних.

У спокої. Шифрувати конфіденційну інформацію, що зберігається в базах даних, на серверах, ноутбуках, мобільних пристроях та у хмарних сховищах.

Під час передачі. Використовувати надійні протоколи шифрування (наприклад, TLS/SSL) для захисту даних під час їх передачі через мережі (внутрішні та зовнішні).

Використовувати шифрування на рівні додатків або токенізацію/маскування: Для особливо чутливих даних використовуйте методи захисту безпосередньо в додатках або замінювати реальні дані на токени/маски.

4. Впровадити безпечне керування ключами. Використовувати централізовані системи (KMS/HSM): Впроваджувати спеціалізовані рішення для безпечної генерації, зберігання, ротації та керування криптографічними ключами. Не зберігайте ключі разом із зашифрованими даними.

5. Захист мережі за рахунок використання брандмауерів, системи виявлення та запобігання вторгненням (IDS/IPS), сегментації мережі для ізоляції критичних систем.

Захист кінцевих точок за рахунок встановлення та регулярно оновленого антивірусного ПЗ та рішення класу EDR (Endpoint Detection and Response) на всіх робочих станціях та серверах. Впровадити політики керування мобільними

6. Проводити навчання та обізнаність співробітників шляхом проведення регулярних тренінгів, які підвищать обізнаність працівників щодо політик

інформаційної безпеки, методів розпізнавання фішингу та інших загроз соціальної інженерії, правил безпечного поводження з даними.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проведено аналіз проблеми, в результаті якого було визначено про необхідність захисту конфіденційної інформації в організаціях. Виток конфіденційної інформації може призвести до того, що організація може отримати фінансові збитки, втрату репутації.

В роботі проаналізовано основні підходи до захисту конфіденційної інформації. Ефективність таких підходів полягає у комплексному підході, який дозволить відповідати Загальному регламенту захисту даних. Щодо основних підходів захисту конфіденційних даних, організації можуть використовувати різноманітні стратегії та методи для захисту конфіденційної інформації від несанкціонованого доступу, розголошення, зміни або знищення. Отже, захист даних повинен передбачати багаторівневий підхід, який зможе поєднувати технологічні рішення, організаційні політики та навчання співробітників.

Проведений аналіз рішень захисту конфіденційних даних дозволив визначити рішення, яке забезпечує багатошаровий захист конфіденційних даних. Fortanix Data Security Manager (DSM) є уніфікованою платформою, яка забезпечує шифрування даних та управління ключами в організаціях, що використовують гібридні та мультихмарні середовища. Дане рішення спрямоване на мінімізацію ризиків витоку даних та забезпечення повного контролю над доступом до інформації.

Аналіз архітектури Fortanix DSM дозволила отримати інформацію щодо складових та основних функцій рішення. Особливість використання такої платформи дозволяє тримати конфіденційні дані зашифрованими протягом усього життєвого циклу даних, а саме під час їх передачі, під час обчислення та під час зберігання. Аналіз функцій платформи Fortanix DSM дозволив отримати зв'язок

між обліковими записами, групами, програмами, ключами, користувачами та плагінами.

В результаті дослідження було розроблено варіант розгортання та налаштування хмарного Fortanix DSM та варіант налаштування користувацьких ролей для організації початкової роботи фахівця з кібербезпеки.

Розроблено загальні рекомендації щодо захисту конфіденційної інформації організацій, які дозволять організаціям відповідати нормам законодавства та використати найкращі методи та засоби.

ПЕРЕЛІК ПОСИЛАНЬ

1. Тріада кібербезпеки. URL: https://www.nist.gov/image/cia-triad .
2. Ідентифікатори співробітників, які можуть виявитися загрозою для вашої компанії. URL: https://deltalogix.blog/en/2021/07/07/internal-attack-4-employee-identikits-that-could-prove-to-be-a-threat-to-your-company/ .
3. Інсайдерські атаки. URL: https://www.ibm.com/think/insights/83-percent-organizations-reported-insider-threats-2024 .
4. GDPR. URL: https://gdpr-info.eu/ .
5. Концепції високої доступності. URL: Fortanix Data Security Manager https://support.fortanix.com/docs/fortanix-data-security-manager-high-availability-concepts-on-prem-only .
6. Посібник з атестації кластера Fortanix Data Security. URL: https://support.fortanix.com/docs/fortanix-data-security-manager-cluster-attestation-guide-on-prem-only .
7. Використання Fortanix Data Security Manager із Veritas NetBackup. URL: https://support.fortanix.com/docs/using-fortanix-data-security-manager-with-veritas-netbackup#40-architecture-diagram .
8. Життєвий цикл безпеки даних. URL: https://www.fortanix.com/blog/beyond-the-buzz-part-1-a-point-of-view-on-the-data-security-lifecycle .
9. HSM as a service. URL: https://www.fortanix.com/solutions/use-case/hsm.
10. Життєвий цикл ключів. URL: https://www.fortanix.com/blog/managing-key-lifecycle-for-enterprise-a-ciso-story .
11. BYOK. URL:https://www.fortanix.com/platform/data-security-manager/bring-your-own-key .
12. Визначення та складові. URL: https://support.fortanix.com/docs/definitions .

13. Початок роботи з DSM. URL: https://support.fortanix.com/docs/users-guide-getting-started-with-fortanix-data-security-manager-ui .

14. HSM. URL:https://support.fortanix.com/v1/docs/users-guide-hsm-gateway .

15. Користувацькі ролі. URL: https://support.fortanix.com/docs/users-guide-custom-role .

16. Закону України "Про інформацію".

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)