

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія контролю доступу до хмарних ресурсів організації на базі
Microsoft Defender for Cloud Apps»**

зі спеціальності

F5 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

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

Владислав ОЛІФЕРЧУК

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61

ОЛІФЕРЧУК Владислав

(прізвище, ім'я)

Керівник

д.ф., доцент СОБЧУК Андрій

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	3
ВСТУП.....	4
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ.....	7
1.1. Аналіз проблеми контролю доступу до хмарних ресурсів в організаціях.....	7
1.2. Аналіз основних загроз і ризиків несанкціонованого доступу до хмарних ресурсів.....	10
1.3. Методологічні основи управління доступом у хмарному середовищі.....	18
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ НА БАЗІ MICROSOFT DEFENDER FOR CLOUD APPS	20
2.1. Аналіз характеристик хмарного середовища, що впливають на безпеку та доступ	20
2.2. Порівняння існуючих рішень для контролю доступу до хмарних ресурсів	22
2.3. Призначення та основні функції Microsoft Defender for Cloud Apps.....	35
3 ТЕХНОЛОГІЯ КОНТРОЛЮ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ НА БАЗІ MICROSOFT DEFENDER FOR CLOUD APPS....	40
3.1. Технологія застосування Microsoft Defender for Cloud Apps.....	40
3.2. Рекомендації щодо забезпечення контролю доступу до хмарних ресурсів організації.....	45
3.3. Рекомендації щодо контролю доступу до хмарних ресурсів на базі Microsoft Defender for Cloud Apps	48
ВИСНОВКИ	52
ПЕРЕЛІК ПОСИЛАНЬ.....	54
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	56

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

SaaS – Software as a Service

IaaS – Infrastructure as a Service

PaaS – Platform as a Service

AWS – Amazon Web Services

GCP – Google Cloud Platform

NIST – National Institute of Standards and Technology

IAM – Identity and Access Management

MFA – Multi-Factor Authentication

SSO – Single Sign-On

CSPM – Cloud Security Posture Management

CASB – Cloud Access Security Broker

CIEM – Cloud Infrastructure Entitlement Management

CDR – Cloud Detection and Response

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation and Response

CI/CD – Continuous Integration and Continuous Delivery

DevSecOps – Development, Security and Operations

OAuth 2.0 – Open Authorization 2.0

DDoS – Distributed Denial of Service

ВСТУП

Хмарні сервіси стали базовою складовою цифрової інфраструктури організацій, оскільки дозволяють швидко масштабувати обчислювальні ресурси, спрощують співпрацю між підрозділами та забезпечують доступ до корпоративних даних і застосунків незалежно від місця перебування користувача. Разом із перевагами хмарна модель суттєво змінює характер ризиків: ресурси стають доступними через публічні мережі, зростає кількість інтеграцій і зовнішніх підключень, а контроль доступу виходить за межі традиційного мережевого периметра. У таких умовах ключовим фактором безпеки стає керування ідентичностями та правилами доступу до даних і сервісів, а не лише захист інфраструктури як такої.

Особливістю хмарного середовища є те, що значна частина доступу до ресурсів відбувається через веб-інтерфейси та API, з використанням різних пристроїв і каналів підключення. Це створює широкий спектр сценаріїв зловживань: використання викрадених облікових даних, доступ із некерованих пристроїв, некоректне налаштування дозволів, неконтрольоване поширення файлів, а також використання сторонніх SaaS-сервісів без погодження з IT-підрозділом. Навіть за наявності багатофакторної автентифікації ризики не зникають повністю, оскільки порушення можуть відбуватися вже після входу користувача в сервіс, коли виконуються небажані операції з даними або змінюються параметри доступу. Тому контроль доступу в хмарі має охоплювати як момент автентифікації, так і контроль дій у межах сесії та подальший моніторинг активності.

У цьому контексті актуальним стає використання платформ, що поєднують видимість використання хмарних застосунків, виявлення ризикових сценаріїв і застосування політик доступу та захисту даних.

Одним із таких рішень є Microsoft Defender for Cloud Apps, яке забезпечує контроль доступу до хмарних сервісів, підтримує виявлення тіньових застосунків, дозволяє застосовувати правила до дій користувачів у сесії та забезпечує спостережуваність через журнали активності. Інтеграція з екосистемою Microsoft, зокрема з Microsoft Entra, створює можливість реалізувати узгоджену модель доступу, у якій умови входу доповнюються контролем операцій із даними та реакціями на ризикову поведінку.

Об'єкт дослідження – контроль доступу до хмарних ресурсів організації.

Предмет дослідження – технологія контролю доступу до хмарних ресурсів організації на базі Microsoft Defender for Cloud Apps.

Мета роботи – розробити порядок застосування технології контролю доступу до хмарних ресурсів організації та сформулювати рекомендації щодо її реалізації на базі Microsoft Defender for Cloud Apps.

Наукові завдання:

визначити ключові ризики та загрози, характерні для доступу до хмарних ресурсів;

узагальнити підходи до побудови моделі контролю доступу з урахуванням контексту підключення та чутливості даних;

проаналізувати функціональні можливості Microsoft Defender for Cloud Apps;

описати варіант впровадження засобів контролю доступу та моніторингу активностей;

сформулювати практичні рекомендації щодо застосування політик доступу й сесійного контролю та перевірки їх ефективності.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, узагальнення рекомендацій з безпеки хмарних середовищ, порівняльний аналіз підходів до контролю доступу, систематизація практичних сценаріїв застосування політик безпеки.

Практичне значення одержаних результатів Практичне значення одержаних результатів: запропоновано порядок застосування Microsoft Defender for Cloud Apps для контролю доступу до хмарних ресурсів організації та сформовано рекомендації, які можуть бути використані як основа для впровадження керованих політик доступу й сесійного контролю, виявлення та обмеження Shadow IT, а також моніторингу активностей користувачів і реагування на ризикові дії у хмарних застосунках.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми контролю доступу до хмарних ресурсів в організаціях

Упродовж останніх років швидкість і зручність переходу до хмарних технологій суттєво змінили підходи організацій до розроблення та експлуатації програмного забезпечення. Водночас зростання залежності від хмарної інфраструктури призвело до розширення площини атак, якою необхідно керувати. Хмарні середовища створюють додаткові ризики, пов'язані з неправильними налаштуваннями, помилками конфігурації або ненавмисним відкриттям доступу до ресурсів (зокрема сховищ даних), що не завжди може бути ефективно виявлено традиційними засобами захисту, орієнтованими на периметр або локальну інфраструктуру.

У таких умовах ключовим є розуміння того, які активи організації опиняються під загрозою, та які механізми мають бути застосовані для їх захисту. Типові проблеми безпеки хмарних обчислень охоплюють як уразливості, що виникають на етапі розроблення, так і ризики, пов'язані з конфігурацією й експлуатацією хмарних сервісів. Відповідно, підхід до забезпечення безпеки має включати практичні заходи, що охоплюють повний цикл — від програмного коду до налаштувань і політик у хмарі.

Хмарні обчислення розглядаються як модель надання обчислювальних послуг, зокрема сховищ, серверів, баз даних і мережевих можливостей, через мережу Інтернет замість використання виключно локальної інфраструктури. Організації отримують доступ до спільного пулу конфігурованих ресурсів, які надаються провайдером, і можуть змінювати їх обсяг відповідно до поточних потреб. Така масштабованість є однією з причин активного впровадження хмари, оскільки дозволяє гнучко підтримувати змінні навантаження та розвиток

цифрових процесів без необхідності пропорційного розширення власного апаратного середовища.

У визначеннях NIST модель хмарних обчислень характеризується п'ятьма ключовими властивостями: самообслуговуванням на вимогу, широким мережевим доступом, об'єднанням ресурсів, швидкою еластичністю та вимірюваним сервісом. Сукупність цих характеристик забезпечує можливість самостійного виділення ресурсів організацією, спільного використання інфраструктури з належними механізмами ізоляції та прозоре споживання послуг за моделлю оплати відповідно до фактичного використання.

Провайдери хмарних послуг, зокрема Azure та Google Cloud, надають ці сервіси разом із вбудованими механізмами безпеки та інструментами адміністрування. На практиці найбільш поширеними моделями надання є SaaS, PaaS та IaaS, які відрізняються рівнем керованості, розподілом відповідальності та ступенем контролю з боку організації. Вибір моделі впливає на те, які саме механізми захисту необхідно забезпечувати на стороні організації, а які — реалізуються на стороні провайдера.

Застосування хмарних моделей також змінює підхід до безпечної розробки та експлуатації програмного забезпечення, оскільки частина задач безпеки переміщується за межі традиційного мережевого периметра та інтегрується у процеси розроблення, налаштування й керування сервісами. У сукупності зазначені моделі формують основу сучасних практик побудови, розгортання та супроводження прикладних систем у хмарі, одночасно підвищуючи вимоги до організації контролю доступу, конфігурації та моніторингу хмарних ресурсів.

Для багатьох компаній хмарна модель є практичним способом підвищити швидкість змін, зменшити витрати та підтримувати конкурентоспроможність без необхідності утримувати складну локальну інфраструктуру. Замість придбання й обслуговування дорогого серверного обладнання організація отримує можливість оплачувати лише фактично спожиті ресурси та оперативно змінювати їх обсяг відповідно до поточних потреб. Така еластичність дає змогу швидко адаптуватися до коливань попиту, технологічних змін та різких піків навантаження, що особливо актуально для сервісів із нерівномірним трафіком.

Хмарні платформи також забезпечують підтримку віддаленої та розподіленої роботи, надаючи співробітникам доступ до систем і даних практично з будь-якого місця за умови застосування механізмів автентифікації, авторизації та політик доступу. Окрім цього, хмара створює сприятливі умови для прискорення життєвого циклу розроблення програмного забезпечення, оскільки у межах єдиного середовища можуть інтегруватися інструменти розроблення, тестування, розгортання та моніторингу, а також засоби автоматизації процесів на етапах SDLC.

У результаті підвищується ефективність взаємодії між підрозділами, спрощується масштабування процесів, зростає операційна продуктивність і скорочується час виведення продукту на ринок. Водночас такі переваги супроводжуються новими вимогами до управління ризиками, оскільки розширення хмарних сервісів і кількості підключених користувачів ускладнює контроль доступу, конфігурацій та подій безпеки. Тому використання хмарних технологій потребує усвідомлення характерних загроз і впровадження механізмів захисту, які забезпечують безпечне використання хмарних ресурсів паралельно з отриманням очікуваних переваг.

Безпека даних у хмарних обчисленнях ускладнюється тим, що інформація постійно переміщується між різними середовищами, командами та межами доступу, а взаємодія із сервісами часто відбувається через мережу та зовнішні інтерфейси. Провайдери хмарних послуг забезпечують захист базової інфраструктури, застосовуючи вбудовані механізми, зокрема шифрування та ведення журналів доступу. Водночас на стороні організації залишається відповідальність за те, як саме дані обробляються, які політики доступу встановлюються та наскільки коректно налаштовані хмарні ресурси й параметри безпеки.

Такий підхід формує розподіл відповідальності між провайдером і клієнтом, причому конкретні межі відповідальності залежать від моделі сервісу. Однак незалежно від моделі, контроль захисту компонентів, що розміщені «всередині» хмари, є постійною задачею організації. Недостатньо надійна автентифікація, надмірні привілеї доступу та відсутність актуальності для

інтерфейсів прикладного програмування можуть створювати умови для компрометації чутливих активів. У цьому контексті безпека хмарних даних орієнтована на збереження інформації приватною та доступною для легітимних користувачів, що узгоджується з базовими принципами тріади CIA: конфіденційності, цілісності та доступності.

Для зниження ризиків необхідним є впровадження контрольованих механізмів доступу, зокрема використання багатофакторної автентифікації та чітко визначених правил авторизації. Додатково важливим є застосування підходу Zero Trust, у межах якого кожний запит на доступ підлягає перевірці, а довіра не надається автоматично жодному користувачу чи пристрою. Така логіка підсилює контроль доступу до хмарних ресурсів і зменшує ймовірність зловживань у разі компрометації облікових даних.

Критичною умовою ефективного захисту є наявність достатньої видимості подій і стану конфігурацій у хмарному середовищі, особливо коли організація має дотримуватися вимог регуляторних або галузевих стандартів. Засоби управління станом безпеки хмарного середовища забезпечують таку видимість, фіксуючи відхилення від заданих політик, помилки конфігурації та ризики, які виникають під час експлуатації. За відсутності подібного контролю навіть одна помилка — наприклад, некоректно налаштоване сховище даних або надто широкі права, надані ключу доступу до API, — може призвести до суттєвих наслідків у вигляді витоку інформації або компрометації ресурсів [1].

1.2. Аналіз основних загроз і ризиків несанкціонованого доступу до хмарних ресурсів

У процесі використання хмарних технологій організації щоденно стикаються з різними факторами, що впливають на рівень захищеності: ризиками, загрозами та практичними труднощами впровадження безпеки. Ці поняття часто сприймаються як тотожні, однак у контексті хмарної безпеки вони мають різний зміст. Розмежування зазначених термінів є важливим, оскільки дозволяє точніше визначати пріоритети захисту хмарних активів, коректно

формувати вимоги до контролю доступу та обирати відповідні механізми безпеки.

Ризик у хмарному середовищі доцільно розуміти як потенційну можливість втрати даних або наявність слабкого місця, яке може бути використане для порушення безпеки. Загроза, своєю чергою, характеризує джерело або тип атаки, тобто конкретного порушника, його наміри та можливі техніки, які можуть бути застосовані для реалізації атаки. Практичні труднощі (виклики) відображають організаційні та технічні бар'єри, що заважають ефективно впроваджувати безпеку в хмарі, зокрема у питаннях регламентів доступу, розподілу відповідальності, автоматизації контролів та підтримки належного рівня видимості подій.

Для ілюстрації відмінностей можна розглянути типовий приклад, пов'язаний із використанням API. Публічно доступна API-кінцева точка, розміщена у хмарі та відкрита для звернень із мережі Інтернет, формує ризик, оскільки створює потенційну поверхню атаки й може стати каналом доступу до чутливих даних. У цьому випадку загрозою виступає зловмисник, який намагається отримати несанкціонований доступ через цю кінцеву точку, використовуючи відповідні техніки (наприклад, підбір параметрів, обхід перевірок, зловживання авторизацією тощо). Водночас практичний виклик для організації полягає в тому, щоб забезпечити належний рівень захисту публічних API, не порушивши їх доступність для легітимних користувачів і клієнтів, для яких ці інтерфейси є необхідними.

Повноцінна стратегія хмарної безпеки повинна враховувати всі три аспекти, оскільки кожний із них описує проблему з різної точки зору. З одного боку, стратегія має зменшувати ризики шляхом впровадження контрольних заходів безпеки та коректної конфігурації ресурсів. З іншого боку, необхідно забезпечувати протидію загрозам через безпечну розробку, належне розгортання та технічні механізми захисту, що ускладнюють або унеможливають реалізацію атак. Окремо важливо усувати організаційні та технічні труднощі, впроваджуючи узгоджені процеси, практики та інструменти, які дозволяють

організації використовувати хмарні ресурси з прогнозованим рівнем безпеки та підтримувати розвиток бізнес-процесів без зниження захищеності.

Повністю усунути ризики в хмарному середовищі неможливо, однак вони можуть бути керованими за умови своєчасного виявлення та впровадження відповідних контролів. Розуміння типових ризиків дозволяє організації завчасно підготуватися до проблем, які найчастіше виникають під час експлуатації хмарних ресурсів, та сформувати практичні механізми контролю доступу, моніторингу й управління конфігураціями. До найбільш поширених ризиків, що впливають на безпеку хмарної інфраструктури, належать неконтрольована площа атак, людський фактор, помилки конфігурації та компрометація даних.

Площа атак у хмарі визначається сумарною «експозицією» середовища, тобто тим, які компоненти, сервіси та інтерфейси доступні ззовні або потенційно можуть бути виявлені й використані порушником. Поширення мікросервісної архітектури, збільшення кількості окремих робочих навантажень і публічно доступних сервісів призводить до того, що кожний новий компонент фактично додає нову точку потенційного впливу. За недостатнього управління організація може не мати повної картини того, що саме є доступним із мережі Інтернет, і виявити проблему лише після виникнення інциденту. Окрему складність створюють непрямі витoki інформації, коли навіть без прямого доступу до ресурсу зловмисник може отримувати допоміжні дані, які спрощують підготовку атаки (наприклад, через аналіз мережових запитів чи метаданих). Це підкреслює, що використання публічної хмари й публічного Інтернету саме по собі формує певний рівень зовнішньої експозиції, який необхідно постійно контролювати.

Суттєвим ризиком для хмарної безпеки є людський фактор. У процесі розроблення, адміністрування та експлуатації систем помилки користувачів, адміністраторів або розробників залишаються одним із найчастіших джерел інцидентів. Особливістю хмарних платформ є те, що їх зручність і швидкість роботи з сервісами можуть підвищувати ймовірність неконтрольованих дій, коли команди починають використовувати API або сервіси без належних політик доступу та без узгоджених процедур безпеки. У таких умовах ризик посилюється тим, що помилка або необережна дія можуть одразу впливати на ресурси,

доступні ззовні. Зниження впливу людського фактора досягається не лише навчанням персоналу, а передусім впровадженням процесів і технічних “обмежувачів”, які підтримують правильні рішення за замовчуванням і мінімізують наслідки помилок у конфігураціях та доступах.

Окремою категорією ризиків є помилки конфігурації. Хмарні провайдери постійно розширюють перелік сервісів, а кількість доступних параметрів налаштувань зростає. Додатково ситуація ускладнюється використанням декількох хмарних платформ одночасно, оскільки різні провайдери можуть мати відмінні підходи до конфігурацій за замовчуванням, різні моделі доступу та особливості реалізації сервісів. У таких умовах організація, яка не має сталих практик безпеки й контролю конфігурацій, може залишати некоректні налаштування, що в подальшому експлуатуються порушниками. Саме помилки конфігурації часто стають “точкою входу”, яка дозволяє зловмиснику перейти від розвідки до прямого впливу на ресурси й дані.

Найбільш критичним наслідком реалізації ризиків у хмарі є витік або компрометація даних (data breach), коли чутлива інформація залишає межі контролю організації без її відома чи дозволу. Дані є ключовою ціллю більшості атак, оскільки можуть бути використані для фінансової вигоди, подальших фішингових кампаній, шантажу або завдання репутаційної шкоди. Неправильні конфігурації та відсутність достатнього захисту на етапі експлуатації можуть призвести до того, що ресурси з даними стають доступними для несанкціонованого отримання. Наслідки витоку залежать від типу даних: персональна інформація може використовуватися для крадіжки ідентичності або соціальної інженерії, а внутрішні документи й корпоративна переписка — для дискредитації організації, порушення її процесів або створення тиску на бізнес.

Управління ризиками безпеки в хмарі базується на системному підході, що включає регулярну оцінку ризиків і виявлення нових слабких місць, пріоритизацію та впровадження контрольних заходів безпеки відповідно до їх критичності, а також документування ризиків, які організація свідомо приймає, із подальшим періодичним переглядом таких рішень. Така модель дозволяє підтримувати керованість хмарних ресурсів, зменшувати вплив типових загроз і

забезпечувати прогнозований рівень захисту під час розвитку хмарної інфраструктури.

У хмарному середовищі загроза розглядається як атака на хмарні активи, спрямована на використання наявного ризику або слабкого місця. На відміну від ризику, який описує потенційну вразливість або можливу втрату, загроза характеризує активну дію порушника, метод атаки або сценарій впливу, у межах якого ризик перетворюється на реальний інцидент. Визначення типових загроз є важливим для формування захисту, оскільки дозволяє співвіднести конкретні сценарії атак із відповідними технічними та організаційними механізмами протидії.

Однією з поширених загроз для хмарних середовищ є експлуатація вразливостей нульового дня. Навіть за умов коректно налаштованої хмарної інфраструктури організація залишається залежною від програмного забезпечення, що використовується на різних рівнях — від операційних систем і компонентів платформи до прикладних сервісів. Вразливості нульового дня є небезпечними тим, що на момент атаки виробник ще не надав виправлення, а отже зловмисник може використати невідомий або непублічний дефект для отримання первинного доступу до середовища. У хмарному контексті це створює ризик «точки входу», який не знімається лише за рахунок правильних конфігурацій, оскільки експлуатація може відбуватися на рівні програмних компонентів.

Окремою категорією є АРТ, що описують складні та цілеспрямовані атаки з довготривалою присутністю порушника в середовищі. На відміну від коротких «разових» атак, АРТ-кампанії передбачають закріплення у системі, приховане переміщення між ресурсами та послідовний пошук цінної інформації протягом тривалого часу. Небезпека таких атак полягає у здатності поєднувати різні техніки — зокрема починати з використання уразливості (в тому числі нульового дня), а далі тривалий час залишатися непоміченими, поступово збільшуючи рівень доступу та збираючи чутливі дані.

Важливим сценарієм є внутрішні загрози, що виникають з боку осіб, які мають легітимний доступ до ресурсів організації. Як правило, до цієї категорії

належать поточні або колишні співробітники, підрядники чи інші суб'єкти, які можуть мати доступ до корпоративних систем, даних та знання про внутрішні процеси. Особливість внутрішніх загроз полягає в тому, що дії порушника можуть виглядати як легітимні операції, а використання наданих прав доступу ускладнює виявлення інциденту. Це підсилює вимоги до принципу найменших привілеїв, моніторингу дій користувачів і контролю доступу до хмарних ресурсів на основі контексту.

Широкою групою загроз є кібератаки, під якими розуміються спроби несанкціонованого доступу до мережі або системи з метою модифікації, викрадення, знищення чи розголошення інформації. У практиці хмарної безпеки поширеними є такі типи атак, як шкідливе програмне забезпечення, фішинг, атаки відмови в обслуговуванні, SQL-ін'єкції, а також атаки, пов'язані з IoT. Для організацій, які використовують хмарні сервіси, ці загрози актуальні, оскільки хмарна інфраструктура часто інтегрована з публічними інтерфейсами та має широкі сценарії віддаленого доступу.

З огляду на різноманіття можливих атак, захист хмарних активів доцільно вибудовувати на основі базових практичних принципів. По-перше, важливо дотримуватися стандартів безпечної розробки під час створення мікросервісів і застосунків, оскільки значна частина інцидентів починається з вразливостей прикладного рівня. По-друге, критичним є системний контроль конфігурацій хмарних ресурсів, який зменшує ймовірність помилок та “проломів” у налаштуваннях доступу. По-третє, за наявності сформованого базового рівня захисту доцільним є проактивний підхід у вигляді пошуку загроз і аномалій у середовищі, що дозволяє виявляти приховані сценарії атак до того, як вони призведуть до суттєвих наслідків.

Практичні виклики хмарної безпеки доцільно розглядати як розрив між теоретично правильними вимогами та реальними умовами впровадження захисту в організації. Усвідомлення необхідності стратегії безпеки саме по собі не вирішує питання, з чого починати, як змінювати підходи в командах і які щоденні дії забезпечують стабільний результат. У цьому контексті типові виклики охоплюють нестачу компетенцій і сформованої стратегії, складність

управління ідентичностями та доступами, проблему несанкціонованого використання хмарних сервісів (Shadow IT), а також потребу дотримання вимог комплаєнсу.

Одним із базових викликів є відсутність цілісної стратегії хмарної безпеки та нестача профільних навичок. Традиційні моделі захисту, характерні для локальних дата-центрів, не повністю відповідають хмарній архітектурі, де інфраструктура є динамічною, керується через API та змінюється швидше. Для ефективного контролю доступу, моніторингу та конфігурацій необхідні специфічні знання про сервіси провайдера, принципи побудови хмарних ресурсів та типові сценарії ризиків. Наявність гнучкості й швидкості в хмарі може одночасно підсилювати вразливості, якщо організація не має достатньої внутрішньої експертизи для розуміння наслідків рішень. Особливо критичними є помилки в трактуванні моделі розподіленої відповідальності, яка визначає зони відповідальності провайдера та клієнта: неправильне розуміння цих меж може призводити до того, що окремі задачі захисту залишаються невиконаними, створюючи «невидимі» прогалини, які згодом експлуатуються порушниками.

Другий важливий виклик пов'язаний з управлінням ідентичностями та доступом. Хоча необхідність IAM є очевидною, складність полягає у практичній реалізації: для великої організації потрібно визначити ролі, права та політики для тисяч користувачів і сервісних облікових записів, не створюючи надмірних привілеїв і не ускладнюючи робочі процеси. Цілісний підхід до IAM доцільно формувати через три взаємопов'язані складові: проєктування ролей, управління привілейованим доступом (PAM) та впровадження ролей у конкретній хмарній платформі. Проєктування ролей має базуватися на реальних функціях користувачів і виконуваних задачах та виконуватися незалежно від конкретного інструмента, що дозволяє зберігати сталість моделі доступу під час зміни постачальника або розширення хмарної інфраструктури. Управління привілейованим доступом визначає, які ролі потребують підвищеного захисту через критичність наданих прав, а також передбачає обмеження кола осіб із доступом до привілейованих облікових даних і регулярну ротацію таких даних. Після цього реалізація ролей у сервісах IAM провайдера стає більш

контрольованою, оскільки організація вже має узгоджену модель доступів і може уникати хаотичного надання прав.

Третій виклик становить Shadow IT — використання хмарних сервісів і ресурсів поза межами стандартних процедур погодження та управління. Причиною є те, що співробітники, зокрема розробники, можуть швидко створювати ресурси у хмарі для виконання робочих задач, використовуючи власні облікові записи й мінімальний набір налаштувань. У результаті виникають активи, які можуть бути недостатньо захищеними, залишатися з типовими конфігураціями або надмірно широкими правами доступу. Додатково проблему ускладнює поширення DevOps-підходів, де команди прагнуть мінімізувати “тертя” та працювати з високою швидкістю змін. За відсутності узгодженого механізму отримання видимості й контролю з боку підрозділу безпеки посилення контролів може сприйматися як перешкода для DevOps, тоді як реальна потреба полягає у вбудуванні безпеки у CI/CD-процеси та уніфікації підходів так, щоб безпека отримувала необхідні дані без уповільнення розгортань. Таким чином, організаційною задачею є пошук балансу між швидкістю впровадження змін і керованістю безпеки на темпах, характерних для хмари.

Четвертий виклик пов’язаний із комплаєнсом у хмарі. Організації повинні дотримуватися вимог нормативних документів і галузевих стандартів, які регламентують роботу з чутливими даними (наприклад, платіжна інформація або медичні записи). У межах виконання таких вимог часто необхідно обмежувати доступ, фіксувати дії користувачів, контролювати операції з даними та мати можливість підтверджувати виконання політик. Якщо заходи контролю доступу не визначені або реалізовані непослідовно, ускладнюється моніторинг доступів і дотримання регламентів, що підвищує ризик порушень і створює проблеми під час внутрішніх або зовнішніх перевірок. У цьому контексті ефективний контроль доступу до хмарних ресурсів виступає не лише засобом захисту від загроз, а й практичним інструментом забезпечення відповідності вимогам щодо обробки та збереження даних [2].

1.3. Методологічні основи управління доступом у хмарному середовищі

У хмарному середовищі контроль доступу набуває центрального значення, оскільки ресурси надаються як сервіс і доступні через мережеві інтерфейси, а керування ними здійснюється переважно через облікові записи, ролі та API. Сутність хмарних обчислень як моделі спільного пулу конфігурованих ресурсів із можливістю швидкого виділення й вивільнення потужностей зумовлює високу динамічність середовища та підвищені вимоги до керованості доступу. У практичному вимірі це означає, що безпека залежить не стільки від «периметра», скільки від коректності ідентифікації суб'єктів доступу, обмеження їхніх повноважень і постійного контролю виконуваних дій у хмарі.

Важливою передумовою побудови захисту є розуміння моделі розподіленої відповідальності між хмарним провайдером і клієнтом. Провайдер забезпечує захист базової інфраструктури та сервісної платформи, тоді як організація відповідає за конфігурації, керування обліковими записами, політики доступу та безпеку даних у межах власних робочих навантажень. Така логіка прямо впливає на те, як визначаються межі контролю доступу: навіть за наявності вбудованих механізмів безпеки провайдера критичним залишається налаштування ролей, привілеїв, умов доступу та моніторинг подій безпеки з боку організації.

Підхід до контролю доступу в хмарі узгоджується з принципами Zero Trust, де кожен запит на доступ розглядається як потенційно ризиковий і має перевірятися з урахуванням контексту. У моделі Zero Trust доступ надається через логіку «точки прийняття рішення» та «точки застосування політики», а правила формуються максимально гранулярно з опорою на принцип найменших привілеїв. Це зменшує наслідки компрометації облікового запису та обмежує можливості горизонтального переміщення порушника в середовищі [3].

З позиції практичної реалізації контроль доступу до хмарних ресурсів зазвичай спирається на поєднання автентифікації, авторизації та умовних політик доступу. Автентифікація підтверджує, хто саме ініціює дію (користувач,

сервіс, застосунок), тоді як авторизація визначає, що дозволено робити в межах наданих прав. Оскільки значна частина ризиків у хмарі пов'язана з надмірними привілеями та помилками конфігурації, ключовими вимогами виступають стандартизація ролей, контроль привілейованих облікових записів і застосування додаткових факторів перевірки (наприклад, MFA) у сценаріях підвищеного ризику. На цьому рівні принципово важливо, щоб політики доступу були узгоджені з бізнес-ролями та реальними задачами користувачів, а не формувалися ситуативно під окремі запити, оскільки саме «точкові» винятки найчастіше створюють довгострокові прогалини в безпеці.

Окремий клас задач виникає у випадку доступу до хмарних застосунків (передусім SaaS), де контроль необхідний не лише на етапі входу, але й у межах сесії користувача. У таких сценаріях застосовуються механізми, що дозволяють у реальному часі відстежувати й обмежувати дії користувачів у хмарних сервісах на основі політик доступу та політик сесії. З практичної точки зору це важливо для зниження ризиків витоку даних та зловживань доступом, коли формально «легітимний» користувач або скомпрометований обліковий запис намагається виконати небезпечні операції (наприклад, масове завантаження даних або доступ із нетипового середовища).

У контексті побудови технології контролю доступу до хмарних ресурсів доцільно також враховувати потребу видимості та керованості використання хмарних застосунків на рівні організації. Для цього застосовуються підходи класу CASB, які орієнтовані на забезпечення прозорості використання хмарних сервісів, підтримку політик безпеки та контроль активностей користувачів у хмарі. У межах такої логіки Microsoft Defender for Cloud Apps позиціонується як рішення, що поєднує видимість і контроль над хмарними застосунками, включно з механізмами адаптивного контролю доступу та можливостями аналізу активностей. Це створює основу для практичної реалізації контролю доступу не лише через «статичні» права, а й через динамічні політики, що враховують ризики, поведінкові ознаки та умови виконання сесії [4].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ НА БАЗІ MICROSOFT DEFENDER FOR CLOUD APPS

2.1. Аналіз характеристик хмарного середовища, що впливають на безпеку та доступ

Контроль доступу в хмарній інфраструктурі доцільно розглядати не як окреме налаштування “вхід/вихід”, а як систему правил, яка визначає хто саме звертається до ресурсу, за яких умов це відбувається, які дії дозволені та як фіксуються події доступу для подальшого аналізу. У хмарі ресурси часто керуються через API та інтеграції, а користувачі працюють із сервісами віддалено; тому доступ формується не лише людськими входами через інтерфейс, а й автоматизованими запитами застосунків, сценаріїв і служб. Саме через це в межах технології контролю доступу важливо чітко визначати суб’єкти доступу та механізми, через які вони отримують повноваження.

У практиці управління доступом до хмарних ресурсів суб’єкти доступу поділяються на дві великі групи: людські та service-to-service. До людських належать працівники, адміністратори, підрядники та інші користувачі, які взаємодіють із хмарними застосунками й даними. До service-to-service належать сервіси, застосунки, агенти автоматизації, компоненти CI/CD та інші технічні сутності, які виконують дії від імені системи або інтеграції. Для другої групи в корпоративних середовищах характерне використання сервісних облікових записів, які представляють “не людину”, а програмну сутність (API, сервіс, застосунок), і працюють у межах заданого контексту безпеки [5].

У екосистемі Microsoft важливе місце займають service principals та managed identities, які використовуються як технологічна основа для автентифікації застосунків і сервісів без необхідності “вшивати” статичні облікові дані у код. Service principal виступає представленням застосунку в Microsoft Entra ID і може отримувати дозволи та права доступу, необхідні для роботи інтеграції. При цьому managed identity є спеціалізованим підходом, коли

для ресурсу створюється керована ідентичність у Entra ID, а доступ до сервісів надається без збереження секретів у кодї; така модель знижує ризики витоку ключів і спрощує контроль доступу на рівні ролей та дозволів.

Наступним базовим елементом технології контролю доступу є автентифікація — перевірка того, ким є суб'єкт доступу. У сучасних корпоративних системах ця задача не обмежується паролем, оскільки підвищення рівня довіри до ідентичності напряду впливає на зниження ризиків компрометації облікових записів. У цьому контексті корисною є логіка, закладена в підходах NIST до цифрової ідентичності: окремо розглядаються питання підтвердження ідентичності, стійкості автентифікації та довіри при федерації (коли доступ забезпечується через зовнішнього постачальника ідентичності). Це підкреслює, що “однакова” автентифікація для всіх сценаріїв не завжди є оптимальною, а рівень перевірки має відповідати критичності ресурсу та ризику доступу [6].

Після автентифікації ключовим стає етап авторизації — визначення дозволених дій. Для хмарних застосунків і API-платформ типово застосовуються токен-орієнтовані підходи, де доступ реалізується через надання обмежених повноважень застосунку або користувачу. Одним з базових стандартів, на якому побудовано багато сучасних інтеграцій, є OAuth 2.0: він описує механізм отримання обмеженого доступу до HTTP-сервісу як від імені користувача, так і “самостійно” від імені застосунку. Для організації це означає, що контроль доступу часто зводиться до коректного управління токенами, областями доступу, часом життя доступу та умовами, за яких видаються або приймаються такі токени.

Оскільки значна частина корпоративних сценаріїв пов'язана із SaaS-застосунками та віддаленою роботою, реальний контроль доступу залежить не лише від того, “чи можна увійти”, а й від того, що дозволено робити після входу. На цьому рівні виникає потреба в механізмах, які забезпечують контроль сесії: обмеження завантаження даних, контроль дій у межах застосунку, реагування на ризикові сценарії (наприклад, нетипова поведінка або спроби масового доступу до даних). У Microsoft Defender for Cloud Apps реалізовано підхід Conditional

Access App Control, який використовує політики доступу та політики сесій для моніторингу й контролю доступу користувачів до хмарних застосунків у режимі реального часу. Це дозволяє переносити акцент із “разового дозволу” на постійно керований доступ під час роботи користувача в застосунку.

Важливим практичним аспектом є те, що контроль доступу в хмарі має враховувати не лише права, а й контекст: тип пристрою, місце підключення, характер запиту, ознаки аномальної активності та критичність даних, до яких здійснюється звернення. Саме тому технологія контролю доступу зазвичай поєднує кілька “шарів”: статичні ролі й дозволи, додаткові умови доступу (наприклад, вимоги до способу автентифікації), а також динамічні обмеження на рівні сесій у хмарних застосунках. У сукупності це формує керовану модель, у якій доступ не є “постійним привілеєм”, а перетворюється на контрольований процес із чіткими правилами, журналюванням подій і можливістю швидкого реагування.

Таким чином, технологія контролю доступу до хмарних ресурсів організації спирається на чітке розділення суб’єктів доступу, коректну побудову автентифікації, застосування стандартизованих механізмів авторизації (зокрема токен-орієнтованих підходів), а також на контроль сесій у хмарних застосунках.

2.2. Порівняння існуючих рішень для контролю доступу до хмарних ресурсів

Інструменти безпеки хмарного середовища — це програмні засоби, призначені для захисту хмарної інфраструктури організації, її прикладних систем і даних від актуальних та нових кіберзагроз. Їх призначення полягає у тому, щоб забезпечити керованість доступу, контроль конфігурацій, виявлення підозрілої активності та зниження ризиків, які виникають унаслідок використання хмарних сервісів, віддалених моделей роботи та широкої інтеграції бізнес-процесів із цифровими платформами.

Традиційно засоби захисту інформаційних систем значною мірою будувалися навколо периметру: застосовувалися мережеві екрани та подібні

механізми, а припущенням було те, що ізольована й «охоронювана» корпоративна мережа є відносно безпечним середовищем. Однак поширення хмарних технологій змінило цю логіку, оскільки дані та сервіси перестали бути прив'язаними до одного фізичного майданчика чи локального серверного сегмента. Інформаційні потоки почали циркулювати між різними локаціями, пристроями та сервісами, а доступ до ресурсів усе частіше здійснюється через мережеві інтерфейси та API. У результаті вимоги до захисту еволюціонували від статичних периметрових підходів до моделі, у якій контроль безпеки “супроводжує” активи організації незалежно від того, де саме вони обробляються та як використовуються.

Прискорене впровадження інструментів хмарної безпеки також зумовлюється низкою практичних чинників. По-перше, для багатьох організацій характерним стало використання багатохмарної моделі, коли одночасно застосовуються декілька платформ або поєднуються різні типи сервісів, що ускладнює уніфікацію політик і створює ризик “розривів” у захисті. По-друге, у хмарі діє модель розподіленої відповідальності: провайдер забезпечує захист базової інфраструктури, тоді як організація відповідає за налаштування безпеки власних застосунків, даних, облікових записів та політик доступу. По-третє, зростає тиск вимог комплаєнсу, оскільки організаціям необхідно підтверджувати належний рівень контролю доступу, журналювання подій і захисту чутливих даних відповідно до норм і стандартів, що діють у конкретній галузі та юрисдикції.

З огляду на ці умови інструменти хмарної безпеки мають бути гнучкими, автоматизованими та масштабованими, а також придатними до застосування в різних платформах і сценаріях. Практична цінність таких засобів полягає у можливості централізовано керувати політиками безпеки, швидко виявляти відхилення в конфігураціях, контролювати доступ користувачів і сервісів, а також підтримувати необхідний рівень видимості подій у середовищі організації.

Узагальнюючи, якщо для локальної інфраструктури акцент робився на “зміцненні периметру”, то в хмарному середовищі організації ключовою стає безперервна керованість доступу, стану конфігурацій і активностей у кожному

сервісі та кожній критичній зоні обробки даних, із можливістю швидкого реагування та підтвердження виконання вимог безпеки.

Інструменти хмарної безпеки є критично важливими для організацій, оскільки інциденти в хмарному середовищі напряду впливають на безперервність бізнес-процесів. Порушення доступності сервісів, компрометація облікових записів або витік даних здатні призводити до простоїв ІТ-систем, зупинки ключових операцій, втрат доходів і додаткових витрат на відновлення. Особливістю таких ситуацій є те, що фінансові наслідки простою можуть швидко накопичуватися, а фактичний збиток визначається не лише тривалістю інциденту, а й критичністю сервісів, що були недоступні для клієнтів та внутрішніх користувачів.

Паралельно зростає інтенсивність і різноманітність атак на хмарні активи організацій. У практиці кіберзахисту суттєву роль відіграють компрометації облікових записів і зловживання доступом, оскільки обліковий запис у хмарі фактично виступає “ключем” до даних і сервісів. Ураження може відбуватися як через фішинг і викрадення облікових даних, так і через експлуатацію вразливостей, помилки конфігурацій, некоректно захищені API, а також через внутрішні зловживання з боку користувачів із легітимним доступом. У багатьох випадках атаки здійснюються організованими групами, які використовують системний підхід: поєднують різні техніки доступу, намагаються закріпитися в середовищі та поступово розширювати привілеї, щоб отримати контроль над даними або вплинути на роботу сервісів.

Додатковим чинником, що підсилює потребу в інструментах хмарної безпеки, є посилення вимог до захисту даних і відповідності регуляторним нормам. Для організації це означає необхідність не лише реалізувати захист “фактично”, а й підтримувати керованість процесів: визначати політики доступу, забезпечувати журналювання дій, контролювати обробку чутливої інформації та бути готовими підтверджувати виконання вимог під час перевірок. Через постійні зміни вимог і практик загроз підтримка актуального стану безпеки стає окремою постійною задачею, яка потребує автоматизації й централізованого контролю.

Водночас важливо враховувати модель розподіленої відповідальності: хмарний провайдер забезпечує захист базової інфраструктури платформи, тоді як організація відповідає за безпеку власних даних, доступів, конфігурацій і прикладних компонентів. Тобто стійкість хмарного середовища значною мірою визначається тим, наскільки послідовно налаштовані ролі й дозволи, чи застосовуються додаткові механізми перевірки доступу, чи контролюються ризикові дії користувачів і чи є видимість подій у хмарних застосунках.

Таким чином, інструменти хмарної безпеки є необхідною складовою захисту сучасної організації, оскільки забезпечують практичну можливість керувати доступом, знижувати ризики компрометації облікових записів, підвищувати стійкість до атак та підтримувати безперервність роботи сервісів за умов постійної зміни загроз і вимог до захисту даних.

У практиці забезпечення безпеки хмарних ресурсів організації використовуються сукупність спеціалізованих інструментів, які закривають різні “шари” середовища: конфігурації інфраструктури, дані, робочі навантаження, доступ користувачів, інтеграції через API, мережеві взаємодії та відновлення після інцидентів. Така різноманітність пояснюється тим, що у хмарі джерелом ризику можуть бути як помилки налаштувань і надмірні привілеї, так і вразливості застосунків, неконтрольовані інтеграції, а також недостатня видимість реальної активності користувачів і сервісів. Відповідно, інструменти хмарної безпеки зазвичай не є “одним продуктом на все”, а формують керований набір класів рішень, які доповнюють одне одного та можуть інтегруватися в єдину систему моніторингу й реагування.

Одним із базових класів є Cloud Security Posture Management — інструменти контролю “стану безпеки” хмарної інфраструктури. Їх призначення полягає у безперервному виявленні небезпечних або некоректних конфігурацій у середовищі (наприклад, надмірно відкриті ресурси, помилки в налаштуваннях доступу, відхилення від політик). CSPM-логіка важлива саме для організацій, які мають складну структуру хмарних ресурсів, кілька підписок/акаунтів та активний темп змін, оскільки ручний контроль конфігурацій у таких умовах стає нестійким. Типовою вимогою є можливість автоматизованого виявлення

проблем і, за потреби, автоматичного виправлення або принаймні формування чітких рекомендацій та сповіщень.

Поруч із CSPM окремо виділяються інструменти Data Security Posture Management, які фокусуються не на інфраструктурі, а на самих даних. У межах DSPM виконується автоматизоване виявлення й класифікація даних, визначення місць зберігання, шляхів переміщення та суб'єктів доступу. Для організації це критично, оскільки реальні ризики часто пов'язані не з “фактом існування сервісу”, а з тим, де знаходиться чутлива інформація, хто має до неї доступ і чи не виникають небезпечні сценарії використання (наприклад, надмірні дозволи, незахищений обмін, некоректно налаштовані ключі доступу). DSPM також використовується як основа для підтримки вимог комплаєнсу, коли необхідно мати контрольовану картину обробки даних.

Для захисту обчислювальних компонентів хмари застосовуються Cloud Workload Protection Platforms, які забезпечують захист робочих навантажень — віртуальних машин, контейнерів і безсерверних функцій — у процесі виконання. Такі засоби орієнтовані на виявлення підозрілої поведінки, контроль уразливостей і підтримку актуального стану систем (зокрема через керування патчів і перевірки конфігурацій workload-рівня). У практиці розрізняються підходи агентного та безагентного контролю: агентний забезпечує глибшу видимість і оперативне реагування, але потребує супроводу та ресурсів на workloads; безагентний швидше масштабується й простіший у впровадженні, однак може давати менше “живої” телеметрії. У складних середовищах часто застосовується комбінована модель, щоб уникнути прогалин.

Окремо важливим для теми контролю доступу є клас Cloud Access Security Broker. CASB розглядається як засіб, що забезпечує керований контроль взаємодії користувачів із хмарними застосунками та сервісами: виявляє використання несанкціонованих сервісів (shadow IT), допомагає запроваджувати політики доступу й захисту даних, а також підтримує аудит активностей. На практиці CASB реалізується двома типовими способами. API-орієнтований підхід інтегрується з хмарними сервісами через їхні API та працює “поза трафіком”, що зручно для інвентаризації, ретроспективного аналізу, перевірок

відповідності та політик на рівні об'єктів у хмарі. Проксі-орієнтований підхід пропускає трафік користувачів через контрольну точку та дозволяє застосовувати політики під час сесії, що є корисним для оперативного блокування ризикових дій (наприклад, завантаження/вивантаження даних).

Проблема надмірних прав доступу в багатохмарних середовищах закривається класом Cloud Infrastructure Entitlement Management. Такі інструменти аналізують фактичні дозволи, виявляють “overprivileged” облікові записи та допомагають реалізувати принцип найменших привілеїв. Для організації це важливо, оскільки навіть один привілейований або некоректно налаштований обліковий запис здатен стати точкою масштабного інциденту — від некоректних змін конфігурації до доступу до даних, які не повинні бути доступними даному суб'єкту.

Для виявлення інцидентів і реагування у хмарі застосовується клас Cloud Detection and Response. Такі засоби використовують поведінкову аналітику й методи виявлення аномалій, аналізують активність користувачів, запити до хмарних API, події конфігурацій та сигнали безпеки. Практично важливою є інтеграція CDR з SIEM/SOAR, що дозволяє не обмежуватися “попередженнями”, а автоматизувати реакції — наприклад, блокування ризикових сесій, ізоляцію скомпрометованих облікових записів або обмеження доступу до чутливих ресурсів.

Окремим напрямом є безпека контейнерів і Kubernetes, оскільки контейнеризовані середовища мають власні специфічні ризики: уразливі образи, помилки налаштувань кластерів, некоректне керування секретами, надмірні дозволи на рівні ролей у кластері. У межах життєвого циклу DevOps такі інструменти інтегруються з CI/CD і реєстрами образів, щоб виявляти проблеми ще до розгортання в продуктивному середовищі, а також контролювати поведінку контейнерів під час виконання.

Базовим “каркасом” доступу у хмарі виступає Identity and Access Management, який забезпечує управління цифровими ідентичностями, ролями, привілеями та процесами автентифікації. Для корпоративного середовища типовими є підтримка SSO, MFA, федерації ідентичності та role-based access

control. IAM задає, хто може працювати з ресурсами та в яких межах, а інші класи інструментів (зокрема CASB/CIEM/CDR) розширюють цей контроль за рахунок контексту, аналізу активності та політик на рівні сесії й даних.

Оскільки API часто є “шаром інтеграції” між сервісами, окремо виділяються інструменти безпеки API. Їх роль полягає у забезпеченні коректної автентифікації й авторизації, аналізі трафіку на аномалії, веденні інвентаризації API та контролі використання, а також у підтримці звітності й контролів відповідності. У корпоративному середовищі це важливо тому, що API можуть перетворюватися на прямі точки входу для атак у разі слабких політик доступу, помилок у перевірках запитів або неконтрольованих ключів доступу.

Мережевий рівень у хмарі підтримується класом Cloud Network Security, який охоплює механізми сегментації, фільтрації вхідного/вихідного трафіку, контролю міжсервісних взаємодій та моніторингу мережевих аномалій. Це забезпечує “технічні межі” між сегментами середовища й зменшує можливості для горизонтального переміщення порушника у випадку часткової компрометації.

Щоб зменшувати ризики експлуатації відомих слабких місць, використовується керування вразливостями у хмарі, яке включає безперервне сканування інфраструктури та застосунків, пріоритизацію знайдених проблем і підтримку процесів виправлення. Для організації принципово важливим є не лише “знайти”, а й вчасно закрити уразливість до того, як вона стане практичним шляхом атаки, особливо в середовищі з великою кількістю сервісів і швидкими релізами.

Окремий блок забезпечення стійкості формують резервне копіювання та аварійне відновлення. Ці засоби підтримують безперервність бізнесу в разі інцидентів, збоїв або руйнівних подій, забезпечують механізми відновлення даних і сервісів, а також допомагають виконувати вимоги щодо зберігання даних та перевірки готовності до відновлення.

Узагальнено, перелічені класи інструментів дозволяють вибудувати комплексну модель хмарної безпеки організації: від контролю конфігурацій і доступів до захисту даних, виявлення атак, реагування та відновлення.

Поряд із використанням окремих класів інструментів безпеки в організаціях поширюється підхід до впровадження інтегрованих платформ, які поєднують ключові функції захисту в межах одного рішення. У цьому контексті розглядаються Cloud-Native Application Protection Platforms — платформи, орієнтовані на централізований контроль безпеки хмарно-нативних робочих навантажень і підтримку узгоджених політик у межах єдиного контуру керування. Практична логіка такого підходу полягає в тому, що організація отримує узгоджену видимість подій та стану середовища і може застосовувати політики захисту без необхідності підтримувати велику кількість окремих компонентів із різними інтерфейсами та правилами.

Застосування CNAPP підходу є доцільним у ситуаціях, коли пріоритетом є уніфікація процесів безпеки й отримання наскрізної видимості по хмарних навантаженнях. Це особливо актуально для організацій, які використовують гібридні або багатохмарні архітектури та потребують послідовного застосування політик у різних середовищах. Інтегрована модель також зменшує операційне навантаження, оскільки скорочується кількість розрізнених систем, які потрібно окремо налаштовувати, інтегрувати та супроводжувати. Додатково важливою є підтримка DevSecOps-процесів: коли контроль безпеки інтегровано у цикл розробки та розгортання, проблеми простіше виявляти на ранніх етапах і швидше усувати, узгоджуючи дії команд розробки й безпеки.

Водночас необхідно враховувати, що універсальні платформи не завжди забезпечують рівень спеціалізації, притаманний “кращим у класі” рішенням. У практиці це проявляється в тому, що окремі функції можуть бути реалізовані достатньо широко, але не завжди з максимальною глибиною для специфічних сценаріїв. Тому підхід best-of-breed може бути більш виправданим у випадках, коли організація має підвищені вимоги до окремих напрямів безпеки, уже експлуатує зрілі засоби захисту та прагне зберегти гнучкість у виборі інструментів для кожної категорії. Така модель також дає змогу зменшувати залежність від одного постачальника, однак потребує більш складної інтеграції, узгодження політик та кореляції подій між різними системами.

Отже, у межах хмарної безпеки організації практично застосовуються два взаємодоповнювальні підходи: або формування набору спеціалізованих інструментів за ключовими категоріями, або впровадження інтегрованої платформи, яка централізує видимість і керованість. Вибір між ними визначається архітектурою хмарного середовища, зрілістю існуючих процесів безпеки, вимогами до контролю доступу й комплаєнсу, а також ресурсами, доступними для супроводу й інтеграції рішень.

У межах вибору та побудови засобів хмарної безпеки для організації окрему роль відіграють вбудовані інструменти захисту, які постачальники хмарних платформ надають разом із власною інфраструктурою. Як правило, такі інструменти найкраще інтегровані у “рідні” сервіси провайдера, підтримують типові сценарії адміністрування та формують базовий рівень контролю за подіями, конфігураціями й ризиками в конкретній хмарі. Водночас їх застосування має природне обмеження: вони орієнтовані насамперед на внутрішню екосистему відповідного провайдера, тому за умов гібридної або багатохмарної архітектури організація часто доповнює їх зовнішніми рішеннями для централізації політик, розширення видимості та покриття “перетинів” між платформами.

Для середовищ Amazon Web Services (AWS) характерним є використання набору нативних сервісів, які закривають основні задачі моніторингу та захисту. Зокрема, механізми на кшталт GuardDuty застосовуються для виявлення підозрілої активності й ознак атак, Security Hub агрегує результати перевірок і сигнали безпеки в єдиному огляді, CloudTrail забезпечує журналювання викликів API та дій користувачів, AWS Config відповідає за безперервне відстеження стану конфігурацій ресурсів, а Inspector використовується для автоматизації процесів виявлення уразливостей у робочих навантаженнях. Перевагою такого підходу є тісна інтеграція з сервісами AWS і підтримка типових workflow адміністрування, однак при використанні інших провайдерів або значній частці SaaS-застосунків організація змушена розширювати контур безпеки за рахунок інструментів, які працюють “поверх” кількох середовищ. Окремо на практиці часто виникає потреба у більш глибокому контролі саме чутливих даних, їх

класифікації та контексту доступу, що не завжди повністю закривається нативними механізмами, і тоді застосовуються рішення класу DSPM або інші засоби управління ризиками витоку даних.

У випадку Microsoft Azure інструменти безпеки зазвичай будуються як частина ширшої Microsoft-екосистеми, що спрощує централізацію керування та кореляцію подій між сервісами. Для прикладу, сервіси на кшталт Defender for Cloud використовуються для оцінювання стану безпеки, контролю рекомендацій і захисту робочих навантажень, Microsoft Sentinel реалізує хмарний контур SIEM/SOAR для збору подій, аналітики та автоматизації реагування, а Key Vault застосовується для безпечного зберігання секретів, ключів шифрування та сертифікатів. Додатково Azure Arc дозволяє поширювати політики та моніторинг на гібридні сценарії, коли частина ресурсів розміщена поза Azure. Разом із тим у практичних сценаріях організацій часто з'являється вимога до більш детальної видимості саме по чутливих даних і їх використанню, зокрема у хмарних застосунках (SaaS), де питання контролю доступу виходить за межі лише “хмарної інфраструктури” та переходить до контролю дій користувача в конкретному сервісі.

Для Google Cloud Platform (GCP) характерним є акцент на підходах нульової довіри та архітектурі, де кожен запит проходить автентифікацію та авторизацію незалежно від “місця” походження. У цьому контексті Security Command Center використовується як центральний елемент оцінювання ризиків, виявлення загроз і контролю відповідності, Cloud Asset Inventory допомагає формувати карту ресурсів і політик для задач управління та аудиту, а BeyondCorp відображає реалізацію принципів Zero Trust для контролю доступу на рівні користувача й пристрою. Як і у випадку інших провайдерів, сильні сторони нативних інструментів проявляються у глибокій інтеграції з власними сервісами, тоді як задачі контекстної класифікації чутливих даних та наскрізної видимості в багатохмарних сценаріях часто потребують додаткових зовнішніх рішень.

Окремо варто враховувати відмінності між open-source та комерційними засобами хмарної безпеки. Відкриті інструменти на кшталт Trivy (сканування контейнерних образів), CloudSploit (контроль конфігурацій у стилі CSPM),

CloudMapper (візуалізація середовищ AWS), OSSEC (host-based IDS) або OpenVAS (сканер уразливостей) можуть бути корисними для вузьких задач, пілотів або як допоміжні компоненти, коли потрібна гнучкість і мінімальні витрати на ліцензування. Водночас у корпоративному середовищі типово критичними стають фактори, які open-source інструменти не завжди забезпечують у потрібному обсязі: централізована інтеграція, масштабована аналітика, гарантована підтримка, безперервні оновлення та зручні механізми впровадження політик і реагування. Комерційні рішення в таких умовах зазвичай краще підходять для побудови цілісного процесу безпеки, оскільки орієнтовані на повне покриття сценаріїв, стабільність експлуатації та відповідність вимогам організації.

Одним із рішень, яке закриває саме контроль доступу до хмарних ресурсів і застосунків на рівні організації, а не лише на рівні окремої хмари. У цій ролі розглядається Microsoft Defender for Cloud Apps, що належить до класу CASB і використовується для виявлення та контролю використання хмарних застосунків, формування політик доступу й поведінки користувачів, а також для керування ризиковими діями в межах сесій. На практиці це дає можливість отримати узгоджену видимість по SaaS-сервісах, виявляти небажані сценарії доступу, застосовувати обмеження до операцій із даними та підсилювати модель Zero Trust у частині “користувач — хмарний сервіс”. Саме тому перехід від загального переліку інструментів хмарної безпеки до розгляду Microsoft Defender for Cloud Apps є обґрунтованим: він переводить фокус із “захисту платформи” на контроль доступу й активностей у хмарних сервісах, що є ключовим для організаційних сценаріїв.

Для організації вибір інструментів хмарної безпеки має виконуватися не за принципом “чим більше продуктів — тим краще”, а як керований процес, у якому засоби захисту відповідають реальним ризикам, архітектурі середовища та можливостям експлуатації. Практично це означає, що перед придбанням або розгортанням рішень доцільно сформувати рамку оцінювання, яка дозволяє зіставити потреби організації з функціональними можливостями інструментів і умовами їх інтеграції.

Початковим етапом є оцінювання поточного рівня зрілості хмарного середовища та безпекових процесів. На практиці важливо розуміти, чи перебуває організація на етапі базового налаштування хмари та міграції сервісів, чи вже експлуатує гібридну або багатохмарну архітектуру з великою кількістю ресурсів, користувачів і інтеграцій. Від цього залежить необхідний рівень покриття: для частини організацій критичним є контроль конфігурацій і ресурсів, для інших — управління ідентичностями та привілеями, для третіх — контроль доступу до хмарних застосунків і захист даних у SaaS-сервісах. Окремо має враховуватися покриття API, оскільки API інтеграції часто перетворюються на один із ключових каналів доступу до даних і функцій хмарних сервісів.

Наступним аспектом є сумісність і інтеграційні можливості. У корпоративному середовищі інструменти безпеки мають не лише “вміти захищати”, а й коректно вбудовуватися в існуючий технологічний стек організації. Критичними стають можливості API-інтеграцій, підтримка автоматизації та взаємодія з наявними засобами моніторингу і реагування (наприклад, SIEM/SOAR, системи обробки інцидентів і заявок, платформи журналювання подій). Важливим є й питання наскрізної видимості: за наявності кількох середовищ організація або формує єдиний контур спостережуваності, або змушена працювати з розрізненими панелями керування, що збільшує ризик пропуску інцидентів і ускладнює аудит. Окремо оцінюється масштабованість — чи зберігає рішення ефективність при зростанні кількості ресурсів, сервісів і користувачів, а також наскільки гнучко воно підтримує розширення політик у процесі розвитку інфраструктури.

Вибір інструментів безпеки також залежить від підходу до архітектури захисту: застосування інтегрованої платформи або набору спеціалізованих рішень. Інтегровані платформи зручні тим, що спрощують керування та дають централізовану картину стану середовища, однак за окремими напрямками можуть поступатися “кращим у класі” рішенням за глибиною функціональності. Спеціалізований підхід, навпаки, дозволяє підібрати найсильніший інструмент у кожній категорії, але потребує більшого обсягу робіт з інтеграції, узгодження політик і супроводу кількох постачальників. Для організації це означає

необхідність обирати баланс між якістю контролів, складністю керування та ресурсами, доступними для експлуатації.

Окремий блок вимог формують питання відповідності та регуляторних зобов'язань. Для організації важливо, щоб рішення підтримувало ведення журналів активності, створювало перевірюваний слід подій та дозволяло формувати звіти, необхідні для внутрішнього контролю та аудитів. Вимога комплаєнсу в цьому контексті не зводиться лише до “наявності звітів”: суттєвими є можливість пов'язати події безпеки з конкретними об'єктами і забезпечити керованість політик доступу, які впливають на реальні бізнес-процеси.

Після вибору інструментів істотне значення має стратегія впровадження. У корпоративних умовах більш стабільним підходом є поетапне розгортання: початкове впровадження в окремому середовищі або підрозділі з подальшим масштабуванням, що дозволяє перевірити ефективність політик і зменшити ризики порушення робочих процесів. Важливою умовою є залучення відповідальних сторін — ІТ, безпеки, власників сервісів і розробників — оскільки саме на стику цих ролей найчастіше виникають проблеми з доступами, винятками та практичним застосуванням політик. Окремо враховується навчання персоналу: для команди безпеки — в частині експлуатації інструментів і реагування, для ширшого кола користувачів — у частині впливу нових правил на щоденну роботу. Контроль успішності впровадження доцільно вимірювати через практичні показники, наприклад скорочення кількості помилкових конфігурацій, зменшення інцидентів доступу, підвищення якості журналювання та стабільність проходження перевірок.

При цьому типові ускладнення мають бути враховані заздалегідь: проблеми інтеграції вирішуються через використання API-орієнтованих підходів і тестування в контрольному середовищі; “втома від сповіщень” зменшується шляхом налаштування політик на пріоритетні ризики та використання автоматизації для відсікання шуму; опір змінам з боку команд знижують через узгодження вимог безпеки з реальними workflow та раннє залучення

відповідальних осіб; фінансові ризики обмежуються завдяки контролю моделі ліцензування та загальної вартості володіння.

Важливим критерієм вибору є також повна вартість володіння, оскільки витрати організації складаються не лише з ліцензії, а й з інтеграції, налаштувань, навчання, супроводу та операційного навантаження. Оцінювання має включати й прогнозування змін у масштабі використання, щоб уникати ситуацій, коли рішення стає економічно невигідним через зростання обсягів даних, кількості ресурсів або користувачів. У цьому контексті додатково враховується доцільність інвестицій у захист порівняно з потенційними втратами від інцидентів і простоїв, оскільки реальний економічний ефект безпеки проявляється в запобіганні збиткам.

Узагальнюючи, підбір інструментів хмарної безпеки для організації має будуватися як баланс між ефективністю контролів, складністю керування та витратами, з урахуванням масштабованості, інтеграційних можливостей і вимог до контролю доступу [7].

2.3. Призначення та основні функції Microsoft Defender for Cloud Apps

Після порівняння класів засобів хмарної безпеки логічним кроком є перехід до платформи, яка дає централізований огляд стану захищеності хмарних ресурсів і водночас підтримує виявлення загроз. У цьому контексті Microsoft Defender for Cloud розглядається як базовий сервіс для керування хмарною безпекою на рівні конфігурацій, рекомендацій та сигналів про інциденти. Його цінність для організації полягає в тому, що контроль безпеки не зводиться до окремих перевірок вручну, а підтримується постійним моніторингом середовища, підсвічуванням ризиків і наданням технічно конкретних кроків для їх зниження.

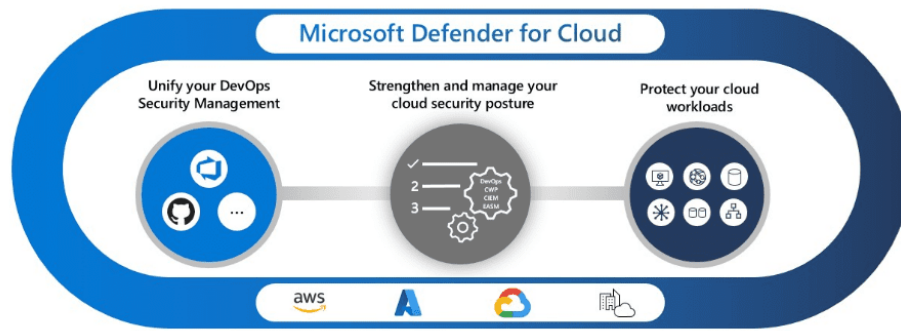


Рис.2.1 Концепція Microsoft Defender for Cloud

За функціональною логікою Defender for Cloud поєднує два взаємодоповнювальні напрями. Перший — Cloud Security Posture Management, що зосереджується на стані захищеності: знаходить небезпечні налаштування, прогалини в контролях та відхилення від базових вимог безпеки, а також дозволяє відстежувати динаміку змін. Другий — захист робочих навантажень і подієва складова, яка дає змогу виявляти підозрілу активність та формувати сповіщення безпеки з контекстом, потрібним для реагування. Така комбінація важлива саме для організаційного середовища, де ризики часто виникають через накопичення дрібних помилок конфігурації, а не лише через складні техніки атак.

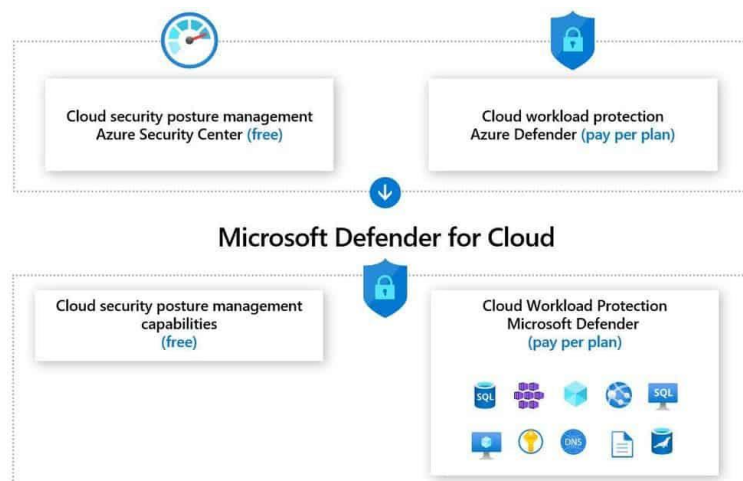


Рис.2.2. Розмежування можливостей Defender for Cloud

Сервіс надає уніфікований індикатор стану — Secure score, який агрегує результати оцінювання в один показник і дозволяє швидко зрозуміти, де

середовище має найбільші прогалини. Практичний сенс цього механізму в тому, що він не просто фіксує факт проблеми, а прив'язує його до конкретних рекомендацій: при усуненні невідповідностей Secure score зростає, а загальний рівень ризику зменшується. Це зручно як для технічної команди, так і для узгодження пріоритетів, бо з'являється проста метрика, яка відображає прогрес підсилення захисту.

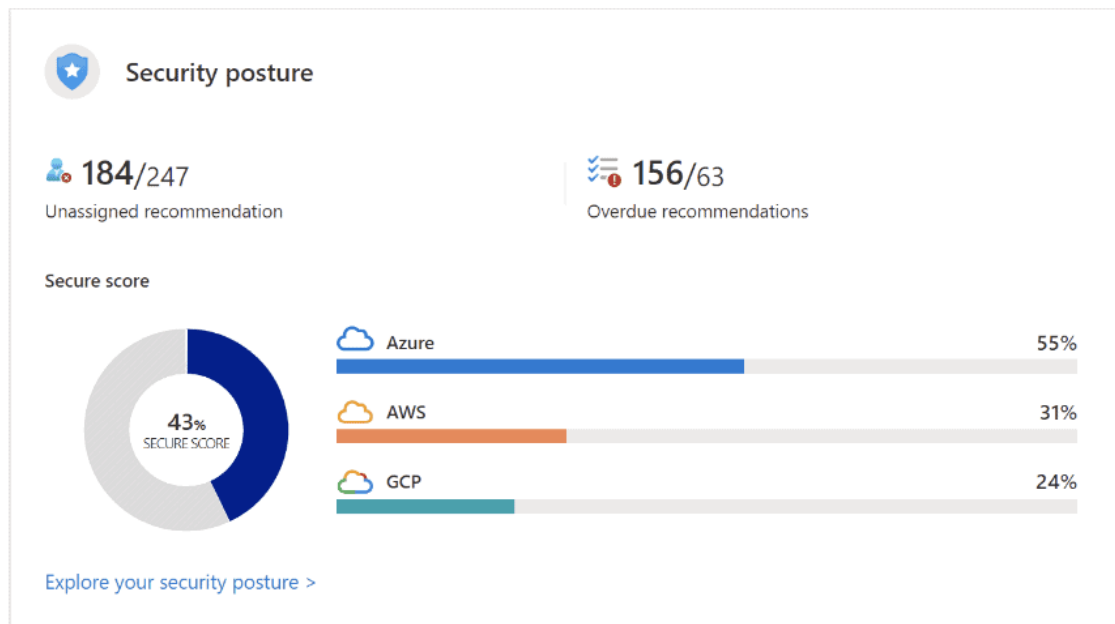


Рис.2.3. Security posture та Secure score для кількох хмарних середовищ.

Важливий момент — спосіб пріоритизації рекомендацій. Defender for Cloud використовує механізм оцінювання ризику, який враховує контекст ресурсу (зокрема конфігурацію, мережеві зв'язки та загальний стан безпеки), потенційну ймовірність експлуатації та бізнес-вплив. У результаті рекомендації впорядковуються не за формальною критичністю, а за тим, наскільки реальним є сценарій компрометації в конкретному середовищі. Для організації це означає, що першими підсвічуються проблеми, які дають найкоротший шлях до інциденту, а не просто найдовший перелік за чеклістом.

Окремо варто підкреслити багатохмарний та гібридний аспект. У реальних умовах організації часто мають не лише Azure-ресурси, а й частину сервісів в інших хмарах або в гібридному форматі. Defender for Cloud підтримує підключення AWS-акаунтів і GCP-проектів, щоб у єдиному інтерфейсі

отримувати огляд середовищ і застосовувати спільну логіку контролю безпеки. Це корисно для зниження фрагментації: без такого підходу команди вимушені працювати в декількох панелях, порівнювати сигнали вручну та ризикувати пропустити слабе місце на стику систем.

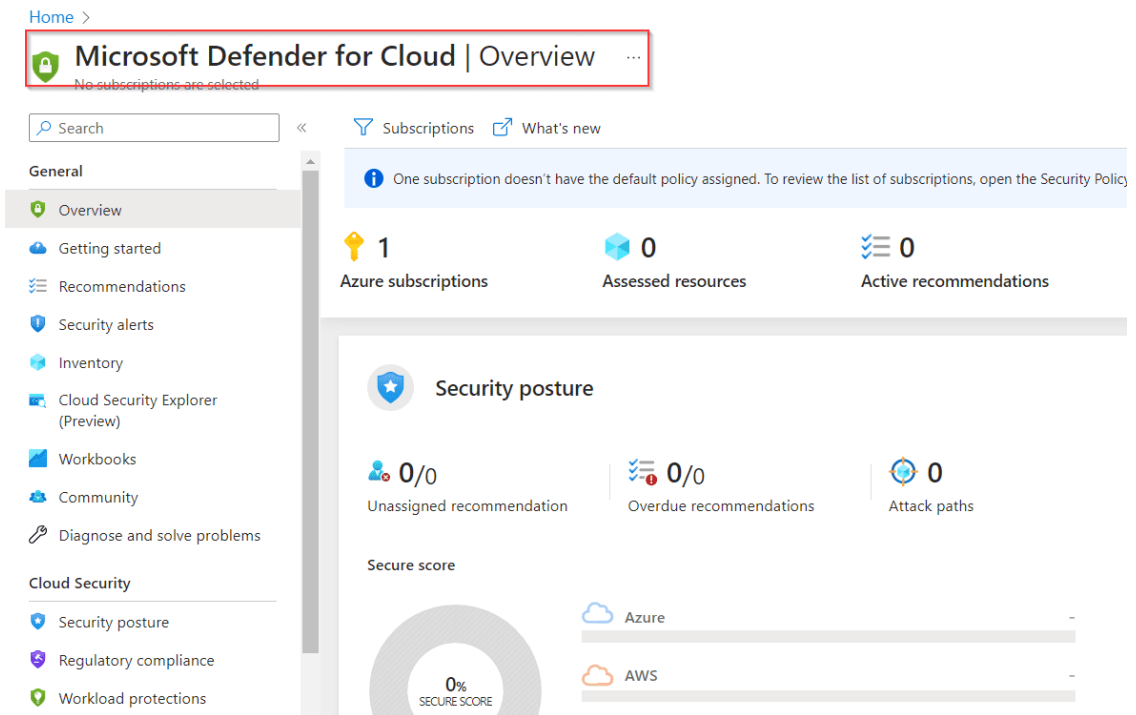


Рис.2.4. Інтерфейс Microsoft Defender for Cloud в Azure Portal

Ще один практичний блок — відповідність вимогам і контроль виконання базових стандартів безпеки. Regulatory compliance dashboard призначений для того, щоб безперервно оцінювати ресурси щодо контролів відповідності та показувати, які саме невідповідності блокують досягнення потрібного рівня. Це спрощує внутрішній контроль і підготовку до аудитів: замість ручного збору доказів з різних сервісів формується централізована картина, де кожна прогалина має технічне пояснення і пов'язані рекомендації.

З точки зору операційної безпеки важливою є подієва частина — Security alerts і загалом сигнали, що можуть вказувати на атаку, компрометацію або підозрілу поведінку. Концептуально це дозволяє перейти від суто профілактичного режиму, тобто виправити налаштування, до режиму виявлення та реагування, побачити атаку, локалізувати, зібрати контекст. У великих

середовищах саме ця зв'язка дає найбільшу користь: навіть коли базові політики прописані, інциденти все одно можливі, і ключовим стає час виявлення та якість контексту для розслідування.

У розрізі теми контролю доступу важливо, що Defender for Cloud допомагає формувати правильний інфраструктурний фундамент: підсвічує надмірні права, небезпечні мережеві експозиції, прогалини в базових захисних налаштуваннях і загалом показує, де контроль доступу або пов'язані з ним конфігурації створюють ризики. Проте контроль доступу до хмарних ресурсів в організації охоплює не лише інфраструктуру, а й рівень використання хмарних застосунків, поведінку користувачів, політики сесій, виявлення ризикових дій та запобігання витоку даних [8].

3 ТЕХНОЛОГІЯ КОНТРОЛЮ ДОСТУПУ ДО ХМАРНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ НА БАЗІ MICROSOFT DEFENDER FOR CLOUD APPS

3.1. Технологія застосування Microsoft Defender for Cloud Apps

Побудова контролю доступу до хмарних ресурсів у Microsoft Defender for Cloud Apps реалізується як поєднання двох площин: отримання видимості щодо використання хмарних сервісів та застосування політик, які обмежують або модифікують доступ залежно від умов сеансу. Логіка підходу полягає в тому, що організація спочатку формує інвентаризацію підключених застосунків і активностей, а далі накладає правила доступу та сесійні обмеження для зниження ризиків витоку даних і зловживань обліковими записами.

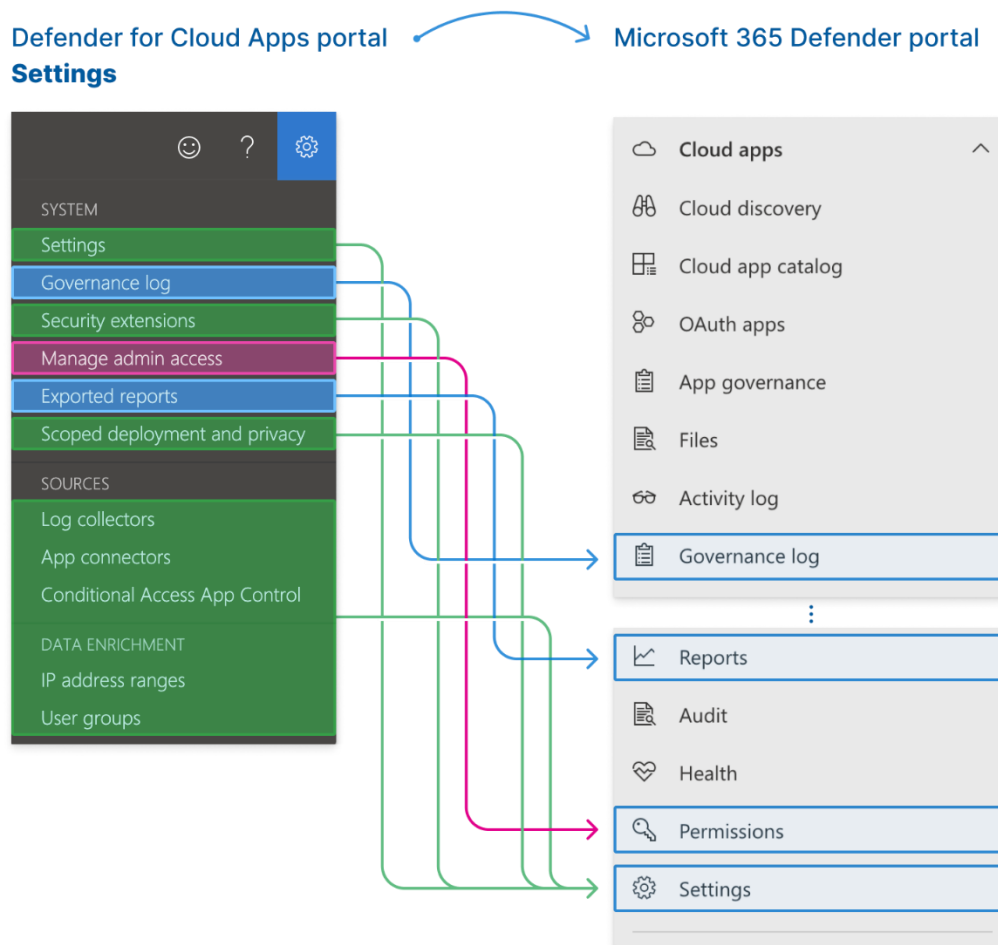


Рис. 3.1. Перехід Defender for Cloud Apps у Microsoft Defender portal

Початковим кроком є підключення керованих хмарних застосунків через механізм app connectors, який працює через API провайдерів сервісів і надає централізовану видимість та керованість у межах Defender for Cloud Apps. Після підключення застосунків формується основа для контролю: стають доступними облікові записи застосунків, журнали активностей, об'єкти даних і контекстні атрибути, які надалі використовуються у політиках. Саме цей етап важливий для подальших сценаріїв контролю, оскільки без підключення застосунку набір сигналів і можливостей реагування буде обмеженим [9].

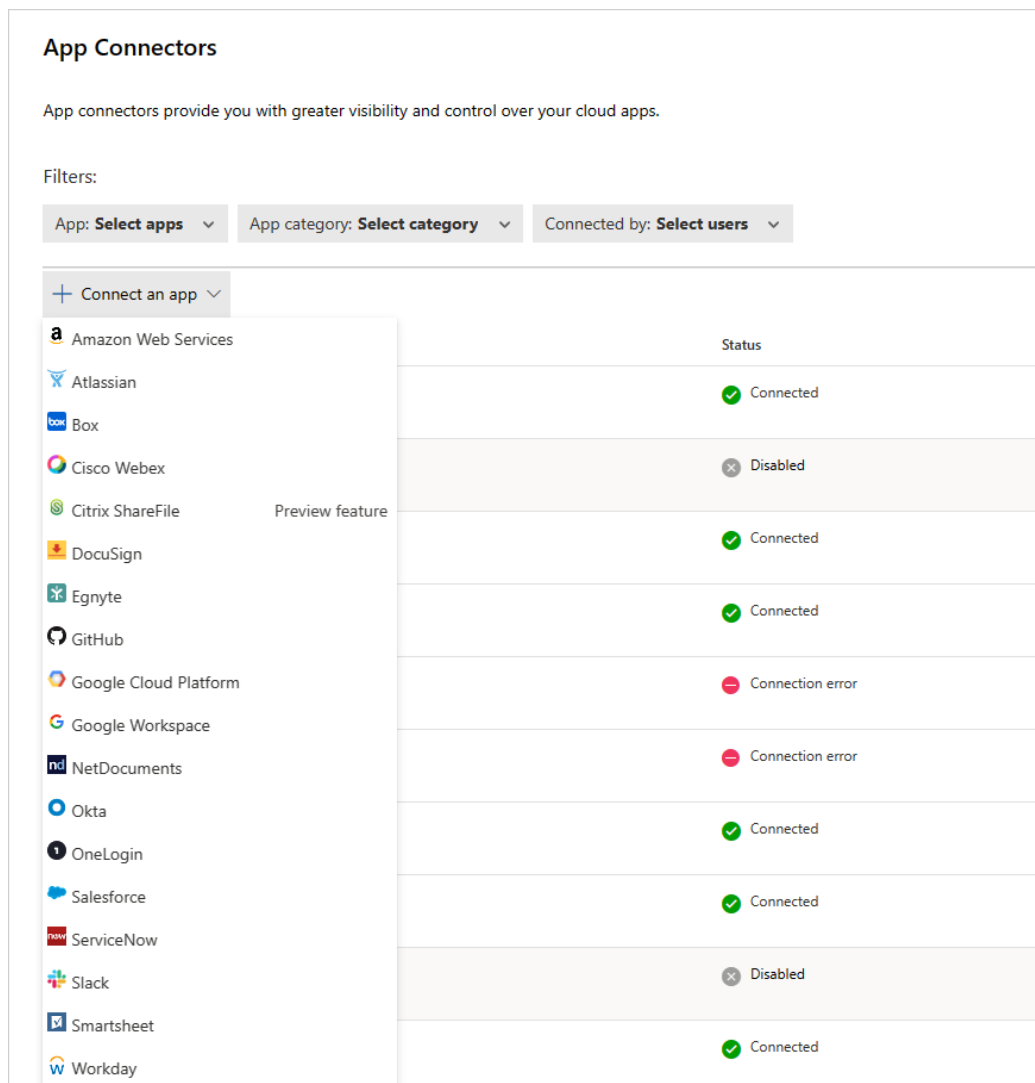


Рис.3.2. Підключення керованих хмарних застосунків

Паралельно з підключенням застосунків забезпечується видимість щодо фактичного використання хмарних сервісів, включно з несанкціонованими або

неконтрольованими сервісами, що з'являються внаслідок Shadow IT. У Defender for Cloud Apps цей напрям реалізується через Cloud Discovery, де на основі журналів/телеметрії формується перелік хмарних застосунків, їхня популярність, профіль ризику та користувацька активність. Така видимість потрібна не лише для інвентаризації, а й для ухвалення рішень, які саме сервіси мають переходити в режим керованого доступу (через підключення та політики), а які мають бути обмежені.

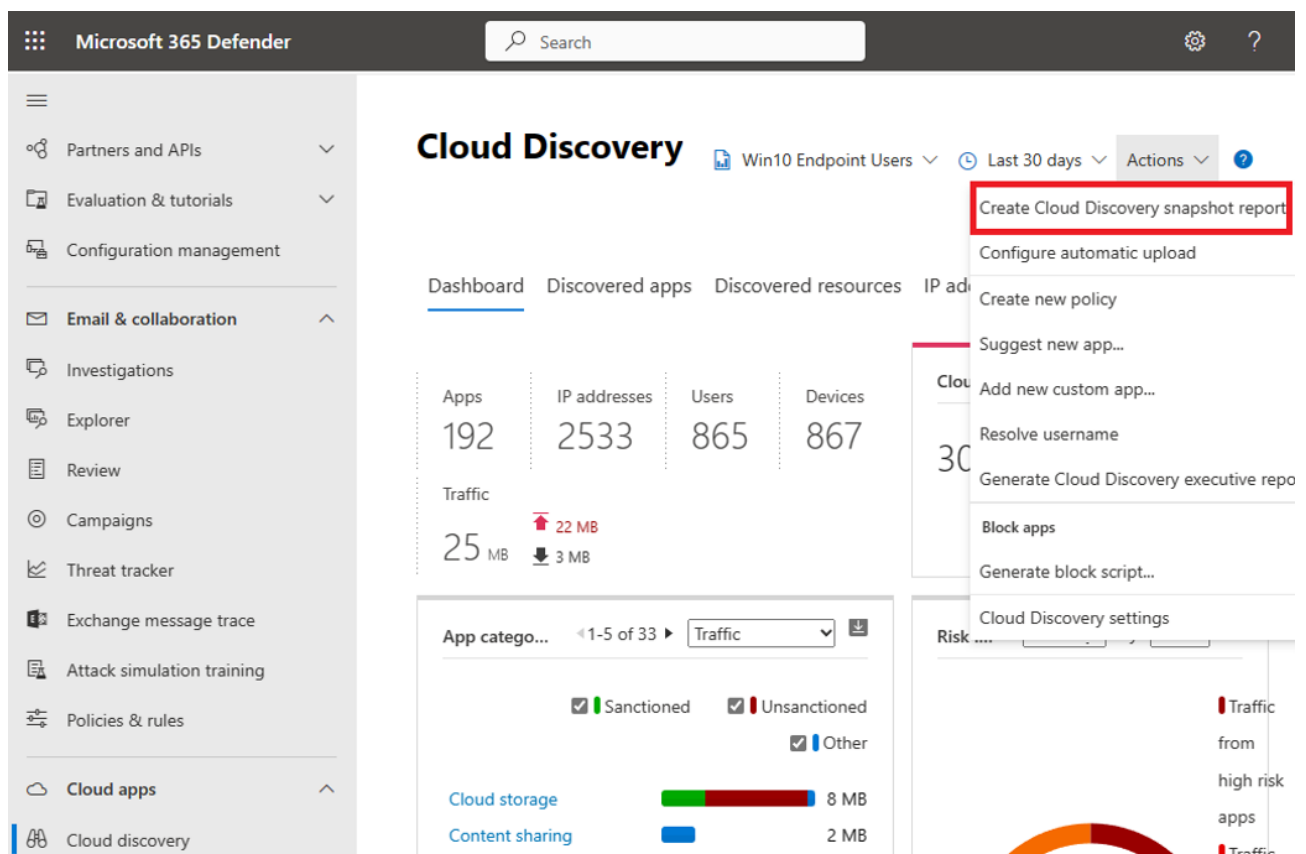


Рис.3.3. Створення snapshot report для виявлення та оцінювання Shadow IT.

Після формування базової видимості ключовим механізмом контролю доступу виступає Conditional Access app control, який забезпечує контроль сесій у реальному часі. Його суть зводиться до того, що доступ користувача до хмарного застосунку проходить через контрольні механізми, які можуть дозволяти, блокувати або обмежувати дії під час активної сесії. У цій моделі використовуються два типи політик: access policies визначають умови допуску до застосунку (хто, звідки, з яким контекстом пристрою або ризику входу), а

session policies накладають обмеження на дії під час роботи (наприклад, блокування завантаження, контроль вставлення/копіювання, моніторинг та інші сесійні контролі). Таким чином, контроль реалізується не як разове рішення на вході, а як керування поведінкою в межах сесії.

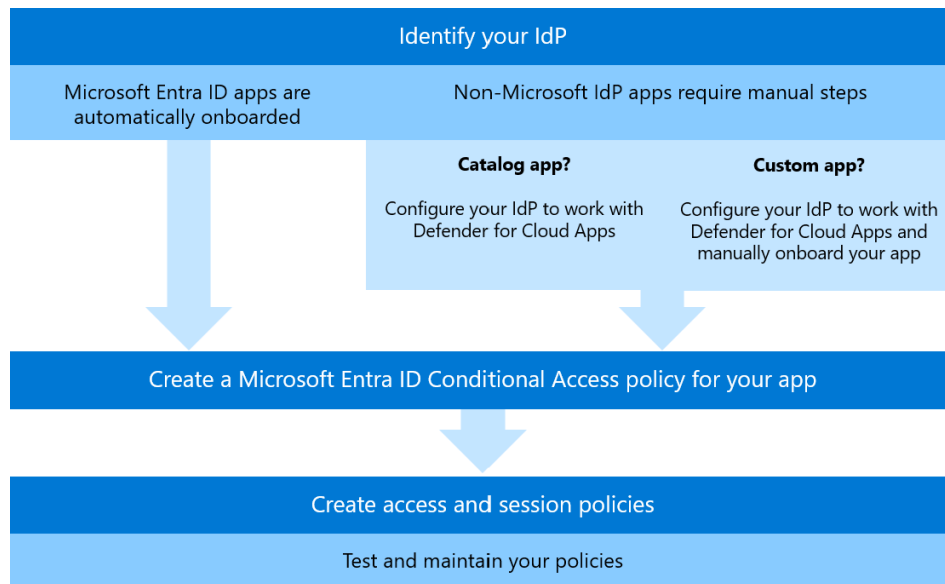


Рис.3.4. Загальна схема впровадження Conditional Access App Control у Microsoft Defender for Cloud Apps.

Практичний сценарій, який найпростіше демонструє прикладний контроль доступу, полягає в обмеженні завантаження даних із корпоративних хмарних застосунків з некерованих або невідповідних пристроїв. У такому підході access policy використовується як умова для переведення сесії під контроль (з урахуванням стану пристрою чи інших атрибутів), а session policy застосовується для конкретної дії, наприклад блокування скачування. Це дозволяє зберегти доступність сервісу для роботи, але зменшити ймовірність винесення даних поза контрольовані межі організації [10].

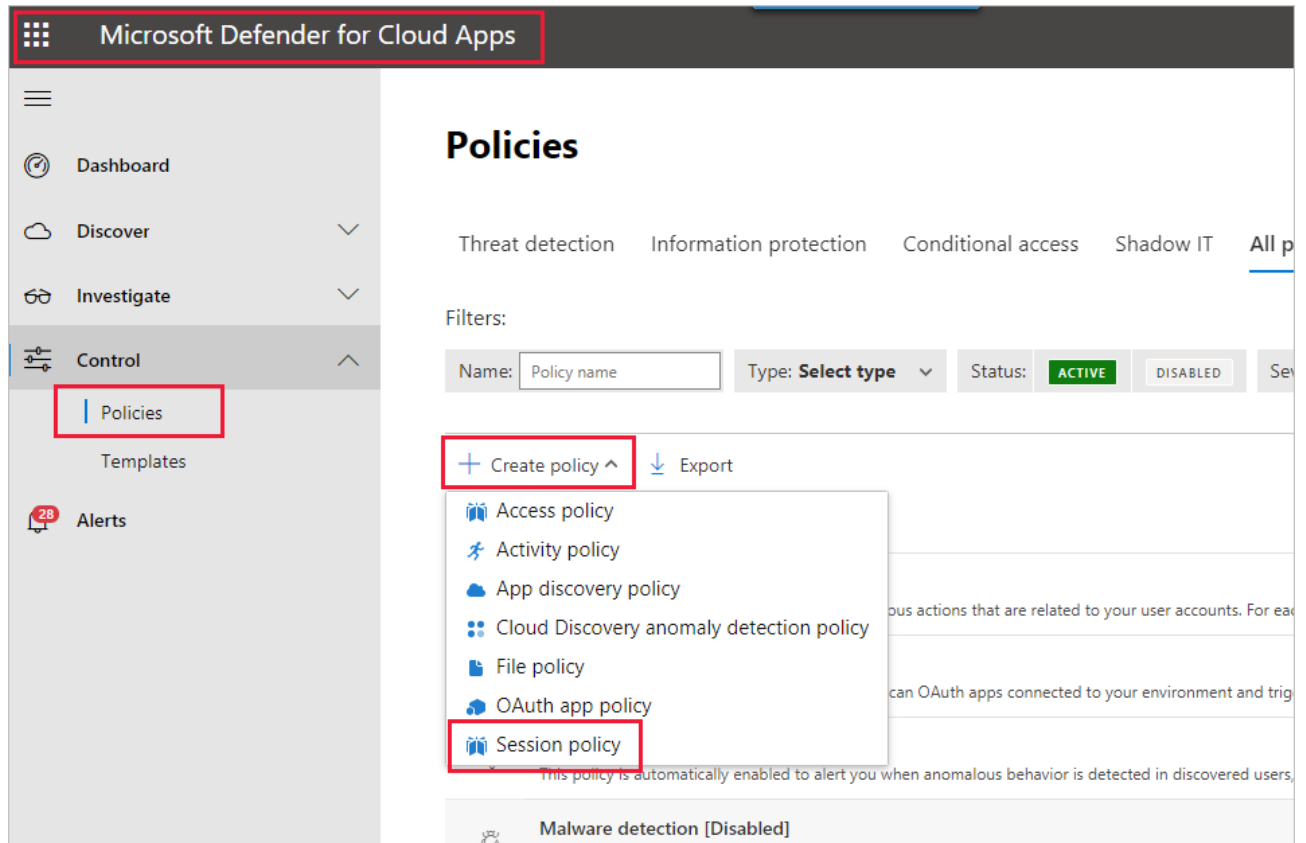


Рис.3.5. Створення Session policy

Окремо враховується, що частина умов доступу може задаватися на рівні Microsoft Entra Conditional Access, де політика формує вимогу застосування session controls і перенаправляє керування сесією до Defender for Cloud Apps. За рахунок цього забезпечується узгодженість ідентифікації та допуску (Entra) із прикладним контролем дій у сесії (Defender for Cloud Apps), що зменшує фрагментацію правил і спрощує керування в корпоративному середовищі.

Після налаштування політик практична частина має завершуватися перевіркою спрацювання контролів і фіксацією результатів у журналах. Для цього використовується журнал активностей, який дозволяє відслідковувати дії користувачів, контекст доступу, підозрілі події та результати застосування політик.

Microsoft 365 Defender

Activity log

Queries: **Select a query** Save as

✕ User agent tag equals Outdated browser, Outdated operating system

+ Add a filter

+ New policy from search Export

Activity	User
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com
Failed log on (Failure message: General failure)	user1@contoso.com

Рис.3.6. Перевірка результатів налаштувань.

Саме цей шар важливий для пояснення керованості рішення: політика не лише блокує або дозволяє дію, а й залишає аудитні сліди для розслідування інцидентів та підтвердження відповідності внутрішнім вимогам контролю доступу [11].

3.2. Рекомендації щодо забезпечення контролю доступу до хмарних ресурсів організації

Контроль доступу до хмарних ресурсів організації має будуватися як керована система правил і перевірок, що охоплює ідентичності користувачів, стан пристроїв, контекст підключення та критичність даних. У хмарному середовищі периметр мережі перестає бути єдиною лінією захисту, тому основним об'єктом контролю стає не місце підключення, а конкретний запит на

доступ: хто звертається, до чого саме, з якого середовища, за яких умов і з яким рівнем ризику. Такий підхід зменшує імовірність несанкціонованого доступу в ситуаціях, коли облікові дані викрадені, пристрій скомпрометований або користувач працює з нестандартної локації [12].

Починати варто з формування зрозумілої моделі доступу, у якій визначено ролі, типові сценарії роботи та перелік ресурсів, що підлягають контролю. Без інвентаризації облікових записів, привілеїв і хмарних сервісів контроль перетворюється на набір точкових обмежень, які легко обійти через паралельні канали доступу або тіньові сервіси. Тому перед застосуванням політик важливо мати актуальну картину: які сервіси використовуються, які групи користувачів у них працюють, де зберігаються дані та які операції виконуються найчастіше. Це створює основу для керованості, коли політики накладаються не на абстрактний хмарний простір, а на конкретні процеси й активи.

Критичним принципом є мінімально необхідні привілеї. Доступ має надаватися рівно в тому обсязі й на той час, який потрібний для виконання робочих задач, без надлишкових дозволів на адміністрування, експорт, масове завантаження або доступ до конфіденційних сховищ. На практиці це означає розподіл ролей, відокремлення адміністративних облікових записів від звичайних користувацьких, обмеження високих привілеїв і контроль за їх використанням. Для чутливих операцій важливо закладати додаткові перевірки: посилена автентифікація, підтвердження з боку керівника або обмеження виконання дій лише з керованих пристроїв.

Окремо варто звернути увагу на автентифікацію. Для хмарних ресурсів базовим стандартом має бути багатофакторна автентифікація, а для привілейованих ролей — посилені механізми на кшталт стійких до фішингу методів входу або додаткових умов доступу. У реальному середовищі більшість інцидентів починається не з технічної вразливості сервісу, а з компрометації облікового запису, тому контроль ідентичностей і сценаріїв входу напряму впливає на загальний рівень захищеності.

Щоб контроль доступу працював не лише на вході, а й під час використання сервісів, варто застосовувати контекстні умови доступу. Рівень

дозволів і набір доступних дій змінюються залежно від того, чи є пристрій керованим, чи відповідає він вимогам безпеки, з якої мережі відбувається підключення, чи є ознаки ризикового входу або аномальної активності. У межах такого підходу користувач може отримати доступ до сервісу для читання, але бути обмеженим у завантаженні файлів або копіюванні даних, якщо робота ведеться з некерованого пристрою. Це дає баланс між доступністю ресурсів і зниженням ризиків витоку.

Для захисту інформації важливо прив'язувати контроль доступу до класифікації даних. Дані з високим рівнем чутливості (персональні дані, фінансові документи, комерційна таємниця) мають супроводжуватися правилами обробки: обмеженням зовнішнього поширення, контролем спільного доступу, заборонаю публічних посилань, фіксацією дій у журналах і можливістю швидко відкликати доступ. Якщо класифікація відсутня або не підтримується політиками, контроль зводиться до загальних заборон, які заважають роботі, але не гарантують захисту саме критичних активів.

Оскільки хмарні середовища зазвичай містять сторонні інтеграції, API-доступ і автоматизацію, окремо слід контролювати технічні облікові записи, ключі доступу та токени. Для них важливі принципи обмеження прав, ротації секретів, розділення середовищ і прив'язки до конкретних задач. Саме надмірно привілейовані інтеграції та довгоживучі ключі часто стають слабким місцем, бо їх складніше відстежувати, ніж дії користувачів у стандартних інтерфейсах [13].

Повноцінний контроль доступу неможливий без спостережуваності та реагування. Журнали входів і дій користувачів мають бути достатньо деталізованими, щоб швидко відновлювати ланцюжок подій, виявляти аномалії та підтверджувати виконання політик. Паралельно потрібні правила виявлення підозрілої активності: масові завантаження, нетипові геолокації входу, спроби доступу до нетипових ресурсів, різке зростання операцій з файлами чи налаштуваннями доступу. У таких випадках ефективною практикою є автоматизовані реакції: блокування сесії, вимога повторної перевірки, тимчасове обмеження дій або постановка інциденту в роботу відповідальним фахівцем.

Окремо варто врахувати організаційний рівень: правила контролю доступу мають бути зрозумілими для користувачів і підтримуватись процесами. Навчання базовим сценаріям безпечної роботи, погоджена модель ролей, регламент роботи з доступами і регулярний перегляд політик зменшують кількість помилок та обходів. У підсумку контроль доступу працює стабільно тоді, коли він не сприймається як випадкові заборони, а як передбачувана система умов, що захищає ресурси й не руйнує робочі процеси [14].

3.3. Рекомендації щодо контролю доступу до хмарних ресурсів на базі Microsoft Defender for Cloud Apps

Застосування Microsoft Defender for Cloud Apps для контролю доступу до хмарних ресурсів доцільно будувати як послідовний перехід від видимості до керованості. На практиці це означає, що спочатку формується інвентаризація використання хмарних сервісів і каналів доступу, а після цього накладаються політики, які регулюють доступ користувачів і дії в межах сесій. Такий порядок дозволяє уникати ситуацій, коли правила безпеки створюються «наосліп» і перекривають легітимні бізнес-сценарії, але при цьому залишають непоміченими тіньові сервіси або альтернативні канали передачі даних.

Першою практичною рекомендацією є підключення ключових корпоративних застосунків через app connectors, оскільки саме це відкриває доступ до централізованих журналів активності, контексту користувачів та подій, а також до інструментів подальшого контролю й реагування. У корпоративному середовищі пріоритет доцільно надавати сервісам, через які проходить основний обіг даних і комунікація, наприклад сховищам файлів, пошті, корпоративним порталам і системам спільної роботи. Після підключення важливо перевірити повноту видимості: чи відображаються активності користувачів, об'єкти даних, типові дії (перегляд, завантаження, поширення), а також чи коректно прив'язуються події до ідентичностей. Без цього подальші політики можуть спрацьовувати непередбачувано або давати неповну картину реального використання ресурсів.

Паралельно має бути увімкнена та налаштована можливість виявлення несанкціонованих або некерованих хмарних сервісів через Cloud Discovery. У межах організації це дозволяє зафіксувати реальну картину використання SaaS, включно з сервісами, які з'явилися без участі ІТ-підрозділу. Варто використовувати результати виявлення як основу для управлінського рішення: які сервіси допускаються до роботи за умови контролю та інтеграції, які мають бути обмежені, а які потребують заміни на керований корпоративний аналог. Практична цінність такого підходу полягає в тому, що контроль доступу не обмежується лише “офіційно дозволеними” застосунками, а враховує фактичні поведінкові шаблони користувачів.

Наступним кроком варто переходити до умовного контролю доступу на рівні сесій через Conditional Access app control. Цей механізм у Defender for Cloud Apps дає змогу керувати не тільки фактом входу, а й тим, що користувач робить у сервісі після автентифікації. У рамках практичного впровадження доцільно розділяти дві логіки: правила доступу (access policies) та правила поведінки в сесії (session policies). Access policies краще використовувати для визначення, за яких умов сесія має потрапляти під контроль, наприклад у випадку некерованого пристрою, нетипової локації, ризикового входу або відсутності необхідного рівня автентифікації. Session policies варто застосовувати для зменшення ризику витоку даних через конкретні операції, наприклад блокування завантаження файлів, обмеження копіювання або накладання додаткових умов на роботу з конфіденційними даними. Такий поділ дозволяє уникнути надмірних заборон: користувачу не обов'язково перекривати доступ повністю, якщо достатньо обмежити найбільш ризикові дії [15].

У типових сценаріях організації одним із найбільш прикладних контролів є обмеження завантаження даних із корпоративних сховищ або офісних сервісів при роботі з некерованих пристроїв. Це особливо актуально для віддаленої роботи й ситуацій, коли співробітники використовують особисті пристрої або тимчасові робочі місця. За цією логікою доступ до сервісу може зберігатися для перегляду й виконання базових операцій, але ризиковані дії, що сприяють винесенню інформації за межі організації, блокуються або контролюються.

Практично це дає контрольований компроміс між доступністю та захистом: бізнес-процеси не зупиняються, але витік через «зручні» функції сервісу ускладнюється.

Щоб забезпечити узгодженість доступу на рівні ідентичностей, важливо пов'язувати політики Defender for Cloud Apps із політиками Microsoft Entra Conditional Access. У такому підході Entra відповідає за допуск і перевірку умов автентифікації, а Defender for Cloud Apps — за контроль дій у межах сесії. Краще уникати дублювання однакових умов у різних місцях, натомість розділяти відповідальність: вимоги до автентифікації, типу входу й загальних умов допуску визначати в Entra, а контроль ризикових дій та обмеження взаємодії з даними реалізувати в сесійних політиках Defender for Cloud Apps. Це спрощує супровід та зменшує ризик конфліктів правил.

Окремий акцент варто робити на контролі доступу до конфіденційних даних, оскільки для хмарних ресурсів саме дані є основним активом. Бажано, щоб політики сесійного контролю були прив'язані до типів файлів, ознак чутливості або критичних розташувань у сховищах, а також до сценаріїв масових операцій. Практично корисними є правила, що реагують на нетипові сплески активності: масове скачування, масове видалення, різке зростання поширень, а також багаторазові спроби доступу до об'єктів із відмовами. Такі події доцільно не лише фіксувати, а й переводити в керовані сценарії реагування, зокрема через автоматичне припинення сесії або вимогу повторної перевірки.

Також важливою частиною є налаштування моніторингу та керованості через журнали активностей і оповіщення. У Defender for Cloud Apps необхідно забезпечити, щоб ключові події відображалися в Activity log і були доступними для фільтрації за користувачем, застосунком, типом дії та результатом політики. Це важливо для пояснення контролю доступу як процесу, який можна перевірити: хто отримував доступ, які обмеження застосовувалися, що було заблоковано і чому. Для організації це створює можливість не лише реагувати на інциденти, а й підтверджувати виконання внутрішніх вимог і політик безпеки під час аудитів або розбору спірних ситуацій.

У підсумку, контроль доступу на базі Microsoft Defender for Cloud Apps доцільно вибудовувати як системну практику: від виявлення хмарних сервісів і підключення ключових застосунків — до сесійного контролю дій, узгодженого з умовним доступом Entra, та подальшої перевірки ефективності через журнали активностей і реагування. Такий підхід дає організації керований баланс між доступністю хмарних ресурсів і зниженням ризиків витоку даних та зловживань доступом [16].

ВИСНОВКИ

Контроль доступу до хмарних ресурсів організації фактично зводиться до керування ідентичностями, контекстом підключення та діями користувача вже після входу в сервіс. Через розподіленість хмарних середовищ і велику кількість інтеграцій недостатньо покладатися лише на мережевий периметр або одноразову перевірку під час автентифікації. Стійкий результат дає підхід, за якого кожен запит на доступ оцінюється з урахуванням ролі користувача, рівня привілеїв, стану пристрою, локації та ризиковості поведінки, а рівень дозволених дій може змінюватися залежно від цих умов. Це дозволяє одночасно зберігати доступність хмарних сервісів для легітимних сценаріїв і зменшувати ризики витоку даних та зловживань доступом.

Загальні рекомендації щодо контролю доступу логічно починаються з інвентаризації хмарних сервісів, облікових записів і привілеїв, оскільки без актуальної картини використання ресурсів будь-які правила залишаються фрагментарними. Критично важливими залишаються принцип мінімально необхідних прав, посилена автентифікація для ризикових і привілейованих сценаріїв, прив'язка політик до чутливості даних, а також спостережуваність і можливість відтворити ланцюжок подій за журналами. Окремої уваги потребують технічні облікові записи, ключі доступу та інтеграції, оскільки саме вони часто накопичують надлишкові дозволи й складніше піддаються контролю, ніж звичайні користувацькі сесії. У результаті найбільш практичним стає підхід, де контроль доступу є не набором заборон, а системою умов і перевірок, яка підлаштовується під реальні робочі процеси.

Практична реалізація цих принципів на базі Microsoft Defender for Cloud Apps дозволяє зібрати ключові елементи в єдину керовану модель. Підключення корпоративних застосунків через app connectors формує основу видимості та контролю, а Cloud Discovery доповнює її за рахунок виявлення тіньових сервісів і реального профілю використання SaaS у межах організації. Після цього Conditional Access app control забезпечує перехід від “допуску до сервісу” до керування діями в межах сесії, коли доступ не обов'язково блокується повністю,

але ризикові операції можуть обмежуватися, контролюватися або фіксуватися. Узгодження сесійного контролю з політиками Microsoft Entra Conditional Access дозволяє розділити відповідальність між перевіркою умов входу та контролем дій після входу, що зменшує дублювання правил і спрощує супровід.

Тому, найбільш стабільний ефект для організації дає модель, у якій контроль доступу будується від видимості до політик, а від політик — до перевірюваного контролю через журнали активностей і сценарії реагування. У такій логіці хмарні ресурси залишаються доступними для роботи, але доступ стає керованим і контекстним: користувач отримує рівно той рівень можливостей, який відповідає умовам підключення та рівню ризику, а критичні дані мають додаткові бар'єри проти витоку. Це дозволяє зменшити залежність від “ідеальної поведінки” користувачів і компенсувати типові ризики хмарного середовища за рахунок чітких правил, спостережуваності та керованості.

ПЕРЕЛІК ПОСИЛАНЬ

1. Security Issues in Cloud Computing: 6 Common Threats and Risks. ASPM, AI Remediation & Secrets Scanning: AI-Native Application Security. URL: <https://www.legitsecurity.com/aspm-knowledge-base/security-issues-in-cloud-computing> (дата звернення: 27.09.2025).
2. 12 Cloud Security Issues: Risks, Threats & Challenges | CrowdStrike. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. URL: <https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-risks/> (дата звернення: 29.09.2025).
3. NIST Technical Series Publications. URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf> (дата звернення: 02.10.2025).
4. Conditional Access app control - Microsoft Defender for Cloud Apps. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad> (дата звернення: 03.10.2025).
5. Introduction to securing Microsoft Entra service accounts. Azure æ□□æ;£ | Azure Docs. URL: <https://docs.azure.cn/en-us/entra/architecture/secure-service-accounts> (дата звернення: 08.10.2025).
6. NIST SP 800-63 Digital Identity Guidelines. URL: <https://pages.nist.gov/800-63-4/> (дата звернення: 10.10.2025).
7. Top 12 Cloud Security Tools: Guide (2025 Updated) | Cyera Blog. Cyera | The Data Security Solution for the Cloud Era. URL: <https://www.cyera.com/blog/top-10-cloud-security-tools-guide> (дата звернення: 14.10.2025).
8. Microsoft Defender for Cloud: Everything You Should Know. K21 Academy. URL: <https://k21academy.com/azure-cloud/microsoft-defender-for-cloud/> (дата звернення: 16.10.2025).
9. Cloud Application Accounts. Microsoft. URL: <https://learn.microsoft.com/uk-ua/defender-cloud-apps/accounts?view=azure-node-2.0.0&> (дата звернення: 21.10.2025).

10. Conditional Access app control - Microsoft Defender for Cloud Apps. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad> (дата звернення: 24.10.2025).

11. Investigate activities - Microsoft Defender for Cloud Apps. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/defender-cloud-apps/activity-filters> (дата звернення: 01.11.2025).

12. SP 800-207, Zero Trust Architecture | CSRC. NIST Computer Security Resource Center | CSRC. URL: <https://csrc.nist.gov/pubs/sp/800/207/final> (дата звернення: 04.11.2025).

13. CIS Critical Security Controls Version 8.1. CIS. URL: <https://www.cisecurity.org/controls/v8-1> (дата звернення: 07.11.2025).

14. The CSA Cloud Controls Matrix (CCM) V4: Raising the cloud security bar. Home | CSA. URL: <https://cloudsecurityalliance.org/blog/2021/01/21/the-csa-cloud-controls-matrix-ccm-v4-raising-the-cloud-security-bar-to-the-next-level> (дата звернення: 12.11.2025).

15. Manage OAuth apps - Microsoft Defender for Cloud Apps. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions> (дата звернення: 14.11.2025).

16. Connect apps to get visibility and control - Microsoft Defender for Cloud Apps. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/defender-cloud-apps/enable-instant-visibility-protection-and-governance-actions-for-your-apps> (дата звернення: 17.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)