МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “**ТЕХНОЛОГІЯ POWER BI ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ УПРАВЛІННЯ ВЕЛИКИМИ ДАНИМИ**”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Максим МАРЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Максим МАРЧЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
к. держ. упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Марченку Максиму Вікторовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Технологія Power BI як інструмент забезпечення кібербезпеки систем управління великими даними”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к. держ. упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *системи управління великими даними (СУВД), забезпечення кібербезпеки СУВД, технологія Power BI у забезпеченні кібербезпеки СУВД*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити загрози кібербезпеці систем управління великими даними.
4.2. Проаналізувати особливості використання інструментів Power BI для забезпечення кібербезпеки в СУВД.
4.3. З’ясувати перспективи і виклики використання Power BI у кібербезпеці СУВД й розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Дослідження загроз кібербезпеці систем управління великими даними	08.04.2025	
4.	Аналіз особливостей використання інструментів Power BI для забезпечення кібербезпеки в СУВД.	22.04.2025	
5.	Виявлення перспектив і викликів використання Power BI у кібербезпеці й розробка практичних рекомендацій щодо його використання в галузі	08.05.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2025	
7.	Оформлення роботи.	22.05.2025	
8.	Оформлення презентації.	03.06.2025	
9.	Отримання рецензії на роботу.	03.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Максим МАРЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачка Марченко М.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технологія Power BI як інструмент забезпечення кібербезпеки систем управління великими даними"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач МАРЧЕНКО Максим у кваліфікаційній роботі дослідив загрози кібербезпеці систем управління великими даними; проаналізував особливості використання інструментів Power BI для забезпечення кібербезпеки в СУВД; з'ясував перспективи і виклики використання Power BI у кібербезпеці СУВД й розробити практичні рекомендації.

МАРЧЕНКО Максим показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача МАРЧЕНКА Максима на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Марченко М.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти МАРЧЕНКА Максима
на тему “Технологія Power BI як інструмент забезпечення кібербезпеки систем управління великими даними”

Актуальність. У сучасних умовах експоненціального зростання обсягів даних організації активно впроваджують системи управління великими даними (СУВД), які стають критично важливими елементами інформаційної інфраструктури. Одночасно значно зростає кількість і складність кіберзагроз, спрямованих на компрометацію великих масивів даних. Традиційні підходи до забезпечення кібербезпеки часто виявляються недостатньо ефективними для захисту розподілених СУВД через їх масштаб та динамічність. У цьому контексті особливого значення набувають інструменти бізнес-аналітики, які можуть функціонувати як потужні засоби моніторингу кібербезпеки, виявлення аномалій та оперативного реагування на інциденти безпеки.

Враховуючи ці аспекти, дослідження технології Power BI як інструменту забезпечення кібербезпеки систем управління великими даними є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено загрози кібербезпеці систем управління великими даними; проаналізовано особливості використання інструментів Power BI для забезпечення кібербезпеки в СУВД; з’ясовано перспективи і виклики використання Power BI у кібербезпеці СУВД й розроблено практичні рекомендації.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Здобувач опрацював достатню джерельну базу: понад 50 публікацій, в тому числі англомовні статті й нормативно-технічні документи.

4. Робота має практичну спрямованість, містить аналіз особливостей і методики застосування Power BI для забезпечення кібербезпеки систем управління великими даними, включаючи конкретні рекомендації щодо впровадження та оптимізації платформи.

Недоліки.

Доцільно було б глибше проаналізувати управлінські аспекти застосування Power BI для забезпечення кібербезпеки систем управління великими даними, зокрема процеси прийняття рішень на основі аналітичних дашбордів та організаційні механізми впровадження таких рішень.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач МАРЧЕНКО Максим заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технології Power BI як інструмент забезпечення кібербезпеки систем управління великими даними. Робота складається зі вступу, трьох розділів, що містять 17 рисунків і 4 таблиці, висновків і списку використаних джерел із 56 найменувань. Загальний обсяг роботи становить 82 аркуша, з яких 5 аркушів займає список використаних джерел.

Метою роботи є дослідження технології Power BI як інструменту забезпечення кібербезпеки систем управління великими даними.

Об’єктом дослідження є забезпечення кібербезпеки систем управління великими даними.

Предмет дослідження – технологія Power BI як інструмент забезпечення кібербезпеки систем управління великими даними.

Методи дослідження. Для вирішення поставленого наукового завдання використано методи аналізу та синтезу для дослідження архітектури СУВД і компонентів Power BI, системний підхід для розгляду взаємодії компонентів екосистеми великих даних, структурно-функціональний аналіз для дослідження механізмів безпеки Power BI, класифікацію для систематизації загроз кібербезпеці, а також аналіз технічної документації та галузевих стандартів.

Як результат у роботі досліджено загрози кібербезпеці систем управління великими даними; проаналізовано особливості використання інструментів Power BI для забезпечення кібербезпеки в СУВД; з’ясовано перспективи і виклики використання Power BI у кібербезпеці СУВД й розроблено практичні рекомендації.

Галузь застосування. Описані підходи можуть бути використані для підвищення рівня кібербезпеки систем управління великими даними в різних галузях економіки, включаючи фінансові установи, телекомунікаційні компанії, медичні заклади, виробничі підприємства та організації сфери послуг, шляхом впровадження платформи Power BI як інструменту моніторингу та аналізу кібербезпеки.

Ключові слова: СИСТЕМИ УПРАВЛІННЯ ВЕЛИКИМИ ДАНИМИ (СУВД), ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СУВД, ТЕХНОЛОГІЯ POWER BI У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ СУВД.

ABSTRACT

The qualification work is devoted to the study of Power BI technology as a tool for ensuring cybersecurity of big data management systems. The work consists of an introduction, three chapters containing 17 figures and 4 tables, conclusions and a list of references which consists of 56 items. The total volume of the work is 82 pages, of which 5 pages are occupied by the list of references.

The purpose of the study is to investigate Power BI technology as a tool for ensuring cybersecurity of big data management systems.

The object of the study is cybersecurity of big data management systems.

The subject of the study is Power BI technology as a tool for ensuring cybersecurity of big data management systems.

Research methods. In order to solve the scientific task, the methods of analysis and synthesis for studying BDMS architecture and Power BI components, systematic approach for examining the interaction of big data ecosystem components, structural-functional analysis for studying Power BI security mechanisms, classification for systematizing cybersecurity threats, as well as analysis of technical documentation and industry standards were used.

As a result, the study explores cybersecurity threats to big data management systems; analyzes the features of using Power BI tools for ensuring cybersecurity in BDMS; clarifies the prospects and challenges of using Power BI in BDMS cybersecurity and develops practical recommendations.

Field of application. The described approaches can be used to increase the level of cybersecurity of big data management systems in various economic sectors, including financial institutions, telecommunications companies, medical facilities, manufacturing enterprises and service organizations, through the implementation of Power BI platform as a tool for cybersecurity monitoring and analysis.

Keywords: BIG DATA MANAGEMENT SYSTEMS (BDMS), CYBERSECURITY OF BDMS, POWER BI TECHNOLOGY IN BDMS CYBERSECURITY.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасних умовах експоненціального зростання обсягів даних організації активно впроваджують системи управління великими даними (СУВД), які стають критично важливими елементами інформаційної інфраструктури. Одночасно значно зростає кількість і складність кіберзагроз, спрямованих на компрометацію великих масивів даних. Традиційні підходи до забезпечення кібербезпеки часто виявляються недостатньо ефективними для захисту розподілених СУВД через їх масштаб та динамічність. У цьому контексті особливого значення набувають інструменти бізнес-аналітики, які можуть функціонувати як потужні засоби моніторингу кібербезпеки, виявлення аномалій та оперативного реагування на інциденти безпеки.

З огляду на зазначене, дослідження технології Power BI як інструменту забезпечення кібербезпеки систем управління великими даними є актуальним науковим завданням.

Мета роботи полягає у дослідженні технології Power BI як інструменту забезпечення кібербезпеки систем управління великими даними.

Об'єкт дослідження – забезпечення кібербезпеки систем управління великими даними.

Предмет дослідження – технологія Power BI як інструмент забезпечення кібербезпеки систем управління великими даними.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити загрози кібербезпеці систем управління великими даними.

2. Проаналізувати особливості використання інструментів Power BI для забезпечення кібербезпеки в СУВД.

3. З'ясувати перспективи і виклики використання Power BI у кібербезпеці СУВД й розробити практичні рекомендації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи аналізу та синтезу для дослідження архітектури СУВД і компонентів Power BI, системний підхід для розгляду

взаємодії компонентів екосистеми великих даних, структурно-функціональний аналіз для дослідження механізмів безпеки Power BI, класифікацію для систематизації загроз кібербезпеці, а також аналіз технічної документації та галузевих стандартів.

Практичне значення одержаних результатів. Проаналізовані підходи до застосування технології Power BI для підвищення кібербезпеки систем управління великими даними можуть бути використані як орієнтир для впровадження сучасних аналітичних рішень у системах моніторингу безпеки організацій. Результати дослідження можуть стати основою для удосконалення механізмів візуалізації загроз, виявлення аномальної активності та побудови ефективних систем аналітики кіберзагроз у різних галузях економіки, що активно використовують технології великих даних.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

РОЗДІЛ 1 ЗАГРОЗИ КІБЕРБЕЗПЕЦІ СИСТЕМ УПРАВЛІННЯ ВЕЛИКИМИ ДАНИМИ

1.1 Основи систем управління великими даними

Сучасні технології дозволяють передавати великі, складні набори найрізноманітніших даних: від даних охорони здоров'я до показників соціальних мереж, майже в реальному часі. Термін "великі дані" (Big Data) використовується для опису цих наборів даних, як структурованих, так і неструктурованих, і зазвичай стосується даних, які неможливо проаналізувати за допомогою традиційних методів. Розмір і складність великих даних натомість вимагають використання спеціалізованого програмного забезпечення, яке, у свою чергу, може потребувати значної обчислювальної потужності й можливостей зберігання. Хоча це дорого, впровадження великих даних дозволяє організаціям отримувати потужні аналітичні висновки та конкурентну перевагу.

Поява аналітики великих даних (ВД) супроводжувалася експоненціальним зростанням глобального обсягу даних. Хоча важко уявити цей величезний інформаційний потік, масштаб ілюструється вибухом мобільного трафіку даних, який, за прогнозами, перевищить 167 ексабайт на місяць у 2024 році. Це частково буде спричинено розширенням "Інтернету речей" (IoT), який охоплює зростаючу мережу підключених пристроїв і сенсорів, що генерують і обмінюються даними в Інтернеті. Пристрої IoT можуть включати будь-що: від розумного годинника, здатного записувати відомості про тренування, до датчика, призначеного для моніторингу функціонування заводського обладнання. На передньому плані ці дані використовуються компаніями зі штучного інтелекту (ШІ) для навчання все більш ефективних алгоритмів ШІ.

Величезний обсяг даних в аналітиці ВД став перешкодою для організацій, які бажають зберігати й аналізувати дані локально. Тому більшість компаній вирішує зберігати дані в хмарі, роблячи їх доступними будь-де і будь-коли. Це призвело до появи моделі "аналітика як послуга" (AaaS), яка дозволяє

організаціям проводити аналітику через хмарну службу передплати і, таким чином, уникнути високих витрат, пов'язаних з локальним зберіганням та обробкою. Дійсно, 2023 рік став поворотним роком для впровадження ВД, з різким збільшенням частки керівників по всьому світу, які вважали, що їхня організація керує інноваціями за допомогою даних.

Незважаючи на обнадійливі показники впровадження, існує ряд викликів. Перша проблема стосується якості даних: лише 37% підприємств повідомляють, що їхні зусилля щодо покращення якості даних були успішними. Загалом, організаціям необхідно буде вирішити питання занепокоєння клієнтів щодо збору даних, оскільки випуск інструментів генеративного ШІ посилює побоювання щодо конфіденційності.

Великі дані – це масиви інформації, що характеризуються значними обсягами, високою швидкістю надходження та різноманітністю форматів, які неможливо ефективно обробляти за допомогою традиційних методів та інструментів. Концепція ВД традиційно описується через модель "3V":

– значний *обсяг* інформації в різних середовищах;
– широка *різноманітність* форматів даних у системах ВД;
– висока *швидкість* генерування, збору й обробки інформації.

У 2001 році аналітик консалтингової компанії Meta Group Inc. Даг Лені вперше сформулював ці три V великих даних. Після придбання Meta Group у 2005 році компанія Gartner зробила цю концепцію популярною. Хоча поняття ВД не обмежується конкретним обсягом інформації, проєкти з їх використанням зазвичай оперують терабайтами, петабайтами і навіть ексабайтами точок даних, які накопичуються протягом певного часу.

Згодом модель "3V" була розширена до "5V" [1] (Рис. 1.1):

Volume (Об'єм) – характеризує масштаби даних, що вимірюються в петабайтах та ексабайтах.

Velocity (Швидкість) – визначає темп надходження даних і потребу в їх оперативній обробці. Сучасні системи повинні обробляти мільйони транзакцій за секунду і надавати результати в режимі реального часу.

Variety (Різноманітність) – відображає різнорідність типів даних: структуровані (реляційні бази даних), напівструктуровані (XML, JSON) та неструктуровані (текст, зображення, відео).

Veracity (Достовірність) – стосується якості й надійності даних.

Value (Цінність) – характеризує потенційну користь та економічну вигоду від аналізу даних.

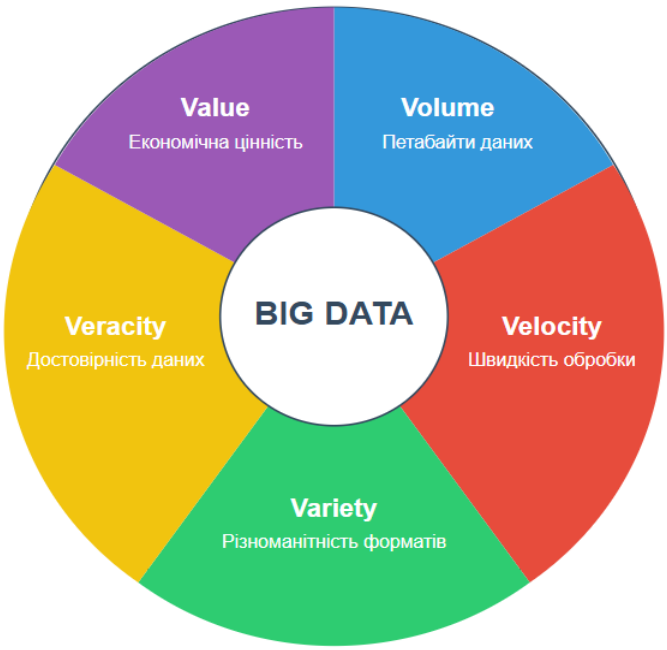

Рис. 1.1. Концепція великих даних

Успішне впровадження технологій великих даних дозволяє організаціям збільшити прибуток. Однак із зростанням обсягів даних та їх значущості для бізнесу збільшуються і ризики, пов'язані з інформаційною безпекою.

Значення великих даних і способи їх застосування. Організації впроваджують ВД у свої системи для оптимізації операційних процесів, покращення якості обслуговування, розробки індивідуалізованих маркетингових ініціатив та інших заходів, спрямованих на збільшення доходу і прибутковості. Компанії, які вміло оперують ВД, отримують стратегічну перевагу над конкурентами, адже можуть ухвалювати більш оперативні й аргументовані рішення.

Наприклад, аналіз ВД надає компаніям глибоке розуміння поведінки споживачів, що дозволяє вдосконалювати маркетингові та рекламні стратегії для посилення взаємодії з клієнтами та підвищення рівня конверсії. Аналізуючи як

історичні, так і оперативні дані, бізнес може відстежувати еволюцію вподобань споживачів і корпоративних клієнтів, що забезпечує гнучкіше реагування на їхні запити й потреби.

У медичній сфері дослідники застосовують ВД для ідентифікації симптомів захворювань і виявлення факторів ризику. Лікарі використовують цю інформацію для більш точної діагностики пацієнтів. Більше того, інтеграція даних із електронних медичних карток, соціальних платформ, Інтернет-ресурсів та інших джерел забезпечує медичні заклади й державні органи своєчасною інформацією про загрози інфекційних хвороб і епідеміологічну ситуацію.

Особливо критичним є використання ВД у таких сферах як охорона здоров'я, фінанси, телекомунікації й державне управління, де компрометація даних може призвести до суттєвих матеріальних і репутаційних втрат. Наприклад, у медичній галузі системи на основі ВД працюють з конфіденційною інформацією пацієнтів, що вимагає підвищених стандартів захисту.

Екосистема СУВД. Архітектура систем управління великими даними (СУВД) є багаторівневою та складною, що відображає потребу в обробці різнорідних даних з високою продуктивністю. Типова архітектура СУВД включає такі компоненти [2] (Рис. 1.2):

Рівень даних забезпечує збір, зберігання та управління великими обсягами даних через розподілені файлові системи (HDFS, GFS), NoSQL бази даних (MongoDB, Cassandra), системи потокової обробки (Apache Kafka, Amazon Kinesis), сховища даних (Data Warehouse).

На рівні обробки реалізуються алгоритми та методи аналізу даних, серед яких: пакетна обробка (Apache Hadoop MapReduce), потокова обробка (Apache Spark Streaming, Flink), гібридні моделі (Lambda архітектура).

Рівень аналітики надає інструменти для аналізу й візуалізації даних, зокрема системи бізнес-аналітики (Tableau, Power BI), машинне навчання та штучний інтелект (TensorFlow, PyTorch), аналітичні платформи (Cloudera, Hortonworks).

Рис. 1.2. Архітектура СУВД

Рівень представлення забезпечує інтерфейси для взаємодії з користувачами (веб-портали і дашборди, мобільні застосунки, API для інтеграції з іншими системами).

Кожен із цих рівнів має власні вразливості й потребує специфічних підходів до забезпечення безпеки. Наприклад, рівень даних вимагає захисту від несанкціонованого доступу та шифрування конфіденційної інформації, тоді як рівень аналітики потребує захисту від витоку персональних даних у процесі аналізу.

Сучасний ландшафт технологій обробки ВД характеризується різноманіттям інструментів і підходів, що постійно еволюціонують. Екосистема ВД складається з різноманітних компонентів та технологій, організованих у взаємопов'язані шари [5].

Hadoop екосистема включає набір потужних інструментів для розподіленої обробки даних. В її основі лежить Apache Hadoop з його розподіленою файловою системою HDFS та моделлю програмування MapReduce. Для роботи з даними використовуються різні інструменти: Apache Hive, що надає SQL-подібний інтерфейс для запитів до даних у Hadoop; Apache Pig, що пропонує

спеціалізовану мову для аналізу даних; та Apache HBase, яка функціонує як розподілена NoSQL база даних для швидкого доступу до великих обсягів даних.

Технології потокової обробки забезпечують аналіз даних у реальному часі. Apache Kafka служить розподіленою платформою для потокової обробки даних з високою пропускною здатністю. Apache Flink пропонує фреймворк для потокової обробки з низькою затримкою та високою точністю. Apache Spark Streaming інтегрується з екосистемою Spark, забезпечуючи уніфікований підхід до обробки як пакетних, так і потокових даних.

Для машинного навчання й аналітики використовується ряд спеціалізованих інструментів. Apache Spark MLlib надає бібліотеку для масштабованого машинного навчання. Фреймворки TensorFlow та PyTorch забезпечують розробку та тренування моделей глибокого навчання. Мови програмування R та Python з їхніми численними бібліотеками широко застосовуються для статистичного аналізу та наукових обчислень.

Хмарні сервіси пропонують інфраструктуру для масштабованої обробки даних. Amazon Web Services надає такі послуги як AWS EMR для обробки даних та Redshift для сховищ даних. Microsoft Azure пропонує HDInsight для управління кластерами Hadoop та Synapse Analytics для аналізу даних. Google Cloud Platform забезпечує такі сервіси як BigQuery для аналітики та Dataproc для обробки даних.

Технології DataOps та MLOps підтримують інтеграцію розробки й операційної діяльності. Apache Airflow використовується для оркестрації потоків даних і автоматизації робочих процесів. Kubernetes забезпечує контейнеризацію та оркестрацію сервісів. Інструменти Jenkins та GitLab CI/CD автоматизують процеси розробки, тестування та розгортання компонентів системи ВД.

Обсяги використання хмарних технологій для обробки ВД зростають щорічно, оскільки вони забезпечують гнучкість, масштабованість та економічну ефективність. Однак, розміщення даних у хмарі створює додаткові ризики для безпеки, пов'язані з контролем доступу, дотриманням регуляторних вимог та захистом від атак на інфраструктуру.

Особливу увагу слід приділити інтеграції технологій ВД з інструментами бізнес-аналітики, такими як Power BI, Tableau чи Qlik, які забезпечують візуалізацію та доступ до результатів аналізу для кінцевих користувачів. Ці інструменти часто стають цілями для атак, оскільки вони мають доступ до агрегованих даних і можуть бути використані для несанкціонованого отримання інформації [3].

1.2 Кібербезпека в контексті великих даних: джерела й тенденції розвитку

Статистика кіберінцидентів у сфері великих даних. За даними звіту IBM Data Breach Report 2024 [4], статистика кіберінцидентів у сфері управління ВД демонструє тривожну тенденцію зростання як кількості, так і складності атак. Середня глобальна вартість інциденту з витоком даних досягла 4,88 мільйонів доларів США, що на 10% більше порівняно з попереднім роком – це найбільше зростання з часів пандемії. Фінансові збитки від інцидентів безпеки включають втрату бізнесу, витрати на відновлення після інциденту та репутаційні втрати.

Статистика свідчить, що щорічне зростання кількості атак на системи ВД становить понад 10%, при цьому 40% організацій повідомили про зберігання даних у множинних середовищах, що значно збільшує поверхню атаки. Середній час для виявлення та усунення інциденту становить 258 днів, причому для виявлення потрібно в середньому 194 дні, а для усунення – ще 64 дні. Інциденти з витоком даних, які включали дані, розміщені у множинних середовищах, потребували найбільше часу для виявлення та усунення – 283 дні.

Фінансовий сектор залишається одним з найбільш атакованих, з середньою вартістю інциденту 6,08 мільйонів доларів США, що на 6% вище порівняно з попереднім роком. При цьому галузь охорони здоров'я зберігає лідерство за вартістю інцидентів: 9,77 мільйонів доларів США, попри зниження на 10,6% порівняно з попереднім роком. Промисловий сектор продемонстрував найбільше зростання витрат – на 830,000 доларів США порівняно з минулим роком.

Аналіз типів атак показує, що скомпрометовані облікові дані є найпоширенішим вектором атаки, складаючи 16% всіх інцидентів із середньою вартістю 4,81 мільйонів доларів США. Фішингові атаки займають друге місце з 15% інцидентів та середньою вартістю 4,88 мільйонів доларів США. Атаки внутрішніх зловмисників коштують найдорожче – в середньому 4,99 мільйонів доларів США, хоча складають лише 7% всіх інцидентів. За даними IBM, 35% інцидентів пов'язані з "тіньовими даними" – неконтрольованими джерелами даних, що збільшує вартість інциденту на 16,2%.

При цьому 46% усіх інцидентів включали персональні дані клієнтів, а 43% – інтелектуальну власність. СУВД з недостатнім захистом підвищують вартість компенсації наслідків інцидентів. Так, організації з низьким рівнем використання ШІ та автоматизації в безпеці мають середню вартість інциденту 5,72 мільйонів доларів США, тоді як організації з високим рівнем автоматизації – 3,84 мільйонів доларів США, що на 1,88 мільйонів доларів США менше [4].

Компанії, які впроваджують комплексні стратегії кібербезпеки для ВД, зменшують середній час виявлення інцидентів та скорочують фінансові втрати. Це підкреслює важливість проактивного підходу до захисту інформаційної інфраструктури.

Основні виклики забезпечення безпеки великих даних. Забезпечення безпеки ВД стикається з унікальними викликами, що виникають через масштаб, різноманітність та складність цих систем. Основні виклики можна згрупувати за такими категоріями (Рис. 1.3).

Технологічні виклики пов'язані з фундаментальними властивостями систем ВД. Масштабованість захисту стає серйозною проблемою, оскільки традиційні засоби безпеки не розраховані на обробку петабайтів даних і мільйонів одночасних транзакцій. Гетерогенність середовища, де поєднуються різноманітні технології та платформи, ускладнює впровадження єдиної стратегії безпеки. Розподілена архітектура суттєво збільшує поверхню атаки та ускладнює

контроль доступу до різних компонентів системи. Необхідність обробки даних у реальному часі створює конфлікт між швидкодією та вимогами безпеки.

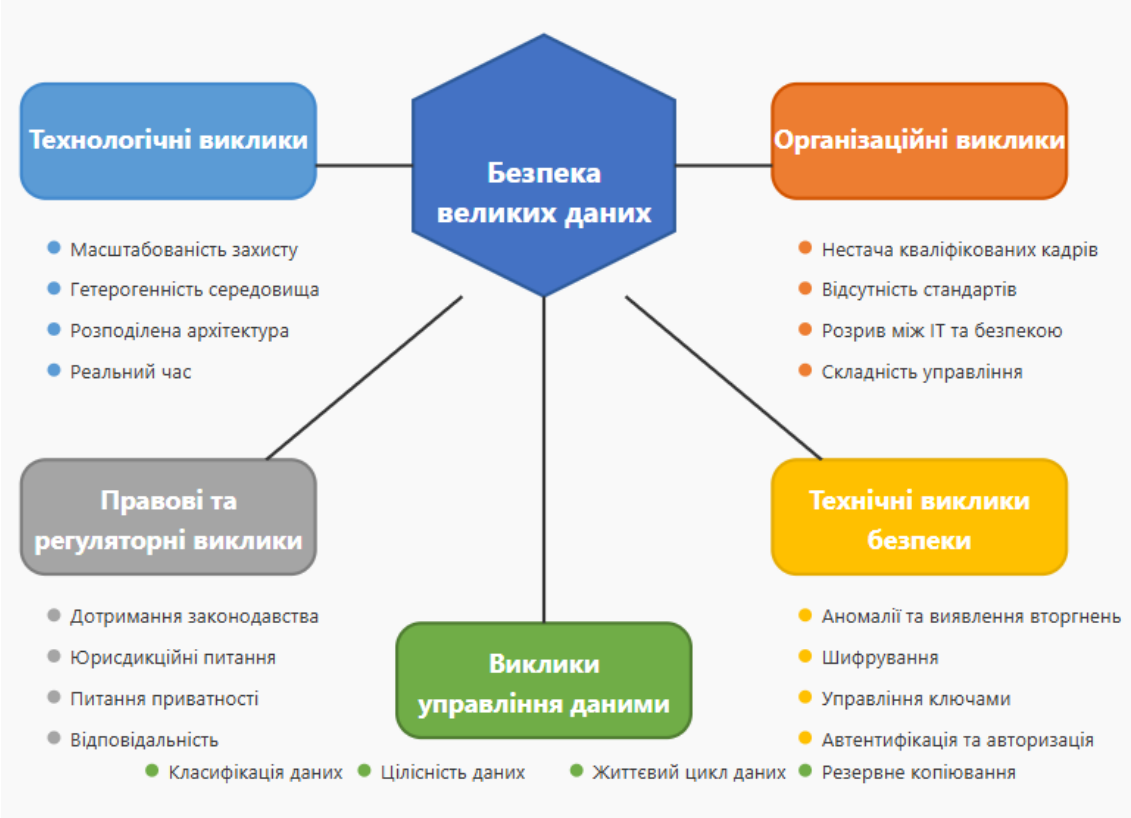

Рис. 1.3. Виклики безпеки великих даних

Організаційні виклики охоплюють кадрові та управлінські аспекти. Нестача кваліфікованих кадрів, які одночасно розуміються на технологіях ВД і кібербезпеці, створює значний бар'єр для впровадження ефективного захисту. Відсутність зрілих стандартів і методологій для захисту ВД ускладнює побудову надійних систем. Розрив між командами розробників IT-рішень та фахівцями з безпеки призводить до непорозумінь та вразливостей. Складність управління заходами безпеки в масштабних проектах вимагає особливої уваги до координації процесів.

Правові та регуляторні виклики пов'язані з необхідністю дотримуватися численних вимог законодавства, таких як GDPR, HIPAA, ISO та інші регуляторні норми [9]. Юрисдикційні питання виникають, коли дані розміщуються у системах, що знаходяться під різними юрисдикціями, створюючи правову невизначеність. Особливу увагу привертають питання приватності, що вимагають знаходження балансу між аналітичною цінністю даних і захистом

персональної інформації. Важливим аспектом є також визначення відповідальних сторін у випадку інцидентів безпеки.

Технічні виклики безпеки стосуються безпосередньо механізмів захисту. Виявлення аномалій і вторгнень у величезних обсягах даних вимагає застосування складних алгоритмів. Шифрування даних стикається з продуктивними обмеженнями при обробці великих масивів інформації. Управління криптографічними ключами потребує створення надійної інфраструктури для їх зберігання та розподілу. Автентифікація та авторизація в розподілених системах повинні забезпечувати надійний контроль доступу без значних затримок.

Виклики *управління даними* зосереджені на питаннях організації роботи з інформацією. Класифікація даних необхідна для визначення критичності та відповідного рівня захисту різних типів інформації. Забезпечення цілісності даних гарантує їх достовірність та надійність для прийняття рішень. Управління життєвим циклом даних вимагає впровадження заходів безпеки на всіх етапах від збору до видалення. Створення надійних систем резервного копіювання ускладнюється через величезні обсяги інформації.

Ці п'ять категорій викликів формують комплексну картину проблематики забезпечення безпеки ВД, вирішення якої потребує системного підходу та співпраці фахівців різних галузей.

Організації, що не мають повноцінної стратегії кібербезпеки для своїх систем ВД через комплексність і швидкозмінність технологій сильно ризикують. Одночасно, компанії, які успішно долають ці виклики, отримують конкурентну перевагу: зменшення операційних ризиків та зростання довіри клієнтів.

Особливо важливим є вирішення проблеми безпеки при використанні аналітичних платформ, таких як Power BI, оскільки вони часто стають "вікном" для доступу до очищених та агрегованих даних, що потенційно може бути використано для витоку інформації.

Тенденції розвитку загроз інформаційній безпеці в контексті ВД характеризуються підвищенням складності та цілеспрямованості атак. Основні напрямки еволюції загроз охоплюють (Рис.1.4):

Рис. 1.4. Тенденції розвитку загроз в контексті великих даних

Про *орієнтованість кібератак на дані* свідчить стійка тенденція до зростання кількості атак, націлених безпосередньо на крадіжку даних. За даними IBM Security [4], у 2024 році 46% усіх інцидентів включали персональні дані клієнтів, що демонструє зростання порівняно з 48% у 2023 році, а 43% включали інтелектуальну власність, що значно перевищує показник 34% попереднього року. Вартість крадіжки інтелектуальної власності також зросла до 173 доларів за запис порівняно з 156 доларами у 2023 році, що свідчить про підвищення цінності таких даних для зловмисників.

З кожним днем зростають масштаби *використання ШІ* в процесі підготовки й реалізації кіберзагроз [6]. Зловмисники активно впроваджують технології машинного навчання для автоматизації процесів зламу, обходу систем виявлення вторгнень, створення таргетованих фішингових атак, аналізу вкрадених даних для виявлення цінної інформації.

Платформи бізнес-аналітики, які агрегують дані з різних джерел, усе частіше стають об’єктами кіберзловмисників, які використовують різноманітні методи, зокрема компрометують облікові записи користувачів аналітичних

систем, здійснюють атаки типу "запит ін'єкцій" для отримання доступу до даних, експлуатують вразливості візуалізаційних компонентів.

Складні *атаки на ланцюжки постачання* відзначаються зростанням масштабів та витонченості. Значна частина сучасних кіберінцидентів пов'язана з атаками на ланцюжки постачання програмного забезпечення, зокрема на залежності та бібліотеки відкритого коду, які широко використовуються в екосистемах ВД [7].

Розвиток *методів обходу захисту* демонструє еволюцію технік протидії захисним механізмам. Поліморфні шкідливі програми, що постійно змінюють свою структуру, безфайлові атаки та шифрування зловмисного трафіку – все це ускладнює виявлення загроз традиційними засобами захисту.

Збільшення масштабів *атак розподіленої відмови в обслуговуванні (DDoS)* становить серйозну загрозу для доступності систем ВД. Використання хмарних ресурсів для реалізації атак дозволяє зловмисникам досягати безпрецедентних масштабів, потенційно паралізуючи роботу цілих організацій.

Інсайдерські загрози залишаються критичним викликом для безпеки великих даних. Значна кількість інцидентів у цій сфері пов'язана з діями внутрішніх порушників, що зумовлює розвиток методів виявлення аномальної поведінки користувачів і посилення заходів проти промислового шпигунства [8].

Атаки на хмарні інфраструктури зростають за кількістю та складністю. Неправильна конфігурація хмарних сервісів, атаки на API та компрометація облікових записів доступу до хмарних сховищ становлять серйозні ризики для організацій, що використовують хмарні платформи для зберігання й обробки ВД.

Регуляторні виклики створюють додатковий тиск на організації, що працюють з великими даними. Дотримання вимог GDPR, CCPA та інших регуляторних актів ускладнюється при роботі з розподіленими системами ВД, а невідповідність може призвести до значних штрафів.

Рух від реактивних до проактивних стратегій захисту свідчить про те, що в майбутньому організації можуть використовувати інструменти кібербезпеки, інтегровані з аналітикою ВД і ШІ, щоб протистояти сучасним загрозам.

1.3 Види й механізми реалізації загроз інформаційній безпеці СУВД

Загрози інформаційній безпеці у сфері великих даних можна класифікувати за різними критеріями, що дозволяє системно підходити до їх аналізу та протидії. Найбільш поширені класифікації включають (Рис. 1.5):

Рис. 1.5. Класифікація загроз СУВД

Розуміння природи та джерел загроз є критично важливим для побудови ефективної системи захисту ВД. Сучасний ландшафт кіберзагроз характеризується значною різноманітністю, що потребує детальної класифікації для кращого розуміння та протидії.

Джерела походження загроз. За джерелом походження загрози традиційно поділяються на три основні категорії. Зовнішні загрози походять від широкого спектру акторів - від окремих хакерів до організованих груп і конкурентів. Ці загрози проявляються у вигляді цільових атак типу APT (Advanced Persistent Threats), які можуть тривати місяцями або навіть роками, масових атак на кшталт спаму та фішингу, а також прямих атак на інфраструктуру через DDoS або перехоплення трафіку [10].

Внутрішні загрози представляють не меншу небезпеку, адже вони походять від самих працівників організації. Ці загрози можуть бути як навмисними, коли співробітник свідомо краде дані, займається саботажем чи промисловим шпигунством, так і ненавмисними, коли безпека порушується

через людську помилку, неправильну конфігурацію систем або недотримання політик безпеки. Особливу категорію становлять змішані загрози, які поєднують зовнішні та внутрішні елементи, наприклад, через соціальну інженерію або компрометацію облікових записів співробітників.

Архітектурний підхід до класифікації передбачає розподіл загроз за компонентами СУВД.

На рівні збору даних організації стикаються з ризиками компрометації датчиків та джерел даних, перехоплення інформації під час її передачі, а також атаками на системи збору та аналізу логів.

Рівень зберігання даних характеризується власним набором викликів, включаючи несанкціонований доступ до сховищ даних, порушення цілісності збереженої інформації та витоки даних через неправильну конфігурацію сховищ.

Системи обробки даних вразливі до атак на обчислювальні кластери, порушень алгоритмів обробки та ін'єкцій шкідливого коду безпосередньо у процеси обробки.

Особливо критичним є рівень аналізу та візуалізації, де зловмисники можуть атакувати системи візуалізації на кшталт Power BI або Tableau, маніпулювати результатами аналізу чи порушувати права доступу до аналітичної інформації.

З точки зору інформаційної безпеки, загрози впливають на три фундаментальні властивості даних.

Загрози конфіденційності проявляються через витік конфіденційних даних, несанкціонований доступ до персональної інформації та невідповідність вимогам приватності, що може призвести до серйозних юридичних наслідків.

Цілісність даних опиняється під загрозою через можливість їх підміни, порушення цілісності алгоритмів обробки та маніпуляції з результатами аналізу, що може призвести до прийняття хибних бізнес-рішень.

Доступність систем порушується через DDoS-атаки на інфраструктуру великих даних, збої в роботі критичних компонентів та ресурсне виснаження систем, що може паралізувати операційну діяльність організації.

Етапи обробки інформації. Життєвий цикл даних створює унікальний контекст для кожного етапу обробки інформації. На етапі збору організації стикаються з ризиками фальсифікації вхідних даних, порушення процедур збору та ін'єкцій на рівні API. Етап передачі даних характеризується загрозами перехоплення інформації, атаками типу "людина посередині" та порушеннями протоколів передачі даних. Під час зберігання виникають ризики витоку з баз даних, криптографічних атак на захищені сховища та компрометації систем резервного копіювання. Етап обробки та аналізу вразливий до атак на алгоритми машинного навчання, порушень процесів обробки даних та інформаційних атак на моделі аналізу. Навіть етап видалення даних несе свої ризики через можливість неповного видалення інформації, її відновлення після видалення та порушення політик утилізації.

Оцінка загроз за рівнем впливу дозволяє організаціям правильно розставляти пріоритети у своїх зусиллях з кібербезпеки. Загрози стратегічного рівня, такі як комплексні APT-атаки, системні порушення безпеки й атаки на критичну інфраструктуру, можуть мати катастрофічні наслідки для всієї організації. Тактичний рівень включає порушення окремих процесів, локальні витоки даних та часткові порушення функціонування, які, хоча й менш руйнівні, все ж можуть завдати значної шкоди. На операційному рівні компанії стикаються з повсякденними викликами у вигляді помилок користувачів, технічних збоїв та порушень політик безпеки, які, незважаючи на їх рутинність, можуть накопичуватися і створювати серйозні проблеми.

Найбільш критичними загрозами у сфері ВД є атаки на системи аналітики та візуалізації, фішингові атаки на користувачів аналітичних систем і компрометація облікових записів. Це підкреслює важливість забезпечення безпеки не лише на рівні зберігання, але й на рівні доступу та використання інформації.

Механізми реалізації кібератак на системи. Механізми реалізації кібератак на інфраструктуру ВД характеризуються надзвичайною складністю та різноманітністю підходів, що значно ускладнює їх своєчасне виявлення та

ефективну протидію. Сучасні кіберзловмисники розробили арсенал витончених методів, спрямованих на компрометацію різних компонентів екосистеми ВД (Рис. 1.6.

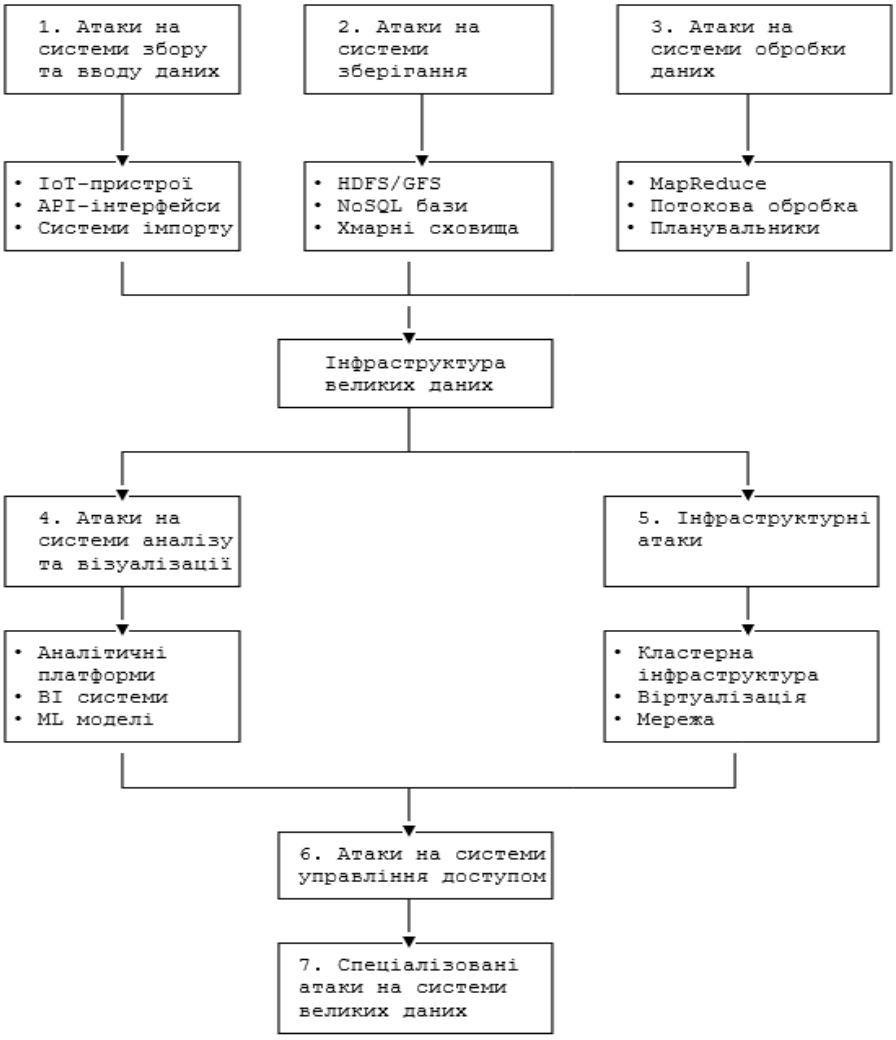

Рис. 1.6. Основні механізми реалізації кібератак на інфраструктуру ВД

Атаки на системи збору та вводу даних становлять першу лінію наступу кіберзловмисників. У сучасному світі IoT мільйони датчиків та IoT-пристроїв стають легкою здобиччю через застарілі прошивки та слабкі механізми захисту. Зловмисники компрометують ці пристрої, підміняють дані безпосередньо на етапі збору або встановлюють приховані бекдори для подальшого доступу. API-інтерфейси, які служать воротами для даних, піддаються ін'єкціям шкідливого коду, DDoS-атакам та експлуатації численних вразливостей. Системи імпорту даних стають векторами атак через впровадження шкідливого коду в імпортовані файли та маніпуляції з форматами даних.

Системи зберігання даних стикаються з цілим спектром загроз. Розподілені файлові системи, такі як HDFS або GFS, вразливі до експлуатації недоліків в системах авторизації, атак на критичні вузли управління та ін'єкцій шкідливого коду безпосередньо в процеси зберігання даних. NoSQL бази даних, популярні в екосистемах великих даних, страждають від специфічних атак - NoSQL-ін'єкцій, експлуатації гнучкості схем даних та вразливостей механізмів реплікації. Хмарні сховища часто стають жертвами через неправильну конфігурацію. Класичним прикладом є публічно доступні S3 бакети, які регулярно призводять до масштабних витоків даних.

Системи обробки даних піддаються складним атакам на обчислювальні процеси. Зловмисники впроваджують шкідливі функції в MapReduce-процеси, маніпулюють проміжними результатами обчислень, атакують системи потокової обробки даних, такі як Kafka або Flink. Особливу небезпеку становлять атаки на планувальники задач. Компрометація YARN або інших систем управління ресурсами може паралізувати всю обчислювальну інфраструктуру через порушення пріоритетів виконання та навмисне виснаження ресурсів.

Системи аналізу та візуалізації стають все більш привабливими цілями для кіберзлочинців. Аналітичні платформи вразливі до SQL-ін'єкцій, компрометації середовищ виконання скриптів на R або Python, маніпуляцій з результатами аналізу. Платформи бізнес-аналітики, такі як Power BI або Tableau, піддаються атакам на системи авторизації, маніпуляціям з джерелами даних та XSS-атакам у веб-інтерфейсах. Особливо небезпечними є атаки на моделі машинного навчання через "отруєння" навчальних даних, генерацію адверсаріальних прикладів та спроби витягнути конфіденційну інформацію з навчених моделей.

Інфраструктурні атаки націлені на фундаментальні компоненти систем ВД. Компрометація вузлів управління кластером може надати зловмисникам повний контроль над всією інфраструктурою. Атаки на віртуалізовані середовища включають експлуатацію вразливостей гіпервізорів, порушення ізоляції контейнерів та компрометацію ізоляції між віртуальними машинами. Мережева інфраструктура страждає від DDoS-атак, перехоплення трафіку між

компонентами системи та порушення мережевої сегментації. Мережева інфраструктура страждає від DDoS-атак, перехоплення трафіку між компонентами системи та порушення мережевої сегментації.

Системи управління доступом залишаються одним з найслабших місць в архітектурі безпеки. Крадіжка облікових даних через фішингові атаки, використання вкрадених API-ключів та експлуатація слабких паролів створюють постійну загрозу. Зловмисники намагаються обійти механізми авторизації через підвищення привілеїв, маніпулюють політиками доступу та експлуатують недоліки багатокористувацької ізоляції.

Спеціалізовані атаки на СУВД використовують унікальні властивості цих систем. Інференційні атаки дозволяють виводити конфіденційну інформацію з агрегованих даних, деанонімізувати користувачів через перехресні запити та реконструювати приватні дані з публічних результатів. Атаки на системи конфіденційності спрямовані на обхід методів диференціальної приватності, порушення псевдонімізації та подолання механізмів додавання шуму. Системи відстеження походження даних піддаються атакам через підміну метаданих та порушення ланцюжків аудиту.

Найбільш поширеними векторами атак на системи ВД залишаються компрометація облікових даних, експлуатація вразливостей програмного забезпечення, неправильна конфігурація систем та атаки на API-інтерфейси. Ця статистика підкреслює критичну необхідність впровадження комплексного підходу до захисту, який охоплює всі компоненти екосистеми ВД: від датчиків збору інформації до кінцевих систем візуалізації та аналітики.

Висновки до розділу 1

Дослідження показало, що з розвитком технологій ВД змінюється і характер загроз, які стають більш цілеспрямованими та складними. Особливу небезпеку становлять загрози, що використовують ШІ та машинне навчання для обходу систем захисту та цільового збору конфіденційної інформації.

Встановлено, що системи управління великими даними мають багаторівневу архітектуру, де кожен рівень має свої специфічні вразливості та вимоги до безпеки. Ефективний захист повинен охоплювати всі компоненти від збору та зберігання до аналізу та візуалізації даних.

Аналіз статистики засвідчив щорічне зростання кількості та складності кіберінцидентів у сфері великих даних, з особливим акцентом на атаки, спрямовані на викрадення даних та компрометацію аналітичних систем. Основними цілями для кібератак часто стають системи бізнес-аналітики, такі як Power BI, оскільки вони надають доступ до агрегованих і структурованих даних. Захист цих систем потребує особливої уваги в контексті загальної стратегії кібербезпеки.

Як відзначено в роботі, забезпечення безпеки ВД вимагає інтеграції технологічних рішень, організаційних заходів і регуляторних практик. Ізольовані підходи до безпеки не здатні забезпечити належний рівень захисту в умовах складних розподілених архітектур. Традиційні методи забезпечення безпеки потребують адаптації для роботи з великими обсягами даних та високою швидкістю їх обробки. Це стимулює розвиток нових підходів, таких як аналітика безпеки на основі машинного навчання та потокова обробка подій безпеки.

Таким чином, забезпечення кібербезпеки в СУВД є комплексним завданням, що вимагає системного підходу, інтеграції різних технологій захисту та постійної адаптації до нових викликів.

РОЗДІЛ 2 ВИКОРИСТАННЯ ІНСТРУМЕНТІВ POWER BI ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУВД

2.1 Архітектура та компоненти Power BI в контексті безпеки

Загальна архітектура платформи Power BI. Microsoft Power BI можна представити як інтегровану систему бізнес-аналітики, що поєднує аналітичні інструменти з механізмами безпеки корпоративного рівня [11]. За даними Gartner Magic Quadrant, платформа займає лідируючі позиції серед рішень для аналітики та бізнес-інтелекту [12]. Платформа розвинулася від базового інструменту візуалізації до комплексної системи, здатної обробляти значні обсяги даних із забезпеченням належного рівня захисту інформації.

Загальна архітектура Power BI показана на рис. 2.1.

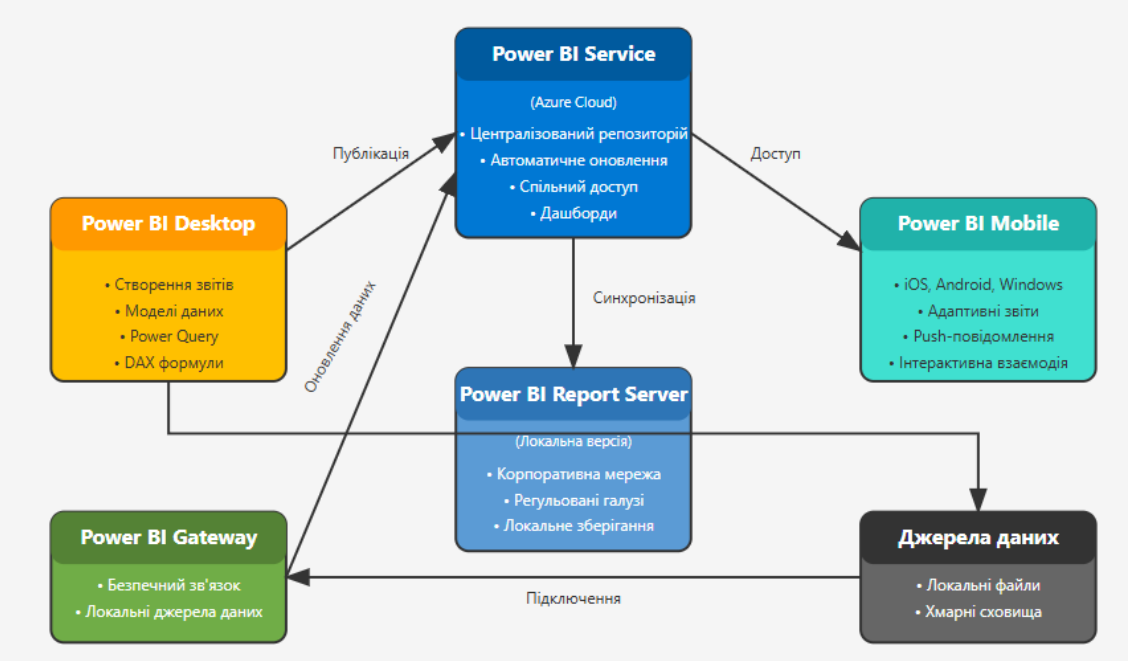

Рис. 2.1. Загальна архітектура Power BI

Основним компонентом архітектури є Power BI Desktop - застосунок для створення звітів та моделей даних. Цей інструмент забезпечує підключення до різноманітних джерел даних, від локальних файлів до хмарних сховищ [13]. Вбудований Power Query дозволяє виконувати трансформації даних, їх очищення та підготовку для аналізу. Користувачі можуть створювати складні

моделі даних, встановлювати зв'язки між таблицями та розробляти DAX-формули для спеціалізованих розрахунків [14].

Після розробки звітів у настільній версії вони публікуються в Power BI Service - хмарну службу на базі Microsoft Azure [15]. Ця платформа функціонує як централізований репозиторій для аналітичного контенту організації. Служба забезпечує автоматичне оновлення даних, створення персоналізованих дашбордів, спільний доступ до звітів і можливість їх вбудовування в інші застосунки.

Для організацій з особливими вимогами до зберігання даних доступний сервер звітів Power BI - локальна версія платформи. Це рішення дозволяє розгортати інфраструктуру Power BI всередині корпоративної мережі, що особливо важливо для компаній у регульованих галузях, таких як фінансовий сектор чи охорона здоров'я.

Мобільні додатки Power BI Mobile для iOS, Android та Windows забезпечують доступ до аналітики з мобільних пристроїв [16]. Ці застосунки адаптують звіти під розмір екрану, підтримують інтерактивну взаємодію з візуалізаціями та можуть надсилати повідомлення при досягненні визначених показників.

Для організацій з гібридною інфраструктурою ключовим компонентом є шлюз даних Power BI, який забезпечує безпечний зв'язок між локальними джерелами даних і хмарною службою. Шлюз даних підтримує роботу з різними системами баз даних і дозволяє налаштувати як планові оновлення, так і прямі запити в реальному часі.

Ключові компоненти безпеки в екосистемі Power BI (Рис. 2.2). Безпека в Power BI базується на концепції поглибленого захисту (Defense in Depth) - багаторівневому захисті, де кожен рівень доповнює та підсилює інші. Такий підхід відповідає рекомендаціям NIST Cybersecurity Framework [17] та забезпечує комплексний захист даних на всіх етапах їх обробки та зберігання [18].

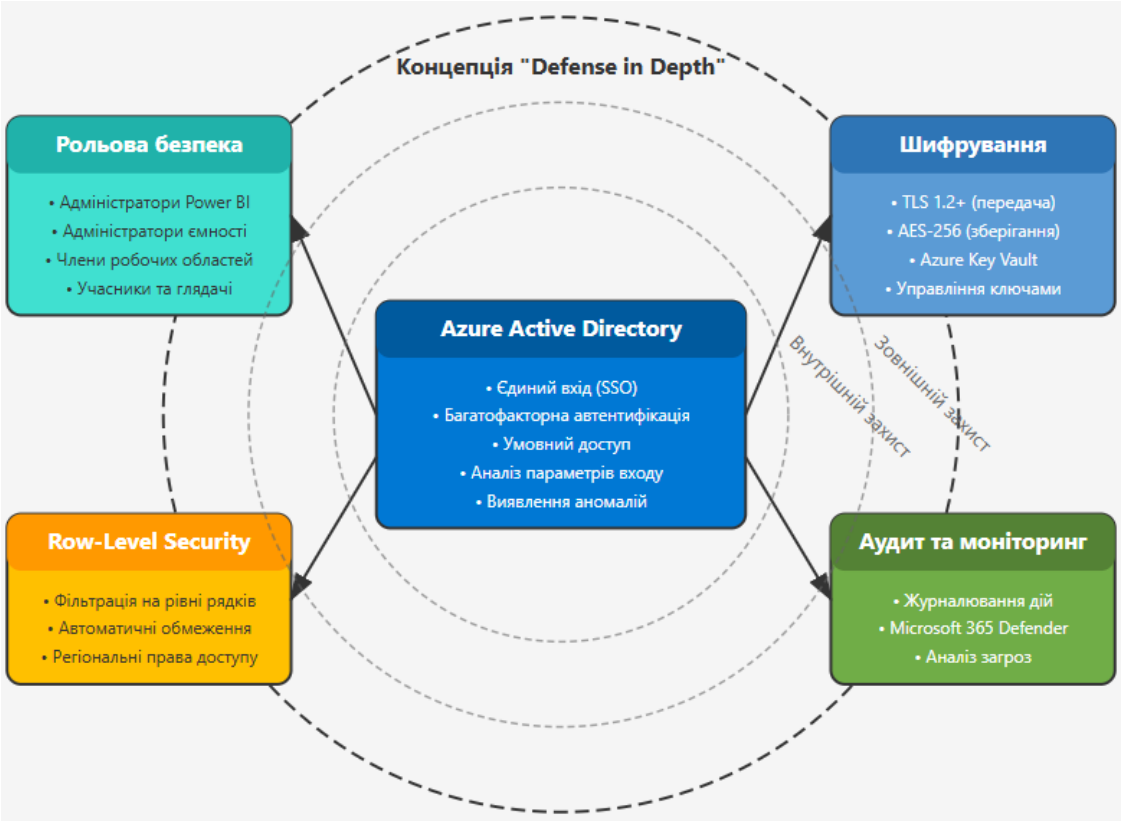

Рис. 2.2. Компоненти безпеки Power BI

Центральним елементом системи безпеки є Azure Active Directory, який управляє ідентифікацією та доступом користувачів [19]. Azure AD забезпечує єдиний вхід (Single Sign-On), багатофакторну автентифікацію та умовний доступ. Система аналізує численні параметри при спробі входу: розташування користувача, тип пристрою, відповідність звичайним патернам поведінки. При виявленні аномалій може вимагатися додаткова верифікація.

Рольова модель безпеки Power BI має чітку ієрархічну структуру. Адміністратори Power BI мають повний контроль над платформою. Адміністратори ємності управляють обчислювальними ресурсами. На рівні робочих областей існують ролі членів, учасників та глядачів з відповідними правами на створення, модифікацію або перегляд контенту.

Безпека на рівні рядків (RLS) дозволяє обмежувати доступ до даних на рівні окремих рядків. Наприклад, регіональні менеджери можуть бачити лише дані своїх регіонів при роботі з тим самим корпоративним звітом. Система автоматично фільтрує інформацію відповідно до прав доступу користувача.

Шифрування реалізовано на всіх рівнях обробки даних. При передачі

використовується протокол TLS 1.2+, для зберігання - алгоритм AES-256 [23]. Управління ключами шифрування здійснюється через Azure Key Vault, що надає організаціям контроль над процесом захисту даних [20].

Система аудиту фіксує всі дії користувачів у платформі: відкриття звітів, експорт даних, зміну прав доступу. Ці журнали можна аналізувати через Microsoft 365 Defender для виявлення потенційних загроз та розслідування інцидентів [21]. Регулярний аналіз логів допомагає забезпечити відповідність регуляторним вимогам.

Інтеграція Power BI з системами управління великими даними. Інтеграція Power BI з СУВД відкриває організаціям широкі можливості для ефективної роботи з масивними обсягами інформації. Сучасні компанії накопичують терабайти і навіть петабайти даних, розміщених у різних системах - від локальних серверів до хмарних платформ. Power BI вирішує складне завдання об'єднання цих розрізнених джерел у єдину аналітичну систему.

Платформа надає готові конектори для підключення до найпопулярніших систем обробки великих даних. Компанії, що використовують Apache Spark для аналітики, можуть безпосередньо підключити Power BI до своїх кластерів. Компанії, які зберігають дані в Databricks або Amazon Redshift, також мають нативну підтримку цих платформ. Широкий спектр конекторів охоплює практично всі основні хмарні сховища даних, що дозволяє організаціям використовувати Power BI незалежно від обраної ними технологічної платформи.

Багато організацій працюють у гібридному середовищі, де частина даних зберігається локально, а частина - у хмарі. Для таких сценаріїв Power BI пропонує технологію шлюзів даних. Локальний шлюз даних виступає безпечним мостом між локальними джерелами даних та хмарною службою Power BI. Цей компонент встановлюється всередині корпоративної мережі та забезпечує захищений канал передачі даних. Для компаній, що використовують віртуальні мережі Azure, доступний шлюз віртуальної мережі, який дозволяє Power BI безпечно підключатися до ресурсів, розміщених у приватних мережах Azure.

Сучасний бізнес потребує інформації в режимі реального часу, і Power BI відповідає на цей виклик через інтеграцію з Azure Stream Analytics. Ця інтеграція дозволяє обробляти потокові дані та миттєво відображати їх на дашбордах. Фінансові установи можуть моніторити транзакції в реальному часі, виробничі підприємства - відстежувати показники обладнання, а ритейлери - аналізувати поточні продажі. Інформаційні панелі оновлюються автоматично при надходженні нових даних, забезпечуючи керівництву актуальну картину бізнес-процесів.

Робота з великими наборами даних вимагає спеціальних підходів, і Power BI пропонує кілька технологій для оптимізації такої роботи. DirectQuery дозволяє виконувати запити безпосередньо до джерела даних без необхідності імпортувати мільярди рядків. Це особливо корисно, коли потрібно працювати з актуальними даними або коли обсяг інформації занадто великий для імпортування. Змішані моделі надають можливість комбінувати імпортовані дані з DirectQuery, створюючи гібридні моделі, що поєднують швидкість локальних даних з актуальністю прямих запитів. Технологія інкрементого оновлення вирішує проблему оновлення великих історичних наборів даних, завантажуючи лише нові або змінені записи, що значно скорочує час оновлення і навантаження на систему.

Безпека залишається пріоритетом при інтеграції з системами ВД. Усі з'єднання використовують захищені протоколи передачі даних, що унеможливлює їх перехоплення під час транспортування. Налаштування мережевої ізоляції забезпечує, що доступ до даних мають лише авторизовані системи та користувачі. Постійний моніторинг з'єднань дозволяє виявляти та блокувати підозрілу активність.

2.2 Механізми забезпечення безпеки в Power BI

Автентифікація та управління доступом. Система автентифікації Power BI базується на Azure Active Directory та реалізує багаторівневий підхід до

контролю доступу. Платформа надає різні методи автентифікації залежно від потреб організації та рівня безпеки.

Базова парольна автентифікація може бути посилена політиками складності паролів та регулярної ротації. Багатофакторна автентифікація (MFA) використовує додаткові фактори верифікації: SMS-коди, мобільні додатки (Microsoft Authenticator, Google Authenticator), апаратні токени FIDO2, біометричні методи. Для автоматизованих процесів та сервісних облікових записів доступна сертифікатна автентифікація на базі стандарту X.509.

На рисунку 2.3 показано архітектуру системи автентифікації Power BI, яка демонструє взаємодію між різними компонентами безпеки та методами верифікації користувачів, включаючи інтеграцію з Azure Active Directory, процеси багатофакторної автентифікації та управління правами доступу.

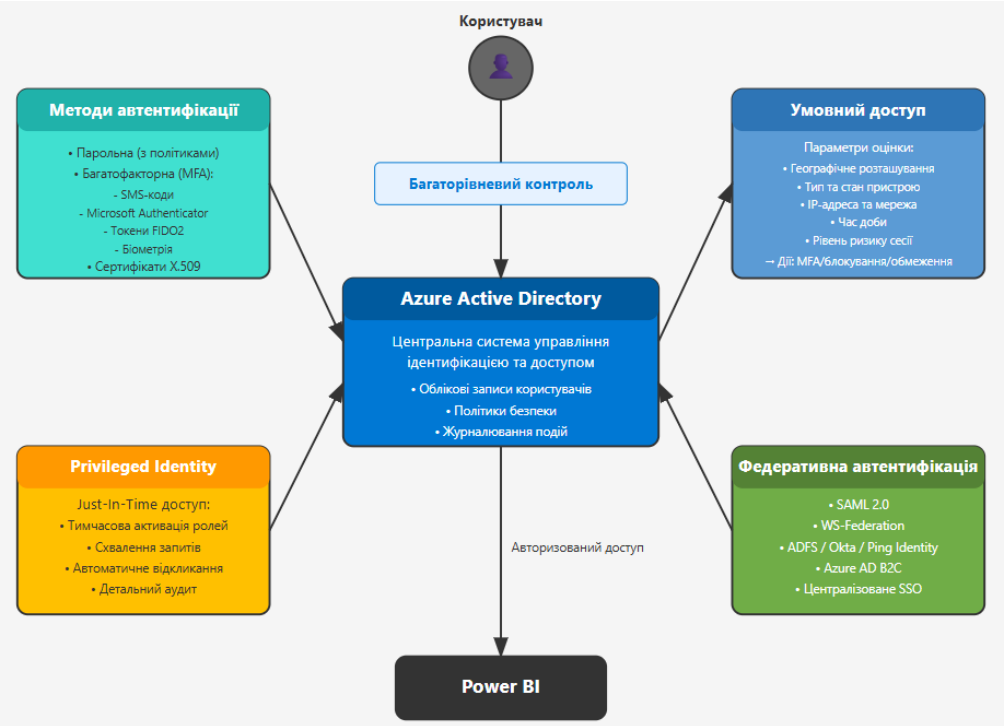

Рис. 2.3. Система автентифікації

Політики *умовного доступу* аналізують контекст кожної спроби входу та застосовують відповідні вимоги безпеки. Система оцінює географічне розташування користувача, тип та стан безпеки пристрою, IP-адресу, мережу підключення, час доби, рівень ризику сесії. На основі цих параметрів можуть

застосовуватися додаткові вимоги: MFA, блокування доступу, обмеження функціональності.

Управління привілейованим доступом (Privileged Identity Management, PIM) реалізує принцип своєчасного адміністрування. Адміністративні ролі активуються лише на обмежений час після схвалення запиту. Система веде детальний аудит всіх привілейованих дій та автоматично відкликає підвищені права після закінчення встановленого терміну. Доступні ролі включають адміністратора Power BI, адміністратора ємності та адміністратора робочої області.

Power BI реалізує *федеративну автентифікацію,* підтримуючи інтеграцію з корпоративними системами управління ідентичністю через стандарти SAML 2.0 та WS-Federation. Це дозволяє використовувати існуючі системи SSO: Active Directory Federation Services (ADFS), Okta, Ping Identity, Azure AD B2C для зовнішніх користувачів. Федеративна автентифікація забезпечує централізоване управління обліковими записами та єдині політики безпеки.

Шифрування даних і захист каналів передачі. Power BI реалізує комплексний підхід до шифрування даних на всіх етапах їх обробки. Платформа використовує індустріальні стандарти криптографії та надає гнучкі можливості управління ключами.

Всі дані в Power BI автоматично шифруються за допомогою шифрування служби сховища Azure з використанням алгоритму AES-256. За замовчуванням ключі управляються Microsoft, але організації можуть використовувати ключі, керовані клієнтом (Customer Managed Keys) через Azure Key Vault. Технологія власних ключів (Bring Your Own Key) дозволяє імпортувати власні ключі з апаратних модулів безпеки. Подвійне шифрування ключів забезпечує подвійний захист критично важливих даних.

Шифрування на рівні додатків. Настільна версія Power BI шифрує локальний кеш даних та тимчасові файли. Файли проектів .pbix підтримують парольний захист. При експорті даних застосовуються політики захисту інформації Microsoft для автоматичного шифрування та маркування файлів.

Окрім цього приватний канал Azure забезпечує приватні з'єднання між Power BI та іншими службами Azure. Кінцеві точки служби віртуальної мережі оптимізують маршрутизацію трафіку. Для гібридних середовищ доступні VPN-тунелі та виділені канали ExpressRoute. Групи безпеки мережі контролюють вхідний та вихідний трафік.

Безпека на рівні рядків (Row-Level Security) дозволяє обмежувати доступ до даних на рівні окремих рядків, створюючи персоналізовані представлення інформації для різних користувачів або груп.

На рисунку 2.4 показано принцип роботи безпеки на рівні рядків у Power BI, який демонструє, як різні користувачі з різними ролями отримують доступ лише до тих даних, які відповідають їхнім правам доступу. Схема ілюструє механізм фільтрації даних на основі ролей користувачів та правил безпеки, що забезпечує персоналізований доступ до інформації без необхідності створення окремих звітів для кожної групи користувачів.

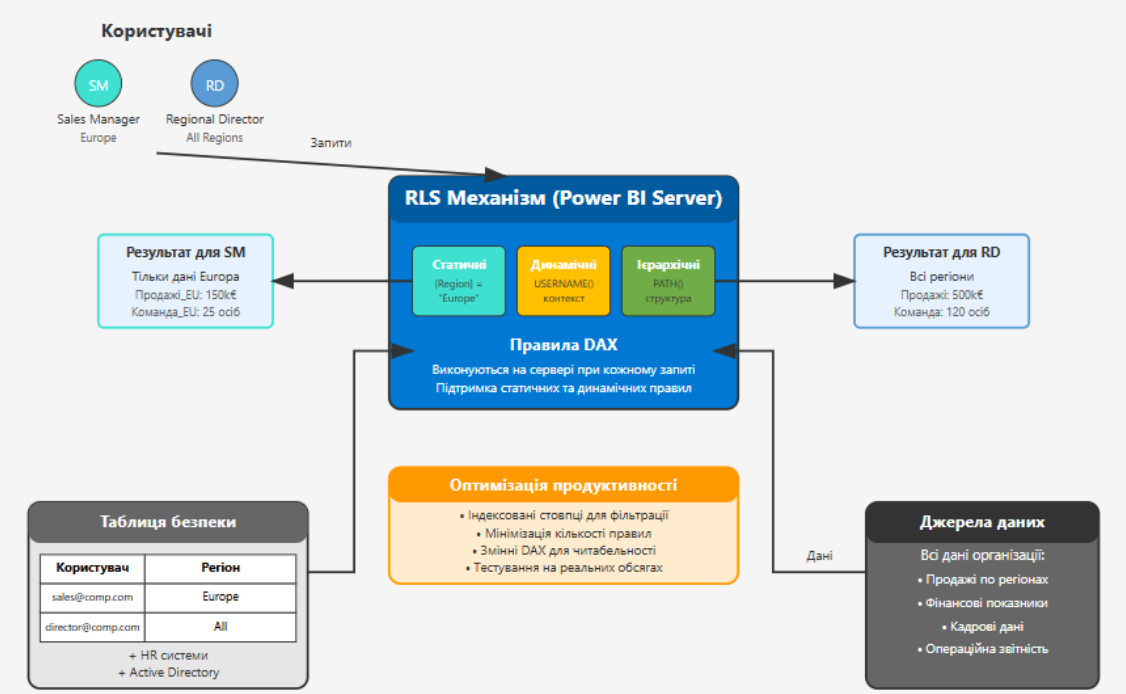

Рис. 2.4. Безпека на рівні рядків.

RLS базується на правилах фільтрації, написаних мовою DAX [22]. Правила виконуються на сервері при кожному запиті, гарантуючи, що

користувач отримує лише дозволені дані. Система підтримує статичні й динамічні правила, які можуть комбінуватися для створення складних моделей безпеки.

Статичні правила використовують фіксовані умови: `[Region] = "Europe"` або `[Department] = "Sales"`. Динамічні правила використовують контекст користувача через функції `USERPRINCIPALNAME()` або `USERNAME()`. Ієрархічні правила реалізуються через функції `PATH` та `PATHCONTAINS` для організаційних структур.

Рекомендований підхід передбачає використання окремих таблиць для управління правами доступу. Таблиця безпеки містить відповідність між користувачами і дозволеними значеннями. Це спрощує адміністрування та дозволяє оновлювати права без зміни моделі даних. Таблиці можуть синхронізуватися з HR-системами або Active Directory.

Правила RLS можуть впливати на швидкість запитів. Для оптимізації рекомендується використовувати індексовані стовпці для фільтрації, мінімізувати кількість правил, застосовувати змінні DAX для покращення читабельності, тестувати продуктивність на реальних обсягах даних [23].

Аудит та моніторинг діяльності користувачів. Система аудиту Power BI забезпечує повну прозорість всіх дій у платформі, дозволяючи організаціям відстежувати використання, виявляти аномалії та забезпечувати відповідність вимогам безпеки [24].

Power BI інтегрується з єдиним журналом аудиту Microsoft 365,, фіксуючи всі події з детальною інформацією: користувач, час, IP-адреса, тип дії, об'єкт операції. Події зберігаються 90 днів за замовчуванням, з можливістю розширення до одного року. Дані аудиту доступні через PowerShell, REST API, центр безпеки та відповідності Office 365.

Система фіксує дії з контентом (створення, модифікація, видалення звітів та наборів даних), адміністративні операції (зміна налаштувань організації, управління користувачами), дії безпеки (спроби входу, зміни прав доступу), використання ресурсів (запити до наборів даних, використання ємності).

Інструменти моніторингу. PowerShell модуль Microsoft. PowerBI. Management дозволяє автоматизувати збір та аналіз подій. Power BI REST API надає програмний доступ до даних аудиту. Центр безпеки та відповідності Office 365 пропонує графічний інтерфейс для пошуку та аналізу подій. Azure Monitor збирає метрики продуктивності та дозволяє налаштовувати сповіщення.

Інтеграція з SIEM. Microsoft Sentinel має нативні конектори для Power BI та готові сценарії реагування на інциденти. Сторонні SIEM-системи (Splunk, QRadar, ArcSight) можуть інтегруватися через API або Azure Event Hub. Можливе налаштування автоматичних сповіщень, створення інцидентів безпеки, автоматизація реагування.

Аналітика використання. Звіти про метрики використання показують статистику використання звітів: кількість переглядів, унікальні користувачі, час завантаження. Аналіз продуктивності допомагає оптимізувати моделі даних та запити. Метрики ємності відстежують використання обчислювальних ресурсів преміум-ємностей.

Автоматизація моніторингу. Power Automate дозволяє створювати потоки для аналізу подій та автоматичного реагування. Алгоритми машинного навчання виявляють аномалії в патернах використання. Можливе автоматичне блокування підозрілої активності, надсилання сповіщень, створення звітів для керівництва.

2.3 Використання Power BI для моніторингу кібербезпеки

Сучасні організації стикаються з постійно зростаючою кількістю кіберзагроз, що вимагає не лише потужних систем захисту, але й ефективних інструментів візуалізації та аналізу даних безпеки. Power BI перетворилася на незамінний інструмент для команд кібербезпеки, допомагаючи перетворювати складні технічні дані на зрозумілі візуальні представлення [25].

На рисунку 2.5 показано приклад інформаційної панелі Power BI для моніторингу кібербезпеки, який демонструє розподіл по кількості загроз в рамках певного періоду, включає середній вплив загроз на систему, час усунення загроз.

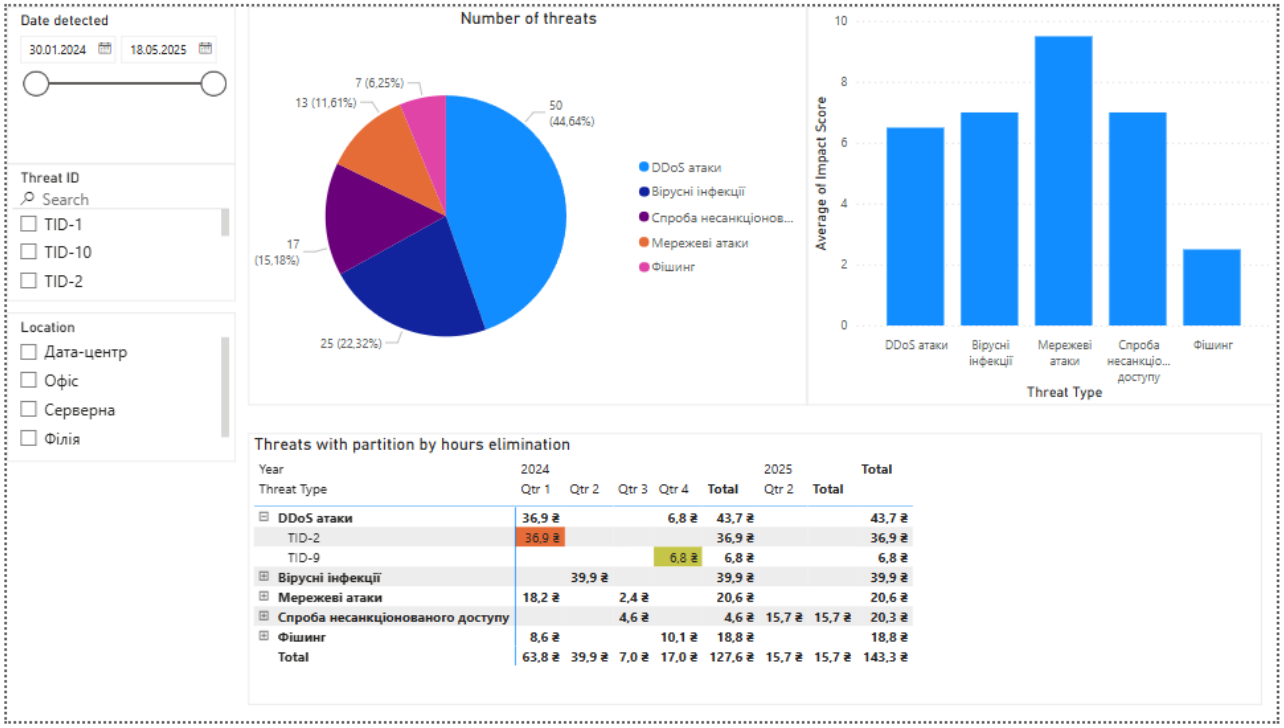

Рис. 2.5. Приклад інформаційної панелі в Power BI

Створення інформаційної панелі для візуалізації загроз. Уявімо ситуацію: о третій годині ночі спрацьовує система виявлення вторгнень. Черговий аналітик безпеки повинен миттєво оцінити масштаб загрози, визначити уражені системи та прийняти рішення про подальші дії. Саме в такі моменти добре спроектований дашборд Power BI стає критично важливим інструментом.

Побудова ефективної системи візуалізації

Створення дашборду безпеки починається з розуміння потреб різних користувачів. Керівництво компанії цікавить загальна картина: чи захищена організація, скільки коштують інциденти безпеки, чи відповідає компанія регуляторним вимогам. Технічні спеціалісти потребують детальної інформації про конкретні загрози, вразливості та інциденти.

Тому ефективна інформаційна панель будується за принципом "від загального до конкретного". На головній сторінці розміщуються ключові

показники: загальний рівень безпеки організації (часто представлений як єдиний числовий показник від 0 до 100), кількість активних інцидентів, середній час реагування на загрози. Ці метрики оновлюються в реальному часі, даючи миттєвий знімок поточного стану.

Далі йдуть більш детальні візуалізації. Географічна карта показує, звідки надходять атаки - раптовий сплеск активності з певної країни може свідчити про цілеспрямовану кампанію. Часова діаграма відображає інтенсивність атак протягом дня або тижня, допомагаючи виявити патерни, наприклад, чи активізуються зловмисники в неробочий час.

Ефективні візуальні елементи. Теплові карти стали одним з найефективніших способів представлення даних безпеки. Замість перегляду сотень рядків логів, аналітик одним поглядом бачить "гарячі точки" - сегменти мережі або географічні регіони з підвищеною активністю. Червоні плями на карті миттєво привертають увагу до проблемних зон.

Шкальні діаграми працюють як спідометр безпеки. Стрілка в зеленій зоні означає нормальний стан, жовта зона сигналізує про необхідність уваги, червона вимагає негайних дій. Такі візуалізації інтуїтивно зрозумілі навіть нетехнічним користувачам.

Каскадні діаграми допомагають зрозуміти, як різні фактори впливають на загальний рівень безпеки. Наприклад, вони показують, що відсутність оновлень на 20% серверів знижує загальний показник безпеки на 15 пунктів, а невиправлені критичні вразливості - ще на 25 пунктів. Це допомагає пріоритезувати зусилля команди безпеки.

Інтерактивність дашбордів. Статичні звіти залишилися в минулому. Сучасні дашборди Power BI дозволяють користувачам активно взаємодіяти з даними. Клік на конкретному інциденті відкриває детальну інформацію: хронологію подій, уражені системи, вжиті заходи. Фільтри дозволяють звузити фокус і подивитися лише критичні інциденти за останню добу або проаналізувати атаки на конкретний сегмент мережі.

Особливо цінною є можливість створювати "закладки" - збережені стани дашборду для різних сценаріїв. Закладка "Ранковий огляд" показує події за ніч, "Аудит для керівництва" приховує технічні деталі та фокусується на бізнес-метриках, "Режим розслідування" відкриває всі технічні панелі для глибокого аналізу. На рисунку 2.6 показано інтерактивні можливості інформаційних панелей Power BI, які демонструють функціональність закладок для різних сценаріїв використання, фільтрацію даних та можливості детального аналізу інцидентів безпеки через інтерактивні елементи управління.

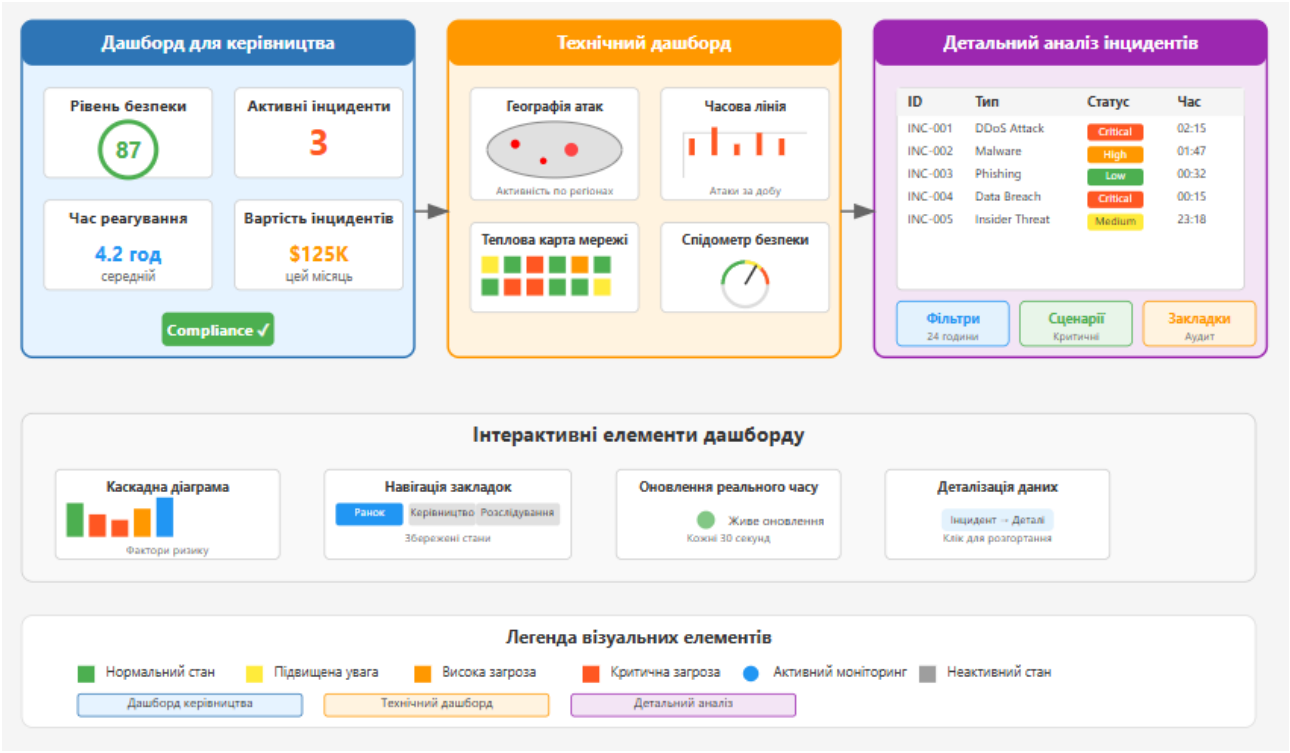

Рис. 2.6. Інтерактивність дашбордів

Аналіз журналів подій і виявлення аномалій. Кожен день інформаційні системи організації генерують мільйони записів у журналах подій. Серед цього океану даних приховані сигнали про потенційні загрози, зокрема спроби несанкціонованого доступу, підозріла мережева активність, аномальна поведінка користувачів. Завдання Power BI полягає у забезпеченні ефективного виявлення аномалій серед величезних масивів даних безпеки.

На рисунку 2.7 показано процес аналізу журналів подій у Power BI, який ілюструє методи консолідації різнорідних джерел даних, алгоритми виявлення

аномалій та способи кореляції подій для ідентифікації потенційних загроз кібербезпеці.

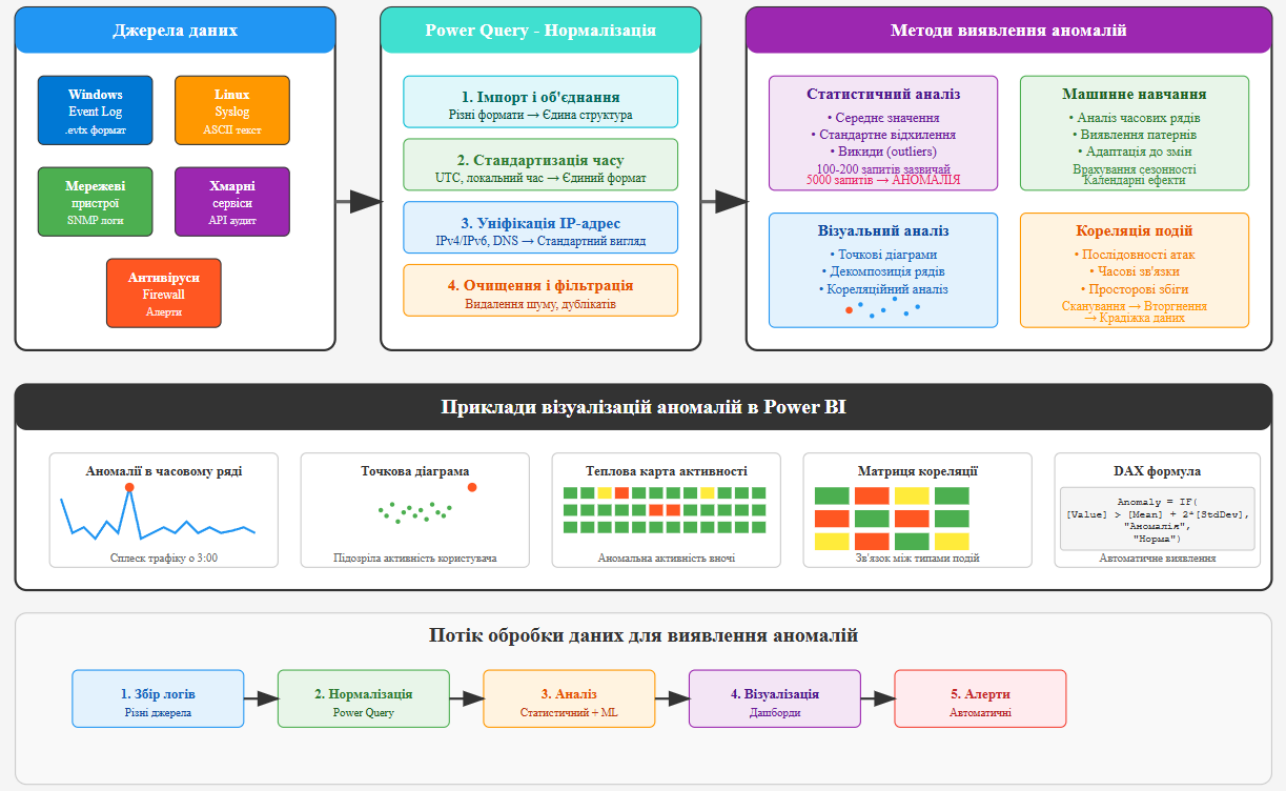

Рис. 2.7. Аналіз журналів

Об'єднання розрізнених джерел даних. Сучасна організація використовує десятки різних систем, кожна з яких веде власні журнали. Сервери Windows записують події в журналах подій, Linux-системи використовують syslog, мережеве обладнання генерує власні логи, хмарні сервіси мають свої системи аудиту. Кожне джерело має унікальний формат, структуру, рівень деталізації.

Power BI через інструменти Power Query дозволяє імпортувати всі ці різнорідні дані та привести їх до спільного знаменника. Процес нормалізації включає стандартизацію часових міток (важливо для кореляції подій), уніфікацію форматів IP-адрес, приведення імен користувачів до єдиного стандарту. Результатом є консолідований набір даних, готовий для аналізу.

Статистичні методи пошуку аномалій. Найпростіший спосіб виявлення аномалій - статистичний аналіз. Power BI розраховує середні значення для різних метрик (кількість спроб входу, обсяг мережевого трафіку, кількість запитів до

бази даних) і визначає нормальний діапазон через стандартне відхилення. Події, що виходять за межі цього діапазону, автоматично позначаються як підозрілі.

Наприклад, якщо користувач зазвичай щоденно генерує 100-200 запитів до бази даних, раптове збільшення до 5000 запитів викличе тривогу. Це може свідчити про спробу масового викачування даних або компрометацію облікового запису.

Машинне навчання для складних патернів. Вбудовані алгоритми ШІ Power BI йдуть далі простої статистики. Вони аналізують історичні дані, вчаться розпізнавати нормальні патерни поведінки й автоматично адаптуються до змін. Алгоритм враховує сезонність (підвищена активність в кінці кварталу може бути нормальною), тренди (поступове зростання трафіку через розширення бізнесу), календарні ефекти (знижена активність у вихідні).

Особливо ефективними є алгоритми виявлення аномалій у часових рядах. Вони можуть розпізнати, що підвищена активність о 9 ранку в понеділок - це нормально (всі приходять на роботу), але така ж активність о 3 ночі в суботу є підозрілою.

Візуальні методи аналізу. Іноді людське око помічає патерни краще за будь-який алгоритм. Power BI надає різноманітні візуалізації для пошуку аномалій. Точкові діаграми відображають тисячі подій на площині, і аномалії часто виділяються як точки, що знаходяться окремо від основної маси даних.

Діаграми декомпозиції часових рядів розбивають складні патерни на компоненти. Аналітик може побачити основний тренд, сезонні коливання та залишкові відхилення. Саме в цих відхиленнях часто приховуються ознаки атак або системних проблем.

Кореляція подій для виявлення складних атак. Сучасні кібератаки рідко складаються з однієї дії. Зловмисники використовують складні сценарії: спочатку сканування мережі, потім спроби підбору паролів, експлуатація вразливостей, закріплення в системі, бокові переміщення, і нарешті - крадіжка даних. Кожна окрема подія може виглядати нешкідливою, але їх комбінація вказує на серйозну загрозу.

Power BI дозволяє створювати правила кореляції, які автоматично виявляють такі складні патерни. Формули DAX можуть аналізувати послідовності подій, шукати збіги в часі та просторі, враховувати контекст. Наприклад, система може виявити, що невдалі спроби входу, після яких протягом години відбувається успішний вхід з нової локації та масовий експорт даних - це ознака компрометації облікового запису.

Інтеграція з SIEM системами. Системи управління інформацією та подіями безпеки (SIEM) є серцем сучасних операційних центрів безпеки. Вони збирають, аналізують та корелюють події з усієї інфраструктури в реальному часі. Power BI доповнює можливості SIEM, додаючи потужні інструменти візуалізації, поглибленої аналітики та звітності.

Синергія двох платформ. SIEM-системи відмінно справляються з операційними завданнями: збір логів, виявлення загроз у реальному часі, автоматизоване реагування [26]. Однак їх можливості візуалізації та довгострокової аналітики часто обмежені. Power BI заповнює цю прогалину, перетворюючи технічні дані SIEM на зрозумілі бізнес-метрики та тренди.

Типовий сценарій інтеграції виглядає так: SIEM збирає та аналізує події, генерує сповіщення про інциденти, автоматизує першочергові дії реагування. Power BI отримує ці дані та створює аналітичні дашборди для керівництва, генерує звіти про тренди безпеки, проводить ретроспективний аналіз інцидентів, допомагає в стратегічному плануванні безпеки.

На рисунку 2.8 показано архітектуру інтеграції між Power BI та SIEM-системами, яка демонструє потоки даних між різними компонентами, механізми обміну інформацією та розподіл функцій між платформами для забезпечення комплексного моніторингу кібербезпеки.

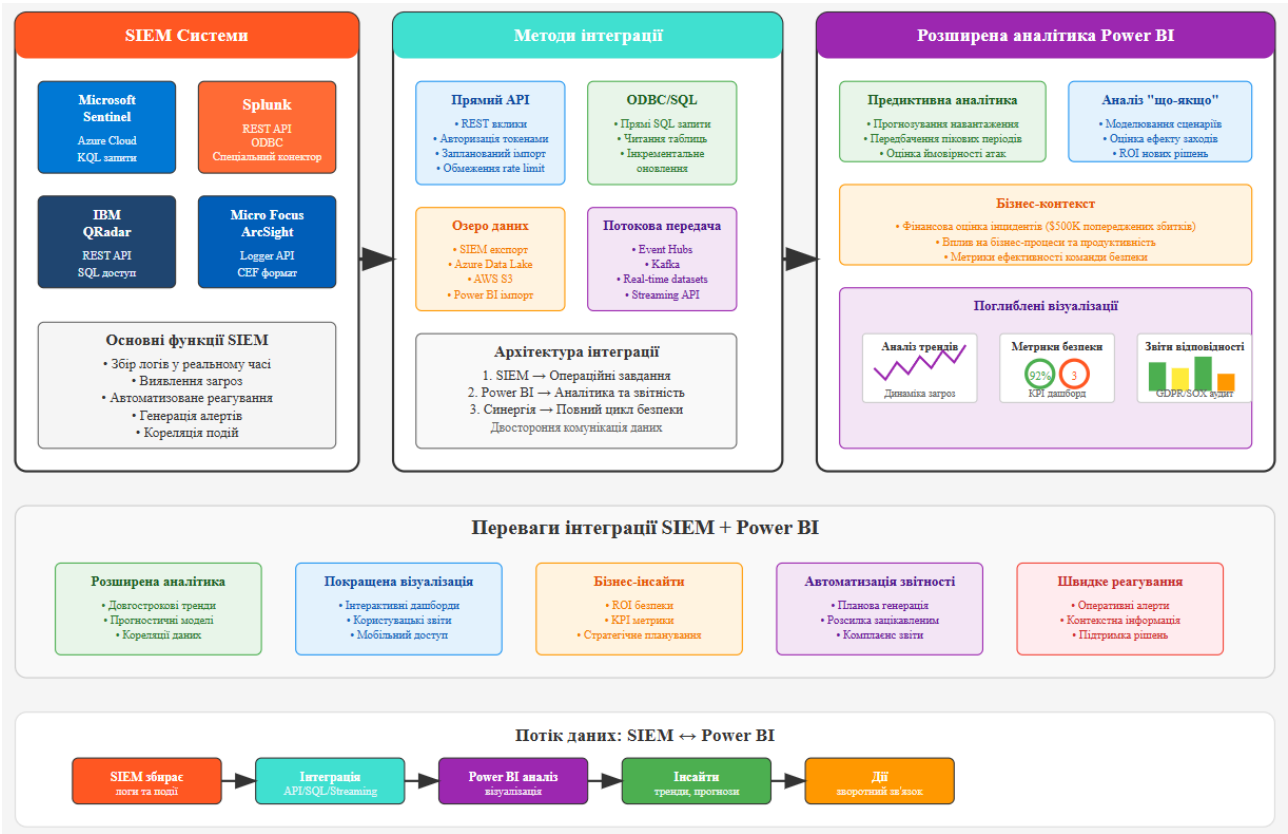

Рис. 2.8. Power BI та SIEM - системи

Технічні аспекти інтеграції. Різні SIEM-системи пропонують різні методи інтеграції. Microsoft Sentinel, будучи хмарним рішенням Azure, має найтісніші зв'язки з Power BI [27]. Дані можна отримувати напряму з робочої області Log Analytics, використовуючи ту ж мову запитів Kusto (KQL). Це дозволяє аналітикам безпеки використовувати знайомі запити в обох системах.

Для Splunk існує кілька варіантів інтеграції. REST API дозволяє виконувати збережені пошуки та отримувати результати. ODBC-конектор забезпечує прямий доступ до даних через SQL-подібні запити. Спеціальний додаток Splunk для Power BI спрощує налаштування з'єднання та надає готові шаблони візуалізацій.

IBM QRadar та ArcSight також підтримують API-інтеграцію, хоча вона може вимагати більше налаштувань. Часто організації використовують проміжний шар - озеро або сховище даних, куди SIEM експортує інформацію для подальшого аналізу в Power BI.

Розширення аналітичних можливостей. Інтеграція з Power BI додає SIEM нові виміри аналізу. Прогнозна аналітика дозволяє прогнозувати навантаження

на команду безпеки, передбачати періоди підвищеної активності загроз, оцінювати ймовірність успіху різних типів атак.

Аналіз "що-якщо" допомагає моделювати різні сценарії. Що станеться, якщо організація впровадить нову систему захисту? Як зміниться профіль ризику? Скільком інцидентам організація зможе запобігти? Power BI дозволяє візуалізувати відповіді на ці питання, допомагаючи приймати обґрунтовані рішення про інвестиції в безпеку.

Бізнес-контекст для технічних даних. Унікальна цінність Power BI полягає в здатності пов'язувати технічні події безпеки з бізнес-контекстом. Замість абстрактних чисел "1000 заблокованих атак", керівництво бачить "не допущено потенційних збитків на $500,000". Це допомагає обґрунтовувати бюджети на безпеку та демонструвати цінність роботи команди.

Дашборди можуть показувати, які бізнес-процеси найбільше страждають від інцидентів безпеки, які відділи генерують найбільше ризиків, як інциденти впливають на продуктивність бізнесу. Така інформація безцінна для пріоритезації заходів безпеки.

Звітність про інциденти безпеки. Коли відбувається серйозний інцидент безпеки, правильна комунікація стає критично важливою. Різні зацікавлені сторони потребують різної інформації: технічна команда - детальний аналіз для усунення проблеми, керівництво - оцінку впливу на бізнес, регулятори - доказ відповідності вимогам, клієнти - запевнення, що їхні дані в безпеці.

На рисунку 2.9 показано структуру системи звітності про інциденти безпеки в Power BI, яка ілюструє різні типи звітів для різних аудиторій, процеси автоматизації генерування документації та механізми адаптації контенту відповідно до потреб різних зацікавлених сторін.

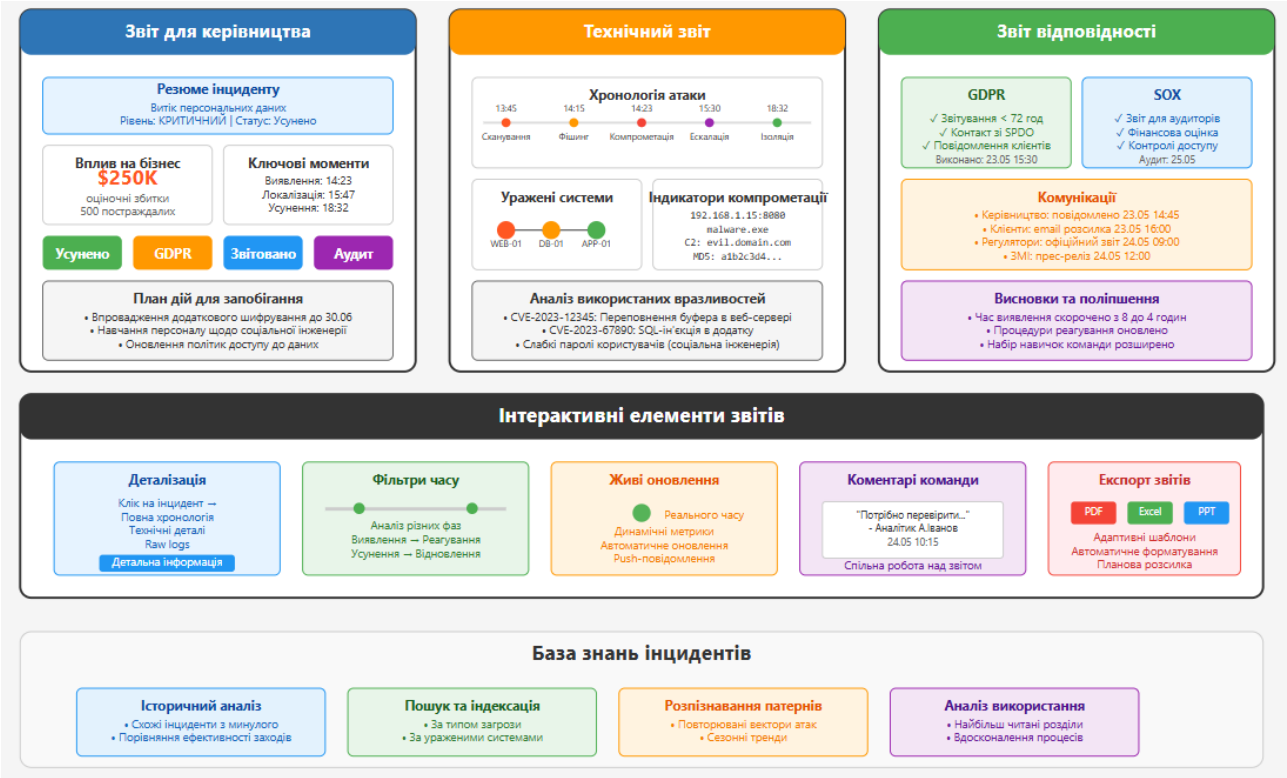

Рис. 2.9. Звітність про інциденти безпеки

Адаптація звітів до потреб аудиторії. Power BI дозволяє створювати багаторівневі звіти, які адаптуються до потреб різних аудиторій. Для вищого керівництва готується стисле резюме на одну сторінку: що сталося, який вплив на бізнес, які дії вжито, що потрібно для запобігання повторенню. Використовуються прості візуалізації - світлофорні індикатори статусу, часова шкала ключових подій, фінансова оцінка збитків.

Для технічної команди створюється детальний технічний звіт: повна хронологія атаки з точністю до секунди, діаграми мережевого трафіку, аналіз використаних експлойтів, індикатори компрометації для пошуку подібних атак. Інтерактивні елементи дозволяють досліджувати дані - фільтрувати події за типом, переглядати первинні журнали, аналізувати залежності між системами.

Для регуляторів готується звіт відповідності: підтвердження дотримання вимог сповіщення (наприклад, 72 години для GDPR), докази вжитих заходів захисту, план усунення виявлених недоліків, хронологія комунікації з постраждалими сторонами [28].

Автоматизація рутинних завдань. Під час інциденту час є критичним ресурсом. Power BI автоматизує багато рутинних завдань звітності. Дані автоматично імпортуються з систем моніторингу, SIEM, тікетних систем. Ключові метрики (час виявлення, час реагування, кількість уражених систем, орієнтовні збитки) розраховуються автоматично.

Шаблони звітів прискорюють процес. Для різних типів інцидентів (витік даних, атака вірусів-вимагачів, DDoS) існують готові шаблони з відповідними розділами та візуалізаціями. Достатньо заповнити специфічні дані інциденту, і базовий звіт готовий.

Інтерактивність для глибокого аналізу. На відміну від статичних PDF-звітів, звіти Power BI залишаються "живими". Читачі можуть взаємодіяти з даними: змінювати часові рамки для аналізу різних фаз інциденту, фільтрувати події за критеріями, переходити від загальної картини до технічних деталей.

Особливо цінною є можливість проведення ретроспективного аналізу. Після завершення інциденту команда може повернутися до звіту і проаналізувати, що можна було зробити краще, які сигнали були пропущені, як покращити процеси реагування. Інтерактивні сценарії дозволяють моделювати альтернативні варіанти дій.

Збереження інституційної пам'яті. Кожен інцидент є уроком для організації. Power BI допомагає створити базу знань з минулих інцидентів. Звіти зберігаються в централізованому репозиторії, індексуються за типом загрози, використаними векторами атаки, ураженими системами. У разі нового інциденту аналітики можуть швидко знайти подібні випадки з минулого та використати набутий досвід.

Аналітика використання звітів показує, які розділи читають найчастіше, які метрики викликають найбільше питань, як довго різні аудиторії працюють зі звітами. Ця інформація допомагає постійно вдосконалювати процес звітності, роблячи його більш ефективним та корисним.

Висновки до розділу 2

У ході дослідження встановлено, що сучасна платформа бізнес-аналітики Power BI може ефективно використовуватися не лише для аналізу бізнес-даних, але й як інструмент забезпечення кібербезпеки в СУВД. Її архітектура дозволяє працювати з різними джерелами інформації, включно з великими обсягами потокових і збережених даних, а також забезпечує гнучкість при інтеграції в локальні та хмарні середовища.

З'ясовано, що важливою перевагою Power BI є її здатність підтримувати багаторівневу систему безпеки, що відповідає концепції поглибленого захисту. До ключових механізмів безпеки належать автентифікація на базі Azure Active Directory, підтримка багатофакторної автентифікації, умовного доступу та рольової моделі, шифрування даних із використанням алгоритмів AES-256, а також аудит усіх дій користувачів. Крім того, завдяки механізмам безпеки на рівні рядків можливо здійснювати персоналізований контроль доступу до даних, що є критично важливим у розподілених або конфіденційних середовищах.

Окрему увагу приділено аналітичним можливостям платформи для моніторингу подій безпеки. Досліджено, що Power BI дозволяє створювати дашборди, які відображають реальний стан безпеки, виявляють аномалії, відстежують підозрілу активність та надають можливості для ретроспективного аналізу кіберінцидентів. Інструменти візуалізації, такі як теплові карти, шкальні діаграми та каскадні графіки, суттєво підвищують ефективність сприйняття інформації, особливо у критичних ситуаціях.

Результати аналізу підтверджують, що Power BI може бути ефективно інтегрована з SIEM-системами, такими як Microsoft Sentinel або Splunk, що значно розширює її функціонал у сфері кіберзахисту. Така інтеграція забезпечує глибоку кореляцію подій, підтримку автоматизованих сценаріїв реагування та формування звітності для різних цільових аудиторій – від технічних фахівців до керівництва й регуляторів.

РОЗДІЛ 3 ПЕРСПЕКТИВИ І ВИКЛИКИ ВИКОРИСТАННЯ POWER BI У КІБЕРБЕЗПЕЦІ СУВД

3.1 Інноваційні технології в Power BI для забезпечення кібербезпеки СУВД

Стрімкий розвиток технологій ШІ та машинного навчання кардинально змінює підходи до забезпечення кібербезпеки в сучасних організаціях. Microsoft Power BI не залишається осторонь цієї революції, активно інтегруючи передові технології, які дозволяють трансформувати традиційні реактивні методи захисту на проактивні стратегії запобігання загрозам (Рис. 3.1). Ця трансформація особливо актуальна для СУВД, де масштаб і складність інформаційних потоків вимагають принципово нових підходів до моніторингу та аналізу безпеки.

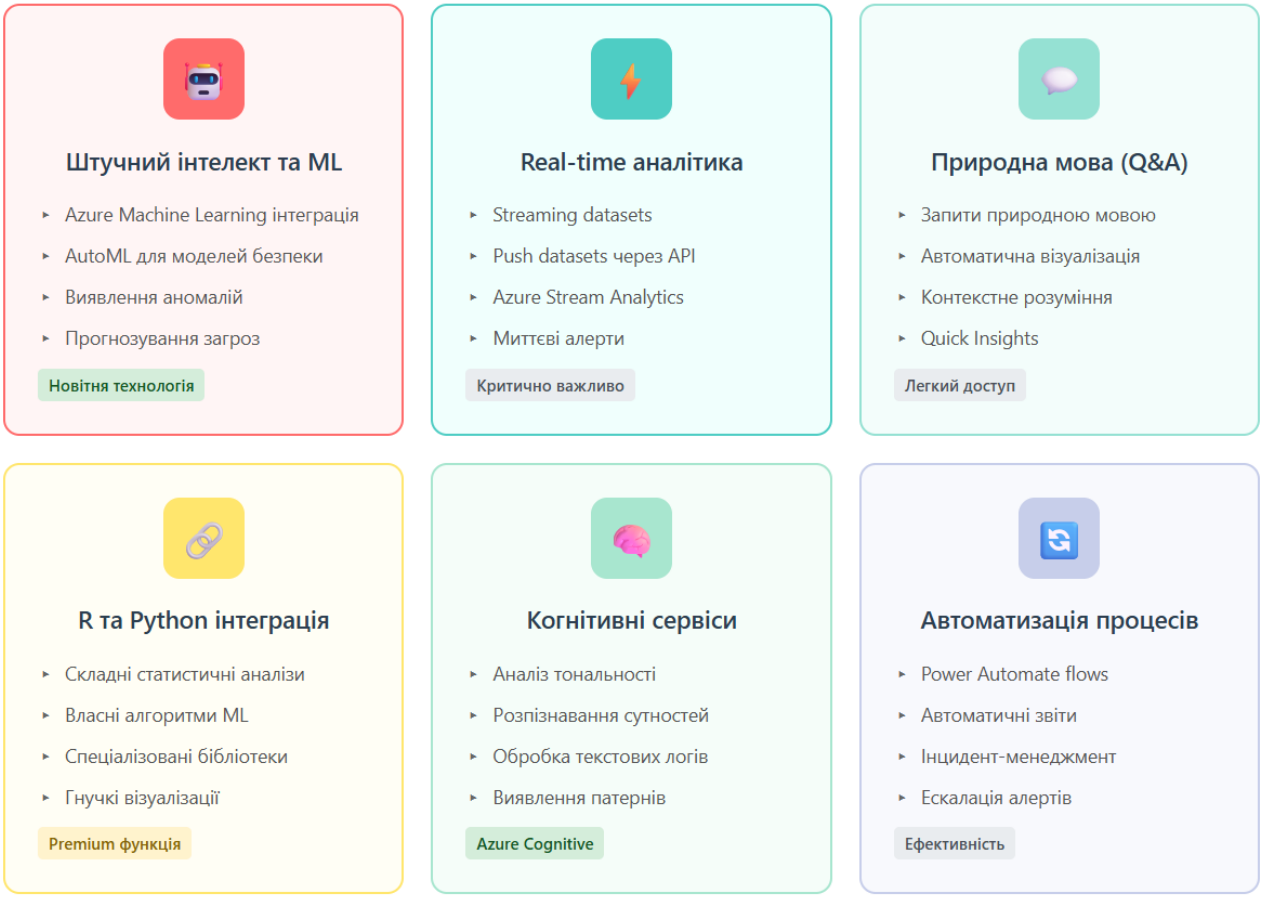

Рис. 3.1. Інноваційні технології Power BI

Технології штучного інтелекту та машинного навчання. Сучасні можливості Power BI у сфері машинного навчання базуються на глибокій інтеграції з хмарним сервесом Azure Machine Learning, що створює потужну синергію між аналітикою даних та ШІ [29]. Ця інтеграція дозволяє організаціям автоматизувати найскладніші процеси виявлення аномалій у великих масивах даних безпеки, які раніше вимагали значних людських ресурсів та експертизи.

Революційною технологією стає Automated Machine Learning (AutoML), яка кардинально спрощує процес створення моделей машинного навчання для задач кібербезпеки. Традиційно розробка таких моделей вимагала глибоких знань у сфері науки про дані та значного часу на експерименти з різними алгоритмами. AutoML автоматизує цей процес, самостійно обираючи найкращі алгоритми, оптимізуючи параметри та створюючи інтерпретовані моделі, які можуть ефективно виявляти нетипову поведінку користувачів, підозрілі патерни доступу до даних та потенційні загрози безпеці.

Особливу цінність представляють вбудовані алгоритми виявлення аномалій, які поєднують статистичні методи з сучасними підходами машинного навчання. Ці алгоритми здатні аналізувати величезні обсяги логів і подій безпеки, виявляючи відхилення від нормальних патернів активності з точністю, недосяжною для традиційних методів [30]. Наприклад, система може автоматично розпізнати, що раптове збільшення кількості запитів до бази даних о третій годині ночі або доступ до конфіденційних документів з нетипової географічної локації можуть сигналізувати про потенційну загрозу.

Технологія Quick Insights використовує алгоритми ШІ для автоматичного виявлення цікавих та потенційно важливих патернів у даних безпеки [31]. Замість того, щоб аналітики витрачали години на пошук аномалій у журналах подій, система автоматично сканує дані, виявляє кореляції та генерує візуалізації, які можуть вказувати на приховані загрози або тенденції. Це особливо корисно при аналізі складних багатовимірних даних, де людський аналіз може пропустити важливі зв'язки між різними типами подій.

Обробка природної мови та Q&A функціональність. Одним із найбільш інноваційних напрямків розвитку Power BI є інтеграція технологій обробки природної мови, що революційно спрощує взаємодію з даними безпеки. Функціональність запитань та відповідей (Q&A) дозволяє аналітикам і керівникам формулювати складні запити звичайною мовою, без необхідності вивчення спеціальних мов запитів або створення складних фільтрів [32].

Уявімо ситуацію, коли керівник служби безпеки хоче негайно отримати інформацію про всі спроби несанкціонованого доступу до фінансових даних за останні три дні з деталізацією по годинах. Замість того, щоб звертатися до технічного фахівця для створення відповідного звіту, він може просто ввести це запитання в Power BI, і система автоматично згенерує необхідну візуалізацію. Технології обробки природної мови розуміють контекст запиту, ідентифікують релевантні набори даних та створюють відповідні графіки або таблиці.

Ця функціональність особливо корисна для нетехнічних користувачів, які потребують швидкого доступу до інформації безпеки, але не мають глибоких знань у сфері аналітики даних. Керівники можуть формулювати запити про користувачів, які працювали з базою даних у вихідні дні, або географічне розподілення IP-адрес, з яких здійснювалися спроби входу за конкретний період часу, отримуючи миттєві відповіді у зручному для сприйняття форматі.

Аналітика у режимі реального часу та потокові дані. У сфері кібербезпеки критично важливим є здатність системи обробляти й аналізувати дані в режимі реального часу. Power BI забезпечує цю можливість через глибоку інтеграцію з Azure Stream Analytics та Event Hubs, створюючи потужну платформу для аналізу потокових даних безпеки [33]. Ця технологія дозволяє обробляти мільйони подій безпеки на секунду та миттєво відображати результати аналізу на дашбордах.

Потокові набори даних забезпечують безперервне оновлення візуалізацій при надходженні нових даних про події безпеки, що критично важливо для операційних центрів безпеки. Уявімо інформаційну панель, яка відображає поточну активність у мережі організації: усі спроби входу й отримання доступу

до конфіденційних файлів, усі випадки аномальної мережевої активності, які миттєво відображаються та аналізуються. Це дозволяє створювати системи раннього попередження, які можуть автоматично сповіщати відповідальних осіб про критичні інциденти в момент їх виникнення.

Активні набори даних (Push datasets) надають можливість програмно надсилати дані до Power BI через REST API, що відкриває широкі можливості для інтеграції з власними системами моніторингу безпеки та SIEM-рішеннями [34]. Організації можуть розробляти спеціалізовані агенти, які збирають дані з різних джерел безпеки і в режимі реального часу передають їх до Power BI для аналізу та візуалізації.

Розширена аналітика з R та Python. Для організацій зі специфічними потребами в аналізі даних безпеки Power BI пропонує можливості інтеграції з мовами програмування R та Python [35]. Ця інтеграція відкриває доступ до величезної екосистеми спеціалізованих бібліотек і алгоритмів, які можуть вирішувати найскладніші завдання кібербезпеки.

Аналітики можуть використовувати потужні статистичні пакети R для глибокого аналізу журналів безпеки, виявлення прихованих кореляцій і патернів, які неможливо виявити стандартними засобами. Python з його багатими бібліотеками машинного навчання дозволяє створювати власні алгоритми виявлення аномалій, кластеризації подій для ідентифікації патернів атак і аналізу мережевого трафіку методами глибокого навчання.

Особливо цінною є можливість виконання R та Python скриптів як на етапі підготовки даних в Power Query, так і при створенні візуалізацій. Це забезпечує неймовірну гнучкість у реалізації складних аналітичних сценаріїв, дозволяючи організаціям адаптувати Power BI до своїх унікальних потреб у сфері кібербезпеки.

Когнітивні сервіси та аналіз неструктурованих даних. Традиційні системи аналізу безпеки зосереджуються переважно на структурованих даних: логах, метриках, числових показниках. Однак значна частина цінної інформації про потенційні загрози міститься в неструктурованих даних: текстових логах, повідомленнях електронної пошти, документах, коментарях користувачів [36].

Інтеграція Power BI з сервісом виявлення аномалій Azure Cognitive Services дозволяє аналізувати ці неструктуровані дані, витягуючи з них цінну інформацію для забезпечення безпеки. Сервіси аналізу тональності можуть автоматично аналізувати внутрішню корпоративну комунікацію для виявлення потенційних ознак незадоволення співробітників, що може сигналізувати про ризик інсайдерських загроз. Технології розпізнавання елементів допомагають автоматично ідентифікувати IP-адреси, доменні імена, хеші файлів та інші індикатори компрометації в текстових логах, значно прискорюючи процеси аналізу та реагування на інциденти.

Azure Cognitive Services може аналізувати часові ряди даних безпеки й автоматично виявляти відхилення, які можуть свідчити про кібератаки або технічні проблеми [37]. Ця технологія особливо ефективна для виявлення повільних або дуже тонких атак, які можуть залишатися непоміченими традиційними методами аналізу.

На рисунку 3.2 показано схему інтеграційного потоку даних між різними компонентами Power BI та зовнішніми системами, яка демонструє процеси збору, обробки та аналізу інформації з використанням технологій штучного інтелекту та когнітивних сервісів для забезпечення кібербезпеки СУВД.

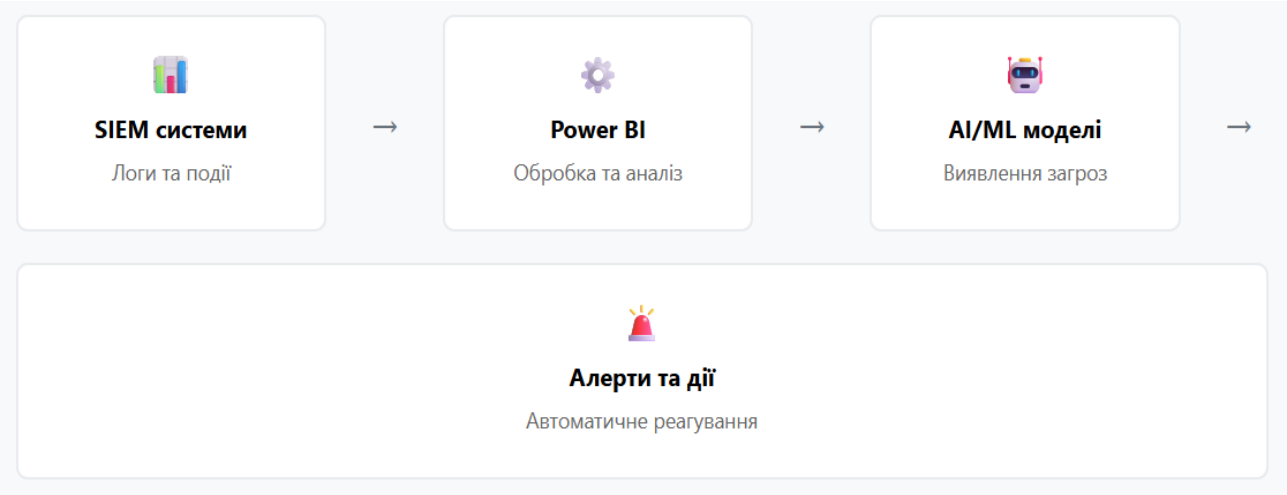

Рис. 3.2. Інтеграційний потік даних

3.2 Виклики впровадження та шляхи оптимізації Power BI

Впровадження Power BI для забезпечення кібербезпеки в СУВД, незважаючи на очевидні переваги та інноваційні можливості, супроводжується рядом серйозних викликів (Рис. 3.3). Розуміння цих викликів і наявність чітких стратегій їх подолання є критично важливими для успішної реалізації проектів цифрової трансформації у сфері кібербезпеки.

Рис. 3.3. Виклики впровадження Power BI

Стратегічні виклики планування та впровадження. Одним із найбільших викликів при впровадженні Power BI для кібербезпеки є правильне стратегічне планування та поетапний підхід до реалізації проекту [38]. Багато організацій припускаються помилки, намагаючись одразу охопити всі аспекти кібербезпеки або впровадити рішення в усіх підрозділах одночасно. Такий підхід часто призводить до перевантаження ресурсів, зниження якості впровадження та опору з боку користувачів.

Ефективна стратегія впровадження повинна базуватися на принципі "безпеки за замовчуванням", коли всі звіти й дашборди безпеки створюються з мінімальними правами доступу з подальшим поступовим розширенням повноважень відповідно до потреб користувачів. Цей підхід допомагає уникнути потенційних витоків даних на початкових етапах впровадження, коли процеси ще не налагоджені, а персонал не має достатнього досвіду роботи з новою системою.

Критично важливим є документування всіх процесів, рішень та конфігурацій для забезпечення відтворюваності й можливості проведення аудиту [39]. Кожна зміна в налаштуваннях безпеки повинна фіксуватися та затверджуватися відповідно до корпоративних процедур, що особливо важливо в регульованих галузях, де дотримання відповідних вимог є обов'язковим.

Організаційні виклики та культурні бар'єри. Найскладнішим аспектом впровадження Power BI для кібербезпеки часто виявляється не технічна складність, а людський фактор. Фахівці з кібербезпеки традиційно звикли до спеціалізованих SIEM-рішень і можуть скептично ставитися до використання платформи бізнес-аналітики для критичних завдань безпеки [40]. Ця недовіра може бути підсилена попереднім негативним досвідом використання недостатньо захищених аналітичних інструментів або побоюваннями щодо надійності й безпеки хмарних рішень.

Подолання цього опору вимагає комплексного підходу до управління змінами, який включає не лише технічне навчання, але й демонстрацію конкретних переваг Power BI через практичні приклади та успішні кейси. Важливо залучати ключових фахівців до процесу впровадження з самого початку, роблячи їх співучасниками змін, а не пасивними реципієнтами нових технологій.

Створення центру компетенцій стає критично важливим елементом успішного впровадження Power BI [41]. Такий центр повинен об'єднувати представників IT-департаменту, команди кібербезпеки та бізнес-користувачів, забезпечуючи міждисциплінарний підхід до подолання викликів. Центр компетенцій відповідає за розробку стандартів використання платформи, створення шаблонів звітів, проведення навчання та надання технічної підтримки користувачам.

Технічні виклики масштабування та продуктивності. При роботі з великими обсягами даних безпеки організації неминуче стикаються з технічними обмеженнями Power BI, які можуть значно вплинути на ефективність рішення. Імпортовані набори даних мають жорсткі ліміти розміру - 1 ГБ для стандартних

ліцензій і 10 ГБ для преміум-ємностей [42]. Для систем, що генерують терабайти логів щомісячно, ці обмеження можуть стати серйозною перешкодою для повноцінного використання всіх можливостей платформи.

Вирішення проблем масштабування вимагає глибокого розуміння архітектурних можливостей Power BI та стратегічного підходу до організації даних. Режим DirectQuery дозволяє працювати з великими наборами даних без необхідності їх імпортування, але за рахунок потенційного зниження швидкості запитів [43]. Композитні моделі надають можливість поєднувати переваги обох підходів, зберігаючи критично важливі дані локально для швидкого доступу та використовуючи DirectQuery для менш критичної інформації.

Інкрементне оновлення стає життєво необхідним інструментом для оптимізації процесів завантаження великих обсягів даних. Замість повторного завантаження всього набору даних система оновлює лише нові або змінені записи, що значно скорочує час оновлення та знижує навантаження на системи-джерела інформації.

Виклики інтеграції з існуючими системами. Практичний досвід впровадження Power BI у корпоративних середовищах часто виявляє, що інтеграція з існуючими системами безпеки значно складніша за початкові очікування. Застарілі SIEM-системи можуть не мати сучасних API для інтеграції, що змушує організації розробляти проміжні рішення або покладатися на менш ефективні методи експорту файлів.

Особливу проблему створює гетерогенність систем безпеки, де різні продукти використовують власні формати даних, схеми класифікації подій та рівні деталізації інформації. Створення єдиного консолідованого представлення вимагає значних зусиль з нормалізації даних, розробки правил трансформації та підтримки відповідностей між різними системами класифікації.

Потоки даних Power BI стають потужним інструментом для вирішення цих викликів, дозволяючи створювати централізовані процеси ETL, які можуть обробляти дані з різних джерел та приводити їх до єдиного стандартизованого формату [44]. Dataflows забезпечують можливість створення універсальних

компонентів трансформації даних, що значно спрощує підтримку та розвиток системи в довгостроковій перспективі.

Виклики управління життєвим циклом контенту. З часом, коли кількість звітів і дашбордів зростає, організації стикаються з новими викликами управління аналітичним контентом. Без належних процесів управління може виникнути хаос дублювання звітів, застарілої інформації та плутанини щодо актуальних версій документів [45]. Особливо критичною ця проблема стає у сфері кібербезпеки, де використання застарілої або некоректної інформації може призвести до серйозних наслідків.

Ефективне управління життєвим циклом контенту вимагає впровадження систематичних процесів версіонування звітів, регулярного аудиту використання, своєчасного архівування застарілого контенту і підтримки актуальної документації. API адміністрування Power BI надає потужні можливості для автоматизації багатьох з цих процесів [46], дозволяючи створювати скрипти для моніторингу використання звітів, автоматичного виявлення дублікатів та управління правами доступу.

Особливу увагу слід приділити створенню процесів ранжування і класифікації контенту, які допомагають користувачам швидко ідентифікувати найбільш релевантні та актуальні звіти. Система тегування та категоризації полегшує пошук необхідної інформації та знижує ризик використання застарілих або некоректних даних.

На рисунку 3.4 показано схему поетапного впровадження функціоналу Power BI для забезпечення кібербезпеки СУВД, яка ілюструє ключові етапи планування, розгортання та оптимізації системи, включаючи процеси навчання

персоналу, інтеграції з існуючими системами та налаштування процедур управління життєвим циклом контенту.

Рис. 3.4. Схема для впровадження функціоналу Power BI

3.3 Рекомендації щодо використання інструментів Power BI для забезпечення кібербезпеки СУВД

Створення ефективної системи кібербезпеки на базі Power BI для СУВД вимагає стратегічного підходу, який враховує як технічні можливості платформи, так і організаційні особливості конкретного підприємства. Рекомендації, представлені в цьому розділі (Рис. 3.5), базуються на аналізі кращих світових практик, офіційних рекомендаціях Microsoft та практичному досвіді впровадження подібних рішень у різних галузях економіки.

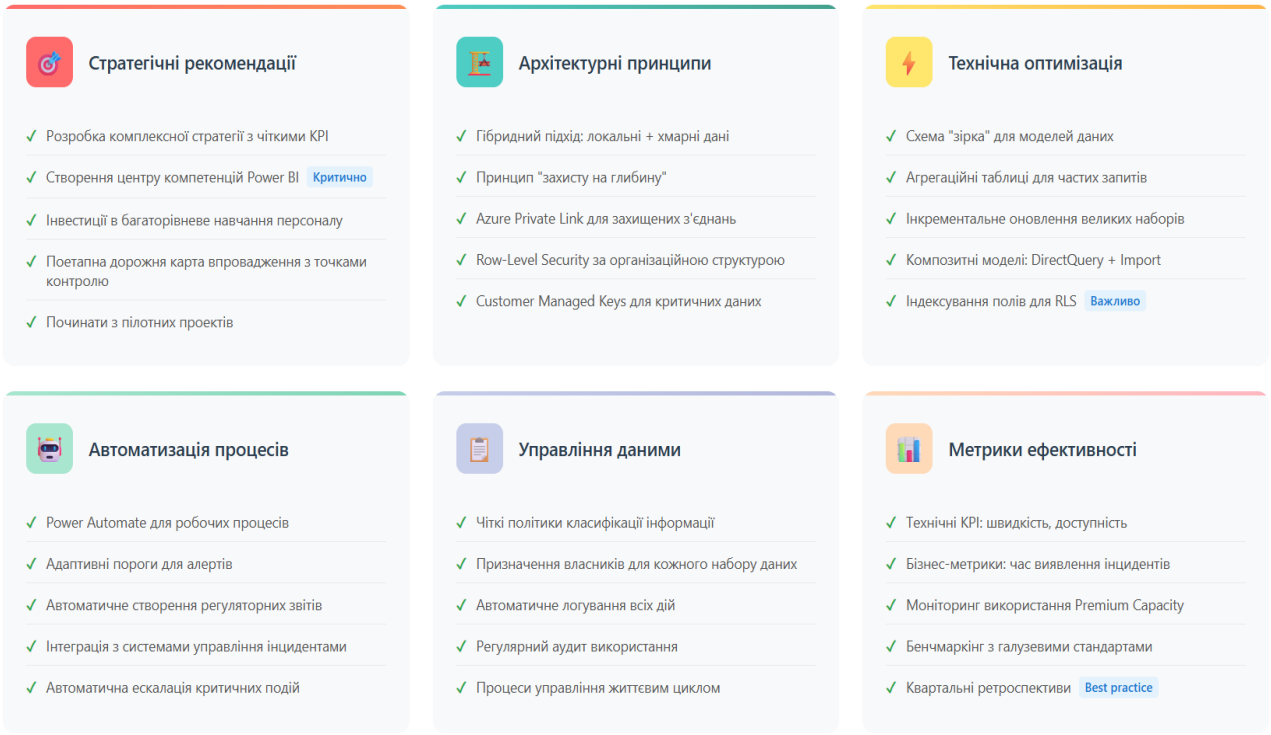

Рис. 3.5. Комплексні рекомендації щодо використання Power BI для кібербезпеки СУВД

Стратегічні рекомендації для організацій. Фундаментом успішного впровадження Power BI для кібербезпеки є розробка комплексної стратегії, яка чітко визначає цілі, очікувані результати та ключові показники ефективності проекту. Організації повинні почати з ретельного аналізу поточного стану своїх систем безпеки, ідентифікації найбільш критичних прогалин і визначення пріоритетних напрямків для впровадження аналітичних рішень.

Ключовим елементом стратегії має стати створення центру компетенцій Power BI, який об'єднає фахівців різних спеціальностей і забезпечить міждисциплінарний підхід до розвитку аналітичних можливостей [47]. Центр компетенцій повинен включати не лише IT-спеціалістів та аналітиків даних, але й представників бізнес-підрозділів, юридичного департаменту і служби кібербезпеки. Така команда зможе забезпечити всебічний підхід до впровадження, враховуючи як технічні аспекти, так і бізнес-потреби організації.

Інвестиції в навчання персоналу повинні розглядатися як критично важлива складова успіху проекту, а не як додаткові витрати [48]. Програма навчання має бути багаторівневою, включаючи базові курси для всіх

користувачів системи, поглиблені програми для аналітиків даних і спеціалізовані тренінги для адміністраторів системи. Особливу увагу слід приділити навчанню принципам безпечної роботи з даними, дотримання політик конфіденційності та розуміння регуляторних вимог.

Організації повинні розробити чітку дорожню карту впровадження, яка передбачає поетапний підхід з регулярними точкам контролю та оцінки результатів. Рекомендується починати з пілотних проектів на обмежених наборах даних або в окремих підрозділах, поступово розширюючи масштаб впровадження після отримання позитивних результатів та накопичення досвіду.

На рисунку 3.6 показано рівні зрілості впровадження Power BI для забезпечення кібербезпеки, які демонструють еволюцію організації від початкового використання базових функцій візуалізації до повноцінної інтегрованої системи моніторингу безпеки з автоматизованими процесами реагування та прогнозованою аналітикою.

Рис. 3.6. Рівні зрілості впровадження Power BI

Архітектурні рекомендації та принципи безпеки. Проектування архітектури Power BI для систем кібербезпеки має базуватися на принципі гібридного підходу, який забезпечує оптимальний баланс між продуктивністю, безпекою та дотриманням регуляторних вимог [49]. Найбільш чутливі та критично важливі дані рекомендується зберігати в локальних системах з використанням локального шлюза даних, тоді як агреговані та знеособлені дані можуть розміщуватися в хмарному середовищі для покращення продуктивності аналітичних процесів.

Архітектура безпеки повинна реалізовувати принцип поглибленого захисту через впровадження багаторівневої системи захисту [50]. На мережевому рівні настійно рекомендується використання Azure Private Link для

забезпечення приватного, захищеного з'єднання з Power BI Service, що мінімізує ризики перехоплення даних під час передачі. На рівні даних необхідно впровадити комплексне шифрування як для даних у спокої, так і під час передачі, з використанням ключів, керованих клієнтом, для найбільш критичної інформації.

Система безпеки на рівні рядків повинна точно відображати організаційну структуру підприємства та принципи розподілу обов'язків у сфері кібербезпеки [51]. Рекомендується створити ієрархічну модель безпеки, яка дозволяє керівникам різних рівнів бачити агреговані дані своїх підрозділів, тоді як рядові працівники мають доступ лише до інформації, необхідної для виконання їх безпосередніх обов'язків. Така модель забезпечує дотримання принципу мінімальних привілеїв та знижує ризики випадкового або навмисного витоку конфіденційної інформації.

На рисунку 3.7 показано архітектуру ієрархічної моделі безпеки Power BI, яка ілюструє принципи розподілу прав доступу відповідно до організаційної структури, механізми контролю на рівні рядків та забезпечення дотримання принципу мінімальних привілеїв для різних категорій користувачів.

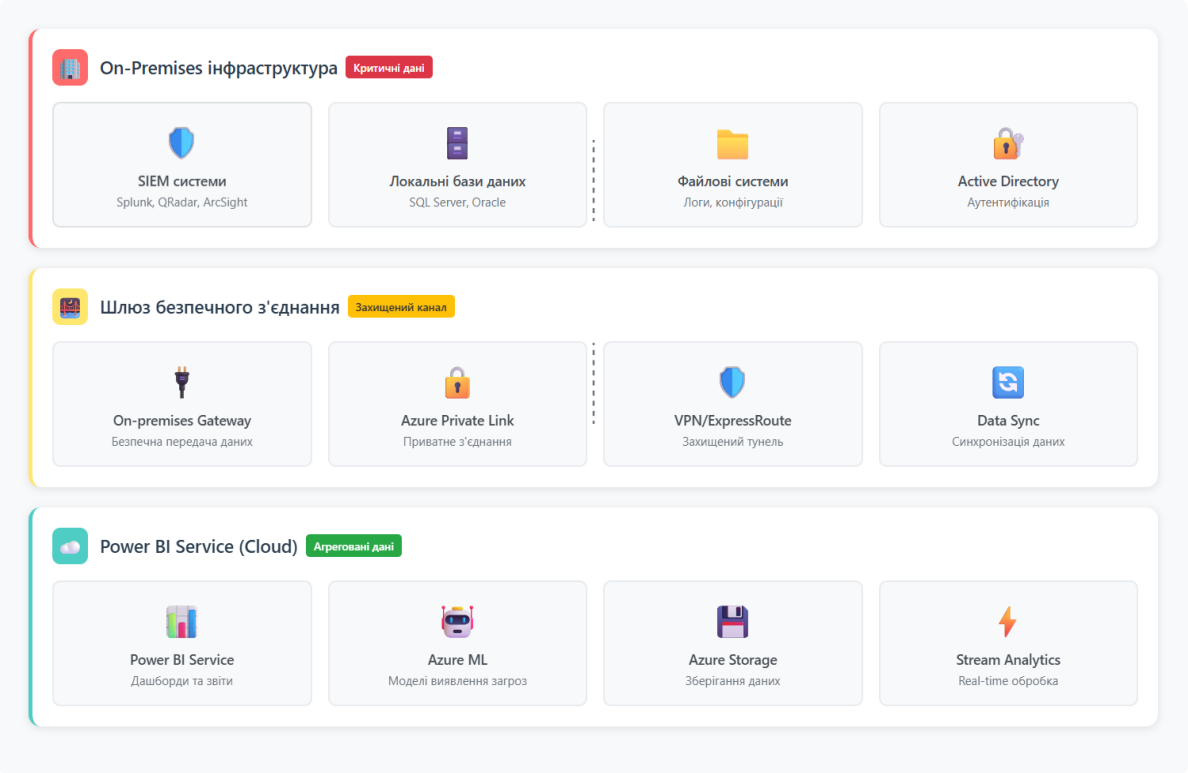

Рис. 3.7. Архітектура ієрархічної моделі безпеки Power BI

Технічні рекомендації для оптимізації продуктивності. Забезпечення високої продуктивності Power BI при роботі з великими обсягами даних безпеки вимагає ретельної оптимізації моделей даних і архітектури системи. Рекомендується використовувати схему "зірка" для організації даних, що забезпечує оптимальну продуктивність запитів і спрощує розуміння структури даних для кінцевих користувачів.

Створення агрегаційних таблиць для часто запитуваних метрик може значно прискорити роботу дашбордів та звітів. Наприклад, замість того, щоб щоразу обчислювати кількість інцидентів безпеки за тиждень на основі детальних записів, краще створити попередньо обчислену таблицю з тижневими агрегатами. Це особливо важливо для історичних даних, які рідко змінюються.

Інкрементне оновлення стає життєво необхідним для великих наборів даних, дозволяючи оновлювати лише нові або змінені записи замість повторного завантаження всього набору даних. Це не лише скорочує час оновлення, але й знижує навантаження на системи-джерела та зменшує витрати на використання обчислювальних ресурсів.

Для систем, що потребують аналізу даних в реальному часі, рекомендується використовувати комбінацію DirectQuery для актуальних даних з імпортованими агрегаціями для історичної інформації [52]. Такий гібридний підхід забезпечує баланс між актуальністю інформації та швидкодією системи. Особливу увагу слід приділити індексуванню полів, які використовуються для фільтрації в системі безпеки на рівні рядків, оскільки неоптимізовані індекси можуть значно сповільнити роботу системи.

Рекомендації щодо автоматизації та інтеграції. Автоматизація процесів моніторингу та реагування на події безпеки є ключовим фактором ефективності сучасних систем кібербезпеки [53]. Платформа автоматизації Power Automate може використовуватися для створення складних робочих процесів, які автоматично реагують на критичні події безпеки, виявлені в Power BI дашбордах. Наприклад, при виявленні аномальної активності система може автоматично

створити тікет в системі управління інцидентами, надіслати сповіщення відповідальним особам та ініціювати процедури початкового реагування.

Налаштування повідомлень при виявленні аномалій повинно бути точно відкаліброваним, щоб уникнути як хибних спрацьовувань, які можуть призвести до "втоми від сповіщень", так і пропуску справжніх загроз. Рекомендується використовувати адаптивні пороги, які враховують історичні дані та сезонні коливання активності.

Автоматичне генерування звітів для регуляторних органів може значно спростити дотримання вимог відповідності. Система може бути налаштована на автоматичне створення стандартизованих звітів про інциденти безпеки, які відповідають вимогам релевантних регуляторних стандартів, таких як GDPR, HIPAA або PCI DSS.

Управління даними. Розробка комплексних політик управління даними є фундаментальною вимогою для забезпечення довгострокового успіху системи кібербезпеки на базі Power BI. Ці політики мають містити чіткі правила класифікації інформації, процедури надання та відкликання доступу, а також процеси управління життєвим циклом даних від їх створення до остаточного видалення.

Для кожного набору даних має бути визначено особу, відповідальну за його актуальність, якість та безпеку. Відповідальний за дані повинен регулярно переглядати права доступу, оновлювати документацію і забезпечувати відповідність даних встановленим стандартам якості. Це особливо важливо для динамічних середовищ, де структура даних і бізнес-процеси часто змінюються.

Система аудиту та моніторингу використання повинна відстежувати всі дії користувачів з даними безпеки [54] Рекомендується налаштувати автоматичне логування доступу до звітів, експорту даних, змін у правах доступу та інших критичних операцій. Ці журнали повинні регулярно аналізуватися для виявлення потенційних порушень безпеки або нетипових патернів використання.

Метрики ефективності та безперервне покращення. Створення системи ключових показників ефективності (KPI) є критично важливим для об'єктивної

оцінки успішності впровадження Power BI для кібербезпеки [55]. Система метрик повинна включати як технічні показники (середній час відповіді на запити, доступність системи, кількість оброблених подій), так і бізнес-метрики (зменшення часу виявлення інцидентів, скорочення витрат на підготовку звітів, підвищення задоволеності користувачів).

Регулярний моніторинг використання ресурсів допомагає оптимізувати витрати і планувати майбутнє масштабування системи. Метрики преміум-ємностей Power BI надають детальну інформацію про використання обчислювальних ресурсів, що дозволяє ідентифікувати потреби в оптимізації або в розширенні ємності задовго до виникнення проблем з продуктивністю.

Бенчмаркінг порівняно з галузевими стандартами та кращими практиками допомагає організаціям оцінити ефективність своїх рішень та ідентифікувати можливості для покращення. Регулярне порівняння власних показників з галузевими еталонами дозволяє своєчасно виявляти відставання та коригувати стратегії розвитку.

Впровадження культури безперервного покращення передбачає регулярний перегляд та оптимізацію всіх аспектів системи - від технічної архітектури до процесів використання. Рекомендується проводити квартальні ретроспективи з ключовими стейкхолдерами для обговорення досягнутих результатів, виявлених проблем і планів розвитку на наступний період.

Висновки до розділу 3

Дослідження показало, що технологія Power BI успішно інтегрує у свою платформу інноваційні технології штучного інтелекту й машинного навчання, з якими нерозривно пов'язане майбутнє кібербезпеки. Аналіз сучасних можливостей показав, що організації можуть значно підвищити ефективність своїх систем безпеки через використання автоматизованого виявлення аномалій, обробки природної мови для спрощення взаємодії з даними й аналітики у режимі реального часу для миттєвого реагування на загрози.

Встановлено, що наявні технічні обмеження платформи можуть бути успішно подолані шляхом правильного архітектурного планування і використання гібридних підходів до організації даних. Більш серйозними є організаційні виклики, пов'язані з культурною адаптацією та необхідністю зміни усталених процесів роботи команд кібербезпеки. Важливим завданням є створення центрів компетенцій, впровадження поетапного підходу до розгортання та налаштування ефективних СУВД.

Результати дослідження підтверджують, що Power BI має значний потенціал для трансформації традиційних підходів до кібербезпеки, особливо в контексті СУВД. Платформа дозволяє організаціям переходити від реактивних до проактивних стратегій захисту, забезпечуючи можливості прогнозування загроз та автоматизації процесів реагування.

Перспективи подальшого розвитку пов'язані з поглибленням інтеграції технологій ШІ, розширенням можливостей аналізу неструктурованих даних і створенням галузевих рішень для специфічних секторів економіки. Power BI має всі передумови для того, щоб стати центральною платформою для операційних центрів безпеки нового покоління, які будуть характеризуватися високим рівнем автоматизації, інтелектуальної аналітики та проактивного реагування на загрози.

ВИСНОВКИ

У ході дослідження встановлено, що сучасна платформа бізнес-аналітики Power BI може ефективно використовуватися не лише для аналізу бізнес-даних, але й як інструмент забезпечення кібербезпеки в СУВД. Її архітектура дозволяє працювати з різними джерелами інформації, включно з великими обсягами потокових і збережених даних, а також забезпечує гнучкість при інтеграції в локальні та хмарні середовища.

З'ясовано, що важливою перевагою Power BI є її здатність підтримувати багаторівневу систему безпеки, що відповідає концепції поглибленого захисту. До ключових механізмів безпеки належать автентифікація на базі Azure Active Directory, підтримка багатофакторної автентифікації, умовного доступу та рольової моделі, шифрування даних із використанням алгоритмів AES-256, а також аудит усіх дій користувачів. Дослідження показало, що з розвитком технологій ВД змінюється і характер загроз, які стають більш цілеспрямованими та складними. Особливу небезпеку становлять загрози, що використовують ШІ та машинне навчання для обходу систем захисту та цільового збору конфіденційної інформації.

Встановлено, що системи управління великими даними мають багаторівневу архітектуру, де кожен рівень має свої специфічні вразливості та вимоги до безпеки. Ефективний захист повинен охоплювати всі компоненти від збору та зберігання до аналізу та візуалізації даних.

Аналіз статистики засвідчив щорічне зростання кількості та складності кіберінцидентів у сфері великих даних, з особливим акцентом на атаки, спрямовані на викрадення даних та компрометацію аналітичних систем. Основними цілями для кібератак часто стають системи бізнес-аналітики, такі як Power BI, оскільки вони надають доступ до агрегованих і структурованих даних. Захист цих систем потребує особливої уваги в контексті загальної стратегії кібербезпеки.

Як відзначено в роботі, забезпечення безпеки ВД вимагає інтеграції технологічних рішень, організаційних заходів і регуляторних практик. Ізольовані підходи до безпеки не здатні забезпечити належний рівень захисту в умовах складних розподілених архітектур. Традиційні методи забезпечення безпеки потребують адаптації для роботи з великими обсягами даних та високою швидкістю їх обробки. Це стимулює розвиток нових підходів, таких як аналітика безпеки на основі машинного навчання та потокова обробка подій безпеки.

Таким чином, забезпечення кібербезпеки в СУВД є комплексним завданням, що вимагає системного підходу, інтеграції різних технологій захисту та постійної адаптації до нових викликів.

Окрему увагу приділено аналітичним можливостям платформи для моніторингу подій безпеки. Досліджено, що Power BI дозволяє створювати дашборди, які відображають реальний стан безпеки, виявляють аномалії, відстежують підозрілу активність та надають можливості для ретроспективного аналізу кіберінцидентів. Інструменти візуалізації, такі як теплові карти, шкальні діаграми та каскадні графіки, суттєво підвищують ефективність сприйняття інформації, особливо у критичних ситуаціях.

Результати аналізу підтверджують, що Power BI може бути ефективно інтегрована з SIEM-системами, такими як Microsoft Sentinel або Splunk, що значно розширює її функціонал у сфері кіберзахисту. Така інтеграція забезпечує глибоку кореляцію подій, підтримку автоматизованих сценаріїв реагування та формування звітності для різних цільових аудиторій – від технічних фахівців до керівництва й регуляторів.

Дослідження показало, що технологія Power BI успішно інтегрує у свою платформу інноваційні технології штучного інтелекту й машинного навчання, з якими нерозривно пов'язане майбутнє кібербезпеки. Аналіз сучасних можливостей показав, що організації можуть значно підвищити ефективність своїх систем безпеки через використання автоматизованого виявлення аномалій, обробки природної мови для спрощення взаємодії з даними й аналітики у режимі реального часу для миттєвого реагування на загрози.

Встановлено, що наявні технічні обмеження платформи можуть бути успішно подолані шляхом правильного архітектурного планування і використання гібридних підходів до організації даних. Більш серйозними є організаційні виклики, пов'язані з культурною адаптацією та необхідністю зміни усталених процесів роботи команд кібербезпеки. Важливим завданням є створення центрів компетенцій, впровадження поетапного підходу до розгортання та налаштування ефективних СУВД.

Результати дослідження підтверджують, що Power BI має значний потенціал для трансформації традиційних підходів до кібербезпеки, особливо в контексті СУВД. Платформа дозволяє організаціям переходити від реактивних до проактивних стратегій захисту, забезпечуючи можливості прогнозування загроз та автоматизації процесів реагування.

Перспективи подальшого розвитку пов'язані з поглибленням інтеграції технологій ШІ, розширенням можливостей аналізу неструктурованих даних і створенням галузевих рішень для специфічних секторів економіки. Power BI має всі передумови для того, щоб стати центральною платформою для операційних центрів безпеки нового покоління, які будуть характеризуватися високим рівнем автоматизації, інтелектуальної аналітики та проактивного реагування на загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Big Data (великі дані): що, навіщо і як? URL: https://surl.li/afplsr

2. Архітектурні моделі Big Data. Технології віртуалізації. Гіпервізори. Контейнерна технологія виконання програмного коду на сервері. SaaS, PaaS і IaaS. URL: https://surli.cc/vilpmk

3. Power BI Security Whitepaper. Microsoft Documentation, *Microsoft*. 2023. URL: https://learn.microsoft.com/en-us/power-bi/guidance/whitepaper-powerbi-security

4. IBM 2024 Data Breach Investigations Report (DBIR). *IBM*. URL: https://www.ibm.com/security/data-breach

5. Demchenko Y., Ngo C., Membrey P. Architecture Framework and Components for Big Data Ecosystem. *Journal of Big Data*. 2022. URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00592-5

6. IBM Security. X-Force Threat Intelligence Index. *IBM*. URL: https://www.ibm.com/security/data-breach/threat-intelligence

7. Synopsys. Open Source Security and Risk Analysis Report. *Synopsys*. 2023. URL: https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

8. Verizon Insider Threat Report. *Verizon*. 2025. URL: https://www.verizon.com/business/resources/T7e2/reports/insider-threat-report.pdf

9. NIST. Framework for Improving Critical Infrastructure Cybersecurity. *NIST*. 2023. URL: https://www.nist.gov/cyberframework

10. MITRE. MITRE ATT&CK Framework for Enterprise. *MITRE Corporation*. 2023. URL: https://attack.mitre.org/

11. Power BI documentation. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/

12. BI Tool Comparison for the Best Analytics Tool Fit. *Analytics8.* URL: https://www.analytics8.com/blog/bi-tool-comparison-choosing-the-best-analytics-tool-for-business/

13. What is Power BI? Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/fundamentals/power-bi-overview

14. Get started with Power BI Desktop. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/fundamentals/desktop-getting-started

15. Power BI Premium whitepaper. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/whitepaper-powerbi-premium-deployment

16. Build Power BI visuals and reports - Training. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/training/paths/build-power-bi-visuals-reports/

17. NIST Cybersecurity Framework. *NIST.* URL: https://www.nist.gov/cyberframework

18. Power BI security whitepaper. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/whitepaper-powerbi-security

19. Azure Active Directory documentation. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/azure/active-directory/

20. Azure Key Vault documentation. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/azure/key-vault/

21. Microsoft 365 Defender documentation. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/microsoft-365/security/defender/

22. Model data in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/transform-model/

23. Learn DAX basics in Power BI Desktop. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/transform-model/desktop-quickstart-learn-dax-basics

24. What is Digital Forensics? Key Phases in Cybersecurity. *EC-Council.* URL: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/

25. Microsoft Fabric adoption roadmap: Governance. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/fabric-adoption-roadmap-governance

26. What Is SIEM? Microsoft Security. *Microsoft Corporation.* URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

27. Microsoft Sentinel documentation. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/azure/sentinel/

28. General Data Protection Regulation (GDPR). GDPR.eu. URL: https://gdpr.eu/

29. Azure Machine Learning integration with Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/transform-model/dataflows/dataflows-machine-learning-integration

30. Anomaly detection in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/visuals/power-bi-visualization-anomaly-detection

31. Quick Insights in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/consumer/end-user-insights

32. Q&A in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/natural-language/q-and-a-intro

33. Real-time streaming in Power BI. Microsoft Learn. *Microsoft Corporation*. URL: https://learn.microsoft.com/en-us/power-bi/connect-data/service-real-time-streaming

34. Push datasets in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/developer/embedded/push-datasets-limitations

35. R and Python scripts in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/connect-data/desktop-python-scripts

36. Azure Cognitive Services. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/azure/cognitive-services/

37. Anomaly Detector service. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/azure/cognitive-services/anomaly-detector/

38. Power BI implementation methodology. Microsoft Adoption Framework. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/powerbi-adoption-roadmap-overview

39. Power BI governance and deployment approaches. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/powerbi-adoption-roadmap-governance

40. Magic Quadrant for Analytics and Business Intelligence Platforms. *Gartner*. URL: https://www.gartner.com/en/documents/5519595

41. Center of Excellence for Power Microsoft Learn. BI. *Microsoft Corporation*. URL: https://learn.microsoft.com/en-us/power-bi/guidance/center-of-excellence-establish

42. Power BI Premium capacity planning. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/enterprise/service-premium-what-is

43. Composite models in Power BI. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/transform-model/desktop-composite-models

44. Performance analyzer in Power BI. Microsoft Learn. *Microsoft Corporation*. URL: https://learn.microsoft.com/en-us/power-bi/create-reports/desktop-performance-analyzer

45. Content lifecycle management. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/powerbi-adoption-roadmap-content-ownership-and-management

46. Power BI REST APIs. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/rest/api/power-bi/

47. Power BI governance framework. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/guidance/powerbi-adoption-roadmap-governance

48. Power BI training and certification. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/certifications/power-bi-data-analyst-associate/

49. On-premises data gateway. Microsoft Learn. *Microsoft Corporation. Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/connect-data/service-gateway-onprem

50. Azure Private Link for Power BI. Microsoft Learn. *Microsoft Corporation*. URL: https://learn.microsoft.com/en-us/power-bi/admin/service-security-private-links

51. Row-level security implementation. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/admin/service-admin-rls

52. DirectQuery optimization. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/connect-data/desktop-directquery-about

53. Power Automate integration. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-automate/get-started-logic-flow

54. Power BI audit logs. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/admin/service-admin-auditing

55. Premium capacity metrics. Microsoft Learn. *Microsoft Corporation.* URL: https://learn.microsoft.com/en-us/power-bi/admin/service-admin-premium-monitor-capacity