|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | |
|  |  | | | |  | | | |  | | |  |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | | | | | | |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
| Пояснювальна записка | | | | | | | | | | | | |
| до бакалаврської роботи | | | | | | | | | | | | |
|  | на тему: | | | | | | | | | | |  |
| **«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОСТУПУ ДО ХМАРНИХ СЕРВІСІВ НА БАЗІ РІШЕННЯ MCAFEE»** | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | | Виконав студент 4 курсу, групи БСД-43 | | | | | | | |
|  |  | | | | спеціальності 125 Кібербезпека | | | | | | | |
|  |  | | | | освітньо-професійної програми «Інформаційна та | | | | | | | |
|  |  | | | | кібернетична безпека» | | | | | | | |
|  |  | | | | (шифр і назва спеціальності) | | | | | | | |
|  |  | | | | Койчев Є.Г. | | | | | | | |
|  |  | | | | (прізвище та ініціали) | | | | | | | |
|  |  | | | | Керівник | | Бойко А.О. | | | | | |
|  |  | | | |  | | | | (прізвище та ініціали) | | | |
|  |  | | | | Рецензент | | |  | | | | |
|  |  | | | | (прізвище та ініціали) | | | | | | | |
|  |  | | | | Нормоконтролер | | | | | |  | |
|  |  | | | |  | | | | (прізвище та ініціали) | | | |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  | КИЇВ – 2023 | | | | | | | | | | |  |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | |
| Інститут | ННІЗІ | | | |  | | | |  | | |  |
| Кафедра | Інформаційної та кібернетичної безпеки | | | | | | | | | | | |
| Ступінь вищої освіти | | | Бакалавр | | | | | |  | | |  |
| Спеціальність | | 125 Кібербезпека | | | | | | |  | | |  |
| Освітньо-професійна програма | | | | | Інформаційна та кібернетична безпека | | | | | | | |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | | ЗАТВЕРДЖУЮ | | | |
|  |  | | | |  | | | | Завідувач кафедри ІКБ | | | |
|  |  | | | |  | | | |  | | | Гайдур Г.І. |
|  |  | | | |  | | | | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | | |
|  |  | | | |  | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
|  | **З А В Д А Н Н Я** | | | | | | | | | | |  |
|  | **НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ** | | | | | | | | | | |  |
|  |  | | | |  | | | |  | | |  |
| Койчеву Євгенію Геннадійовичу | | | | | | | | | | | | |
| (прізвище, ім’я, по батькові) | | | | | | | | | | | | |
| 1. Тема бакалаврської роботи: | | | | «Дослідження шляхів та розробка рекомендацій | | | | | | | | | |
| щодо забезпечення безпеки доступу до хмарних сервісів на базі рішення McAfee» | | | | | | | | | | | | |
| керівник бакалаврської роботи | | | | | Бойко Анна Олександрівна, асистент. | | | | | | | |
|  |  | | | | (прізвище, ім’я, по батькові, науковий ступінь, вчене звання) | | | | | | | |
| затверджені наказом закладу вищої освіти від «\_\_\_ » \_\_\_\_\_\_\_\_2023 року № \_\_\_\_. | | | | | | | | | | | | |
|  |  | | | |  | | | |  | | |  |
| 2. Строк подання студентом бакалаврської роботи | | | | | | | | | | 28.05.2021 р. | | |
|  |  | | | |  | | | |  | | |  |
| 3. Вихідні дані до бакалаврської роботи | | | | | |  | | | | | |  |
| хмарні сервіси; | | | | | | | | |  | | |  |
| рішення забезпечення безпечного доступу до хмарних сервісів від McAfee; | | | | | | | | | | | | |
| наукова та технічна література, експлуатаційна документація, нормативні | | | | | | | | | | | | |
| документи, міжнародні стандарти. | | | | | | | | |  | | |  |
|  |  | | | |  | | | |  | | |  |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | |
| 1. Актуальність проблеми забезпечення безпечного доступу до хмарних сервісів. | | | | | | | | | | | | |
| 2. Аналіз хмарних технологій та існуючі загрози. | | | | | | | | | | | | |
| 3. Методи та засоби забезпечення безпеки хмарних технологій за допомогою CASB. | | | | | | | | | | | | |
| 4. Рекомендації щодо забезпечення безпечного доступу в хмарі. | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Перелік графічного матеріалу | | | | |  | |  | |
| 1. Тема бакалаврської роботи. | | | | | | | | |
| 2. Об’єкт, предмет, мета та наукові завдання дослідження. | | | | | | | | |
| 3. Результати аналізу класифікації надання послуг хмарних сервісів та атак на хмари. | | | | | | | | |
| 4. Результати аналізу методів та засобів забезпечення безпеки хмарних сервісів.. | | | | | | | | |
| 5. Призначення та можливості рішення McAfee MVISION Cloud. | | | | | | | | |
| 6. Рекомендації щодо забезпечення безпечного доступу в хмарі.. | | | | | | | | |
| 7. Висновки за результатами роботи. | | | | | | | | |
|  | | | | | | | | |
| 6. Дата видачі завдання | | | 15.02.2023 р. | | | | | |
|  | |  | |  |  | |  | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | |  | |
|  | |  | |  |  | |  | |
| №  зп | Назва етапів  бакалаврської роботи | | | | | Строк виконання етапів бакалаврської роботи | | Примітка |
| 1. | Визначення актуальності проблеми забезпечення безпечного доступу до хмарних сервісів | | | | | 15.02.2023 р. | |  |
| 2. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | | | | | 22.02.2023 р. | |  |
| 3. | Аналіз методів та засобів забезпечення безпеки хмарних технологій. | | | | | 26.03.2023 р. | |  |
| 4. | Розроблення рекомендацій щодо застосування рішення McAfee для забезпечення безпеки хмарних сервісів. | | | | | 30.04.2023 р. | |  |
| 5. | Оформлення результатів дослідження. | | | | | 18.05.2023 р. | |  |
| 6. | Підготовка доповіді до захисту. | | | | | 28.05.2023 р. | |  |
|  | | | | | |  | |  |
|  | |  | | Студент | Койчев Є.Г. | | | |
|  | |  | |  | (підпис) | | прізвище та ініціали | |
|  | |  | |  |  | |  | |
| Керівник бакалаврської роботи | | | | |  | | Бойко А.О. | |
|  | |  | |  | (підпис) | | прізвище та ініціали | |
|  | |  | |  |  | |  | |

**ВІДГУК РЕЦЕНЗЕНТА**

на бакалаврську роботу

студентаКойчева Євгенія Геннадійовича

на тему: «Дослідження шляхів та розробка рекомендацій щодо забезпечення безпеки доступу до хмарних сервісів на базі рішення McAfee»

**Актуальність:** Сьогодні користувачі будь-якої із існуючих операційних систем постійно використовують хмарні технології. Робота присвячена одному з найперспективніших напрямків розвитку телекомунікацій – хмарним сервісам. Хмарні сервіси дозволяють зберігати дані в мережі і отримувати до них доступ з будь-якого пристрою. Сьогодні існує кілька моделей обслуговування та існуючих рішень, кожна з яких має свої переваги та недоліки, а також певну сферу застосування. Тому тема бакалаврської роботи є актуальною і своєчасною.

**Позитивні сторони:**

1. Зміст роботи відповідає завданню. Студент показав високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.

2. Обґрунтовано необхідність використання хмарних сервісів. Достатньо успішно викладено матеріали щодо моделей розгортання та забезпечення безпеки в хмарі.

3. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

**Недоліки:**

1. В роботі доцільно було б розглянути питання кібербезпеки щодо застосування хмарних обчислень в корпоративних мережах.
2. 2. Слід було провести аналіз додаткової технічної літератури по темі бакалаврської роботи.

**Висновок:** Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Койчев Є.Г.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

|  |  |  |
| --- | --- | --- |
| Якість роботи | | Підпис рецензента (\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  Підпис засвідчую  Підпис особи, що засвідчує (\_\_\_\_\_\_\_\_\_\_\_\_) |
| Виконано на замовлення підприємства |  |
| Виконано за тематикою НДР |  |
| Виконано з макетом |  |
| Виконано з застосуванням ЕОМ та МПТ | √ |
| Має практичну цінність | √ |
| Проект-частина комплексної теми |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | |
| **ПОДАННЯ**  **ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ** | | | | | | | | |
| Направляється студент | | Койчев Є.Г. | | | до захисту бакалаврської роботи | | | |
|  | | (прізвище та ініціали) | | |  | | | |
| спеціальності 125 Кібербезпека | | |  | | |  | |  |
| освітньо-професійної програми | | | Інформаційна та кібернетична безпека | | | | | |
|  |  | | (шифр і назва спеціальності) | | | | | |
| на тему: | «Дослідження шляхів та розробка рекомендацій щодо забезпечення | | | | | | | |
| безпеки доступу до хмарних сервісів на базі рішення McAfee». | | | | | | | | |
| Бакалаврська робота і рецензія додаються. | | | | | |  | |  |
| Директор інституту | | |  | | | Савченко В.А. | | |
| (підпис) (прізвище та ініціали) | | | | | | | | |
|  |  | |  | | |  | |  |
|  | **Довідка про успішність** | | | | | | |  |
| Койчев Є.Г. | | | за період навчання в інституті | | | | | |
| (прізвище та ініціали студента) | | |  | | |  | |  |
| ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:  національною шкалою: відмінно \_\_\_\_%, добре \_\_\_\_%, задовільно \_\_\_\_%;  шкалою ECTS: А \_\_\_\_%; В \_\_\_\_%; С \_\_\_\_%; D \_\_\_\_%; Е \_\_\_\_%. | | | | | | | | |
| Секретар інституту, факультету (відділення) | | | | | |  | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  | **Висновок керівника бакалаврської роботи** | | | | | | |  |
| Студент ***Койчев Є.Г.*** обрав тему роботи, метою якої було дослідження шляхів та розробка рекомендацій щодо забезпечення безпеки доступу до хмарних сервісів на базі рішення McAfee. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Койчев Є.Г. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану бакалаврську роботу студента Койчева Євгенія Геннадійовича на оцінку **«добре»** та присвоїти їй кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека. | | | | | | | | |
| Керівник бакалаврської роботи | | | | | |  | | Бойко А.О. |
|  |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  |  | |  | | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |
|  | **Висновок кафедри про бакалаврську роботу** | | | | | | |  |
| Бакалаврська робота розглянута. Студент | | | | Койчев Є.Г. | | | | |
|  |  | |  | (прізвище та ініціали) | | | | |
| допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії. | | | | | | | | |
| Завідувач кафедри Інформаційної та кібернетичної безпеки | | | | | | |  |  |
| (назва) | | | | | | | | | |
|  |  | |  | | |  | | Гайдур Г.І. |
|  |  | | (підпис) | | | (прізвище та ініціали) | | |
| “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |  | | |  | |  |
| **РЕФЕРАТ** | | | | | | | | |
|  |  | |  | | |  | |  |
|  |  | |  | | |  | |  |
| Текстова частина бакалаврської роботи: 49 сторінок, 6 рисунків, 12 джерел.  *Об’єкт дослідження* – процес забезпечення доступу до хмарних сервісів.  *Предмет дослідження* – методи та засоби забезпечення безпеки доступу до хмарних сервісів на базі рішення McAfee.  *Мета роботи* – аналіз існуючих загроз хмарних сервісів та розробка рекомендацій щодо захисту.  *Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.  В роботі приведено основні відомості хмарні сервіси.  Проаналізовано різні види загроз та наведено їх класифікацію.  Досліджено методи та засоби забезпечення безпеки хмарних сервісів на базі рішення CASB.  Досліджено можливості програмного комплексу McAfee MVISION Cloud.  Галузь використання – кібербезпека хмарних технологій.  ХМАРНІ СЕРВІСИ, ХМАРНІ ТЕХНОЛОГІЇ, ХМАРНІ ОБЧИСЛЕННЯ, БЕЗПЕКА, ЗАГРОЗА, ХМАРА. | | | | | | | | |
|  | | | | | | | | |

**ЗМІСТ**

Стор.

[**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ** 8](#_Toc73045638)

[**ВСТУП** 9](#_Toc73045639)

[**1 АНАЛІЗ СУЧАСНОГО СТАНУ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ЗЕБЗЕПЕЧЕННЯ БІЗНЕС ПРОЦЕСІВ** 11](#_Toc73045640)

[1.1. Використання хмарних сервісів в IT 11](#_Toc73045641)

[1.2. Класифікація сучасних хмарних сервісів 13](#_Toc73045642)

[1.3. Існуючі загрози хмарних обчислень 18](#_Toc73045643)

[1.4. Реалізація хмарних сервісів на основі CASB 21](#_Toc73045644)

[**2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ НА БАЗІ РІШЕННЯ CASB** 24](#_Toc73045645)

[2.1. Основні критерії для вибору CASB 24](#_Toc73045646)

[2.2. Визначення типових рішень для надання безпеки хмарних сервісів 26](#_Toc73045647)

[2.3. Огляд ринку CASB 28](#_Toc73045648)

[**3 РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ЗЕБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ НА БАЗІ РІШЕННЯ MCAFEE** 35](#_Toc73045649)

[3.1. Атаки на хмари і рекомендації щодо їх усунення 35](#_Toc73045650)

[3.2. Огляд рішення McAfee MVISION Cloud 37](#_Toc73045651)

[3.3. Основні характеристики та приклади використання McAfee MVISION Cloud 38](#_Toc73045652)

[**ВИСНОВКИ 51**](#_Toc73045653)

[**ПЕРЕЛІК ПОСИЛАНЬ 53**](#_Toc73045654)

[**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 55**](#_Toc73045655)

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SIEM – Security information and event management

ISV – Independent Software Vendor

VAR – Value at risk

ПЗ – Програмне забезпечення

VOIP – Voice over IP

ЦОД – Центр обробки даних

BYOD – Bring your own device

PCI DSS – Payment Card Industry Data Security Standard

DLP – Data Leak Prevention

UEBA – User and Entity Behavior Analytics

VPN – Virtual Private Network

SSO – Single Sign-On

NGFW – Next Generation Firewall

IPS – In Plane Switching

CSPM – Cloud Security Posture Management

SSPM – SaaS Security Posture Management

ZTNA – Zero Trust Network Access

# ВСТУП

Актуальність теми. Хмарні сервіси — новітній вид мережевих послуг, які дозволяють інформаційними засобами віртуального середовища розширити програмно-технічні ресурси комп’ютерного пристрою користувача. Поява хмарних сервісів стала можливою у процесі розвитку технологій хмарних обчислень (англ. Cloud Computing), які реалізуються за умов динамічного масштабного доступу до розподілених зовнішніх мережевих ресурсів. Надання такого доступу, як відокремлена послуга, залишається різновидом хмарних технологій.

Для реалізації використовують віртуальні машини, що функціонують у великих дата-центрах і замінюють собою фізичні персональні комп’ютери (ПК) та сервери. Головна відмінність від звичайного використання програмного забезпечення в хмарних сервісах полягає в тому, що користувач може поєднувати внутрішні ресурси свого комп’ютерного пристрою та програмні ресурси, які надаються йому як інтернет-сервіс. При цьому він має повний доступ до управління власними даними, але не може управляти операційною системою чи програмною базою, за допомогою яких ця робота відбувається.

Хмарні технології мають цілу низку переваг: користувач може задіяти віртуальний комп’ютер практично будь-якої конфігурації для виконання ресурсоємних завдань; може працювати в будь-якому місці за умов використання комп’ютерного пристрою, що має підключення до інтернету; користувач застрахований від збоїв у роботі пристрою і може за потреби ділитися результатами роботи з іншими користувачами. Для організацій перевагою використання є зниження витрат на обслуговування, підтримку, модернізацію та адміністрування комп’ютерного обладнання і програмного забезпечення.

Метою роботи є аналіз існуючих загроз хмарних сервісів та розробка рекомендацій щодо захисту.

Об’єкт дослідження – процес забезпечення доступу до хмарних сервісів.

Предмет дослідження – методи та засоби забезпечення безпеки доступу до хмарних сервісів на базі рішення McAfee.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є опрацювання новітніх технологій в галузі забезпечення безпеки хмарних сервісів.

Практичне значення одержаних результатів. Нові наукові результати, отримані в роботі, можуть бути використані при проектуванні та подальшому розгортанні системи захисту хмарних сервісів.

# 1 АНАЛІЗ СУЧАСНОГО СТАНУ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ЗАБЗЕПЕЧЕННЯ БІЗНЕС ПРОЦЕСІВ

## **Використання хмарних сервісів в IT**

З моменту зародження промисловості та торгівлі люди потребували дедалі кращих способів зберігання даних і доступу до них у разі потреби. Якщо в до комп’ютерну еру цінна інформація зберігалася фізично на папері, сьогодні дані переважно зберігаються на жорстких дисках комп’ютерів і серверів. Ці жорсткі диски та сервери можуть швидко та зручно зберігати, обробляти та отримувати значні обсяги даних. Однак як жорсткі диски, так і сервери мають свої обмеження, і враховуючи швидкість, з якою сьогоднішній бізнес і промисловість розвиваються, потреба в сховищах, які можуть зберігати й обробляти все більші обсяги даних, стає пріоритетом. Ось тут на допомогу прийшли хмарні обчислення.

До появи платформ Cloud Computing компанії переважно покладалися на сервери, бази даних, апаратне забезпечення, програмне забезпечення та інші периферійні пристрої, щоб вивести свій бізнес в Інтернет. Компанії були змушені купувати ці компоненти, щоб переконатися, що їхні веб-сайти чи програми досягли користувачів. Крім того, підприємствам також потрібна була команда експертів для керування апаратним і програмним забезпеченням, а також моніторингу інфраструктури. Хоча цей підхід був практичним, він мав свої унікальні проблеми, як-от висока вартість налаштування, складні компоненти та обмежений простір для зберігання тощо. Хмарні обчислення були створені для вирішення цих проблем. Давайте тепер зануримося в те, що таке хмарні обчислення, і зрозуміємо концепцію хмари.

Хмарні обчислення – це мережа віддалених серверів, розміщених в Інтернеті для зберігання та отримання даних. Хмара надає низку ІТ-сервісів, таких як сервери, бази даних, програмне забезпечення, віртуальне сховище та мережа, серед іншого. З точки зору неспеціаліста, хмарні обчислення визначаються як віртуальна платформа, яка дозволяє зберігати та отримувати доступ до ваших даних через Інтернет без будь-яких обмежень. Компанії, які пропонують усі згадані вище послуги, називаються хмарними провайдерами. Вони надають вам можливість зберігати та отримувати дані та запускати програми, керуючи ними через портали конфігурації. Два з найкращих хмарних провайдерів, доступних на сьогодні, — Amazon Web Services і Microsoft Azure.

Переваги хмарних обчислень

Сьогодні хмарні платформи пропонують деякі вагомі переваги, які спонукають компанії використовувати хмарні обчислення. Ці основні переваги включають:

* швидкість
* вартість
* масштабованість
* доступність
* краща безпека

1. Швидкість

Якщо потрібен ІТ-ресурс або послуга з хмари, вони будуть доступні майже миттєво та готові до виробництва практично одночасно. Це означає, що продукт, послуга та дата запуску виходять на ринок майже одразу, що є значною перевагою перед використанням застарілого середовища. Це допомогло багатьом компаніям принести прибуток значно швидше після їх запуску.

2. Вартість

Планування та придбання відповідного типу обладнання завжди було проблемою в традиційному застарілому середовищі. Якщо компанія купує обладнання, яке не відповідає потребам, то, ймовірно, доведеться жити з цією покупкою нескінченно довго. Однак це не проблема з хмарою, оскільки не потрібно купувати апаратне забезпечення. Натомість, організація платить за використання апаратного забезпечення хоста, і якщо воно не відповідає потребам, можна його звільнити та замінити на кращу конфігурацію. Таким чином заощаджується багато грошей, оскільки платите лише за використаний час.

3. Масштабованість

У застарілому середовищі прогнозування попиту — це робота повний робочий день, але за допомогою хмарних служб можна легко налаштувати автоматизований інструмент моніторингу, який виконає цю роботу. Ця інформація дозволить точно збільшити або зменшити швидкість роботи, яка виконується, залежно від потреб.

4. Доступність

Хмарні обчислення дозволяють отримувати доступ до ресурсів, даних, послуг і програм з будь-якого місця, якщо є підключення до Інтернету. Якщо немає підключення до Інтернету, деякі інструменти та методи дозволять отримати доступ до хмари, коли це буде потрібно.

5. Краща безпека

Забезпечення збереження даних у безпечному та надійному місці є пріоритетом для всіх компаній. Хмара забезпечує надійне сховище для даних клієнтів, але дозволяє отримати до них доступ у будь-який час і будь-де, коли це потрібно. Крім того, усі дані, що зберігаються в хмарі, зашифровані та захищені, щоб їх неможливо було підробити [1,3].

## **1.2 Класифікація сучасних хмарних сервісів**

Хмарні обчислення розмножуються, в результаті чого їх класифікують на кілька різних категорій. Проте з різних категорій виділяється шість. Ці шість категорій далі поділяються на дві частини: категорія хмарного розгортання та категорія хмарних послуг.

Хмарні обчислення поділяються на три категорії залежно від розгортання, зокрема:

* Публічна хмара
* Приватна хмара
* Гібридна хмара.

Решта три категорії поділяються на основі послуг, які вони пропонують, зокрема:

* Інфраструктура як послуга (IaaS)
* Платформа як послуга (PaaS)
* Програмне забезпечення як послуга (SaaS) [1].

Хмарні категорії на основі моделей розгортання

1. Публічна хмара

У загальнодоступній хмарі все зберігається та доступне через Інтернет. Ця система розгортання дозволяє будь-кому з відповідними дозволами отримати доступ до деяких програм і ресурсів. Найбільш захоплююча частина загальнодоступної хмари полягає в тому, що організація не володіє жодним компонентом, наявним у ній, будь то апаратне забезпечення, програмне забезпечення чи програма. Усіма компонентами тут керує провайдер. Amazon Web Services і Microsoft Azure є двома яскравими прикладами публічної хмари.

2. Приватна хмара

Приватна хмара використовується виключно в організаціях, вони можуть використовувати її локально або передати її іншим постачальникам хмарних послуг. Ця інфраструктура працює суто в приватній мережі, що означає, що люди, присутні в мережі, можуть отримати доступ лише до неї. Хмара VMware і деякі продукти AWS є одними з прикладів приватної хмари.

3. Гібридна хмара

Ймовірно, це захоплююча форма хмарних обчислень, яка містить функціональні можливості як публічних, так і приватних хмар. Організації, які використовують гібридну хмару, можуть зберігати частину своїх даних локально, а частину – у хмарі. NASA є найвідомішим прикладом організації, яка використовує гібридну хмару. Він використовує приватну хмару для зберігання конфіденційних даних і використовує загальнодоступну хмару для збереження та обміну даними, які можуть переглядати громадськість у всьому світі.

Хмарні категорії на основі моделей обслуговування

1. Інфраструктура як послуга (IaaS) і платформа як послуга (PaaS)

Інфраструктура як послуга (IaaS) надає споживачам фундаментальні обчислювальні, мережеві та сховища ресурси на вимогу, через Інтернет і на основі оплати за використання. Використання хмарної інфраструктури за схемою «оплата за використання» дозволяє компаніям заощадити на придбанні, управлінні та підтримці власної ІТ-інфраструктури. Крім того, хмара легко доступна. Більшість великих постачальників хмарних послуг, включаючи Amazon Web Services (AWS), Google Cloud, IBM Cloud і Microsoft Azure, пропонують IaaS зі своїми хмарними обчислювальними службами.

Платформа як послуга (PaaS) надає клієнтам повну хмарну платформу — апаратне забезпечення, програмне забезпечення та інфраструктуру — для розробки, запуску та керування додатками без витрат, складності та негнучкості створення й підтримки цієї платформи на місці. Організації можуть звернутися до PaaS з тих самих причин, з яких вони шукають IaaS; вони хочуть збільшити швидкість розробки на готовій до використання платформі та розгортати програми з передбачуваною та економічно ефективною моделлю ціноутворення.

2. Програмне забезпечення як послуга (SaaS)

Незважаючи на те, що програмне забезпечення як послуга (SaaS) схоже на використання IaaS і PaaS, описане вище, воно насправді заслуговує окремої згадки через незаперечну зміну, яку ця модель внесла в те, як компанії використовують програмне забезпечення. SaaS пропонує доступ до програмного забезпечення онлайн через підписку, замість того, щоб ІТ-командам доводилося купувати та встановлювати його на окремих системах.

Провайдери SaaS, такі як Salesforce, надають доступ до програмного забезпечення будь-де та будь-коли, якщо є підключення до Інтернету. Ці інструменти відкрили доступ до більш просунутих інструментів і можливостей, таких як автоматизація, оптимізовані робочі процеси та співпраця в режимі реального часу в різних місцях.

4. Випробування та розробка

Одним із найкращих випадків використання хмари є середовище розробки програмного забезпечення. Команди DevOps можуть швидко створити середовища розробки, тестування та виробництва, адаптовані до конкретних потреб. Це може включати, але не обмежуватися, автоматизоване надання фізичних і віртуальних машин.

Щоб проводити тестування та розробку власними силами, організації повинні забезпечити бюджет і створити середовище тестування з фізичними активами. Потім йде встановлення та налаштування платформи розробки. Все це часто може збільшити час, необхідний для завершення проекту, і розтягнути віхи. Хмарні обчислення пришвидшують цей процес за допомогою хмарних інструментів розробки, які роблять створення програм і програмного забезпечення швидшим, простішим і економічнішим.

Однією з головних переваг хмарних обчислень є те, як вони спрощують процес DevOps, конвеєри CI/CD і хмарні вдосконалення (наприклад, мікросервіси, безсерверний режим і контейнеризація). Ці технології призвели до швидкого прискорення та інновацій, але також вимагають самопідтримуваної хмарної інфраструктури для підтримки сотень сервісів.

5. Аналітика великих даних

Використовуючи обчислювальну потужність хмарних обчислень, компанії можуть отримати потужну інформацію та оптимізувати бізнес-процеси за допомогою аналізу великих даних.

Щодня з корпоративних кінцевих точок, хмарних програм і користувачів, які з ними взаємодіють, збирається величезна кількість даних. Хмарні обчислення дозволяють організаціям використовувати величезну кількість як структурованих, так і неструктурованих даних, доступних для використання переваг отримання бізнес-цінності.

Зараз роздрібні торговці та постачальники отримують інформацію, отриману з моделей купівлі споживачів, щоб націлити свої рекламні та маркетингові кампанії на певний сегмент населення. Платформи соціальних мереж є основою для аналізу моделей поведінки, які організації використовують для отримання значущої інформації. Такі компанії, як ці та інші, також можуть використовувати глибші знання за допомогою машинного навчання (ML) і штучного інтелекту (AI), двох можливостей, які стали можливими завдяки хмарним обчисленням.

Дізнайтеся більше про тонкощі цих технологій, прочитавши «ШІ проти машинного навчання проти глибокого навчання проти нейронних мереж».

6. Хмарне сховище

Хмарне сховище даних дозволяє автоматично зберігати файли в хмарі, а потім до них можна отримати доступ, зберігати та отримувати з будь-якого пристрою з підключенням до Інтернету. Замість того, щоб підтримувати власні центри обробки даних для зберігання, організації можуть платити лише за обсяг хмарного сховища, який вони фактично споживають, і робити це без турбот про щоденне обслуговування інфраструктури зберігання. Результатом є вища доступність, швидкість, масштабованість і безпека середовища зберігання даних.

У ситуаціях, коли діють правила та занепокоєння щодо конфіденційних даних, організації можуть зберігати дані як локально, так і поза приміщенням, у приватній або гібридній хмарній моделі для додаткової безпеки.

7. Аварійне відновлення та резервне копіювання даних

Ще однією перевагою використання хмари є економічна ефективність рішення для аварійного відновлення (DR), яке забезпечує швидше відновлення з сітки різних фізичних місць за набагато нижчою ціною, ніж традиційний сайт аварійного відновлення.

Створення сайту DR і тестування плану безперервності бізнесу може бути надзвичайно дорогим і трудомістким завданням з основними засобами. Однак, будучи в хмарі, організації можуть відтворювати свій робочий сайт і постійно відтворювати дані та параметри конфігурації, заощаджуючи значний час і ресурси.

Так само резервне копіювання даних завжди було складною та довготривалою операцією. Хмарне резервне копіювання, хоч і не є панацеєю, але, звичайно, далеке від того, що було раніше. Тепер організації можуть автоматично надсилати дані в будь-яке місце з упевненістю, що ні безпека, ні доступність, ні пропускна здатність не є проблемою.

Хоча ці сім найпопулярніших способів використання хмарних обчислень не є вичерпними, вони показують чіткі стимули для використання хмари для підвищення гнучкості ІТ-інфраструктури, а також максимального використання аналітики великих даних, мобільних обчислень і нових технологій [4].

## **1.3 Існуючі загрози хмарних обчислень**

Хмарні обчислення надають користувачам зручність збільшувати робочі навантаження, не маючи накладних витрат, пов’язаних із підтримкою фізичної інфраструктури, підвищуючи рівень впровадження. Оскільки все більше організацій використовують хмару в тій чи іншій формі, це приносить із собою чималу частку загроз безпеці.

1. Identity First Security

Передбачається, що до 2023 року 75% збоїв у системі безпеки будуть виникати через неадекватне керування ідентифікацією, доступом і привілеями. Зловживання обліковими даними зараз є найпопулярнішою технікою, яка використовується для зломів. Більшість зловмисників постійно націлюються на каталог компанії та інфраструктуру ідентифікації з феноменальним успіхом. Ідентифікація є ключовою технікою бокового переміщення через мережі з повітряним проміжком, на яку сьогодні припадає більшість порушень.

2. Неправильна конфігурація хмари

Неправильні конфігурації хмарної інфраструктури залишаються головною причиною порушень безпеки хмарних обчислень у всьому світі, про що свідчать повідомлення про порушення даних таких компаній, як Verizon і Adobe Creative Cloud. Серед найпоширеніших проблем конфігурації хмарної інфраструктури:

* Незахищений контроль доступу до ресурсів;
* Розкриті облікові дані в публічних сховищах.

Оскільки переважна більшість зламів хмари виникає через неправильну конфігурацію, послідовний моніторинг неправильної конфігурації хмари стає першорядним.

3. Відмова в обслуговуванні

Через необхідність підключення до Інтернету для доступу до хмарних середовищ особливо вразливі до атак типу «відмова в обслуговуванні» (DoS) і «розподілена відмова в обслуговуванні» (DDoS).

Зловмисники можуть заповнити хмарну мережу організації великою кількістю веб-трафіку, таким чином зробивши ресурси недоступними як для клієнтів, так і для співробітників/персоналу. Чим більша частина інфраструктури знаходиться в хмарі, тим смертоноснішою буде атака DoS.

Щоб зменшити ризик атак DoS:

* Обмежте доступ до мережевих портів, протоколів і служб, щоб мінімізувати поверхню атаки;
* Використовуйте балансувальники навантаження та мережі доставки контенту (CDN), щоб обмежити одиничні точки відмови;
* Майте базову лінію нормального трафіку, щоб ви могли помітити будь-що ненормальне;
* Встановіть брандмауер веб-додатків (WAF), щоб захистити від будь-кого, хто використовує відомі вразливості.

4. Внутрішні загрози

Цілих 43% порушень безпеки відбуваються зсередини організації. Інсайдерські атаки можуть бути зловмисними (як у випадку незадоволених співробітників) або ненавмисними.

Належне навчання та обізнаність є ключем до пом’якшення інсайдерських атак. Дотримуйтесь принципу найменших привілеїв під час розробки засобів керування доступом у вашому середовищі, щоб обмежити шкоду, яку можуть завдати працівники, і створіть належний протокол виключення персоналу.

Найважливіше те, що безпека в хмарі – це питання не тільки людей, але й технічного. Турбота про своїх співробітників зменшить ризики того, що негідники завдадуть шкоди організації.

5. Знижена видимість інфраструктури

Природа використання стороннього постачальника для обчислень означає, що передається частковий контроль постачальнику хмарних послуг (CSP). У цьому випадку організація не володіє фізичною інфраструктурою, що ускладнює повну видимість використання вашої інфраструктури та ресурсів, особливо без відповідних технічних знань.

Хмара працює за моделлю спільної відповідальності між організацією та постачальником хмарних послуг (CSP). Хоча це означає, що CSP керує фізичною інфраструктурою, все одно несете відповідальність за забезпечення безпеки даних і робочих навантажень програм у хмарі.

Ця відсутність видимості є поширеним симптомом у багатьох заплутаних хмарних середовищах, що робить його готовим для витоку даних і загроз, таких як наступна в цьому списку — несанкціоноване використання хмарних робочих навантажень.

6. Несанкціоноване використання хмарних робочих навантажень

Більшість основних CSP працюють за моделлю самообслуговування. Це полегшує користувачам миттєво ініціалізацію та деініціалізацію робочих навантажень залежно від їхніх потреб.

З іншого боку, така простота використання також дає можливість використовувати Shadow IT або IT-ресурси, які користувачі створюють і використовують без відома IT-команди. Shadow IT має власний набір ризиків, включаючи (але не обмежуючись ними):

* Підвищений ризик втрати та витоку даних
* Несподівані витрати
* Порушення відповідності

Обов’язково дотримуйтеся принципу найменших привілеїв і дозволяйте створення робочих навантажень лише тим користувачам, яким це потрібно робити як частину їх роботи. Налаштуйте журнал аудиту та механізми попередження, щоб ви могли відстежувати всі дії, що відбуваються всередині, і легко позначати будь-які несанкціоновані дії.

7. Незахищені API

У вашій інфраструктурі можуть бути жорсткі елементи керування, але незахищені API додатків можуть пробити діри в захисті вашого середовища та створити вхідний отвір. Багато API мають власні вразливості безпеки, які в разі використання можуть поставити під загрозу ваше хмарне середовище.

Щоб пом’якшити цю загрозу, попросіть ІТ-групу перевірити кожну зовнішню програму, яку планує використовувати будь-яка команда, і знати про будь-які ризики перед впровадженням. Слідкуйте за оновленнями безпеки та виправленнями програм.

8. Питання відповідності та регулювання

Нарешті, організації повинні відстежувати та дотримуватися багатьох нормативних актів залежно від географії діяльності та типу галузі. Оскільки нові нормативні акти з’являються, а старі оновлюються в міру зміни ландшафту, організаціям може бути складно не відставати.

Постійна хмарна відповідність виявилася основним рішенням регуляторних проблем. Це означає постійний моніторинг хмарної відповідності, а не лише роботу над цим під час сезону аудиту.

Проведення належної перевірки на ранніх стадіях процесу зменшує високі витрати, пов’язані з недотриманням вимог [5].

## **1.4 Реалізація хмарних сервісів на основі CASB**

Посередники безпеки доступу до хмари (CASB) — це локальні або хмарні точки застосування політики безпеки, розміщені між споживачами хмарних послуг і постачальниками хмарних послуг для поєднання та включення корпоративних політик безпеки під час доступу до хмарних ресурсів. CASB консолідують кілька типів забезпечення виконання політики безпеки. Приклади політик безпеки включають автентифікацію, єдиний вхід, авторизацію, зіставлення облікових даних, профілювання пристрою, шифрування, токенізацію, журналювання, попередження, виявлення/запобігання зловмисному програмному забезпеченню тощо [6].

Основною метою CASB є захист конфіденційних даних організації від крадіжки, втрати чи витоку. CASB заповнюють прогалину в безпеці, утворену переходом до хмари та вибухом кінцевих точок. Основні функції CASB включають:

Управління даними

CASB відповідає за керування використанням хмари організації з детальною видимістю та широким набором елементів керування на основі ідентифікації користувача, служби, програми, активності, місцезнаходження чи кінцевої точки. Вони також автоматизують керування порушеннями політики даних за допомогою різноманітних дій, таких як блокування, перевизначення, попередження, шифрування або карантин. CASB надасть ІТ-команді зведення дій, вжитих у відповідь на порушення політики

Безпека даних

CASB працює для захисту та запобігання крадіжці, втраті або витоку даних у всіх хмарних службах і програмах за допомогою шифрування, токенізації або інших методів. Вони встановлюють інструменти та процеси запобігання втраті даних (DLP) для даних, що використовуються, переміщуються чи перебувають у стані спокою з будь-якої хмарної служби чи програми до будь-якої кінцевої точки. Вони також проактивно відстежують хмарне середовище безпеки на наявність порушень політики. Підприємство інтегрує CASB у свою ширшу стратегію безпеки та архітектуру безпеки.

Захист від загроз

CASB забезпечить повну видимість і контроль над усіма організаційними даними в усіх хмарних службах. Вони виявляють та ізолюють хмарні загрози, зокрема зловмисне програмне забезпечення та програми-вимагачі. CASB використовує штучний інтелект (AI), машинне навчання (ML) та інші інтелектуальні інструменти автоматизації для виявлення аномальної поведінки, а також таких загроз, як програми-вимагачі та шкідливі програми. Вони постійно розвиваються, щоб реагувати на постійну мінливу картину загроз і забезпечувати постійний захист від загроз. CASB сповістить групу безпеки хмари про будь-які активні загрози або аномальну діяльність [7].

# 2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ НА БАЗІ РІШЕННЯ CASB

## **2.1 Основні критерії для вибору CASB**

Подібно до безпеки кінцевих точок і безпеки центру обробки даних, хмарна безпека вимагає комплексного цілісного підходу. CASB є критично важливим компонентом хмарної безпеки, але компаніям потрібні додаткові рішення, такі як захищені веб-шлюзи, безпека електронної пошти, рішення для моніторингу загальнодоступних хмар, інтегровані хмарні рішення з брандмауером нового покоління та інші.

Основні критерії при виборі CASB

Безпека користувача

Першою перешкодою для організацій, які намагаються забезпечити достатню безпеку користувачів, є видимість. У великих організаціях є велика кількість користувачів, які мають доступ до кількох програм у кількох хмарних середовищах. Рішення CASB має забезпечувати чітку видимість активності користувачів у всіх програмах SaaS, до яких вони мають доступ.

Хоча значна видимість користувача є критичною, видимості недостатньо для досягнення повної безпеки користувача. Використовуючи дані та аналітику, отримані завдяки глибокій видимості, організації можуть забезпечити значний захист від загроз для своїх користувачів. Експоненціальне зростання мультихмарної діяльності збільшило периметр атаки, і ІТ-фахівці не можуть встигати за всіма сповіщеннями про загрози. Широкомасштабна аналітика та машинне навчання дозволяють рішенню CASB автоматизувати попередження про загрози та реагувати на них, щоб досягти більш надійної та гнучкої безпеки користувачів.

Безпека даних

Першим кроком до забезпечення безпеки даних є контроль. Організації повинні обмежувати доступ до тих областей, де інформація не є критичною для виконання службових обов’язків працівника. Коли зловмисники опиняться в мережі, вони спробують переміститися вбік, щоб отримати доступ до захищених даних. Хоча організації можуть довіряти своїм співробітникам і надавати доступ, це може значно збільшити площу атаки. У разі сумнівів обмежте точки доступу важливими даними.

Подібно до безпеки користувачів, видимість є вирішальним кроком для підвищення безпеки даних. Зберігання конфіденційних даних у багатохмарному середовищі може бути жахливим. Крім того, зростання кількості хмарних рішень і точок віддаленого доступу в організаціях збільшило обсяг спільної роботи з даними. Все більше організацій обмінюються конфіденційними даними в кількох хмарних середовищах. Контроль доступу до конфіденційних даних може бути дуже ефективним, але в мережі постійно створюватимуться нові з’єднання. У результаті організаціям постійно потрібна видимість телеметричних даних, щоб зрозуміти, де потрібно застосовувати їх політики доступу.

Безпека програми

Організації часто були б налякані, якби побачили кількість додатків, які використовує вся їх мережа. Програми можуть бути дуже корисними, але важливо знати, які з них мають доступ до організаційних даних у будь-який момент часу. Рішення CASB має забезпечувати виявлення та видимість підключених додатків сторонніх розробників і дозволяти клієнту відключатися від ризикованих або невідповідних додатків.

Після виявлення програми CASB має класифікувати її. У деяких випадках, як-от Google Apps, ці програми можуть несвідомо мати доступ до конфіденційних даних. Хоча це може здатися нешкідливим, шкідливий додаток може завдати серйозної шкоди. Щоб дозволити співробітникам працювати ефективно, але безпечно, CASB має швидко класифікувати: що це за програма? це безпечно? До яких даних він має доступ? Рішення CASB можуть використовувати дані рейтингів довіри спільноти, щоб допомогти визначити ризики, пов’язані з певними програмами.

Після виявлення та класифікації програму слід увімкнути або вимкнути. У більшості випадків програму завантажували або використовували для підвищення продуктивності співробітника. Якщо програму було класифіковано як безпечну та корисну, а дозволи належні, її можна залишити. Якщо програму класифікують як загрозу, її слід негайно відключити. [8].

## **2.2 Визначення типових рішень для надання безпеки хмарних сервісів**

Сучасна мережева інфраструктура стала дуже гнучкою, поширюючись на хмару — SaaS, IaaS і PaaS; і до суміші додається все більше хмарних додатків — дозволених чи несанкціонованих ІТ. Крім того, зростає кількість розосереджених пристроїв і користувачів, які підпадають під такі категорії, як пристрої, керовані користувачами (BYOD), IoT, тіньові ІТ та віддалені працівники. Традиційний підхід до безпеки має менший сенс у таких дуже різноманітних і розподілених середовищах.

Можливість відстежувати та керувати використанням хмарних додатків стала важливою для забезпечення безпеки підприємства. Замість того, щоб прямо забороняти хмарні служби та потенційно впливати на продуктивність співробітників, організації повинні прийняти новий підхід для подолання цього недоліку та захисту сучасної інфраструктури. Cloud Access Security Broker (CASB) — це нова технологія безпеки, яка спеціально вирішує проблеми, пов’язані з хмарою.

Нижче наведений список із семи найкращих брокерів безпеки доступу до хмари (CASB):

McAfee MVISION CASB, який забезпечує видимість і контроль над даними та загрозами в загальнодоступних, приватних і гібридних хмарних середовищах.

Netskope Провідне рішення CASB, яке дозволяє організаціям швидко визначати та керувати використанням хмарних програм, незалежно від того, керовані вони чи некеровані.

Microsoft Defender for Cloud App Рішення CASB, яке працює в кількох хмарах.

Proofpoint CASB Поставляється з автентифікацією SAML на основі ризиків, веб-ізоляцією та функціями віддаленого доступу без довіри, які допомагають запобігти хмарним загрозам.

Symantec CloudSOC Багаторежимний CASB із надійною видимістю, безпекою даних і можливостями захисту від загроз для пом’якшення шкідливого вмісту в хмарних додатках, тіньових ІТ-службах і ризики відповідності.

Lookout CASB Хмарна платформа CASB, яка забезпечує інтегровану хмарну безпеку та захист даних.

Ідея CASB полягає в тому, щоб дозволити компаніям безпечно використовувати хмару, одночасно захищаючи конфіденційні корпоративні дані. Він забезпечує видимість і контроль над даними та загрозами в хмарі. Це досягається шляхом використання автоматичного виявлення для складання списку всіх програм третьої хмари, включаючи рівень ризику, пов’язаний з кожною програмою та тими, хто їх використовує. Потім він використовує статистичні дані для встановлення політики та її застосування. За допомогою CASB організація може сподіватися на досягнення видимості, відповідності, безпеки даних і виявлення загроз у своїх хмарних службах. Рішення CASB можна розгорнути локально або в хмарі за допомогою режимів API-Control, Reverse Proxy або Forward Proxy.

Існує три види CASB:

Лише API: Забезпечує лише керування, без безпеки та захист Zero-Day

Багаторежимний режим першого покоління: забезпечує керування та безпеку, але не захист Zero-Day.

Multi-mode Next-Gen: Забезпечує керування, безпеку та захист Zero-Day [9].

## **2.3 Огляд ринку CASB**

Ринок CASB швидко розвивається з новими варіантами використання та функціональними можливостями для задоволення дедалі складніших вимог хмарної безпеки. Завдяки різноманітності рішень CASB вибір правильного для вашого бізнесу може бути складним завданням. Те, що ідеально підходить з точки зору ціни, характеристик і функціональності для однієї організації, може не підходити для іншої.

Потрібно визначити випадки використання CASB і шукати рішення, які найкраще відповідають потребам організації. Також потрібно з’ясувати, чи CASB інтегрується з іншими існуючими програмами безпеки у мережі, такими як DLP, SIEM, брандмауери та інші.

1. McAfee MVISION

McAfee MVISION Cloud — це CASB, яка забезпечує видимість і контроль над даними та загрозами в загальнодоступних, приватних і гібридних хмарних середовищах. Це один із провідних продуктів CASB, який був названий лідером у магічному квадранті Gartner для CASB у 2020 році. MVISION Cloud забезпечує аналітику в режимі реального часу та можливості аналізу загроз за допомогою штучного інтелекту, включаючи сповіщення про поведінку користувачів. Продукт найкраще підходить для великих організацій, таких як фінансові, медичні та державні установи, а також для інших, які активно використовують хмару. Крім того, каталог McAfee CASB Connect включає десятки попередньо інтегрованих програм, таких як Office 365, AWS, Box, Slack, Salesforce тощо, які спрощують безпечне впровадження будь-якої хмарної служби.

Підхід MVision дозволяє використовувати практично будь-яку модель розгортання, яку можна забажати, будь то повністю хмарна, локальна чи якийсь гібридний формат. Крім того, MVISION Cloud працює на основі агентів і може бути розгорнуто за допомогою API, методів прямого або зворотного проксі.

Ключові особливості:

• Виявлення: отримайте повну видимість даних, контексту та поведінки користувачів у всіх хмарних службах, користувачах і пристроях.

• Захист: застосовує безперервний захист конфіденційної інформації, куди б вона не потрапляла в хмарі чи за її межами.

• Правильно: Виконайте дії в реальному часі в хмарних службах, щоб виправити порушення правил і зупинити загрози безпеці.

• Автоматизована аналітика поведінки користувачів і об’єктів (UEBA) для виявлення загроз для хмарних середовищ

• Інтеграція API із хмарними службами для керування доступом користувачів, співпрацею та даними в режимі реального часу, а також прямим і зворотним режимами проксі для посилення контролю над тіньовими ІТ та доступом персональних пристроїв до хмари.

2. Netskope CASB

Netskope — це провідне рішення CASB, яке дозволяє організаціям швидко визначати та керувати використанням хмарних програм, незалежно від того, керовані вони чи некеровані. Netskope було визнано лідером у магічному квадранті Gartner 2020 для CASB; і 2021 Gartner Peer Insights Customers’ Choice для CASB. Netskope Security Cloud запобігає викраденню конфіденційних даних і усуває сліпі зони, націлюючи та контролюючи діяльність у тисячах хмарних (SaaS та IaaS) служб. Орієнтований на дані підхід, прийнятий Netskope Security Cloud, дозволяє забезпечувати видимість і дані в реальному часі, а також захист від загроз щоразу, коли пристрій підключається до хмари.

Netskope підтримує багаторежимні варіанти розгортання від режиму розгортання лише через API до кількох варіантів у реальному часі, включаючи програмне забезпечення кінцевої точки для захисту користувачів у роумінгу. Крім того, його можна на 100% розгорнути в хмарі, локально або в гібридній формі.

Основні функції та можливості включають:

• Оцінка ризику хмарних додатків: Індекс хмарної довіри Netskope (CCI) автоматично перевіряє ваш трафік, щоб виявити загальний профіль ризику для програм, які використовуються у середовищі.

• Netskope DLP: Netskope DLP забезпечує контекстну обізнаність про вміст, який використовується в хмарі, включаючи вбудоване застосування політик безпеки в реальному часі для запобігання втраті даних

• Видимість і контроль: Netskope Cloud XD забезпечує детальну видимість і контроль над вашими хмарними службами, а також виконує аналіз великих даних для усунення сліпих зон.

• Оптимізовані операції: розвідка загроз Netskope Виявляє, пом’якшує та усуває загрози від внутрішніх/зовнішніх користувачів, зламані облікові записи та загрози привілейованим користувачам у хмарних програмах.

• Настроювана інформаційна панель: настроюване подання всіх SaaS, IaaS, веб-активностей, користувачів і пристроїв.

3. Microsoft Defender для хмарної програми

Microsoft Defender for Cloud App (офіційно Microsoft Cloud App Security) — це рішення CASB, яке працює в кількох хмарах. Він забезпечує широку видимість, контроль над переміщенням даних і складну аналітику для виявлення та боротьби з кіберзагрозами в хмарних службах Microsoft і сторонніх розробників. Він був визнаний лідером у магічному квадранті Gartner 2020 для CASB.

Він підтримує різні режими розгортання, включаючи збір журналів, конектори API та зворотний проксі. Крім того, Microsoft Cloud App Security вбудовано інтегрується з провідними рішеннями Microsoft і розроблено з урахуванням професіоналів із безпеки.

Основні функції та переваги:

• Виявляйте та контролюйте використання Shadow IT: визначте хмарні програми, служби IaaS і PaaS, які використовуються організацією.

• Захищайте свою конфіденційну інформацію будь-де в хмарі: розумійте, класифікуйте та захищайте доступ до конфіденційних даних у спокої.

• Захист від кіберзагроз і аномалій: виявляйте незвичайну поведінку в хмарних програмах, щоб ідентифікувати шахрайські програми та скомпрометованих користувачів і автоматично виправляти їх

• Оцініть відповідність своїх хмарних додатків: оцініть, чи відповідають ваші хмарні додатки вимогам відповідності

• Керуйте доступом до програм і ресурсів: виявляйте та керуйте тіньовими ІТ у своїй організації.

Microsoft Cloud App Security — це послуга передплати на основі користувачів, а ліцензія надається за місячною моделлю. Його можна ліцензувати як окремий продукт або як частину розділів кілька різних планів ліцензування.

4. Бітглас CASB

Bitglass (нещодавно придбана компанією Forcepoint) — це американська компанія, яка розробляє програмне забезпечення безпеки в хмарі, заснована в 2013 році. Це хмарне безагентне багаторежимне рішення CASB наступного покоління, орієнтоване на малого та середнього бізнесу та великі підприємства. Bitglass є одним із провідних продуктів CASB на ринку. Він був визнаний лідером у магічному квадранті Gartner 2020 для CASB. Bitglass поєднує прямі та зворотні проксі-сервери для виявлення загроз, які мережеві зворотні проксі-сервери можуть пропустити. Крім того, Bitglass здатний генерувати сповіщення в режимі реального часу, щоб допомогти керувати інцидентами та реагувати.

Ключові особливості:

• Захист даних у русі: завдяки надійному хмарному механізму DLP і можливостям Zero-day Threat Protection

• Видимість і аналітика: Bitglass дає змогу переглядати в одній панелі між програмами деталі використання хмари вашими співробітниками та інші дані аналітики поведінки користувачів.

• Безагентний захист: безагентні проксі Bitglass забезпечують проміжний трафік між хмарою та будь-якою кінцевою точкою

• Shadow IT Discovery: Bitglass використовує штучний інтелект і технології машинного навчання для автоматичного індексування та класифікації відомих і невідомих хмарних програм

• Керування API: Bitglass забезпечує керування API для всіх значущих програм SaaS

• Керування ідентифікацією: Bitglass включає такі служби керування ідентифікацією, як SAML, SSO, автентифікація Active Directory, контекстний MFA тощо

Bitglass відомий своєю простотою, надійними функціями безпеки та чудовою службою підтримки. Однак деякі клієнти стурбовані тим, що він зберігає дані в сторонній хмарі, що призводить до проблем з безпекою та відповідністю.

5. Proofpoint CASB

Proofpoint CASB оснащено автентифікацією SAML на основі ризиків, веб-ізоляцією та функціями віддаленого доступу без довіри, які допомагають запобігти хмарним загрозам. Він також інтегрується з API-інтерфейсами хмарних служб, гібридними інструментами керування ідентифікацією та іншими продуктами безпеки (зокрема Proofpoint Threat Response) для виявлення та стримування загроз.

Proofpoint CASB поєднує аналіз загроз на основі машинного навчання з індивідуальними індикаторами ризику для аналізу поведінки користувачів і виявлення аномалій у хмарних програмах, а також у разі зламу хмарного облікового запису.

Основні функції та переваги:

• Видимість, орієнтована на людей: отримуйте уявлення про використання хмари на глобальному рівні, рівні програми та користувача

• Перевірений розширений захист від загроз: поєднуйте індикатори ризику для користувача з міжканальним аналізом загроз для виявлення аномалій у хмарних програмах.

• Безпека даних з урахуванням ризиків: Proofpoint CASB допомагає ідентифікувати дані, які знаходяться під загрозою, втратили або скомпрометовані облікові записи.

• Керування програмами сторонніх розробників і Shadow IT: Proofpoint CASB допомагає вам виявляти та керувати шкідливими програмами сторонніх розробників та іншими прогалинами безпеки у ваших хмарних програмах.

6. Symantec CloudSOC

Symantec CloudSOC — це багаторежимний CASB із надійною видимістю, безпекою даних і можливостями захисту від загроз для пом’якшення шкідливого вмісту в хмарних додатках, тіньових ІТ-службах і ризики відповідності. CloudSOC ідеально підходить для середніх і великих підприємств, які використовують інші хмарні продукти Symantec, і організацій, які активно використовують хмару.

CloudSOC легко інтегрується з іншими продуктами Symantec для корпоративної безпеки, щоб забезпечити розширені функції безпеки в хмарі. Symantec стверджує, що має найнадійніше хмарне DLP-рішення завдяки технології ContentIQ DLP, що базується на наукових даних. Він також оснащений інтелектуальним UEBA та можливостями машинного навчання一, що дозволяє адаптувати політику. Крім того, хмарна SOA підключається до Symantec Global Intelligence Network (GIN) і отримує переваги від даних про загрози, зібраних через кінцеву точку, електронну пошту та веб-трафік від усієї клієнтської бази Symantec.

7. Lookout CASB (офіційно CipherCloud)

Lookout CASB — це хмарна платформа CASB, яка забезпечує інтегровану хмарну безпеку та захист даних. Lookout CASB працює в усіх режимах — на основі API, зворотного та прямого проксі-сервера, пропонуючи максимальне охоплення варіантів використання, видимість і контроль над усіма користувачами, пристроями та хмарними службами. Крім того, він має понад 20 000 хмарних додатків, профільованих у своїй базі знань, що дає змогу оцінювати ризик використання кожного хмарного сервісу.

Механізм політики Lookout CASB дозволяє адміністраторам застосовувати централізовані політики захисту даних. Централізовані процедури, які виконуються через Lookout CASB, додатково відстежують, виявляють, класифікують і усувають доступ до конфіденційних даних у хмарних додатках, а також застосовують автоматизовані дії з виправлення. Крім того, з оголошеннями. Механізм аналітики поведінки користувачів і суб’єктів (UEBA) від Lookout, безперервний моніторинг користувачів, пристроїв і активності додатків для виявлення аномальної поведінки виконується в кількох санкціонованих хмарних додатках і запобігає скомпрометації облікових записів зловмисними інсайдерами та зовнішніми загрозами [10].

# 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ НА БАЗІ РІШЕННЯ MCAFEE

## **3.1 Атаки на хмари і рекомендації щодо їх усунення**

1. Традиційні атаки на ПЗ

Уразливості операційних систем, модульних компонентів, мережевих протоколів - традиційні загрози, для захисту від яких досить встановити міжмережевий екран, firewall, антивірус, систему запобігання вторгнень (Intrusion Prevention System - IPS) і інші компоненти. При цьому важливо, щоб ці кошти захисту ефективно працювали в умовах віртуалізації.

1. Функціональні атаки на елементи хмари

Цей тип атак пов'язаний з багатошаровістю хмари, загальним принципом безпеки. У статті про небезпеку хмар було запропоновано наступне рішення: для захисту від функціональних атак для кожної частини хмари необхідно використовувати такі засоби захисту: для проксі - ефективний захист від DoSатак, для веб-сервера - контроль цілісності сторінок, для сервера додатків - екран рівня додатків, для СУБД - захист від SQL-ін'єкцій, для системи зберігання даних - правильні бекапи (резервне копіювання), розмежування доступу. Окремо кожні з цих захисних механізмів вже створені, але вони не зібрані разом для комплексного захисту хмари, тому завдання по інтеграції їх в єдину систему потрібно вирішувати під час створення хмари.

1. Атаки на клієнта

Більшість користувачів підключаються до хмари, використовуючи браузер. Тут розглядаються такі атаки як Cross Site Scripting, викрадення паролів, перехоплення веб-сесій, людина посередині і багато інших. На поточний момент, найбільш ефективним захистом від даного виду атак є правильна аутентифікація і використання шифрованого з'єднання (SSL) з взаємною аутентифікацією. Однак ці кошти захисту не дуже зручні і дуже марнотратні для творців хмар. У цій галузі інформаційної безпеки є ще безліч невирішених завдань.

1. Атаки на гіпервізор

Гипервизор є одним з ключових елементів віртуальної системи. Основною його функцією є поділ ресурсів між віртуальними машинами. Атака на гіпервізор може привести до того, що одна віртуальна машина зможе отримати доступ до пам'яті і ресурсів іншої. Також вона зможе перехоплювати мережевий трафік, відбирати фізичні ресурси і навіть витіснити віртуальну машину з сервера. В якості стандартних методів захисту рекомендується застосовувати спеціалізовані продукти для віртуальних середовищ, інтеграцію хост-серверів зі службою каталогу Active Directory, використання політик складності і старіння паролів, а також стандартизацію процедур доступу до керуючих засобів хостсервера, вбудований брандмауер хоста віртуалізації. Також можливе відключення таких часто невикористовуваних служб як, наприклад, веб-доступ до сервера віртуалізації.

1. Атаки на системи управління

Велика кількість віртуальних машин, які використовуються в хмарах, вимагає наявності систем управління, здатних надійно контролювати створення, перенесення та утилізацію віртуальних машин. Втручання в систему управління може привести до появи віртуальних машин - невидимок, здатних блокувати одні віртуальні машини і підставляти інші [6].

Найбільш ефективні способи захисту в області безпеки хмар опублікувала організація Cloud Security Alliance (CSA). Проаналізувавши опубліковану компанією інформацію, були запропоновані наступні рішення [5]:

1. Збереження даних. Шифрування

Шифрування - один з найефективніших способів захисту даних. Провайдер, що надає доступ до даних, повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також, в разі відсутності необхідності, безповоротно видаляти.

1. Захист даних при передачі

Зашифровані дані при передачі повинні бути доступні тільки після аутентифікації. Дані не вийде прочитати або зробити зміни, навіть в разі доступу через ненадійні вузли. Такі технології досить відомі, алгоритми і надійні протоколи AES, TLS, IPsec давно використовуються провайдерами.

1. Аутентифікація

Аутентифікація - захист паролем. Для забезпечення більш високої надійності часто вдаються до таких засобів як токени і сертифікати. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації також рекомендується використовувати LDAP (Lightweight Directory Access Protocol) і SAML (Security Assertion Markup Language).

1. Ізоляція користувачів

Використання індивідуальної віртуальної машини і віртуальної мережі. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій як VPN (Virtual Private Network), VLAN (Virtual Local Area Network) і VPLS (Virtual Private LAN Service). Часто провайдери ізолюють інформацію користувачів один від одного за рахунок зміни коду в єдиній програмному середовищі. Такий підхід має ризики, пов'язані з небезпекою знайти дірку в нестандартному коді і отримати доступ до даних користувачів. У разі можливої помилки в коді один користувач може отримати дані іншого користувача [12].

## **3.2 Огляд рішення McAfee MVISION Cloud**

Компанія Gartner займається дослідженням ринкових інформаційних технологій та оприлюднює свої оцінки діяльності учасників світового ІТ-ринку на основі оригінальних методик, одна з яких отримала назву «Магічний квадрат».

Опубліковано дослідження, відповідно до якого компанії McAfee, розробник засобів захисту від поглибленої інформаційної безпеки в четвертому розрізі знаходиться «лідером» «Чарівного квадранта» в номінації «Брокери безпеки хмарного доступу». Результати досліджень говорять про те, що McAfee володіє найбільшою повною оцінкою майбутньої системи безпеки небезпечних рішень, а також надає хороші можливості для його реалізації у відеозбереженні інноваційних продуктів та технологій.

Покладення оцінки роботи компанії стало можливим завдяки інноваційному продукту McAfee MVISION Cloud. Це рішення забезпечує захищені підключення та доступ до хмарного сервісу, оптимізацію хмарних вичислювальних навантажень, у тому числі контейнерних рахунків та надійний інструмент управління безпекою обласних SaaS-платформ. Доступне рішення McAfee MVISION Cloud успішно використовується для захисту загальнодоступних та корпоративних обласних платформ та сервісів.

Суть методики Gartner Magic Quadrant, оцінка компаній за принципом «повного бачення» та «можливості реалізації» технології. Це експертна методика розподіляє ігровий ринок за чотирма квадратами «ніші ігроки», «претенденти», «провідці» та «лідери». Наявність компанії McAfee у Gartner Magic Quadrant і, тим більше, її лідерське положення у верхньому квадраті говорить про високі технологічні та риночні досягнення. McAfee демонструє збалансований прогрес, піднімає планку конкуренції та демонструє вплив на весь ринок [9].

## **3.3. Основні характеристики та приклади використання McAfee MVISION Cloud**

McAfee MVISION Cloud - засіб хмарного захисту, який забезпечує захист даних і блокування загроз в хмарі на платформах SaaS, PaaS і IaaS з єдиної хмарної точки застосування політик.

Рішення McAfee дає змогу збирати повну інформацію про використання хмари і про всі хмарні дані, контролювати дані та активність в хмарі з будь-якого пристрою.

Приклади використання:

* Застосування політик запобігання витоків даних (DLP) до даних в хмарі. При цьому забезпечується синхронізація з політиками DLP для кінцевих точок.
* Запобігання несанкціонованого поширення конфіденційних даних серед тих, кому вони не призначаються.
* Блокування синхронізації і завантаження корпоративних даних на особисті пристрої.
* Виявлення зламаних облікових записів, внутрішніх загроз і шкідливих програм.
* Шифрування хмарних даних за допомогою ключів, винятковий доступ до яких є тільки у користувача.
* Можливість збирати інформацію про несанкціоновані додатки і контролювати їх функції.
* Аудит помилок конфігурації в порівнянні з галузевими показниками; автоматичне зміна налаштувань.

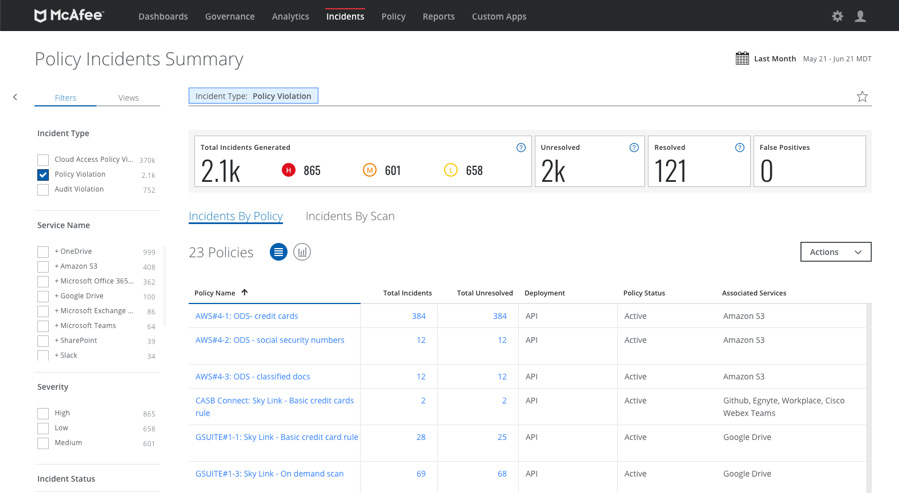


Рис.3.1. Вкладка конфігурації політик запобігання витоків даних

**Функції платформи MVISION Cloud**

1. Модуль застосування уніфікованих політик

Застосовує уніфіковані політики до всіх збереженим і переданих даним у всіх хмарних службах. Використовує шаблони політик, імпортує політики з існуючих рішень або створює нові.

1. Готові шаблони політик

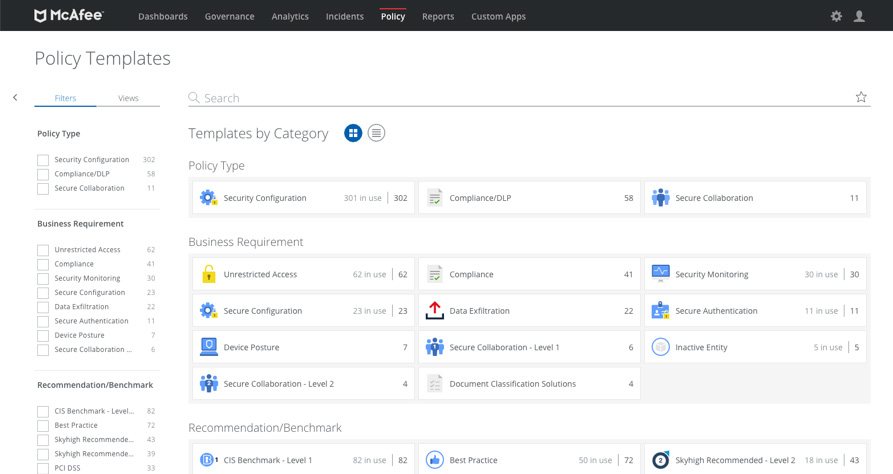
Функція пропонує готові шаблони політик на основі бізнес-вимог, нормативно-правового відповідності, галузевих показників, тестів продуктивності хмарних служб і третіх сторін.

1. Майстер створення політик

Визначає індивідуальні політики на основі правил, пов'язаних булевої логікою, а також на основі винятків і багаторівневих рішень проблем безпеки в залежності від серйозності інцидентів.

1. Управління інцидентами за допомогою політик

Функція пропонує єдиний інтерфейс для аналізу інцидентів, вжиття заходів реагування вручну і виконання автоматичного відкоту з метою відновлення файлів і дозволів на доступ до нього.

Рис.3.2. Шаблони політик

1. Реєстр хмарних служб

Надає найбільший і точний в світі реєстр хмарних служб з оцінкою за шкалою CloudTrust від 1 до 10 на основі оцінки ризиків по 261 пункту

1. Захист конфіденційності

Функція використовує незворотний односторонній процес локальної розмітки ідентифікаційних даних користувача і маскування корпоративних ідентифікаційних даних.

1. Автономне усунення загроз

З метою скоротити обсяг аналізу інцидентів вручну, функція навчає користувачів усувати інциденти, пов'язані з порушеннями політики, а після їх усунення автоматично усуває оповіщення про інциденти.

1. Навчання в додатках

Функція навчає користувачів в режимі реального часу усувати інциденти в тому вбудованому додатку електронної пошти, додатку для обміну миттєвими повідомленнями або спільної роботи, в якому стався інцидент

1. Модуль зіставлення дій, працює на основі штучного інтелекту

Використовує штучний інтелект для розпізнавання додатків і зіставлення дій користувачів з уніфікованим набором дій, забезпечуючи стандартизований моніторинг і управління додатками.

1. Багатохмарний захист

Застосування уніфікованого набору політик безпеки до всіх хмарним службам, що дозволяє зіставляти порушення політик і розслідувати дії, аномалії і загрози на рівні окремих сервісів.

1. Аналітика вмісту

Використовуючи ключові слова, заздалегідь певні буквено-цифрові шаблони, регулярні вираження, метадані файлів, цифрові відбитки документів і баз даних, ця функція дозволяє ідентифікувати конфіденційні дані в хмарних сервісах.

1. Аналітика взаємодії

Функція допомагає виявляти детально налаштовані дозволу читача, редактора і власника на доступ до файлів і папок, до яких надано доступ окремим користувачам, всім співробітникам організації або всім, у кого є посилання.

1. Аналітика доступу

Функція розпізнає контекст доступу, в тому числі операційну систему пристрою, стан управління пристроєм, його місце розташування, а також корпоративні і особисті облікові записи.

1. Аналітика використання хмари

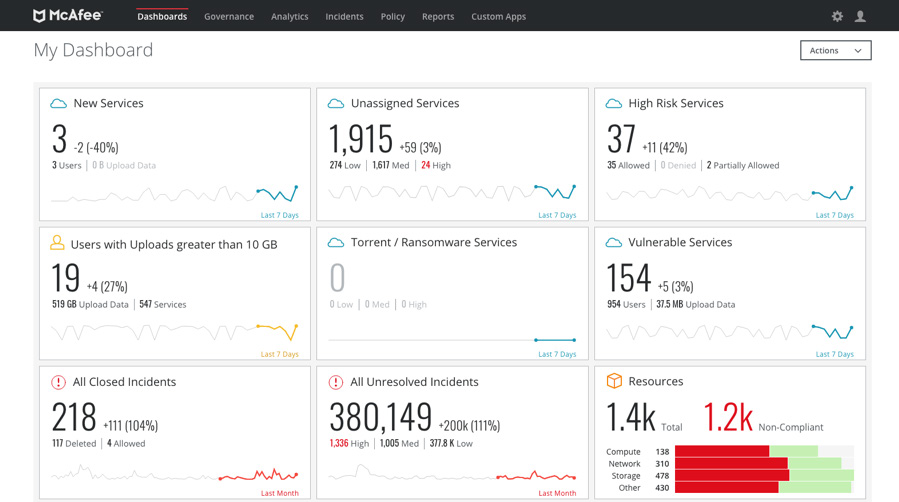
Функція дозволяє узагальнювати інформацію про використанні хмари, в тому числі про хмарних службах, з якими працює користувач, обсязі даних, зокрема завантажень, зокрема відвідувань і про дозволених або заборонених діях за певний період часу.

Рис. 3.3. Панель аналітики

1. Моніторинг активності в хмарі

Дозволяє вести докладний журнал аудиту всіх дій користувачів і адміністраторів з метою полегшити проведення розслідувань і комп’ютерно-технічних експертиз після інциденту.

**Контроль даних і активності в хмарі**

1. Запобігання витоків даних в хмарі (DLP)

Функція забезпечує застосування політик відповідно до вашими власними правилами для вмісту, щоб запобігти витоку структурованих і неструктурованих даних, вмісту файлів в хмарних додатках і інфраструктурі. Локальні політики та правила для вмісту McAfee® Data Loss Prevention (DLP) можна синхронізувати з MVISION Cloud і застосовувати до хмарних сервісів.

1. Контроль даних з багатьох джерел

Функція застосовує політики DLP до даних, завантажуваних в хмару, створюваним в хмарі, викачуваним з хмари, а також до даних, над якими працюють спільно і якими обмінюються між хмарами в різних службах.

1. Багаторівневе реагування

Функція задає політики для декількох рівнів небезпеки і забезпечує застосування різних заходів реагування в залежності від рівня небезпеки інциденту. Заходи реагування, наприклад сканування трафіку за технологією DLP, можуть бути ініційовані автоматично при виявленні помилки конфігурації в ході аудиту.

1. Приміщення в карантин

Функція ізолює файли, що активують політики, в безпечному місці в тій хмарної службі, де вони були виявлені. McAfee ніколи не зберігає файли, поміщені в карантин.

1. Шифрування

Функція захищає конфіденційні дані, застосовуючи перевірені колегами схеми шифрування структурованих і неструктурованих даних зі збереженням їх функцій. для шифрування використовуються ключі, керовані на рівні клієнта.

1. Управління правами на доступ до даних

Функція забезпечує захист за допомогою управління правами на доступ до файлів, завантажуваних в хмарні служби або викачуваним з них. Тим самим ваші конфіденційні дані будуть захищені, де б вони не знаходилися.

1. Контроль спільної роботи

Зменшує повноваження доступу до файлів і папок для конкретних користувачів до рівня редактора або читача, скасовує дозволи і посилання загального доступу. Дозволи можуть надаватися виходячи з рівня конфіденційності даних.

1. Підключення додатків

Функція забезпечує збір інформації про сторонніх додатках, підключених до санкціонованим хмарних сервісів (наприклад, про додатки Marketplace). З її допомогою можна здійснювати контроль на основі політик за використанням сторонніх додатків. контроль виконується з урахуванням конкретних користувачів, додатків або дозволів на доступ.

1. Видалення

З метою забезпечення нормативно-правового відповідності функція безповоротно видаляє з хмарних служб дані, що порушують політику.

1. Контроль доступу на основі аналізу контексту

Для запобігання завантаження і скачування даних функція дозволяє застосовувати правила доступу (З низьким ступенем деталізації) для дозволу або блокування сеансів на основі ризиків на рівні послуг, типу пристрою і детального контролю на рівні активності.

1. Адаптивна аутентифікація

Шляхом інтеграції з рішеннями для управління ідентифікацією на основі політик контролю доступу забезпечує включення додаткових етапів аутентифікації в режимі реального часу.

1. Контроль за хмарними додатками

Детальна політика контролю за несанкціонованими хмарними службами, в тому числі можливість дозволяти або блокувати дії і контролювати доступ до даних несанкціонованих користувачів - і все це за допомогою консолі MVISION Cloud.

**Захист від загроз хмарної безпеки та від помилок конфігурації**

1. Аудит налаштувань безпеки

Дозволяє виявляти поточні настройки безпеки хмарних додатків або інфраструктури і рекомендує модифікації для підвищення рівня безпеки на основі передових галузевих стандартів, наприклад контрольних показників Центру інтернетбезпеки (Center for Internet Security — CIS). Аудити можуть проводитися з метою попереджувального зниження ризику перед розгортання коду в моделі «інфраструктура як послуга» (IaaS).

1. Автоматичне усунення помилок конфігурації

Дозволяє забезпечити реагування на основі політик на помилку конфігурації, виявлену в ході аудиту, і автоматично змінити відповідні налаштування, наприклад відключити загальний доступ для контейнера зберігання в рамках моделі IaaS.

1. Аналіз поведінки користувачів і об’єктів (UEBA)

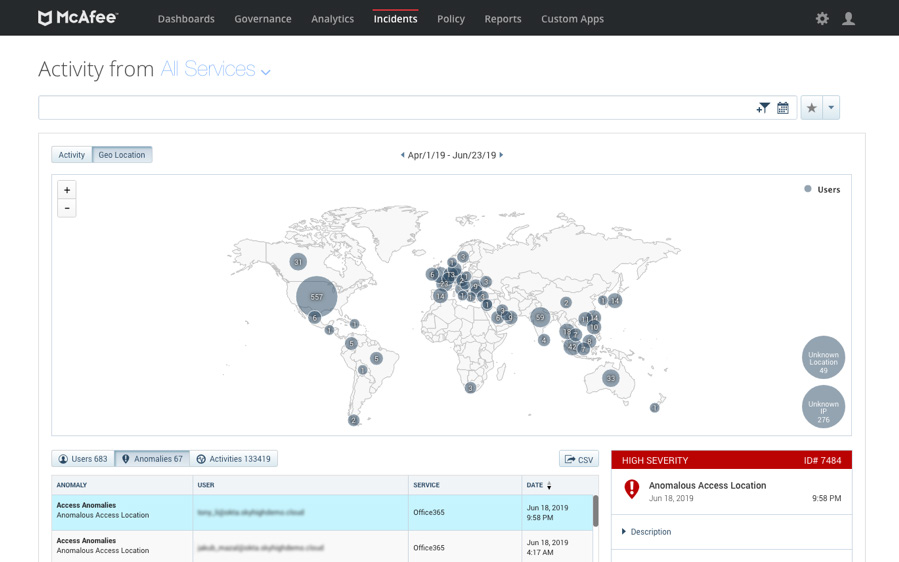
Функція автоматично будує модель, що самонавчається на основі множинних евристичних алгоритмів і методів машинного навчання і виявляє ознаки дій, що свідчать про наявність загроз з боку користувачів в різних хмарних сервісах.

1. Інтерактивне навчання

Дозволяє внести вклад людини в моделі машинного навчання і пропонує їх попередній перегляд в режимі реального часу, що відображає зміни чутливості на аномалії, виявлені системою.

1. Виявлення злому облікового запису

Функція аналізує спроби входу в систему, для того щоб виявити випадки підозрілого доступу з різних регіонів, атаки методом перебору и ненадійні місця розташування, які є ознаками злому облікового запису.

Рис. 3.4. Виявлення активності з різних регіонів

1. Виявлення внутрішніх загроз

Функція застосовує машинне навчання для виявлення дій, що сигналізують про недбалу і шкідливу поведінку, в тому числі про викрадення конфіденційних даних зловмисниками всередині самої організації.

1. Аналітика привілейованих користувачів

Допомагає виявляти надмірні повноваження користувачів, неактивні облікові записи, несанкціонований доступ, а також недозволене підвищення рівня привілеїв і підготовку облікових даних користувачів.

1. Виявлення шкідливих програм

Функція виявляє шкідливі програми і виявляє випадки поведінки, що свідчать про дію шкідливого ПЗ, що використовується для ексфільтраціі даних з хмарних служб. Сканування хмарних служб на наявність ознак злому може виконуватися на вимогу (В ретроспективі) і в режимі реального часу.

1. Видалення шкідливих програм

Функція блокує складні загрози шляхом повної нейтралізації та безповоротного видалення шкідливих програм.

**Режими розгортання**

**McAfee Sky Link** підключається до API-інтерфейсів хмарних служб з метою збору інформації про дані і про дії користувачів, а також з метою застосування політик як до збережених даних, так і до всіх завантажуваних або загальних даних в режимі майже реального часу.

**McAfee Lightning Link** встановлює пряме з'єднання з хмарними службами по допоміжному каналу з метою застосування політик в режимі реального часу з повним охопленням даних, користувачів і пристроїв.

**McAfee Ground Link** виступає в якості посередника підключень між McAfee і локальними службами каталогів LDAP, рішеннями DLP, проксі-серверами, брандмауерами і службами управління ключами.

**McAfee Sky Gateway** забезпечує застосування вбудованих політик до переданих даним в режимі реального часу.

**Режим електронної пошти** використовує власний потік обробки пошти з метою застосування політик до всіх повідомлень, відправляється службою Exchange Online, безпосередньо або в режимі пасивного моніторингу.

**Універсальний режим** встановлюється безпосередньо між користувачем і хмарної службою і управляє трафіком після аутентифікації, з охопленням всіх користувачів і всіх пристроїв, без використання агентів.

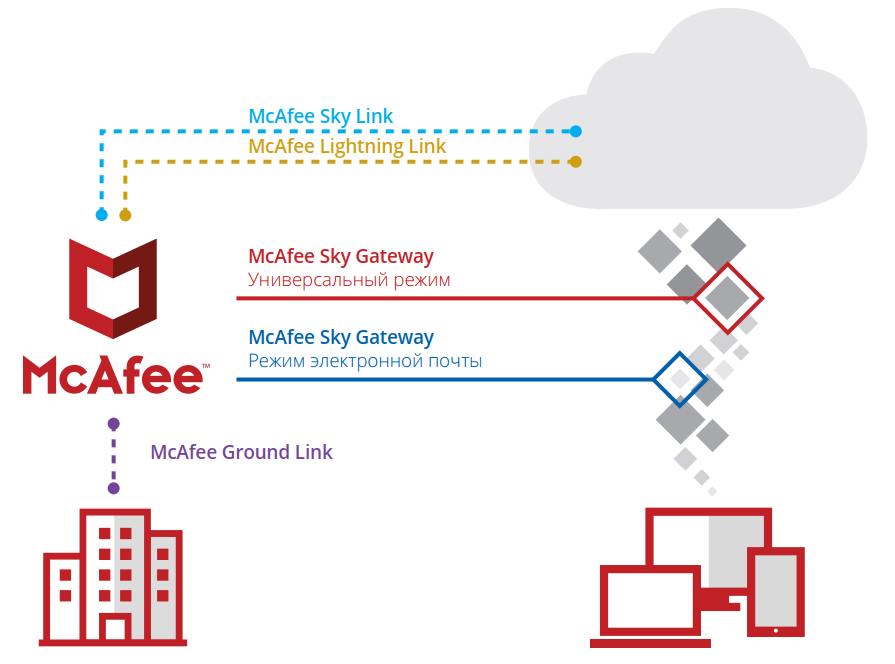


Рис.3.5. Режими розгортання

**Додаткові функції MVISION Cloud Security**

**Cloud Security Advisor** - це портал на платформі MVISION Cloud Security, що дозволяє клієнтам відслідковувати хід процесу забезпечення безпеки. Він надає підприємствам індивідуальні рекомендації про те, як встановити пріоритет дій щодо впровадження хмарних засобів захисту.

Cloud Security Advisor включає в себе наступні компоненти:

Звіт про безпеку хмари. Огляд ключової статистики використання, сфокусований на основні показників забезпечення безпеки, таких як обсяг застосування хмарних технологій, число інцидентів, дані, схильні до ризику, і кількість користувачів.

Оцінка і квадрант Cloud Security Advisor. Цей показник оцінює рівень збору інформації про загрози і рівень контролю середовища за 100-бальною шкалою. Оцінки розраховуються на основі показників і ходу процесу забезпечення хмарної безпеки і наводяться в порівнянні з аналогічними показниками інших підприємств галузі (аналогічного розміру).

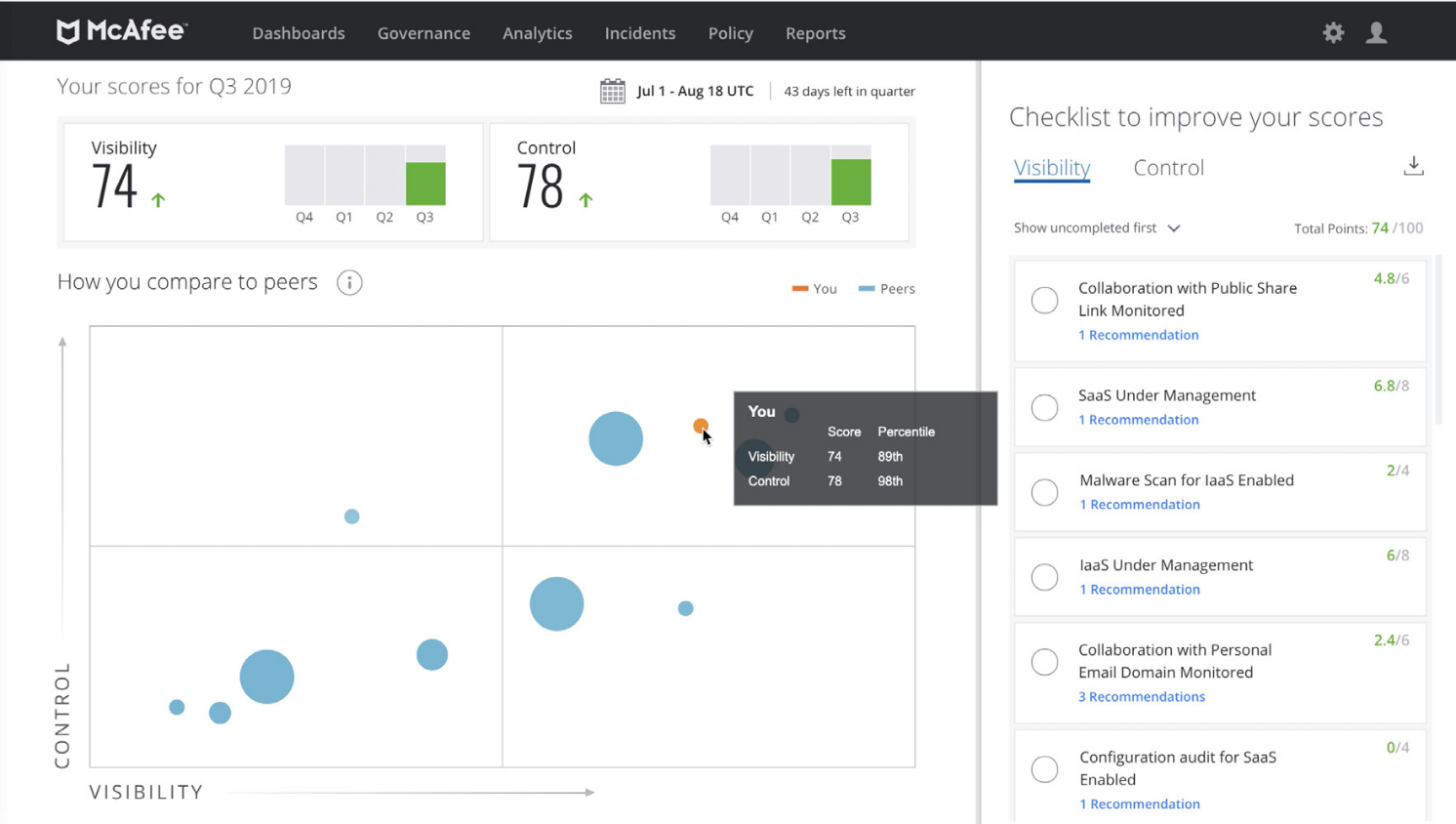


Рис. 3.6. Квадрант Cloud Security Advisor

Рекомендації щодо захисту хмари. Підприємствам пропонується набір індивідуальних розпорядчих рекомендацій щодо підвищення рівня хмарної безпеки. рекомендації відсортовані в порядку першочерговості. Кожній рекомендації присвоєно певну кількість балів залежно від ступеня потенційного впливу.

**MVISION Cloud for Containers**. Природним продовженням віртуалізації є контейнерні робочі навантаження. Вони оптимізовані, що дозволяє в повній мірі використовувати переваги хмари. MVISION Cloud Container Security надає єдину платформу безпеки хмарних обчислень. На платформі реалізовані стратегії оптимізованого використання контейнерів з метою забезпечити безпеку динамічних, постійно мінливих контейнерних робочих навантажень і інфраструктури, від якої вони залежать.

MVISION Cloud for Containers виконує наступні функції:

Оцінка вразливості компонентів контейнера. Функція оцінює вбудований в контейнери код під час компонування і потім, через певні проміжки часу, щоб визначити, чи піддаються контейнери відомим ризикам або ці ризики знижуються. Тим самим зменшується ймовірність проникнення зловмисників в контейнерну робоче навантаження.

Управління станом хмарної безпеки для контейнерної інфраструктури та систем оркестрації типу Kubernetes. Функція дозволяє стежити за тим, щоб конфігурація середовища не була джерелом ризику та для того, щоб конфігурація середовища не змінювалася з часом, стаючи схильною до ненавмисному ризику.

Наносегментація для комунікації між контейнерами. Принцип Zero Trust («нульової довіри»): не довіряй, а перевіряй. Виявляє дії в мережі комунікації між запущеними в контейнерах процесами і здійснює моніторинг цих дій, використовуючи методи, відповідні динамічному характеру контейнерів і не враховують зовнішні фактори, такі як IP-адреса. Виявляє випадки аномальної комунікації і сповіщає про них користувача або блокує їх (в залежності від уподобань користувача). Виявляє зміни в шаблонах комунікації між версіями контейнерів згодом при зміні додатків. Використовує в якості способу забезпечити захист робочих навантажень гарантовано працездатні конфігурації, не прагнучи встежити за еволюцією свідомо «поганих» конфігурацій [10].

# ВИСНОВКИ

У першому розділі роботи були розглянуті наступні моделі надання послуг за допомогою хмари: це інфраструктура як послуга (IaaS), платформа як послуга (PaaS) і програмне забезпечення як послуга (SaaS). Хмара може бути розгорнута як: приватна, публічна, громадська або гібридна, персональна.

При використанні хмарних технологій, компанії можуть знизити витрати на побудову центрів обробки даних, закупівлю серверного та мережевого обладнання, апаратних і програмних рішень. В майбутньому організації будуть все частіше будувати свою роботу за межами периметра мережі, відповідно, вектор щодо забезпечення інформаційної безпеки буде поступово зміщуватися в бік захисту хмарної інфраструктури, де будуть зберігатися критично важливі для бізнесу даних. Хмари поступово стають переважною частиною інфраструктури компаній, кількість хмарних споживачів в найближчі роки значно збільшиться, тому компаніям доведеться приділяти пильну увагу питанням забезпечення безпеки доступу в хмари і захисту даних, що зберігаються в ньому.

В другому розділі були розглянуті основні рішення CASB. CASB є рішенням, яке дозволяє організаціям запобігати непередбаченим загрозам, створювані різноманітністю хмарних сервісів. Розглянутий клас рішень контролює доступ, трафік, завантаження і зберігання даних на хмарних платформах, наочно представляючи інформацію про використання дозволених і недозволених, відповідно до встановлених політиками ІБ в кожній конкретній організації, хмарних сервісів і додатків. CASB запобігає несанкціоновані дії користувачів з правами доступу, виявляє аномальну активність, в тому числі пов'язану з діями різних шкідливих програм. Незважаючи на те, що в даний час ринок рішень класу CASB ще знаходиться на стадії розвитку, вибір постачальників величезний. На світовому ринку вже представлені і активно використовуються компаніями різних сфер діяльності майже два десятка рішень.

В третьому розділі дипломної роботи було розглянуто заходи щодо забезпечення безпеки в хмарі, серед яких присутні такі рекомендації як: використання багатофакторної автентифікацію і шифрування, організація адекватного контролю доступу, використання інструментів захисту і раннього виявлення загроз.

Також, для забезпечення безпеки рекомендується використовувати CASB. Одними з ключових функцій є:

* контроль діяльності;
* дотримання політик безпеки і правил в хмарної інфраструктурі;
* підтримання продуктів всіх найбільших постачальників служб SaaS;
* контроль використання хмари;
* захист інформації від несанкціонованого доступу;
* захист даних від зовнішніх і внутрішніх загроз;
* захист хмари від впровадження шкідливих програм і подальшого поширення.

# ПЕРЕЛІК ПОСИЛАНЬ

* 1. What is Cloud Computing and Who Uses Cloud Services? [Електронний ресурс] – Режим доступу: https://www.simplilearn.com/tutorials/cloud-computing-tutorial/what-is-cloud-computing

1. Wayne Jansen, Timothy Grance Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, 2011. [Електронний ресурс] – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-144/SP800- 144.pdf
2. 12 Benefits of Cloud Computing [Електронний ресурс] – Режим доступу: https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/
3. Top 7 Most Common Uses of Cloud Computing [Електронний ресурс] – Режим доступу: https://www.ibm.com/cloud/blog/top-7-most-common-uses-of-cloud-computing
4. Top Cloud Computing Security Threats To Watch For [Електронний ресурс] – Режим доступу: https://www.horangi.com/blog/7-cloud-computing-security-threats-to-watch-for
5. Cloud Access Security Brokers (CASBs) [Електронний ресурс] – Режим доступу: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs
6. CLOUD ACCESS SECURITY BROKER (CASB) [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-access-security-broker-casb/
7. What Is a CASB? [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/security/what-is-a-casb.html#~choosing-a-casb
8. Magic Quadrant for Cloud Access Security Brokers [Електронний ресурс] – Режим доступу: <https://www.gartner.com/doc/reprints?id=1-1XOEZTG0&ct=191024&st=sb> (дата доступу 28.08.2020)
9. 7 Best Cloud Access Security Brokers (CASB) [Електронний ресурс] – Режим доступу: https://www.comparitech.com/net-admin/best-cloud-access-security-brokers/
10. McAfee MVISION Cloud / Лист даних [Електронний ресурс] – Режим доступу: <https://www.mcafee.com/enterprise/ru-ru/products/mvision-cloud.html>
11. Cloud Computing Attacks: What Are They and How to Prevent Them? [Електронний ресурс] – Режим доступу: https://www.computer.org/publications/tech-news/trends/prevent-cloud-computing-attacks

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)