ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО—НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ БАЗ ДАНИХ ПІДПРИЄМСТВА»

Виконав студент 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Тимофєєв А.В.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ - 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“24” лютого 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Тимофєєву Артему Вікторовичу
(прізвище, ім’я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо захисту баз даних підприємства»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна інформаційна система;
програмний комплекс IBM Security Guardium Data Protection;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Аналіз баз даних та їх вразливостей
1.1 Визначення БД та їх види
1.2 Необхідність захисту баз даних
1.3 Статистика атак та витоку інформації
2. Дослідження методів захисту баз даних
2.1 Рішення, їх переваги та недоліки

2.2 Порівняння рішень

3. Розробка рекомендацій щодо захисту баз даних підприємства

3.1 Вибір продукту, щодо захисту БД

3.2 Налаштування та захист баз даних підприємства

3.3 Розробка рекомендацій щодо захисту баз даних підприємства на основі IBM Security Guardium Data Protection

Висновки

Перелік посилань

Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Аналіз теоретичних основ щодо захисту баз даних підприємства.	24.02.2023 р.	
2.	Дослідження методів атак на бази даних та визначення типології методів захисту від них.	15.03.2023 р.	
3.	Прикладне вирішення питання атак та визначення вектору можливого вирішення програмними та організаційними методами.	01.04.2023 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів захисту баз даних підприємства.	29.04.2023 р.	
5.	Оформлення результатів дослідження.	20.05.2023 р.	
6.	Підготовка доповіді до захисту.	29.05.2023 р.	

Студент Тимофєєв А.В.

(підпис) прізвище та ініціали

Керівник бакалаврської роботи Марченко В.В.

(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Тимофєєва Артема Вікторовича
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту баз даних підприємства»

Актуальність: У нашому світі цифрові технології і збереження інформації в електронному вигляді стали невід'ємною частиною функціонування багатьох підприємств. Захист баз даних є критично важливим завданням, оскільки вони містять цінну і конфіденційну інформацію. У зв'язку зі зростанням кількості кібератак і загроз безпеці даних, розробка ефективних заходів захисту баз даних стає надзвичайно важливою для забезпечення безпеки і недоступності для несанкціонованого доступу.

Саме тому дослідження захисту баз даних є досить актуальною.

Позитивні сторони:

1. Проведено аналіз баз даних та їх вразливостей, визначено необхідність захисту, включаючи випадки атак на баз даних
2. Досліджено методи та засоби захисту баз даних, їх переваги та недоліки.
3. Розроблено рекомендації щодо організаційних та програмних засобів на основі програмного продукту IBM Security Guardium Data Protection.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково—технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. Використаний програмний продукт наданий на випробувальний період, та не надає повного функціоналу, що не дає можливості провести детальніші дослідження
2. Дослідження були проведені на базі даних, що не дає можливості відобразити всі можливості програмного продукту.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Тимофєєв А.В.** — присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна а кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект—частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Тимофєєв А.В. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
Освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту баз даних підприємства».
Бакалаврська робота і рецензія додаються.
Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Тимофєєв А.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Тимофєєв А.В.*** обрав тему роботи, метою якої було дослідження методів та розроблення рекомендацій щодо захисту баз даних. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Тимофєєв А.В. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Тимофєєва Артема Вікторовича на оцінку **«добре»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна а кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Тимофєєв А.В.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 59 сторінки, 30 рисунків, 3 таблиці, 18 джерел.

Об'єкт дослідження реагування на атаки баз даних підприємства.

Предмет дослідження – методи та засоби боротьби з атаками на бази даних.

Мета роботи – дослідження методів та розроблення рекомендацій щодо захисту баз даних.

Методи дослідження – опрацювання експлуатаційної документації інформації, міжнародні стандарти, практичне випробування.

В роботі приведено основні відомості про корпоративну інформаційну систему, загрози базам даних та кіберзлочини.

Проаналізовано різні види загроз та наведено їх класифікацію.

Досліджено методи та засоби впливу атак на бази даних підприємств та визначено можливі способи протидії.

Дослідження проведені на основі програмного засобу IBM Security Guardium Data Protection.

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування програмного забезпечення та підвищення рівня обізнаності для запобігання кіберінцидентів з базами даних основою яких є атаки.

Галузь використання – кібербезпека баз даних підприємств.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД - Бази даних

СКБД - Системи керування базами даних

ООБД - Об’єктно-орієнтовані бази даних

ІТ - Інформаційні технології

SQL - Structured query language

GDPR - General Data Protection Regulation

OEM - Original equipment manufactured

SOC - Security Operation Center

ВСТУП

Актуальність дослідження. Ні одне сучасне підприємство не може обійтися без використання баз даних в своїй діяльності. Бази даних – важливий актив для будь-якого підприємства. В базі даних зберігаються персональні або конфіденційні дані, тому необхідно відповідально віднестися до їх захисту.

Будь-які несправності в роботі бази даних можуть спричинити катастрофічні наслідки. За сучасними дослідженнями, збитки в грошовому еквіваленті від порушення хоча б одного з властивостей «конфіденційність-цілісність-доступність» запису бази даних складає від 100 до 250 $. Кошти витрачаються на відновлення втрачених даних, розслідування факту втрати даних, ліквідацію збитків іміджу компанії . Як висновок, проблема забезпечення безпеки баз даних є надзвичайно актуальною.

Під «захистом БД» розуміють різні методи для запобігання несанкціонованому доступу до інформації, що зберігається в таблицях.

Одним з вразливих місць при забезпеченні безпеки даних , є занадто велика кількість людей, які мають доступ до них на різних рівнях. Загрози щодо збереження в базах даних інформації можуть виникнути не тільки ззовні, але і зсередини з боку легальних користувачів. Як типовий приклад - скачування бази даних системним адміністратором перед звільненням, або дії щодо бази даних співробітником, який має доступ до неї за посадовими обов'язками. Таким чином, незалежно від рівня захищеності каналів доступу до інформації, не можна бути абсолютно впевненими, що безпека баз даних відповідає корпоративним вимогам. У банкових установах, наприклад, в базах даних зберігається інформація про клієнтів, їх рахунки, грошові транзакції. Надзвичайно вважлива роль інформації в житті сучасних підприємств призвела до зростання обсягів даних. Більше половини з них зберігаються в форматі баз даних. Часто в загальній масі присутня і «конфіденційна» інформація. Атаки на БД є дуже небезпечними і затратними для підприємств. Зловмисники зазвичай прагнуть отримати доступ до таких видів

інформації, як внутрішня корпоративна інформація, персональні дані співробітників, фінансова інформація, інформація про клієнтів, інтелектуальна власність, аналіз діяльності конкурентів, банківська та транзакційна інформація. Ця інформація зазвичай зберігається в корпоративних сховищах фірм і базах даних різного обсягу. Все це говорить про необхідність забезпечення захисту як операційних систем так і баз даних. Наразі робота по забезпеченню безпеки БД акцентована на подоланні існуючих та вже відомих вразливостей конкретної СКБД. Виробники СКБД обмежуються розвитком концепції конфіденційності, цілісності та доступності даних. Даний підхід вирішує конкретні завдання, проте не сприяє розробці загальної концепції безпеки для СКБД. Це ускладнює завдання щодо забезпечення безпеки сховищ даних на підприємствах.

Запорука успішного захисту БД – це визначення даних, які потребують захисту (інтелектуальна власність, фінансова інформація, персональні дані) та методів захисту їх від різних типів загроз. Для розробки процесу забезпечення безпеки БД необхідно розуміти чинні стандарти, такі як PCI DSS, ФЗ «Про персональні дані», закон Сарбейнса-Окслі, Basel II та ін. Також, дії щодо безпеки БД повинні бути інтегровані з загальним процесом забезпечення інформаційної безпеки корпоративної мережі. Таким чином, сучасні дослідження безпеки систем управління базами даних обмежуються розвитком і покращенням концепції конфіденційності, доступності і цілісності даних, але це не відповідає сучасним вимогам щодо систем захисту та інформаційної безпеки програмного забезепечення в контексті конкретних методів захисту.

Об'єкт дослідження – реагування на кіберінциденти як складова частина забезпечення безпеки баз даних підприємства.

Предмет дослідження – методи та засоби боротьби з атаками на бази даних.

Мета роботи – дослідження методів та розроблення рекомендацій щодо захисту баз даних.

Завдання бакалаврської роботи:

Методи дослідження – опрацювання експлуатаційної документації інформації, міжнародні стандарти, практичне випробування.

Практичне значення одержаних результатів: рекомендації щодо захисту баз даних можуть бути використані у сфері забезпечення кібербезпеки у підприємствах.

1 АНАЛІЗ БАЗ ДАНИХ ТА ЇХ ВРАЗЛИВОСТЕЙ

1.1 Визначення БД та їх різновиди

База даних – сукупність даних, організованих відповідно до концепції, яка описує характеристику цих даних і взаємозв'язки між їх елементами, зберігається в комп'ютері або іншому електронному пристрої.

БД дозволяє організувати, зберігати та управляти великими обсягами інформації, яка може бути доступна для використання різними користувачами. Вона складається з таблиць, які містять інформацію про різні аспекти діяльності організації або індивідуального користувача, такі як клієнти, замовлення, продукти, співробітники та інше [1].

БД може бути використана для збереження, пошуку, оновлення та видалення даних в залежності від потреб користувача. Вона є важливим інструментом для багатьох бізнесів та організацій для ефективного управління даними та прийняття рішень.

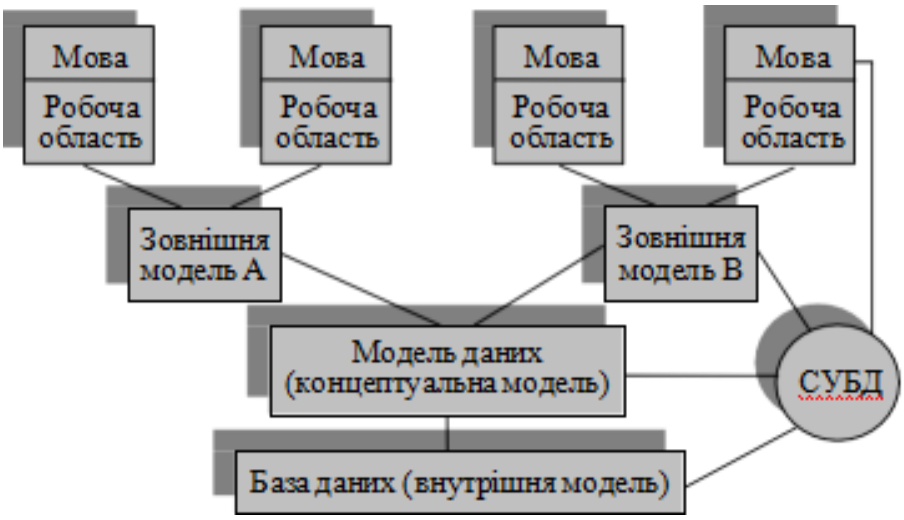

Рис.1.1. Модель бази даних

За загальне управління системою бази даних відповідає адміністратор бази даних, котрий виконує такі функції:

- визначення інформаційного змісту бази даних;

- визначення структури зберігання даних;
- взаємодія з користувачами;
- забезпечення перевірки достовірності інформації;
- визначення повноважень доступу;
- визначення методів архівації та поновлення даних;
- управління ефективністю функціонування СКБД.

Проектування бази даних відбувається на основі концептуальних вимог її кінцевих користувачів. Під час проектування бази даних враховується таке:

- база даних повинна задовольняти актуальним інформаційним потребам;
- дані перед включенням до бази даних повинні перевірятися на достовірність;
- доступ до даних повинні мати тільки особи з відповідними повноваженнями;
- база даних повинна легко розширятися під час реорганізації та збільшення обсягів предметної області.

Етапи проектування бази даних:

1. Визначення мети створення бази даних.
2. Проектування концептуальної моделі бази даних.
3. Проектування зовнішніх моделей даних.
4. Проектування внутрішньої моделі даних.
5. Оцінка внутрішньої моделі даних.
6. Реалізація бази даних.
7. Аналіз ефективності бази даних.

За моделлю організації даних розрізняють такі бази даних :

- *Ієрархічна*. Ієрархічна база даних може бути представлена як дерево, що складається з об'єктів різних рівнів. Між об'єктами існують зв'язки типу «предок-нащадок». При цьому можлива ситуація, коли об'єкт не має нащадків або має їх декілька, тоді як у об'єкта-нащадка обов'язково тільки один предок.

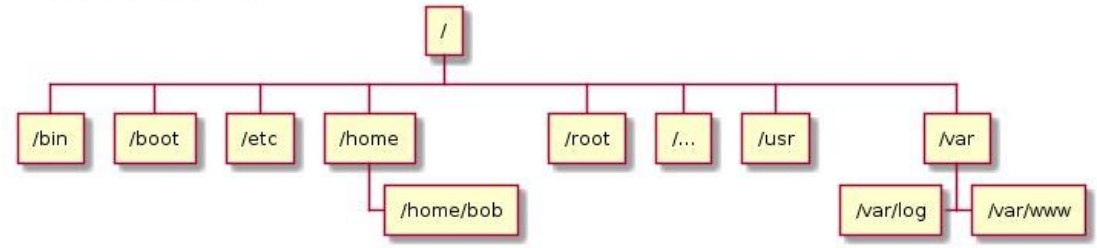

Рис.1.2. Ієрархічна БД

- *Мережна*. Така база даних подібна до ієрархічної, за винятком того, що кожен об'єкт може мати більше одного предка.

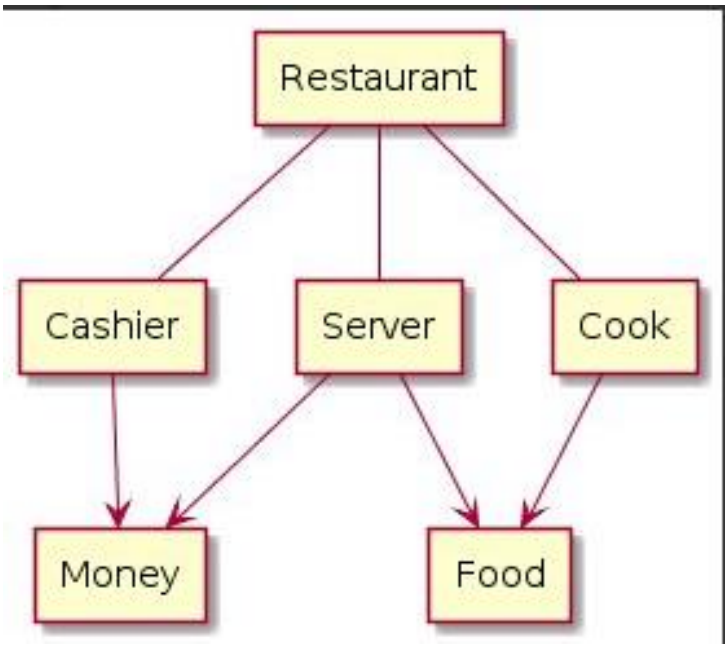

Рис.1.3. Мережна БД

- *Реляційна*. Реляційні бази даних (Relational Database): це тип баз даних, які використовуються для зберігання та організації даних у вигляді таблиць, які складаються зі стовпців і рядків. Реляційні бази даних використовують структуру даних, яка дозволяє зв'язувати дані між собою, що дозволяє більш ефективно працювати з ними.

Можна виділити такі переваги реляційної моделі даних:

- простота. Запити формулюються у термінах інформаційного змісту без урахування складних аспектів системної реалізації;
- непроцедурні запити. Запити можуть бути сформульовані

непроцедурною мовою, тому що вони не будуються на основі заздалегідь визначеної структури;

- незалежність даних. Під час використання реляційної моделі інтерфейс користувача не пов’язаний з фізичною структурою даних та доступом до них;
- теоретичне обґрунтування. Під час проектування бази даних застосовуються методи, які побудовані на нормалізації відношень. Нормалізація — це структурування даних таким чином, щоб уникнути непотрібного дублювання даних та забезпечити швидкий шлях пошуку необхідних даних.

Цитата Мартіна Фаулера про реляційні СКБД

«...багато хто віддав перевагу реляційним системам баз даних, оскільки використовуваний у яких стандартизований мову SQL відкривав можливості безболісного переходу від однієї СКБД до іншої. Хоча скористалися ними практично лише одиниці, думка про можливу зміну постачальника СКБД, не пов'язаної з скільки-небудь відчутними витратами, зігрівала всіх»

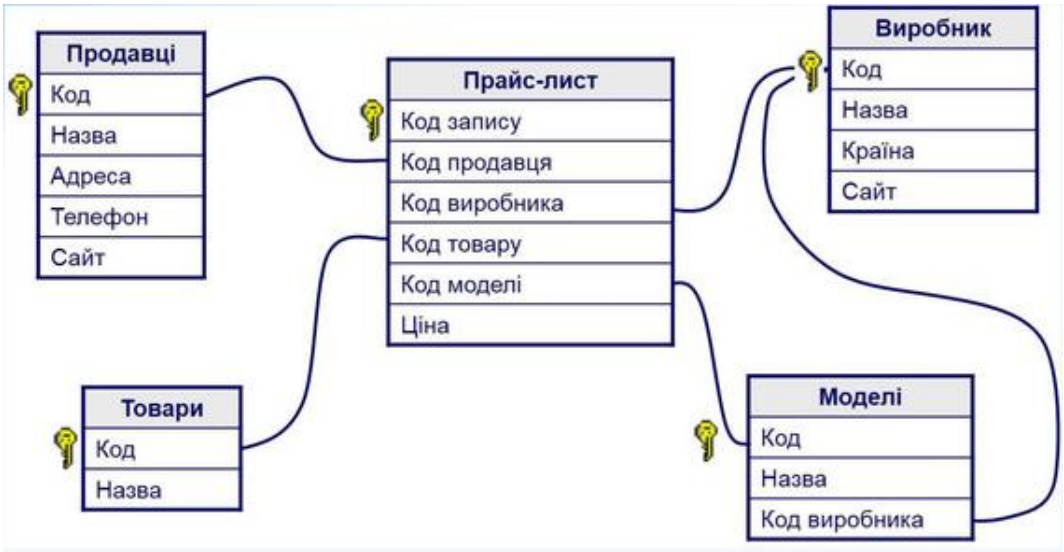

Рис.1.4. Реляційна БД

- *Хмарна*. Ця база даних дозволяє вам зберігати, керувати та отримувати їх структуровані, неструктуровані дані через хмарну платформу. Ці дані доступні через Інтернет. Хмарні бази даних також називають базою даних як послуга (DBaaS), оскільки вони пропонуються як керована служба.
- *NoSQL*. Це підхід до проектування таких баз даних, які можуть вмістити

найрізноманітніші моделі даних, альтернатива традиційним реляційним базам даних, в яких дані розміщуються в таблицях, а схема даних ідеально розроблена до побудови бази даних (корисні для великого набору розподілених даних)

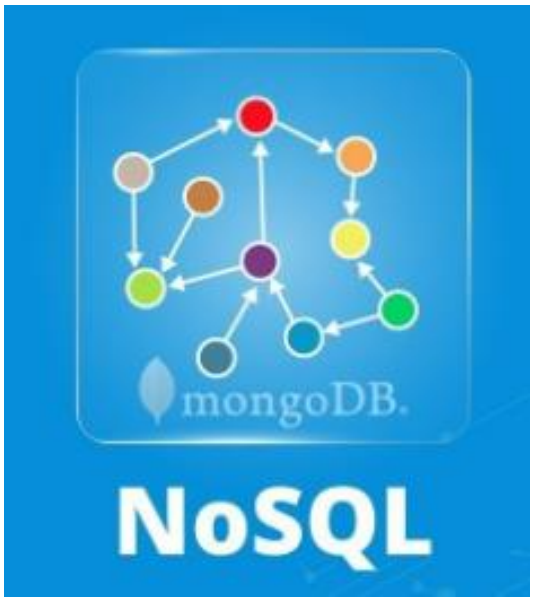

Рис.1.5. NoSQL БД

- *Об'єктно-орієнтована*. Об'єктно-орієнтовані бази даних (ООБД) (Object-Oriented Database): це тип баз даних, які використовуються для зберігання та організації об'єктів, що містять дані та методи, які обробляють ці дані. Об'єктно-орієнтовані бази даних дозволяють використовувати принципи об'єктно-орієнтованого програмування при роботі з даними [2].

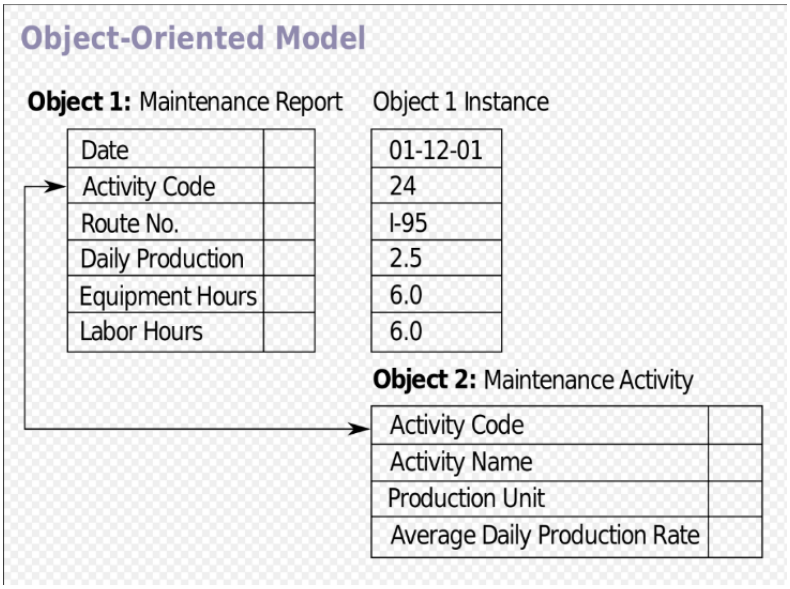

Рис.1.6. Об’єктно-орієнтовна БД

За розміщенням даних виділяють такі види баз :

- Локальна, або централізована. Така база даних підтримується на одному комп'ютері.
- Розподілена. Частини такої бази даних розміщують на різних комп'ютерах мережі.

За технологією фізичного зберігання виділяють:

- БД у вторинній пам'яті (традиційні).
- БД в оперативній пам'яті (in-memory database).
- БД у третинній пам'яті (tertiary database).

1.2 Необхідність захисту баз даних

Є дві основні причини, що змушують приватні компанії та державні установи витрачати все більші суми на захист БД.

По-перше, це кіберзлочинність. Постійне вдосконалення інструменту зловмисників, поява нових програм-вимагачів, безфайлові способи проникнення і ризик того, що хтось зі співробітників виконає дії, що несуть загрозу конфіденційної інформації. Тільки за 2019 рік, згідно з дослідженнями Data Breach QuickView Report, було розкрито понад 9 мільярдів облікових записів, що містять персональну інформацію. За розвитком злочинних технологій розвиваються і рішення, що допомагають захистити таємні відомості. Важливо вживати превентивні заходи, такі як налаштування конфігурації брандмауера, для обмеження доступу до вхідного і вихідного підозрілого трафіку, а також реалізувати рішення і процедури на випадок небажаного порушення безпеки.

По-друге, це проблема відповідності. Міжнародне законодавство щодо захисту персональної інформації постійно вдосконалюється і стає все більш жорстким. Відповідальність за недоторканність конфіденційних відомостей покладається на організації, які їх збирають в процесі своєї діяльності. Причому в залежності від галузі та типу інформаційних активів, нормативні вимоги можуть істотно відрізнятися. Щоб бути конкурентними на ринку, українським компаніям

необхідно відповідати цим стандартам, вкладати більше фінансових ресурсів в забезпечення захисту БД.

Бази даних зберігають широкий спектр інформації, яка є ключовою для діяльності підприємств. Вона може включати наступні типи даних:

Особисті дані клієнтів: Бази даних часто містять особисту інформацію про клієнтів, таку як імена, адреси, номери телефонів, електронні пошти, дані про транзакції та історії покупок. Ці дані є конфіденційними і підприємство має відповідальність зберігати їх в захищеному середовищі.

Фінансові дані: Бази даних можуть містити фінансову інформацію, таку як банківські реквізити клієнтів, кредитні картки, операції з грошима, рахунки та інші фінансові транзакції. Ця інформація є особливо цінною для зловмисників і повинна бути належним чином захищена.

Комерційна інформація: Бази даних можуть містити деталі про продукти або послуги, їх характеристики, ціни, склад та інші важливі комерційні дані. Ця інформація може бути використана конкурентами або зловмисниками з метою викриття комерційної таємниці підприємства.

Дані про співробітників: Бази даних можуть містити особисту інформацію про співробітників, таку як особисті дані, контактну інформацію, деталі про заробітну плату, податкові реквізити, інформацію про працевлаштування та інші документи. Зберігання цих даних безпечним чином є важливим з міркувань конфіденційності та дотримання правил захист [3].

Ще БД можуть зберігати в собі :

Текстові дані: Це включає інформацію у вигляді тексту, таку як назви, описи, коментарі, статті, документи.

Числові дані: Це числові значення, які можуть бути використані для розрахунків, статистики, фінансових даних тощо. Наприклад, це можуть бути ціни, кількість одиниць товару, дохід, вік, рейтинг.

Дати та час: Інформація про дату та час, така як дати народження, дати транзакцій, терміни дії контрактів, графіки роботи.

Фотографії та зображення: Бази даних можуть зберігати фотографії,

зображення, логотипи, діаграми, схеми, графіки.

Відео та аудіо: Бази даних можуть містити відео- та аудіозаписи, наприклад, відео-інструкції, аудіозаписи дзвінків, музичні файли, аудіокниги.

Електронні форми: Це дані, що вводяться в електронні форми, наприклад, дані замовлення, анкети, реєстраційні форм.

Географічні дані: Інформація, пов'язана з місцезнаходженням, наприклад, адреси, географічні координати, картографічні дані.

Відносини між даними: Бази даних дозволяють зберігати зв'язки між різними даними. Наприклад, зв'язок між замовленнями та клієнтами.

Таблиця 1.1

Бази даних за типом

Тип даних	Характеристика
Character	Може містити всі символи клавіатури, максимальна дов- жина — 254
Currency	Грошовий тип, може приймати значення від –900E8 до +900E8, містить 4 дробові розряди
Float	Може містити цифри, десяткову крапку. Максимальна довжина поля — 20 символів
Numeric	Може містити цифри, десяткову крапку. Максимальна довжина поля — 20 символів (ціла частина + дробова частина + 1, якщо є десяткова крапка)

Продовження таблиці 1.1

Бази даних за типом

Тип даних	Характеристика
Date	Містить дату в такому вигляді: місяць/число/рік, напри- клад, 10/31/01
Date Time	Містить дату та час, наприклад, 10/31/01 11:59 PM
Double	Може містити числові дані, але обчислення виконуються з більшою точністю, ніж з даними типу Numeric
Logical	Логічний тип даних. Може приймати два значення T (True) та F (False)
Memo	Дозволяє зберігати текст необмеженого розміру. Дані у цьому випадку зберігаються в іншому файлі
General	Може містити OLE-об’єкти, компоненти Windows, об’єкти, що створені в інших додатках
Character (binary)	Може містити будь-які 8-бітні значення та символ null (0)
Memo (binary)	Дозволяє зберігати відсканові зображення, оцифровану музику тощо

Не варто робити висновки, що якщо у вашій базі даних не зберігається жодних персональних даних користувачів або даних банківських карток, то вона не становить інтересу для зловмисників. Будь-яка інформація несе цінність, і, відповідно, її витік призведе до збитків для організації.

Прикладів може бути багато: скомпрометовані дані програм лояльності, систем обробки замовлень, навіть знеособлені, в руках конкурентів — це потужна зброя. Не кажучи вже про дані, викрадені з банківських систем.

Важливо відзначити, що втрата даних для бізнесу небезпечна не тільки тому, що з отриманих відомостей можна зробити будь-які висновки щодо ведення бізнесу, але й тому, що сам факт розкрадання даних у компанії завдає шкоди її

авторитету [4].

1.3 Статистика атак та витоку інформації

Бази даних, мабуть, досі залишаються найпоширенішою технологією для зберігання та керування важливою для бізнесу цифровою інформацією. Параметри виробничого процесу, конфіденційні фінансові транзакції або конфіденційні записи клієнтів – усі ці цінні корпоративні дані мають бути захищені від компрометації їх цілісності та конфіденційності, не впливаючи на їх доступність для бізнес-процесів. Оскільки все більше і більше компаній здійснюють цифрову трансформацію, проблеми з безпечним зберіганням, обробкою та обміном цифровими даними продовжують зростати. Оскільки середня вартість витоку даних сягає 4 мільйонів доларів США, лише прямі фінансові втрати можуть бути катастрофічними для багатьох компаній, навіть не беручи до уваги непряму репутаційну шкоду. Резонансні «мегазломи», які розкривають мільйони записів конфіденційних даних, можуть легко збільшити ці витрати до сотень мільйонів доларів, але навіть жертви менших зловмисників тепер стикаються з дедалі суворішими штрафами. У наш час більшість компаній використовують різні типи баз даних та інших сховищ даних для структурованої та неструктурованої інформації залежно від потреб свого бізнесу. Нещодавно запроваджені нормативні акти щодо захисту даних, такі як GDPR Європейського Союзу чи нещодавно затверджений CPRA в Каліфорнії (новий Закон про права на конфіденційність значно наблизить законодавство Каліфорнії до еквівалента GDPR) не роблять різниці між реляційними базами даних, озерами даних або файловими сховищами – усі дані однаково чутливі незалежно від основного стека технологій. Просто відслідковувати всю цифрову інформацію є великою проблемою, але розуміння того, які дані є більш конфіденційними відповідно до різних політик і правил, а потім вибір і застосування необхідних можливостей захисту даних і управління вже занадто важке завдання навіть для найбільших компаній. Сфера безпеки баз даних охоплює різні засоби контролю безпеки для самої інформації, яка зберігається та обробляється в системах баз даних, базових

обчислювальних і мережевих інфраструктурах, а також програмах, які отримують доступ до даних. Сюди входять, серед іншого, можливості захисту даних, детальний контроль доступу, моніторинг активності, аудит і функції відповідності, а також інші засоби, необхідні для комплексного багаторівневого захисту від зовнішніх і внутрішніх загроз. Оскільки кількість і різноманітність цифрової інформації, якою керують організації, продовжує зростати, складність IT-інфраструктури, необхідної для підтримки цієї цифрової трансформації, також зростає.

Останнім часом фіксується сплеск витоків даних, передумовою яких виступає банальна незахищеність СКБД від уразливостей; зростає кількість інсайдерських атак, тобто - розкрадань даних співробітниками, в основному з метою подальшого перепродажу. За даними аналітичного центру "Гарда Технології", у 2019 році на чорний ринок баз даних потрапили дані 70 млн. клієнтів більш ніж 40 банків. 91% усіх викрадених баз даних виставлялися на продаж співробітниками банків, 8% - посередниками, наприклад, сторонніми командами. І лише 1% даних стали доступні завдяки вразливості в банківських системах.

Здавалося б, база даних має бути максимально захищена всіма можливими силами. Однак, лише 15% всіх витрат на безпеку спрямовуються на захист баз даних, у той час як на безпеку мережі йде 67%. На жаль, основна проблема недбалого ставлення до питання захищеності даних - людський фактор: або відповідальні особи впевнені, що дані компанії нікому не цікаві і тому не можуть стати кінцевою метою зловмисників, або надто покладаються на засоби інформаційної безпеки компанії (до речі, часто вони обмежуються лише антивірусами та файрволлами). Надмірна довіра роботодавців та неуважність до розмежування прав доступу також відкривають можливості для розкрадання даних власними співробітниками.

Головне, на що хочеться звернути увагу: захист даних потрібно здійснювати на кожному контурі: і на зовнішньому (VPN, Антивірус, міжмережеві екрани тощо), і на середньому (розподіл прав та контроль доступу), і на внутрішньому –

безпосередньо на рівні бази даних!

6 квітня 2022 року компанія InfoWatch опублікувала дослідження витоків інформації обмеженого доступу, зареєстрованих у 2021 році у всьому світі. Усього за аналізований період у відкритих джерелах було 1729 випадків витоку конфіденційної інформації з компаній та держорганів, що на 28,1% менше, ніж за аналогічний період 2020 року (2406 випадків). Скомпрометованими виявилися 8,42 млрд записів персональних (ПДн) та платіжних даних, що на 28,8% менше, ніж у 2020 році, коли кількість записів, що втекли, становила понад 11,82 млрд (за уточненими даними). Кількість записів також виявилася меншою, ніж в аномальному за цим показником 2019 році (15,1 млрд), але більше, ніж у 2018 році (7,24 млрд).

На думку аналітиків InfoWatch, зниження кількості опублікованих у ЗМІ та інших відкритих джерел випадків витоків може бути пов'язане, насамперед, з ослабленням у низці компаній контролю за дистанційними співробітниками внаслідок пандемії (звідси могла зрости латентність витоків внутрішнього характеру) та посиленням у великих компаніях організаційно -технічних заходів щодо захисту інформаційної інфраструктури, у тому числі впровадження DLP-систем. Крім цього, серед причин скорочення кількості витоків, що стали відомими громадськості, автори звіту відзначають поширення раніше викрадених баз конфіденційних даних, необхідних реалізації шахрайських схем. Зокрема, використовуючи дані з витоків минулих років, зловмисники влаштовували атаки фішингу, експлуатуючи теми, пов'язані з виплатами на дітей, дотаціями та іншими заходами підтримки населення під час пандемії. Важливим чинником стримування зростання витоків також стало розвиток шкідливого ПЗ, націленого перш за все на блокування доступу до даних або їх шифрування з метою отримання викупу, а не на викрадення інформації.

У звіті Verizon від 16 серпня 2022 року про розслідування витоків даних йдеться про те, що майже 50% усіх витоків даних сталися через крадіжку облікових даних. Відповідно до того ж звіту, вкрадені облікові дані найчастіше використовуються для атак на веб-програми.

За підсумками 2021 року інциденти, що сталися внаслідок дій зовнішніх порушників, склали майже 2/3 випадків, що є дзеркальною картиною порівняно з тією, що спостерігалася ще кілька років тому, коли основними джерелами порушень виступали співробітники. Це може бути пов'язане зі становленням широкого спектру хакерських угруповань, підвищенням доступності шкідливого програмного забезпечення (у тому числі в міру розвитку моделі RaaS – «шкідливе програмне забезпечення як послуга»). Ймовірно, прийняті в зарубіжних країнах регламенти (наприклад, GDPR у країнах ЄС), які наказують обов'язкове оповіщення регуляторів про витік у найкоротші терміни, можуть суттєво спотворювати реальну картину порушень – у такій ситуації багатьом компаніям вигідно звинувачувати у всьому хакерів, приховуючи, зокрема, прогалини в організації безпечної віддаленої роботи та захищаючи свій імідж. У результаті частка навмисних випадків серед усіх зареєстрованих витоків у глобальному масштабі продовжила зростати та досягла 82%. Частка навмисних витоків внутрішнього характеру (з вини співробітників) знову становила понад 50%.

Розподіл по галузях показав, що до трійки лідерів із витоків стабільно входять високотехнологічні компанії, організації зі сфери охорони здоров'я та держсектор [5].

COVID-19

4 серпня 2020 року експертно-аналітичний центр InfoWatch опублікував дослідження, присвячене вивченню випадків витоків конфіденційної інформації, що стосується коронавірусної інфекції – COVID-19. За перше півріччя 2020 року зафіксовано 72 випадки навмисного чи випадкового витоку у світі. В результаті всіх виявлених витоків скомпрометовано персональні дані 3,43 млн людей у світі.

Дослідження показало, що піковим місяцем за компрометацією конфіденційної інформації став квітень 2020 року, як у глобальному, так і в російському масштабі і великою мірою вони стосувалися компрометації даних пацієнтів з коронавірусом. Майже половина всіх випадків, пов'язаних з COVID-19 у світі сталася з медичних установ, на їхню частку припало понад 43% усіх витоків на тему COVID-19.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ БАЗ ДАНИХ

2.1 Рішення, їх переваги та недоліки

Захист баз даних є важливим завданням для будь-якого підприємства, оскільки вони містять конфіденційну інформацію про клієнтів, співробітників та інші важливі дані, які можуть стати об’єктом крадіжки або кібератак. Ось деякі методи захисту баз даних, які можна використовувати для захисту підприємства:

Аутентифікація та авторизація користувачів: Найбільш простий та ефективний спосіб захисту бази даних полягає в обмеженні доступу до неї за допомогою паролів, логінів та ідентифікаторів користувачів. Необхідно встановити правильні рівні доступу до бази даних для кожного користувача в залежності від його потреб та повноважень.

Шифрування даних: Шифрування даних є одним з найбільш ефективних методів захисту баз даних. Для цього можна використовувати різні алгоритми шифрування, такі як AES, RSA, і т.д. Шифрування даних можна застосовувати для захисту не тільки паролів та логінів користувачів, а й основних даних, що зберігаються в базі даних.

Захист від SQL-ін'єкцій: SQL-ін'єкція є однією з найбільш поширених атак на бази даних. Це вразливість, яка використовується зловмисниками для внесення шкідливого коду в запити до бази даних. Для захисту від SQL-ін'єкцій необхідно використовувати підготовлені запити та обмеження введення користувача.

Аудит та журналювання: Аудит та журналювання баз даних дозволяє виявляти несанкціоновані спроби доступу до бази даних та зберігати інформацію про кожну дію користувачів. Це дозволяє виявляти вразливості та відстежувати зловмисників у разі їхнього вторгнення в систему.

Резервне копіювання: Резервне копіювання є важливим методом захисту баз даних від втрати даних внаслідок випадкових помилок або зламів системи. Резервні копії повинні робитися регулярно і зберігатися в безпечному місці.

Фізична безпека: Безпека фізичного доступу до серверних приміщень, де

зберігаються бази даних, також є важливим методом захисту. Це може включати контроль доступу до серверних приміщень за допомогою карток доступу, відеоспостереження, а також віддалений моніторинг [6].

Ось ще декілька рекомендацій щодо захисту БД :

Захист доступу: Встановлення рівнів доступу до бази даних залежно від ролі користувача. Наприклад, адміністратор баз даних повинен мати повний доступ, а звичайні користувачі повинні мати доступ лише до необхідної для їх роботи інформації.

Моніторинг активності користувачів: Відстеження активності користувачів бази даних. Це допоможе виявити можливі порушення безпеки та запобігти їх поширенню.

Перевірка на вразливості: Регулярна перевірка на наявність вразливостей у базі даних. Це дозволить виявити потенційні проблеми та запобігти їх експлуатації.

Обмеження підключень: Обмеження підключень до бази даних з зовнішніх джерел. Це допоможе запобігти несанкціонованому доступу до бази даних.

Оновлення ПЗ: Регулярне оновлення програмного забезпечення бази даних.

Важливою характеристикою баз даних та клієнтських додатків є їх доступність. Але чим вони доступніші, тим більш вразливі і тим складніших засобів захисту вони потребують, які, в свою чергу, знижують їх доступність. Це замкнене коло ставить перед бізнесом цілий ряд задач, нехтування якими може призвести до втрати конкурентних переваг та зупинки бізнесу. Найефективнішим рішенням буде комплексний підхід з централізованим управлінням [7].

Якщо взяти варіанти задіяних рішень, то отримаємо :

Таблиця 2.1

Програми для управління БД

Назва	Опис	Виробники та продукти
Системи оцінки вразливостей (VA)	Автоматизовані рішення для безперервного моніторингу мережі та оцінки вразливостей. Дають повне уявлення про динаміку змін в мережі і допомагають виявляти нові вразливі місця.	Tenable, GFI
Системи аналітики поведіки користувачів (UEBA)	Рішення на базі машинного навчання для виявлення безпекових аномалій. Використовують розширені способи аналізу всіх типів даних в мережі, а також активності користувачів для виявлення типових і нетипових сценаріїв поведінки.	Microsoft, Exabeam
Системми виявлення загроз на рівні кінцевих пристроїв (EDR)	Рішення для моніторингу активності користувачів на рівні ендпоїнт та пропорційної відповіді у разі виявлення аномальної активності чи прямої загрози. Можуть самостійно ізолювати підозрілий ендпоїнт пристрій та сповіщати команду мережевої безпеки про подію.	McAfee, ESET, Defender, Carbon black, Panda
Системи захисту баз даних (DB Security)	Набори програмних та апаратних інструментів для встановлення та підтримки цілісності, доступності і конфіденційності баз даних.	IBM, Imperva, TrustWave

Продовження таблиці 2.1

Програми для управління БД

Назва	Опис	Виробники та продукти
Системи моніторингу продуктивності додатків (APM)	Програмні засоби APM фіксують дані про ефективність додатків, поведінку користувачів, дані про безпеку та іншу інформацію. Дозволяють не тільки збирати дані для підвищення безпеки мережі, але й оптимізувати користувацький досвід та перевірити функціональність програми додатків.	AppDynamics, Dynatrace
Брандмауери вебдодатків (WAF)	Рішення для HTTP-додатків, які захищають від найбільш поширених атак типу XSS (міжсайтовий скриптинг) та SQL-ін'єкцій. WAF орієнтовані на захист серверів та баз даних.	F5, Fortinet

Серед ризиків безпеці будь-якого типу потенційно піддаються такі :

- Атаки на відмову в обслуговуванні призводять до порушення законного доступу до даних.

- Пошкодження або втрата даних через людські помилки, програмні помилки або саботаж.

- Неналежний доступ до конфіденційних даних з боку адміністраторів або інших облікових записів із надмірними правами.

- Зловмисне програмне забезпечення, фішинг та інші типи кібератак, які компрометують законні облікові записи користувачів.

- Невиправлені вразливості безпеки або проблеми конфігурації в програмному забезпеченні бази даних, які можуть призвести до втрати даних або проблем з доступністю.

- Атаки, спеціально створені для націлювання на бази даних через інтерфейси додатків або API, як-от впровадження SQL для реляційних баз даних і подібні експлойти для рішень NoSQL і Big Data.

- Розкриття конфіденційних даних через погане керування життєвим циклом даних. Це включає в себе неправильно захищені резервні копії, тестування або аналітичні дані без належного маскування тощо.

- Несанкціонований доступ до зашифрованих конфіденційних даних через неправильне керування ключами – це особливо критично для хмарних середовищ, де шифруванням часто керує постачальник хмарних послуг.

- Недостатній моніторинг і аудит – не тільки вони створюють значний ризик невідповідності, але відсутність захищеного від втручання аудиторського сліду також значно ускладнює судові розслідування та реагування на інциденти.

Отже, було розроблено безліч технологій і рішень для усунення цих ризиків, а також забезпечення кращого моніторингу активності та виявлення загроз. Охопити їх усіх лише в одному рейтингу продукту було б досить складно. Крім того, КупінгерКоул (KuppingerCole) давно наголошує на важливості стратегічного підходу до інформаційної безпеки [8].

Тому клієнтам рекомендується дивитися на продукти безпеки баз даних і великих даних не як на ізольовані точкові рішення, а як на частину загальної корпоративної стратегії безпеки, яка базується на багаторівневій архітектурі та об’єднана централізованим управлінням, управлінням і аналітикою.

Вибираючи продукт, обов’язково треба враховувати наступне [9]:

- загальна функціональність
- розмір компанії
- кількість клієнтів
- кількість розробників
- партнерська екосистема
- моделі ліцензування
- підтримка платформи

Продукти та їх характеристика

Amazon Web Services

Переваги :

Широкий вибір спеціально розроблених механізмів баз даних і варіантів неструктурованого зберігання.

Повний набір можливостей захисту даних для реляційних баз даних.

Повністю керована безпека та конфіденційність даних для зберігання S3.

Глибока інтеграція з керуванням ідентифікацією, аналітикою безпеки та іншими службами AWS.

Недоліки :

Доступно лише в хмарі AWS або на інших платформах, розміщених на AWS.

Можливості захисту даних можуть суттєво відрізнятися в різних механізмах баз даних.

Зосереджено лише на керованих службах хмарних баз даних.

Comforte AG

Переваги :

Унікальна надійна, масштабована та відмовостійка архітектура для критично важливих випадків використання.

Підтримуються гнучкість розгортання, гібридна хмара та сценарії як послуга.

Шлюз безпеки для програм SaaS.

Широкий вибір прозорих варіантів інтеграції додатків, підтримка великих даних і потокової обробки

каркаси.

Велика увага до дотримання нормативних вимог, таких як PCI DSS і GDPR.

Недоліки :

Немає можливостей оцінки вразливості.

Механізм виявлення даних є продуктом стороннього OEM.

Дещо обмежена видимість ринку за межами фінансової галузі

Data Sunrise

Переваги :

Тісно інтегрований багатофункціональний пакет безпеки бази даних охоплює всі основні поверхні атак.

Широкий спектр підтримуваних баз даних SQL і NoSQL, неструктурованих сховищ даних.

Підтримка кількох хмарних баз даних і служб зберігання спрощує гібридне розгортання.

Менеджер відповідності нормативним вимогам бази даних автоматизує дотримання основних правил конфіденційності.

Недоліки :

Покладається на хмарні платформи для масштабованості та розгортання високої доступності.

Орієнтований на невеликі компанії, не підходить для проектів масштабу підприємства.

Відносно невелика присутність на ринку.

Delphix

Переваги :

Базується на універсальній, високопродуктивній і економічній технології віртуалізації даних.

Підтримка широкого діапазону типів баз даних і неструктурованих файлових систем.

Можливості прозорого маскування та токенізації даних.

Повністю підтримує робочі процеси самообслуговування для споживачів даних.

Попередньо налаштований для відповідності GDPR.

Недоліки :

Захист даних не є основним напрямком рішення.

Додаткове сховище потрібно надати окремо.

Обмежені функції моніторингу та аналітики

IBM Security Guardium

Переваги :

Повний спектр можливостей безпеки для структурованих і неструктурованих даних.

Підтримка гібридних багатохмарних середовищ.

Розширені великі дані та когнітивна аналітика.

Інтегрована екосистема з продуктами безпеки, ідентифікації й аналітики IBM і сторонніх розробників.

Велика мережа технологічних партнерів і торгових посередників.

Недоліки :

Налаштування та операції можуть бути складними для деяких клієнтів.

Можливості захисту даних на основі технології OEM третьої сторони.

Не зовсім доступний для менших організацій.

Imperva

Переваги :

Інтегрований платформний підхід до захисту даних.

Майже повне охоплення життєвого циклу захисту даних.

Розширена аналітика безпеки та аналітика поведінки.

Велика увага до захисту хмарних даних.

Надзвичайно широка підтримка різнорідних джерел даних.

Недоліки :

Обмежена видимість на ринку безпеки даних, особливо за межами Північної Америки.

Розширені функції захисту даних (шифрування, токенізація), доступні лише через інтеграцію.

Пропозиція SaaS ще не доступна для корпоративних клієнтів.

MS Azure

Переваги :

Сильний досвід як у розробці баз даних, так і в хмарних платформах.

Можливості, доступні майже для всіх етапів життєвого циклу захисту

інформації.

Інноваційна технологія безпечного анклаву для найвищого рівня ізоляції.

Потужне керування доступом і аналітика безпеки в хмарі Azure.

Недоліки :

Більшість функцій доступні лише в хмарі Azure.

Можливості захисту суттєво відрізняються між підтримуваними базами даних.

Виявлення та класифікація даних ще не у виробництві.

Oracle

Переваги :

Автономна хмарна платформа баз даних, що виключає адміністративний доступ людини.

Можливості безпеки інтегровані безпосередньо в ядро бази даних.

Широкий спектр інструментів і послуг для всього життєвого циклу захисту інформації.

Захищена хмарна інфраструктура додає ще один рівень захисту.

Комплексна база даних і оцінка ризиків даних.

Недоліки :

Більшість засобів безпеки підтримують лише бази даних Oracle.

Продукти Big Data і NoSQL ще не інтегровані з рішеннями безпеки RDBMS.

Присутність сегменту ринку DBaaS все ще відносно невелика, але зростає.

Thales

Переваги :

Комплексне виявлення та класифікація даних, прозоре шифрування, токенізація, контроль доступу

і можливості маскування.

Найширша підтримка керування корпоративними ключами, включаючи KMIP, TDE, Always Encrypted і Cloud Key

управління

Висока продуктивність завдяки підтримці апаратного шифрування.

Централізоване керування всіма середовищами, навіть продуктами сторонніх розробників

Стандартні API для додавання підтримки шифрування до існуючих програм.

Недоліки :

Немає можливостей запобігання загрозам.

Інтеграція на рівні програми непрозора, вимагає змін у програмах [10].

2.2 Порівняння рішень

Таблиця 2.2

Оцінка критеріїв рішень

Критерії оцінки	Назва продукту								
	AWS	Comforte	DS	Delphix	IBM	Imperva	Azure	Oracle	Thales
Безпека	5	5	5	4	5	5	5	5	5
Функціональність	3	5	5	3	5	5	4	5	4
Інтероперабельність	4	5	5	4	5	5	4	5	5
Зручність використання	4	5	5	5	5	5	4	5	5
Розгортання	4	5	5	5	5	5	4	5	5

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ БАЗ ДАНИХ ПІДПРИЄМСТВА

3.1 Вибір продукту, щодо захисту БД

Корпорація IBM є багатонаціональною технологічною та консалтинговою компанією зі штаб-квартирою в Армонку, Нью-Йорк, США. Маючи понад 100-річну історію, IBM пройшла шлях від виробника комп'ютерного обладнання до пропозиції широкого спектру програмних рішень та інфраструктури, хостингу та консалтингових послуг на таких цінних ринках, як бізнес-аналітика, аналітика даних, хмарні обчислення, віртуалізація та інформаційна безпека [11].

IBM Security Guardium – комплексна платформа безпеки даних, що забезпечує повний набір функцій, включаючи виявлення та класифікацію, звітування про права, захист даних, моніторинг активності та розширену аналітику безпеки даних у різних середовищах: від файлових систем до баз даних і платформ великих даних до гібридні хмарні інфраструктури.

Серед ключових функцій платформи Guardium — виявлення, класифікація, оцінка вразливості та звітування про права в неоднорідних середовищах даних; шифрування, редагування даних і динамічне маскування в поєднанні зі сповіщеннями в реальному часі та автоматичним блокуванням зловмисного доступу; а також моніторинг активності та розширена аналітика безпеки на основі машинного навчання.

Автоматизована відповідність даних і можливості аудиту з прискорювачами відповідності для певних інфраструктур, таких як PCI, HIPAA, SOX або GDPR, гарантують, що дотримання суворих інструкцій із захисту персональних даних стане безперервним процесом, не залишаючи прогалин ні для аудиторів, ні для зловмисників.

IBM Cloud Pak for Data, сучасна хмарна інтегрована платформа керування даними компанії, тепер підтримує пряму інтеграцію з Guardium для перевірки конфіденційних даних у будь-яких активах, якими керує рішення.

1. Розумійте ризики даних

Сучасні підприємства мають складну IT-інфраструктуру, розгорнуту в гібридних багатохмарних середовищах, створюючи острови конфіденційних даних у структурованих і неструктурованих сховищах. Не знаючи, які активи у вас є, де вони знаходяться та їхні основні ризики, можуть виникнути проблеми безпеки.

За допомогою Guardium Data Protection користувачі можуть планувати виявлення та класифікацію даних, переглядати результати та вживати заходів із оптимізованою видимістю.

2. Виявляйте вразливі місця

Уразливості інфраструктури, якщо їх не усунути, можуть зробити вашу організацію відкритою для шкідливих порушень безпеки. Понад 3200 оціночних тестів Guardium Data Protection допомагають вам завчасно виявляти вразливості, викликані неправильними конфігураціями, пропущеними виправленнями тощо. Ваше підприємство може автоматизувати сканування, переглядати результати, звітувати та вживати своєчасних заходів для зменшення ризиків, перш ніж їх можна буде використати.

3. Державні права

Захист ваших даних означає забезпечення належного доступу потрібних користувачів до потрібних даних за правильних умов. Можливості звітування про права Guardium Data Protection забезпечують детальну видимість привілеїв доступу користувачів вашої бази даних. Звіти про повноваження можна інтегрувати в ширшу програму керування ідентифікацією та доступом, щоб краще перевіряти та затверджувати права.

4. Спростіть відповідність

Розвиваються мандати щодо конфіденційності вимагають від організацій впровадження надійних заходів безпеки, особливо щодо конфіденційних даних. Бути в курсі мінливих нормативних актів і одночасно відстежувати прогрес у підтримці відповідності може бути трудомістким і ресурсомістким завданням. Guardium Data Protection може допомогти прискорити звітування про

відповідність за допомогою керованого підходу до виявлення та класифікації регульованих даних, застосування попередньо визначених політик і звітів для перевірки та затвердження.

5. Виявлення аномалій

Команди безпеки змушені захищатися від складних загроз, спрямованих на їхні дані, багато з яких походять із брандмауерів організації. Зловмисники можуть використовувати викрадені облікові дані, щоб злитися з законними користувачами, що ускладнює виявлення. Guardium Data Protection можна легко налаштувати для виявлення різних зовнішніх і внутрішніх загроз, орієнтованих на дані. Розташовані за ступенем серйозності, загрози можна сортувати, досліджувати та усувати для своєчасного реагування.

6. Захист гібридної хмари

Компанії використовують гібридні мультихмарні технології, щоб отримати гнучкість і конкурентну перевагу. Однак розширення обсягу даних збільшує площу атаки організації, що призводить до додаткових проблем із безпекою даних і відповідністю. Guardium Data Protection допомагає вам керувати безпекою та дотриманням нормативних вимог у локальних і багатохмарних розгортаннях, відстежуючи загрози та забезпечуючи консолідоване централізоване уявлення про ваші ризики та відповідність у ваших середовищах.

7. Оптимізація SOC

З огляду на те, що команди безпеки розтягнуті та стикаються з постійно зростаючою кількістю сповіщень про загрози, сучасні аналітики перевантажені намаганнями щодня керувати тисячами потенційних вразливостей, загроз і атак. Guardium Data Protection генерує високоточні сповіщення шляхом попередньої обробки та фільтрації шуму від відповідних подій. Організації можуть інтегрувати ці сповіщення зі своїм Центром операцій безпеки для кореляції на рівні підприємства, дослідження та своєчасного реагування.

8. Оптимізуйте IT-операції

Ефективна програма захисту даних вимагає тісної співпраці між певними групами зацікавлених сторін, наприклад командами керування базами даних,

власниками додатків та командами IT-інфраструктури. Guardium Data Protection забезпечує міжфункціональну співпрацю шляхом інтеграції з інструментами керування IT-послугами та безпекою, такими як ServiceNow, Cyber Ark, Identity Governance and Intelligence та IBM Security Resilient, для забезпечення операційної ефективності та замкнутого реагування.

9. Guardium Insights

Більшість нормативних актів тепер вимагають від організацій зберігати дані аудиту та мати доступ до них протягом більш тривалого часу; в окремих випадках до трьох-п'яти років. Guardium Data Protection забезпечує повну інтеграцію з IBM Security Guardium Insights для IBM Cloud Pak for Security. Забезпечуючи тривале збереження даних, швидшу звітність і повну видимість даних аудиту, ця інтеграція дозволяє організаціям задовольняти свої звіти про відповідність на вимогу [12.]

Основні функціональні можливості продукту:

- Моніторинг і контроль усієї активності здійснюється за допомогою спеціальних агентів SK-TAP які автоматично виявляють бази даних незалежно від використовуваних протоколів та використання рідного аудиту систем баз даних. Також можливий пасивний моніторинг за допомогою аналізу копії трафіку мережі;

- Багатофакторні політики безпеки – дозволяють обмежувати дії користувачів на підставі правил, які можуть перевіряти, звідки користувач ініціював з'єднання, за допомогою якого програмного забезпечення робиться спроба змінити дані, в який час це відбувається і які саме дані він збирається змінити. Контроль аномалій. Контролює витік типів даних, що захищаються (номери кредитних карт, номери паспортів тощо). Оповіщення про порушення політик та блокування запитів до БД, карантин користувачів. У випадках несанкціонованої або підозрілої активності користувача, компанії можуть вибірково блокувати окремих користувачів, заборонивши їм доступ до системи на певний час, що дозволить уникнути можливої втрати цінних даних, поки ця активність не буде уважно досліджена на предмет зловживань;

- Підтримка різнорідних середовищ – дозволяє здійснювати моніторинг та контроль усіх найбільш поширених СКБД, включаючи Oracle, MS SQL, PostgreSQL, MySQL та інше (більше п'ятдесяти типів);

- Виявлення вразливостей та аналіз ризиків (IBM Guardium VA) – сканує інфраструктури даних (бази даних, сховища даних та середовища великих даних), щоб виявити вразливості та запропонувати заходи щодо їх усунення. Рішення виявляє уразливості, такі як відсутні виправлення, слабкі паролі, несанкціоновані зміни та неправильно налаштовані привілеї. Надаються повні звіти, а також пропозиції щодо усунення всіх уразливостей. Оцінка вразливості виявляє уразливості поведінки, такі як спільне використання облікового запису, надмірні адміністративні входи в систему та незвичайні дії в неробочий час. Він визначає загрози та прогалини у безпеці в базах даних, які можуть бути використані хакерами;

- Динамічне маскування - маскування (заміна) значень чутливих даних горизонтально по рядках і вертикально по колонках, наприклад кредитні дані клієнтів [13].

На рисунку показані декілька параметрів по яким я вибирав цей продукт, а саме [14]:

- Оцінка вразливості
- Відкриття та Класифікація
- Безпека, орієнтована на дані
- Моніторинг та Аналітика
- Запобігання загрозам
- Управління доступом
- Аудит і Відповідність
- Розгортання та Масштабованість

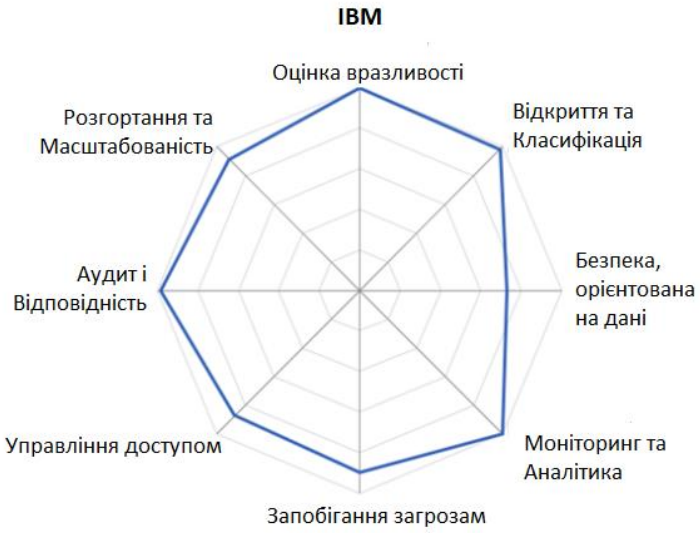

Рис.3.1. Параметри захисту програми

3.2 Налаштування та захист баз даних підприємства

Рис.3.2. Авторизація

Рис.3.3. Початковий екран та бокова панель

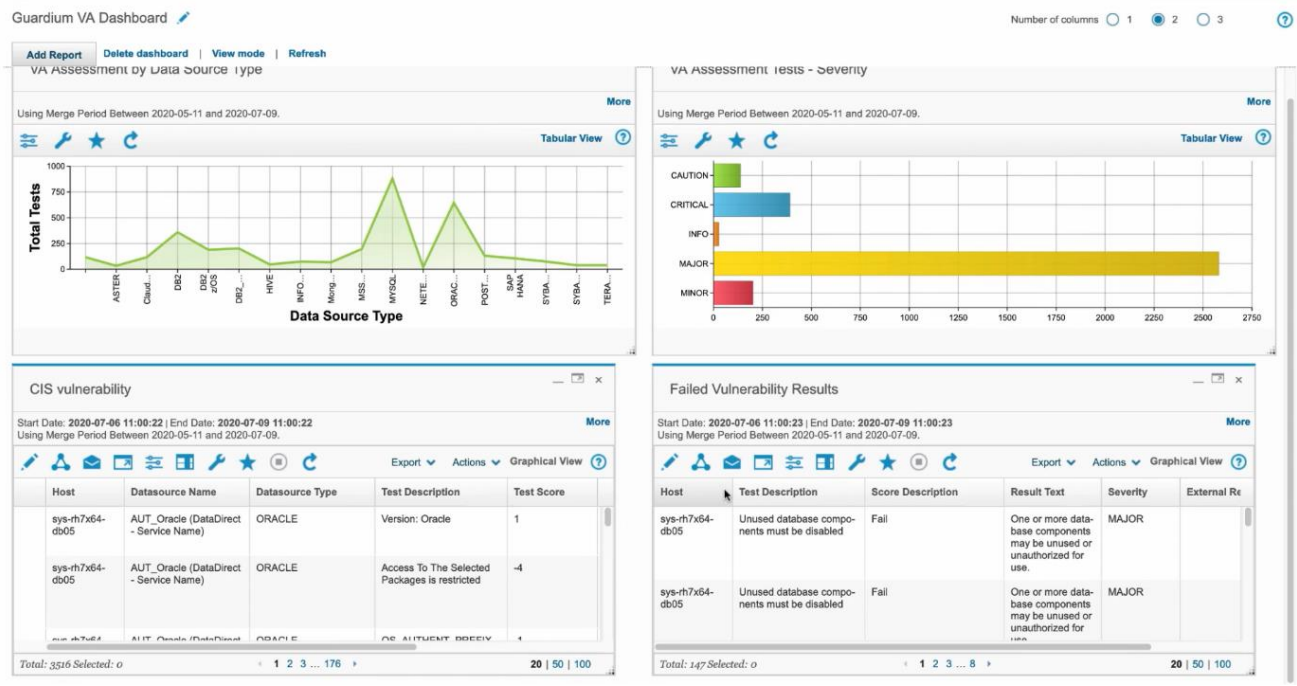

Рис.3.4. Мультивікно сканування вразливостей

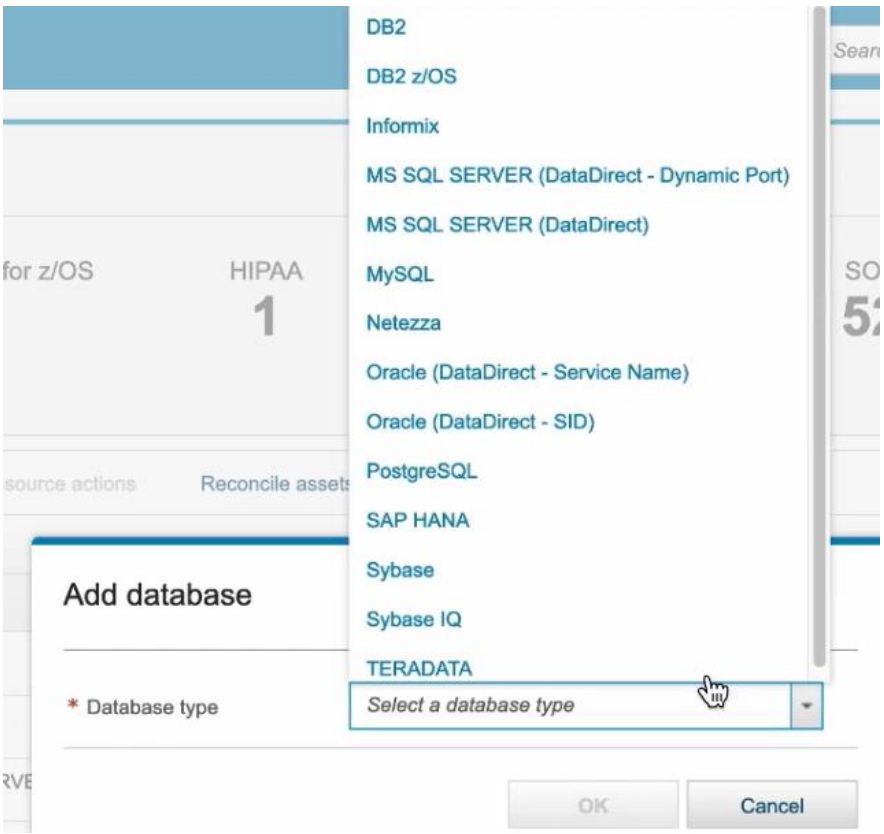

Рис.3.5. Різновиди баз даних які можна додати

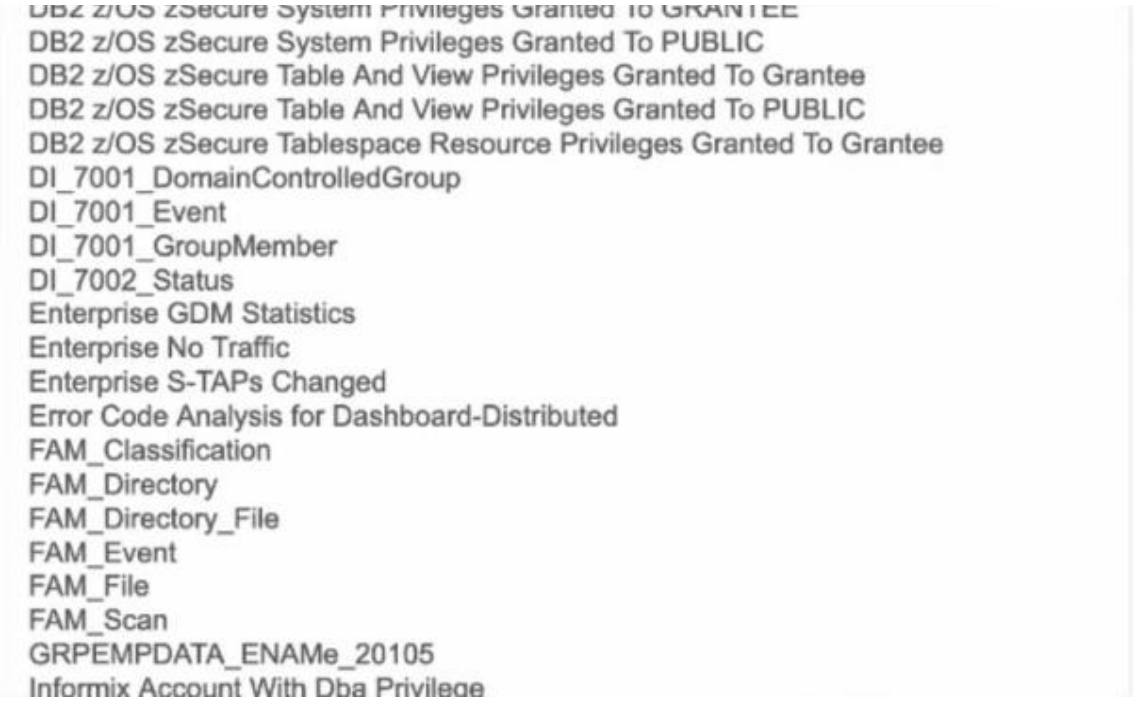

Рис.3.6. Попередньо визначені звіти про права бази даних (шаблони)

Групи та їх налаштування

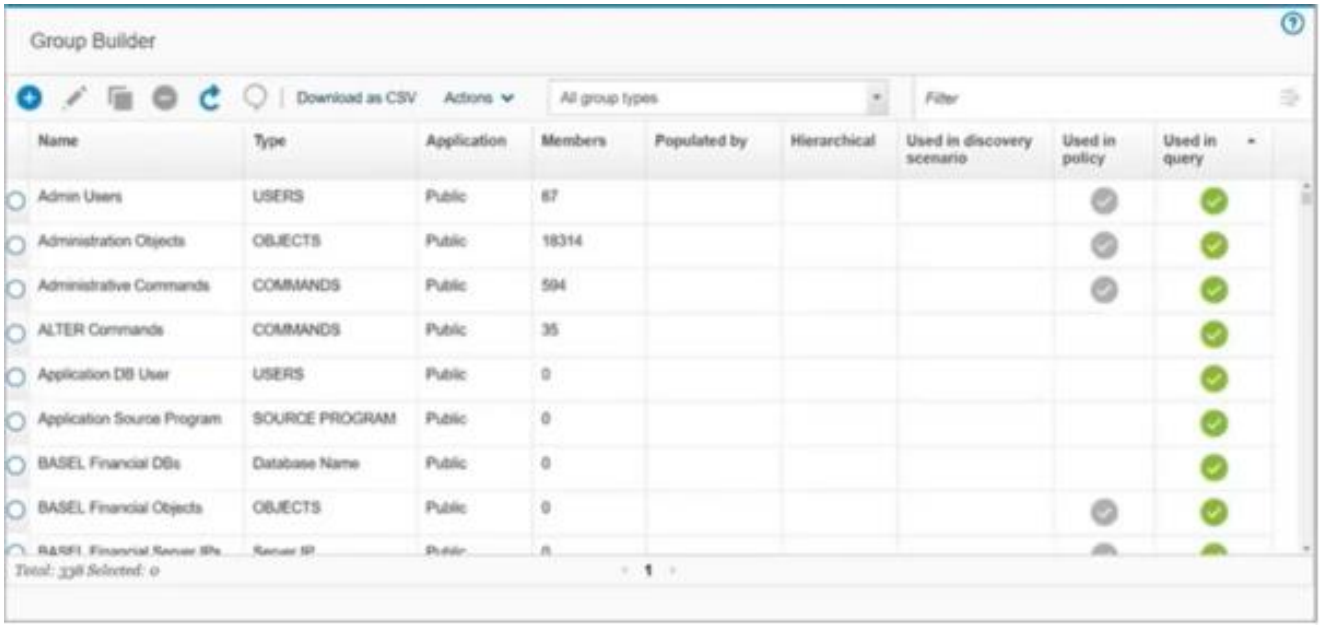

Рис.3.7 - Конструктор груп

Методи створення груп [15]:

1. Вручну
2. Імпорт із CSV
3. LDAP
4. Вибірка з іншої групи
5. Поповнення за допомогою запиту
6. Зовнішнє джерело даних
7. Команд GrdAPI

Де знайти Group Builder ? Setup > Tools and Views > Group Builder

- Список груп у вигляді таблиць; показує існуючі у системі групи; можливість модифікувати, клонувати, видаляти та створювати групи, а також їх поповнювати.

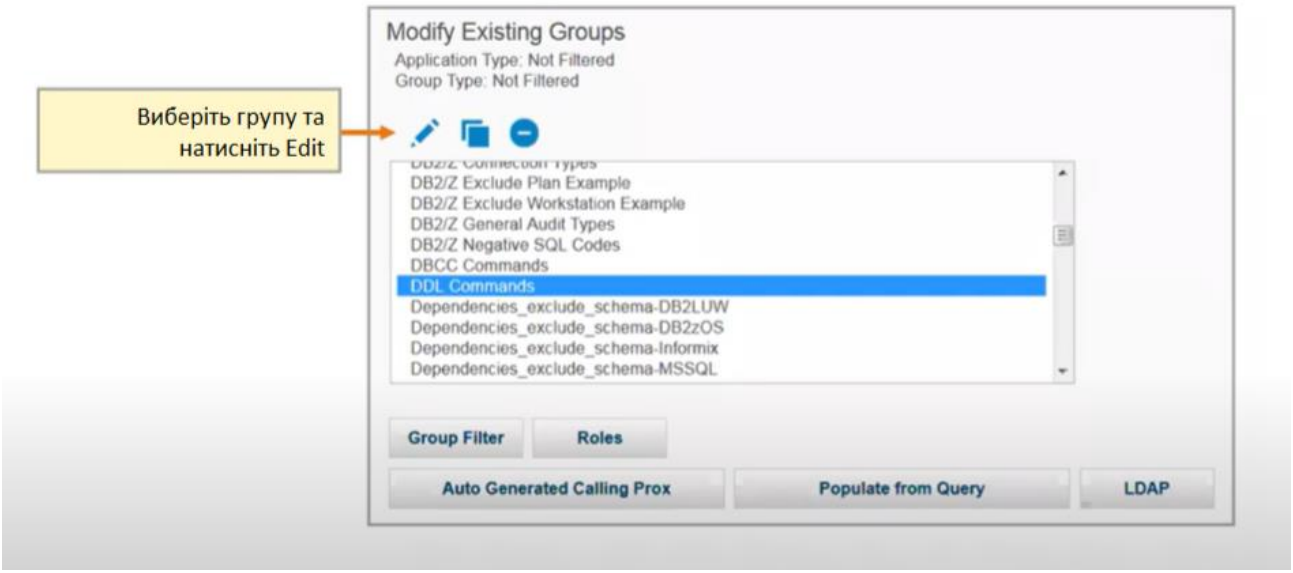

Рис.3.8 Внесення змін

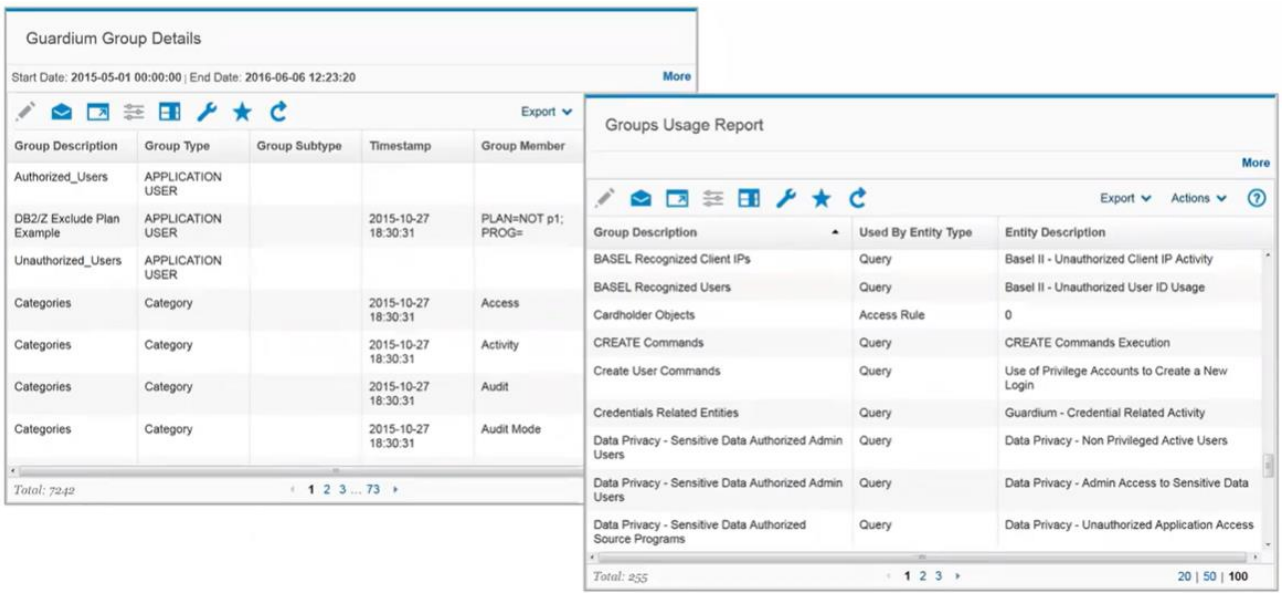

Рис.3.9 Звіти по групам

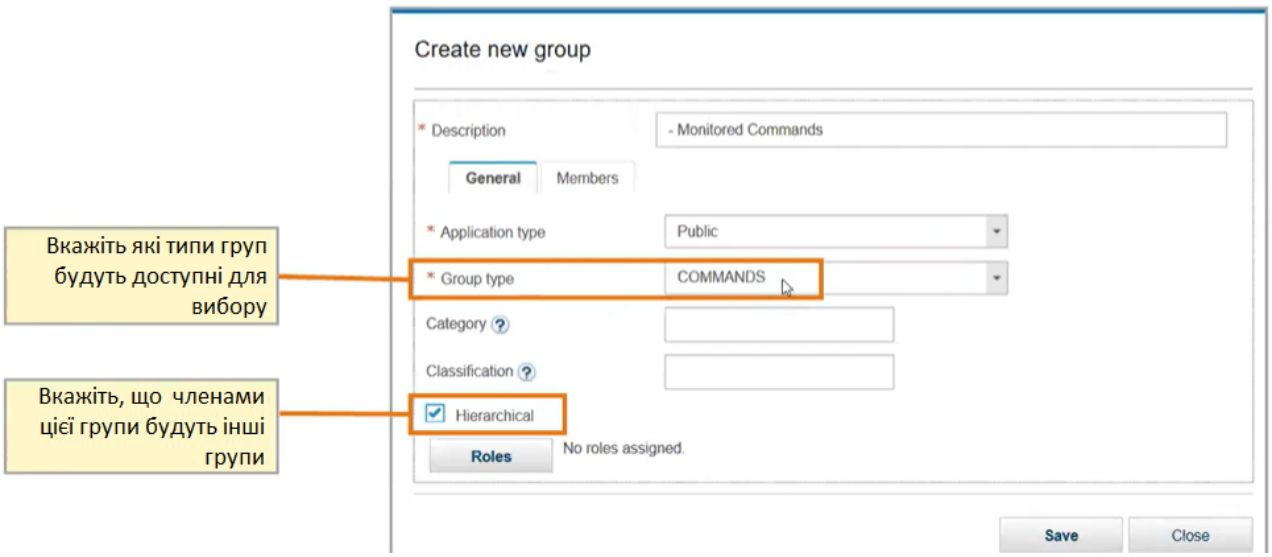

Рис.3.10. Ієрархічні групи

Конструкти та журналування

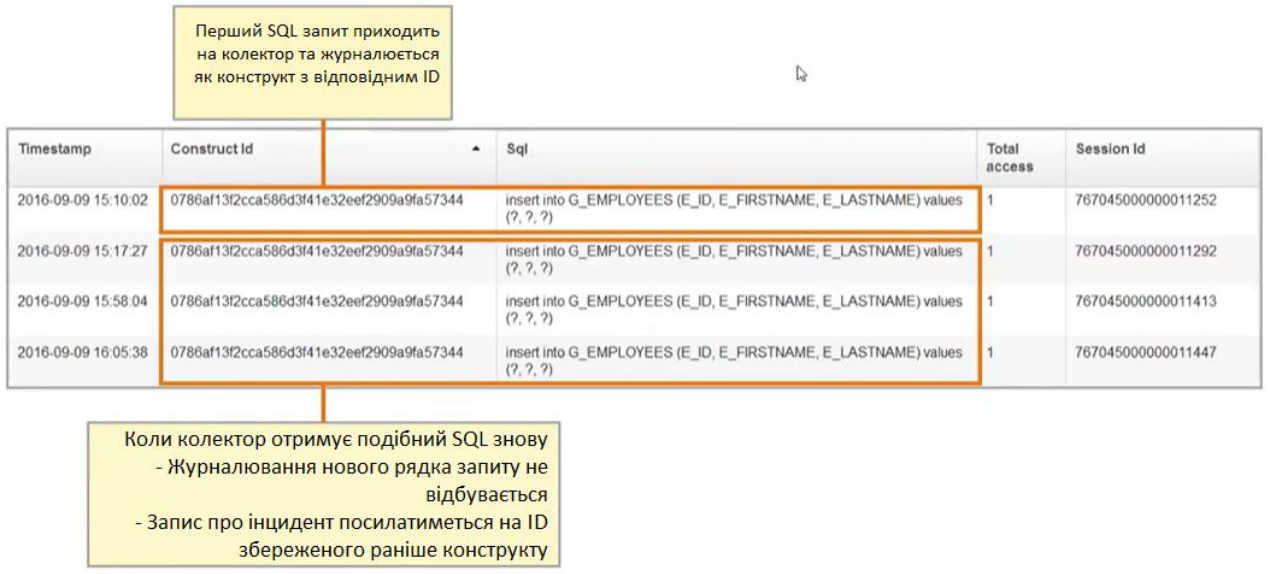

Рис.3.11. Конструкти

Такий метод журналування дозволяє зберегти пристойні обсяги дискового простору.

У наведеному нижче прикладі сніфер записав три записи. Якби кожне входження було окремо зареєстровано, було б зареєстровано 1266 рядків.

Рис.3.12. Економія місця

Інші опції журналування :

- Log full details per session
- Log masked details
- Log only
- Quick parse
- Quick parse native
- Quick parse no fields
- Skip logging

Рис.3.13. Попередньо налаштовані типи регулювання моніторингу (шаблони)

Політики

Забезпечення безпеки даних вимагає застосування політик.

Політика - це впорядкований набір правил, які застосовують сніфер до кожного отриманого запиту.

Типи політик :

Data security

Session level

Classification

File monitoring

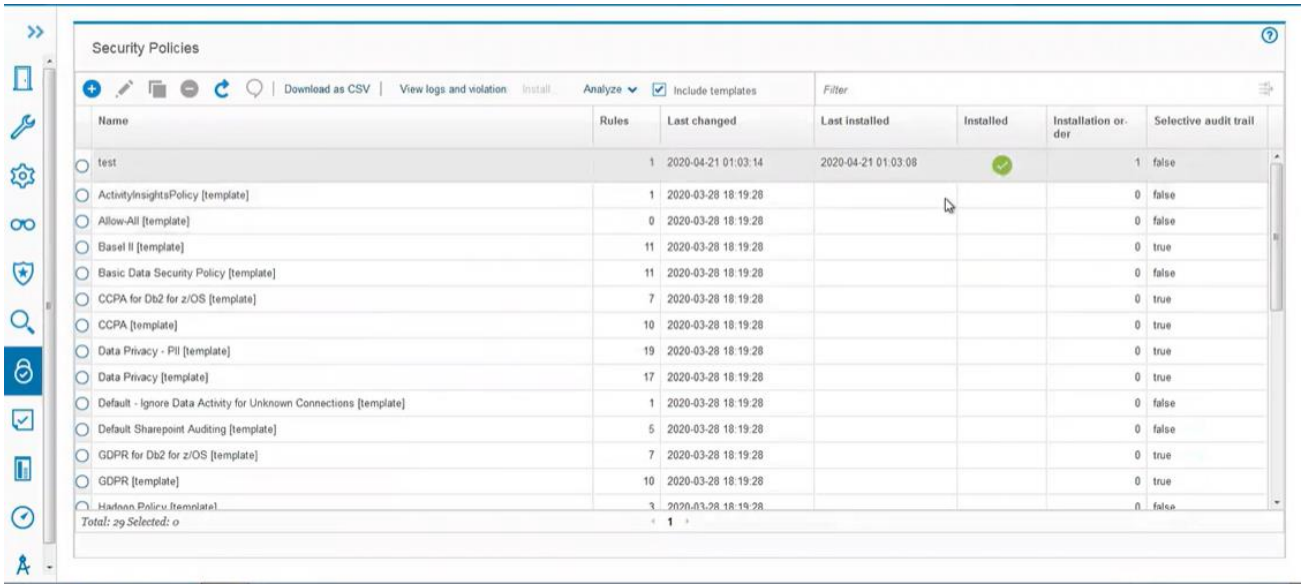

Рис.3.14. Політики

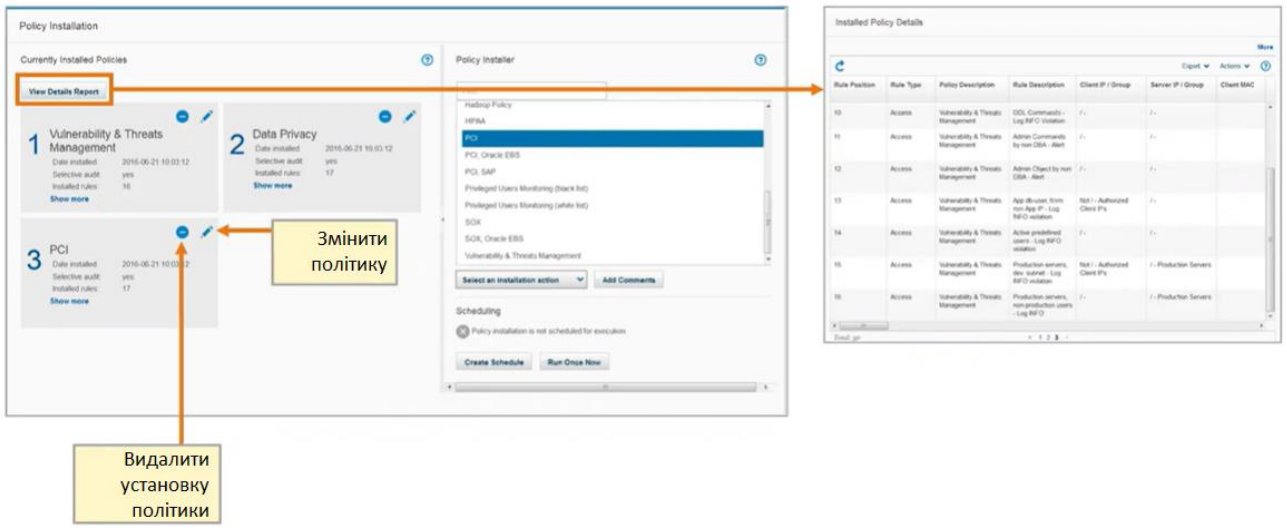

Рис.3.15. Перегляд поточних встановлених політик

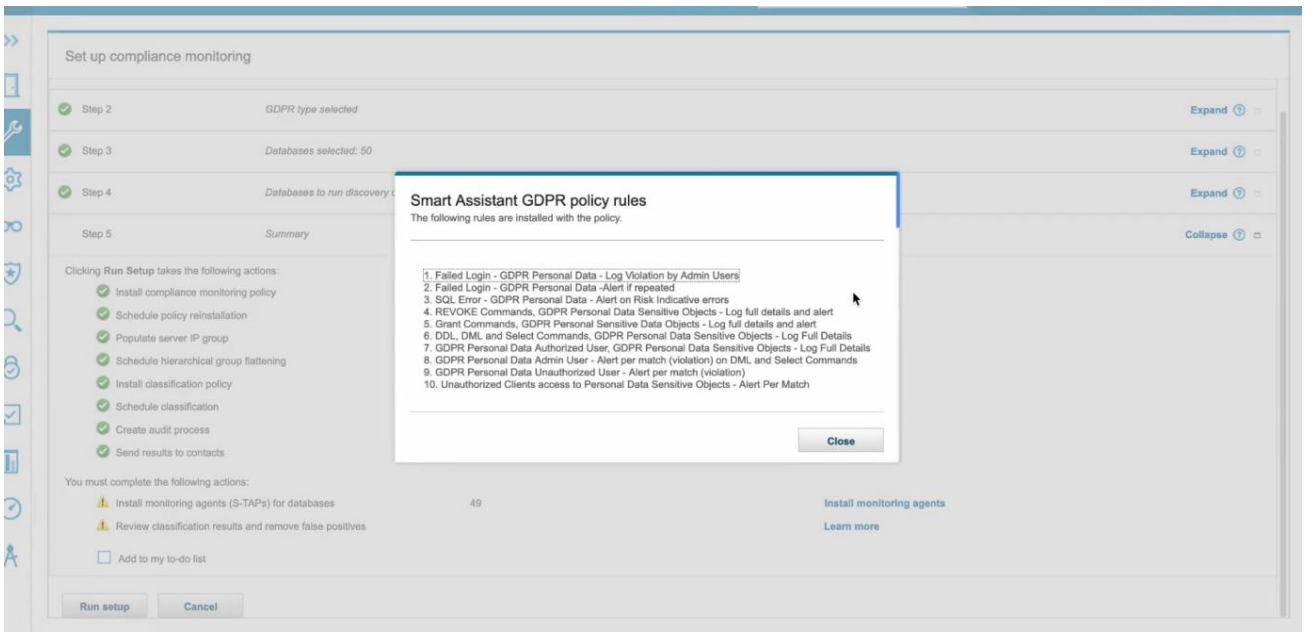

Рис.3.16. Розумний помічник правил політики

В кожній політиці є набір правил. Порядок виконання правил має бути коректним. Дії та налаштування можуть вплинути на логіку, закладену в політиці.

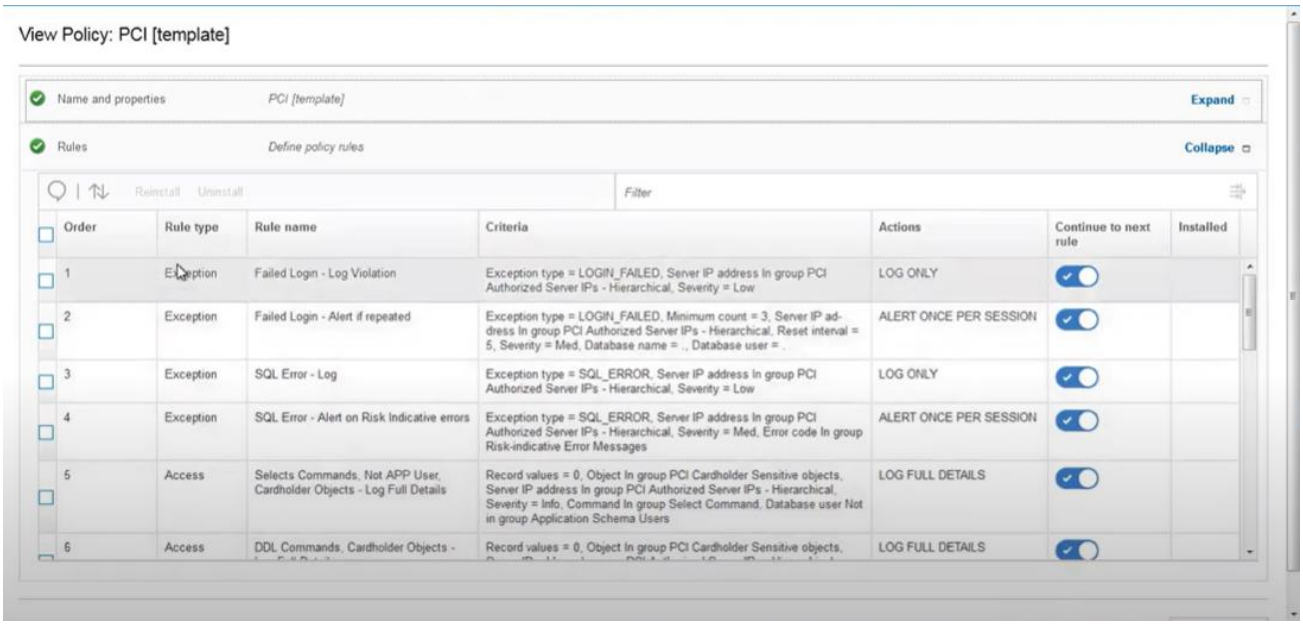

Рис.3.17. Набір правил в політиці

Правила бувають трьох типів :

Access

Exception

Extrusion

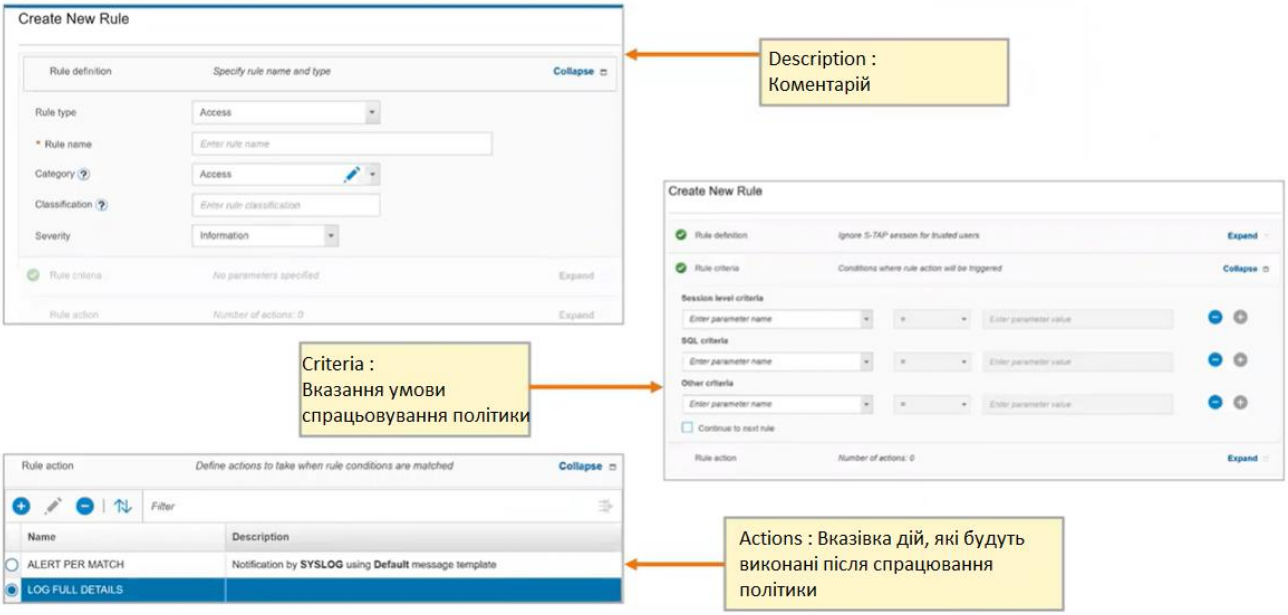

Рис.3.18. Налаштування правил

Опис правил [16]

Rule type : Access, Extrusion, Exception

Rule name : Несе в собі опис застосування правила

Category : Використовуються для угруповання та створення звітів

Classification : Використовуються для угруповання та створення звітів

Severity : Код важливості повідомлення (Info, Low, Medium, High)

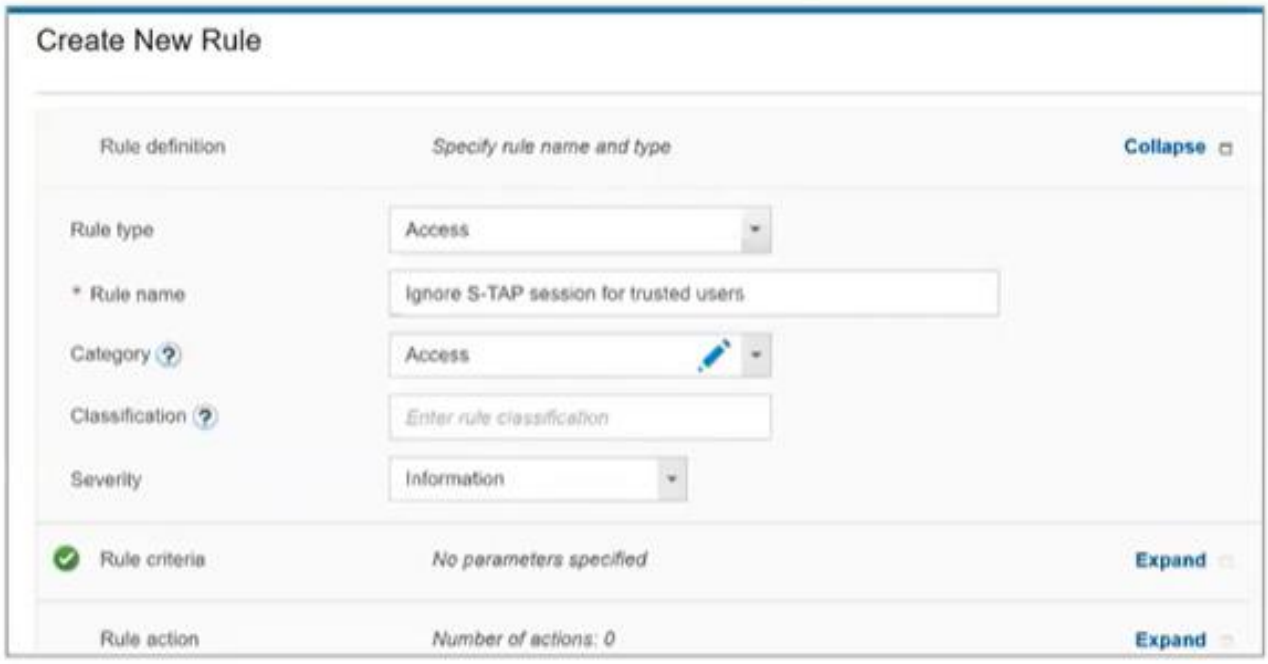

Рис.3.19. Вікно нового правила

3.3 Розробка рекомендацій щодо захисту баз даних підприємства на основі IBM Security Guardium

Клієнт звертається до серверу на якому встановлений S-TAP який зеркалює трафік на Сніфер, після цього отримані дані піддаються парсингу та після цього токени на які були розбиті дані - записуються в базу дани[. Також на малюнку зображено, що за замовчуванням Result sets - не записуються, але їх можна включити. Хочу відзначити, що за замовчуванням записуються : помилки, сам SQL, невдалі спроби виконати щось (напр.log in), інформація по сесії [17].

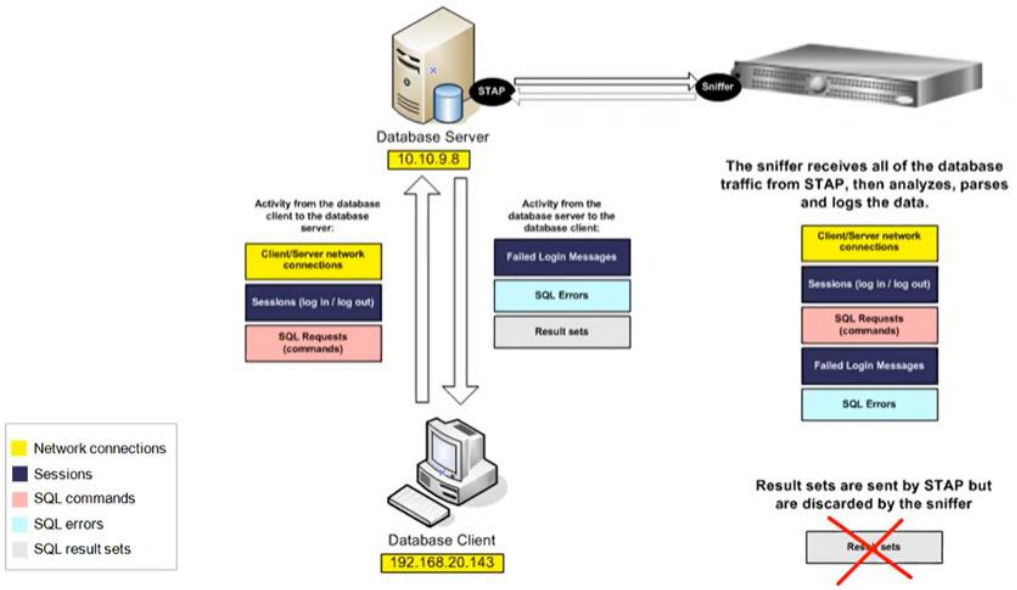

Рис.3.20. Трафік

На малюнку показана основна робота Сніфера : захоплення та аналіз трафіку на стороні колектору, парсинг інформації, виймається SQL та запис.

Приклад токенів :

- IP сервера = 10.10.9.8
- IP клієнта = 192.168.20.143
- Ім’я користувача = Скотт
- Назва програми = SQL Plus (Oracle)

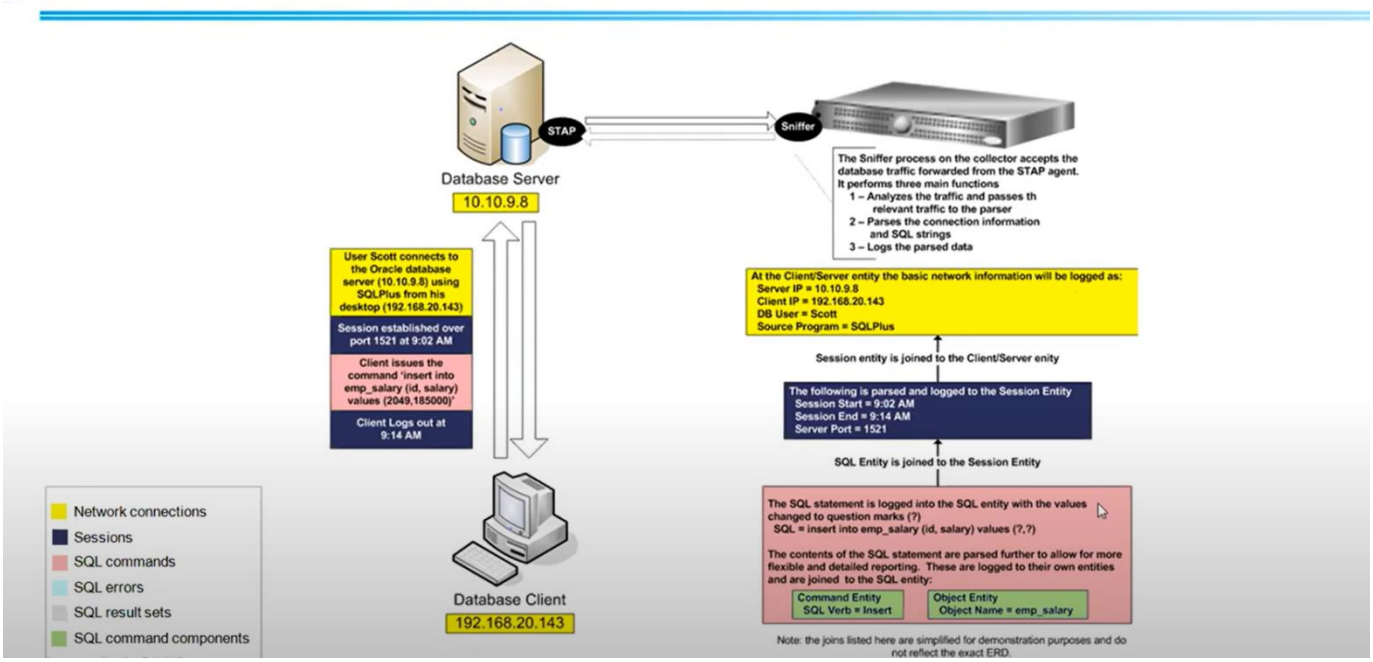

Рис.3.21. Парсинг та журналування

Зображуєтьс S-TAP сесія. На Сніфер передаються дані які захоплюються S-TAP, парсинг, застосовується політика і під наш Access rule підпадає ігноруваання цієї сесії. Запис, що була сесія - обов’язково буде, проте ніяких уточнюючих даних не запише. Можна помітити, що Сніфер передає S-TAP щоб він більше не передавав трафік з певної сесії (вважається що я довіряю цій сесії).

Важливо, що ця дія підпадає тільки під звичайних користувачів, адмінам - ми навпаки всі обмеження посилюємо !

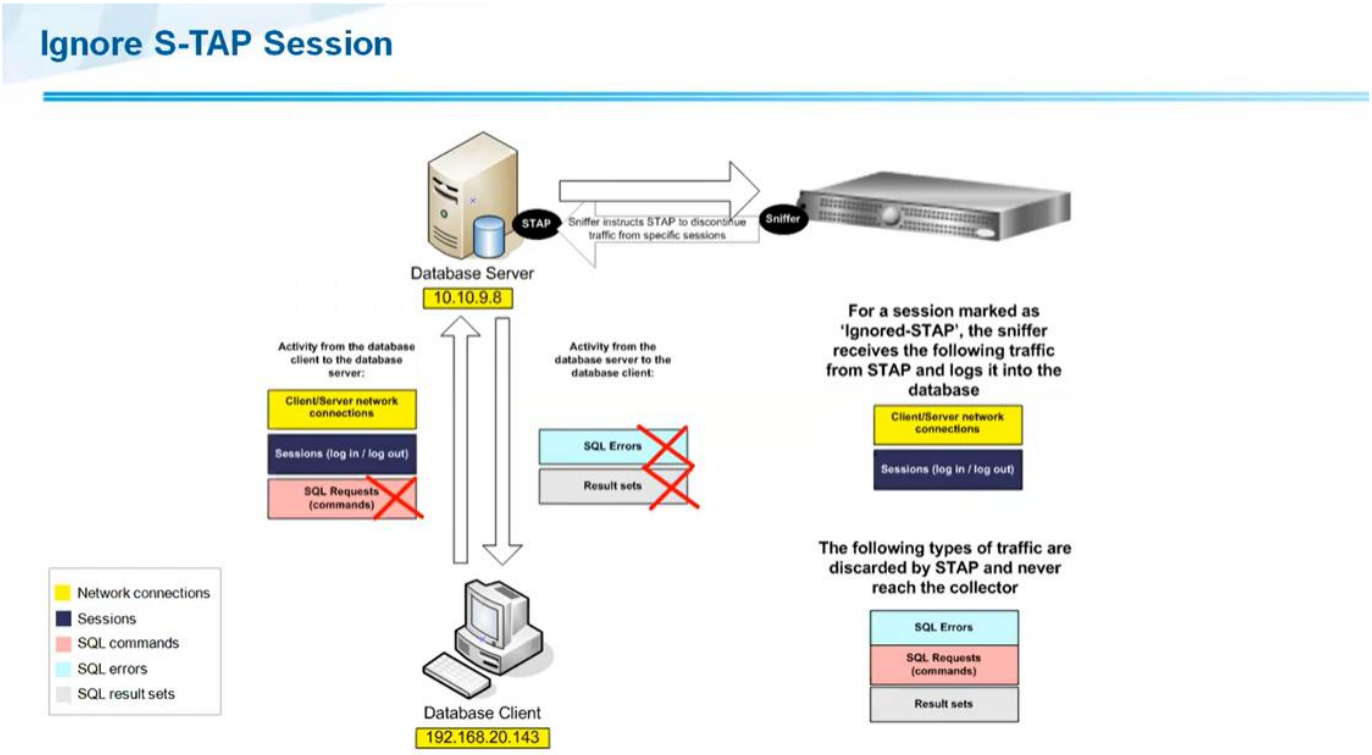

Рис.3.22. Правило ігнорування

Після того як ми починаємо працювати з даними використовуючи Extrusion rules, у нас з'являється багато можливостей, наприклад робота з редакцією і таким чином маскувати деякі чутливі дані. Тобто користувач робить запит з бази даних (в нашому випадку номери соціального страхування), а ми на рівні S-TAP та Extrusion rules застосовуємо маскування. Бачимо, що користувач на виході отримує змінені дані. Користувач не бачить повні дані.

Застосовується здебільшого для користувачів у яких недостатньо прав [18].

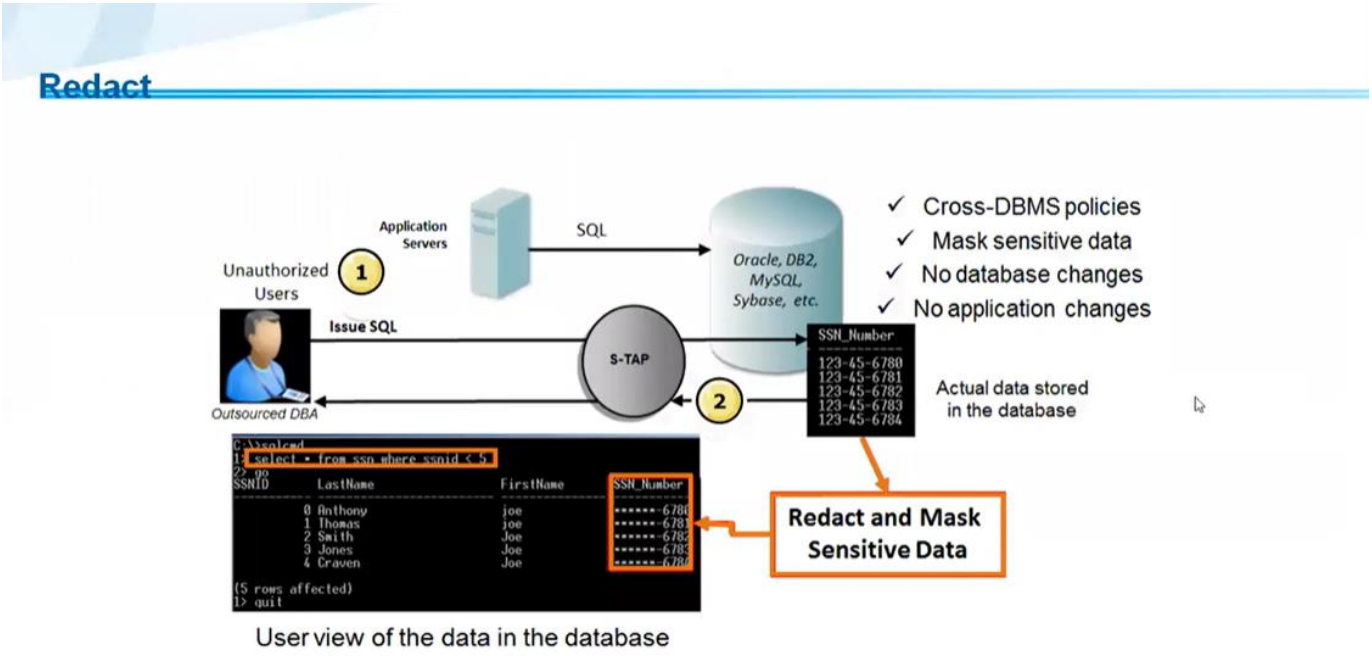

Рис.3.23. Робота приховування даних

S-GATE - це компонент S-TAP. Ще S-GATE називають Guardium Firewall. За замовчуванням виключений (через завелику затримку у відгуку). Функціонал чимсь схожий на редактор, він цікавий тим, що Адміністратор може запобігти доступ до даних (перервати сесію).

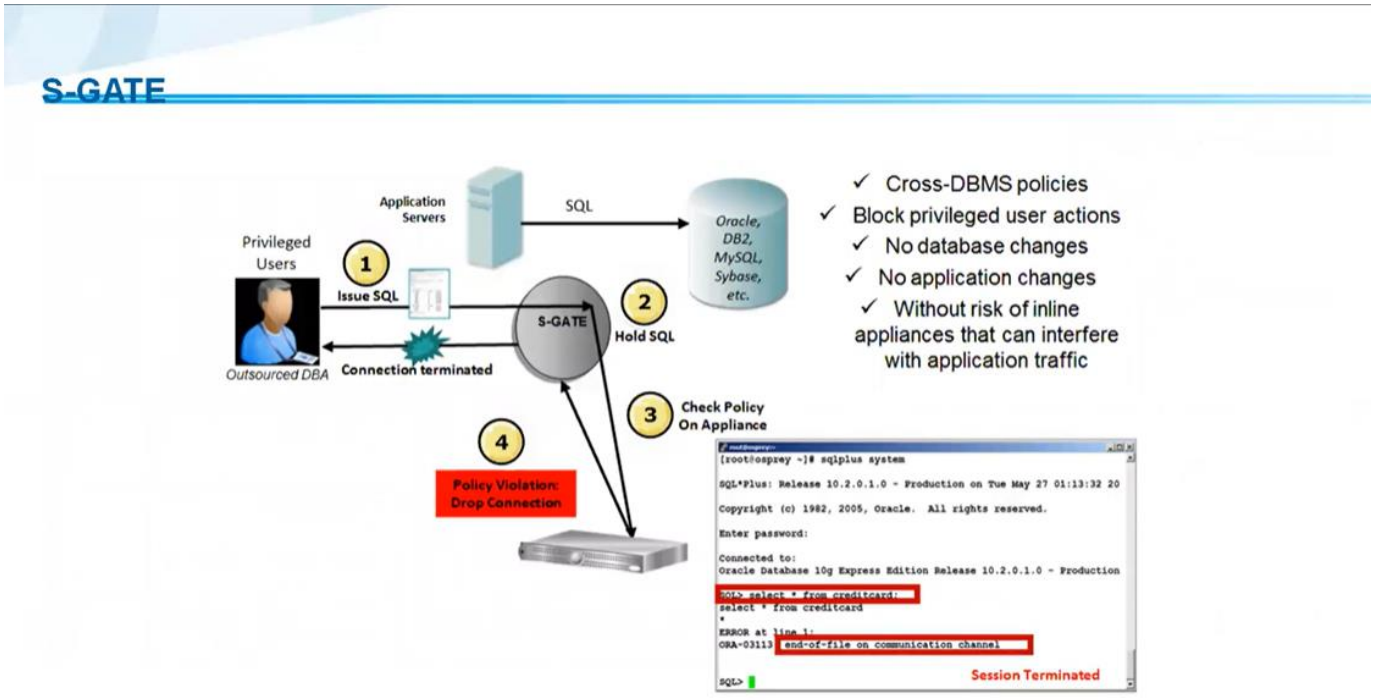

Рис.3.24. Робота S-GATE

ВИСНОВКИ

Проведено аналіз захищеності баз даних. Досліджено шляхи та вироблено рекомендації щодо захисту баз даних. Виявлено основні проблеми та слабкі сторони баз даних, їх потенційні загрози. Відібрано найактуальнішу програму захисту та загально окреслено її можливості, проаналізовано різні моменти роботи з базами даних.

Дослідження також виявило вразливості у базах даних підприємства. Це можуть бути слабкі паролі, недостатні права доступу до даних, застаріле програмне забезпечення або недостатнє шифрування. Виявлення цих вразливостей допомагає визначити пріоритети щодо впровадження заходів захисту. Захист баз даних є неперервним процесом, тому важливо регулярно моніторити та оновлювати заходи безпеки. Дослідження дало змогу розробити план постійного моніторингу та оцінки ефективності заходів безпеки баз даних підприємства.

В цілому, дослідження показало що саме сприяє покращенню безпеки, зменшенню ризиків витоку даних та забезпеченню надійного функціонування баз даних. Однак, важливо пам'ятати, що безпека баз даних - це постійний процес і вимагає систематичного оновлення та удосконалення заходів захисту від нових загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Как обеспечить безопасность баз данных: инструменты и методики. URL: https://infocity.tech/2020/04/kak-obespechit-bezopasnost-baz-dannyh-instrumenty-i-metodiki/ (дата звернення: 30.02.2023)

2. Шифрування та захист баз даних. URL: https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/ (дата звернення: 30.02.2023)

3. Системи управління базами даних. URL: http://dcmaup.com.ua/assets/files/informatika-i-kompyuterna-tehnika-v-chastina.pdf (дата звернення: 01.03.2023)

4. Об’єкти бази даних.URL: https://www.databasetour.net/ua/documentation/database-objects.htm (дата звернення: 05.03.2023)

5. Як убезпечити базу даних BAS. URL: https://inteltech.com.ua/uk/blogs/yak-ubezpechyty-bazu-danyh-1s (дата звернення: 05.03.2023)

6. Захист баз даних та веб-додатків. URL: https://netwave.ua/direction/zahyst-baz-danyh-veb-dodatkiv/ (дата звернення: 15.03.2023)

7. Що таке база даних.URL: https://hostiq.ua/wiki/ukr/database/ (дата звернення: 23.03.2023)

8. Що таке бази даних, їх призначення та види. URL: https://futurenow.com.ua/shho-take-bazy-danyh-yih-pryznachennya-ta-vydy/ (дата звернення: 25.03.2023)

9. 11 типів сучасних баз даних : короткий опис, схеми і приклади БД. URL: https://senior.ua/articles/11-tipv-suchasnih-baz-danih-korotkiy-opis-shemi--prikladi-bd (дата звернення: 28.03.2023)

10. Что такое реляционная база данных. URL: https://aws.amazon.com/ru/relational-database/?nc1=h_ls (дата звернення: 02.04.2023)

11. Порівняння різних технологій СКБД. URL: https://rdb.dp.ua/uk/chapter_01 (дата звернення: 19.04.2023)

12. 2023 DATA THREAT REPORT. URL: https://cpl.thalesgroup.com/data-threat-report#download-popup (дата звернення: 03.05.2023)

13. IBM Security Guardium Data Protection. URL: https://www.ibm.com/security/digital-assets/guardium/data-protection-demo/index.html (дата звернення: 08.05.2023)

14. Управление инцидентами. URL: https://icore.kz/upravlenie-inczidentami/ibm-security-guardium-data-protection/ (дата звернення: 10.05.2023)

15. Data Protection Demo. URL: https://www.ibm.com/products/ibm-guardium-data-protection (дата звернення: 11.05.2023)

16. Войтюшенко Н. М., Остапець А. І. Інформатика і комп’ютерна техніка : 2 видання. Київ : Центр учбової літератури, 2009. 560с.

17. Добролюбова М. В. Програмування баз даних : конспект лекцій. Київ : КПІ ім.Ігоря Сікорського, 2021. 275с.

18. Завадський І.О. Основи баз даних. Київ : ПП, 2011. 193с.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)