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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо керування ідентифікацією та доступом користувачів за допомогою Microsoft Entra ID»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Мілана ГОРОВА
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ГОРОВА Мілана
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 56 сторінки, 26 рисунки, 26 джерел.

Об'єкт дослідження – процеси ідентифікації користувачів та керування доступом на підприємствах.

Предмет дослідження – методи та засоби ідентифікації користувачів і керування доступом на основі рішення Microsoft Entra ID.

Методи дослідження – опрацювання тематичної літератури, інтернет-джерел, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Ідентифікація користувачів на підприємстві на основі Microsoft Entra ID є важливим аспектом забезпечення безпеки та ефективного управління доступом до ресурсів. Microsoft Entra ID дозволяє підприємствам централізовано керувати ідентифікацією та автентифікацією користувачів, забезпечуючи високий рівень захисту даних. Використовуючи різні методи і засоби для ідентифікації користувачів, Microsoft Entra ID дозволяє здійснювати контроль доступу до як локальних, так і хмарних ресурсів.

Дослідження охоплює методи і засоби впровадження ідентифікації, з особливим акцентом на рішенні Microsoft Entra ID, для підвищення безпеки даних. Аналізовано технічну літературу та наукові джерела і виявлено переваги застосування цього рішення порівняно з альтернативними методами.

В результаті дослідження розроблено рекомендації щодо інтеграції Microsoft Entra ID у процеси ідентифікації користувачів, спрямовані на забезпечення вищого рівня безпеки доступу до інформації. Практичне застосування результатів роботи може знайти використання у сферах, де критично важливим є забезпечення надійності і безпеки даних.

Галузь використання – кібербезпека ідентифікації користувачів на підприємствах

КІБЕРБЕЗПЕКА, MICROSOFT ENTRA ID, ІДЕНТИФІКАЦІЯ, SSO, КЕРУВАННЯ ДОСТУПОМ, ДОСТУП ДО ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ІДЕНТИФІКАЦІЇ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

Azure AD - Azure Active Directory

RTO - Recovery Time Objective (Цільовий час відновлення)

DPE - Domino's Pizza Enterprises Ltd.

MFA - Мультіфакторна аутентифікація

RBAC - Рольова модель доступу

IAM - Identity and Access Management (Системи управління ідентифікацією та доступом)

SSO - Single Sign-On

API - Application programming interface

SaaS - Software as a service (Програама як послуга)

ВСТУП

В умовах сучасного світу та цифрового середовища, де дані є одним з найцінніших активів підприємства, ефективне керування ідентифікацією та доступом користувачів стає критично важливою складовою безпеки та продуктивності. З ростом обсягів даних, збільшенням кількості пристроїв, користувачів та використанням хмарних послуг, деяким організаціям доводиться стикатися зі складними викликами щодо управління доступом до своїх систем та ресурсів.

Дослідження шляхів та розроблення рекомендацій у сфері керування ідентифікацією та доступом користувачів стає актуальною проблемою, оскільки вимагає поєднання найновітніших технологічних рішень з розумінням потреб та викликів, що виникають у конкретному бізнес-контексті. Це дослідження не лише спрямоване на забезпечення високого рівня безпеки даних, але й на оптимізацію процесів, забезпечення зручності для користувачів та зменшення ризиків, пов'язаних із нецільовим використанням або зловживанням доступом.

У цьому контексті, важливим є ретельний аналіз сучасних методів та технологій управління ідентифікацією та доступом, а також розроблення стратегій, що враховують специфіку конкретних організацій, їх бізнес-процесів та потреб користувачів. Це дозволить ефективно впровадити рішення згідно унікальних вимог кожного підприємства, забезпечити максимальну ефективність, безпеку та зручність в управлінні ідентифікацією та доступом.

Об’єкт дослідження – процеси ідентифікації користувачів та керування доступом на підприємствах.

Предмет дослідження – методи та засоби ідентифікації користувачів і керування доступом на основі рішення Microsoft Entra ID.

Мета роботи – розробити рекомендації щодо застосування методів та

засобів ідентифікації користувачів на підприємствах на базі Microsoft Entra ID та надати рекомендації щодо їх реалізації.

Наукові завдання:

дослідити сутність проблеми ідентифікації користувачів на підприємствах;

проаналізувати основні методики ідентифікації користувачів;

проаналізувати існуючі рішення для ідентифікації користувачів та керування доступом;

проаналізувати методи та засоби ідентифікації користувачів на базі рішення Microsoft Entra ID;

запропонувати варіант алгоритму ідентифікації користувачів на базі Microsoft Entra ID;

розробити рекомендації щодо застосування методів та засобів ідентифікації користувачів на підприємствах.

Методи дослідження – опрацювання тематичної літератури, інтернет-джерел, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів ідентифікації користувачів на підприємствах на основі Microsoft Entra ID, а також розроблено рекомендації фахівцям з інформаційної безпеки щодо їх реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ ТА ДОСТУПУ КОРИСТУВАЧІВ НА ПІДПРИЄМСТВІ

1.1 Аналіз проблеми ідентифікації та доступу користувачів на підприємстві

Дослідження проблеми ідентифікації та доступу користувачів на підприємстві включає аналіз різних аспектів безпеки та управління доступом. Згідно Постанова Каб. Міністрів України від 29.03.2006 р. № 373, Ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Ідентифікація дозволяє суб'єктові повідомити своє ім'я за допомогою певного параметру — ідентифікатора (для прикладу, логін), який є відомим іншій стороні. В момент ідентифікації відбувається порівняння заявленого суб'єктом даних на відповідність відомих іншій стороні. В разі успішної ідентифікації відбувається Автентифікація. Шляхом автентифікації інша сторона може остаточно переконатись, що суб'єкт саме той за кого він себе видає за допомогою паролю, коду чи іншим методом.

Існує декілька методів ідентифікації користувачів. Розглянемо найпоширеніші.

Логін та паролі чи PIN-коди - найбільш традиційний метод, який використовується частіше за все. Він найпростіший у впровадженні, але не є достатньо надійним. Має ряд проблем: часто містить слабкі паролі, користувачі можуть повторно використовувати паролі для входу на інші сервіси, злочинцям,

які отримали данні для входу шляхом витоку інформації, простіше видати себе за суб’єкт, яким вони не являються.

Біометричні дані частіше використовуються відбитків пальців, розпізнавання обличчя, сканування райдужної оболонки ока. Відносно новий спосіб ідентифікації, який все частіше використовується в повсякденному житі (наприклад: розблокування смартфону). Проблеми: приватність, можливість помилкових відмов, супроводжених фізіологією людини чи навколишнім середовищем (наприклад: мокрі руки, погане освітлення чи травма людини). Також цей спосіб буде проблемно впровадити на підприємстві для постійного способу ідентифікації.

Токени та смарт-карти, тобто, *фізичні пристрої*, які генерують або зберігають одноразові паролі чи спеціальні коди. Є поширеним способом ідентифікації на підприємствах та легко реалізувати. Проблеми: втрачання або крадіжка токенів чи носіїв.

Мультіфакторна аутентифікація (MFA) - комбінація двох або більше методів аутентифікації для підвищення безпеки. Є одним з найкращих шляхів вирішення проблем. MFA часто використовується на різних сервісах чи підприємствах.

Розглянемо коротко розглянемо найпопулярніші методи доступу.

Рольова модель доступу (RBAC) - доступ надається на основі ролей користувачів. Доступ до мережі компанії або її активів, зазвичай, залежить від посади співробітника. Наприклад, бухгалтер має можливість дізнатися як загальну фінансову звітність, так і конкретно з продажу, тоді як менеджер з продажу має доступ лише до останньої. Однією з найскладніших проблем в управлінні великими мережами є складність адміністрування безпеки. Контроль доступу на основі ролей офіційно сформульований у 1992 році Девідом Феррайоло та Ріком Куном, став переважною моделлю розширеного

контролю доступу. Проблеми: складність налаштування, підтримки та моніторингу, потреба в регулярному перегляді та оновленні ролей.

Модель доступу на основі атрибутів, коли доступ надається на основі атрибутів користувачів і контексту. Це модель контролю доступу до об'єктів, заснована на аналізі правил для атрибутів об'єктів чи суб'єктів, можливих операцій з ними та оточення, що відповідає запиту. Ці системи управління доступом забезпечують мандатне та вибіркове керування доступом. Політика на основі атрибутів робить управління доступом ефективнішим, зменшуючи складність нормативних вимог. Одна й та ж сама політика, заснована на атрибутах, може використовуватись у різних системах. Це допомагає керувати доступом до ресурсів у межах однієї компанії чи між кількома партнерськими. Таке централізоване управління доступом передбачає єдине авторитетне джерело для правил доступу, що робить необов'язковими перевірки відповідність вимогам кожної конкретної системи зі своєї політикою. Але не обходиться без проблем: існує складність управління атрибутами та є необхідність постійного моніторингу.

Дискреційний контроль доступу, коли користувачі самі контролюють доступ та вид використання ресурсу. Цей метод управління доступом передбачає право власника або адміністратора об'єкта визначати та контролювати всіх, хто має доступ до системи або ресурсів, ґрунтуючись на ідентифікаційну інформацію про суб'єктів, допущених до контрольованої системи. Модель дискреційного доступу є простою в налаштуванні та управлінні, й сумісна з багатьма програмними забезпеченнями та операційними системами. Перевага дискреційного контролю доступу полягає в тому, що адміністратор може легко й швидко налаштувати дозвіл, обираючи, хто й куди зможе отримати доступ. Проблеми: занадто багато повноважень надається адміністратору списку, що може спричинити ненавмисне надання доступу стороннім суб'єктам, які можуть порушити цілісність системи безпеки організації та розпорядитися ресурсом без відома власника.

Мандатний контроль доступу, коли доступ надається на основі центральних політик безпеки. В обов'язковій моделі контролю доступу застосовується поняття «мітка об'єкта» або «мандат», який визначає ступінь важливості ресурсу та присвоюється йому в момент створення. У мандатній моделі користувачі не змозі змінювати рівень доступу до ресурсів, перевищуючи той, що був наданий адміністратором. Якщо є необхідність підвищити рівень доступу - створюється новий профіль з обліковими даними користувача. Адміністратору надається право змінювати налаштування тільки відповідно параметрами системи, які визначаються загальною політикою безпеки об'єкта. Обов'язковий контроль доступу доцільно використовувати на об'єктах та для організацій, де потрібна максимальна безпека й обмеження. Отож, виникають наступні проблеми: негнучкість, труднощі в налаштуванні для великих організацій.

1.2. Аналіз підходів до вирішення проблеми ідентифікації та доступу користувачів

Розглянемо декілька варіантів підходів, які забезпечують надійний контроль та безпеку доступу до ресурсів підприємства.

Впровадження *однофакторної аутентифікації* за допомогою паролів та PIN-кодів - найбільш поширений метод, де користувач вводить секретне слово або номер для доступу. Переваги: Легкість впровадження та використання, низькі витрати на підтримку. Недоліки: Низька безпека через слабкі паролі та можливість їхнього зламу, а також високий ризик соціальної інженерії та фішингу.

MFA – це комбінація паролів з біометричними даними (відбитки пальців, розпізнавання обличчя), токени або смарт-карти в поєднанні з паролями, одноразові паролі, що надсилаються на мобільні пристрої. Переваги: Значно вищий рівень безпеки та захист від більшості типів атак, включаючи фішинг та підбор паролів. Недоліки: потребує додаткових ресурсів та часу на впровадження та може бути незручним для деяких користувачів.

Біометрична аутентифікація, де можуть бути відбитки пальців, розпізнавання обличчя або райдужної оболонки ока чи розпізнавання голосу. Переваги: Висока унікальність і, на даний момент, складність підробки. Також це зручно для користувачів, які можуть не запам’ятовувати паролі. Недоліки: висока вартість обладнання, впровадження а також можуть виникнути проблеми з приватністю та захистом біометричних даних, що може спровокувати ще більші витрати на захист даних.

RBAC, тобто призначення доступу на основі ролей користувачів, що призначає адміністратор. Переваги: централізоване управління доступом. Цей метод полегшує управління доступом для нових співробітників та зміну ролей при підвищенні чи зміні посади працівниками. Недоліки: необхідність в регулярному перегляді чи оновленні ролей, що може бути складно для великих організацій з динамічними структурами.

Системи управління ідентифікацією та доступом (Identity and Access Management, IAM) – це централізоване управління обліковими записами користувачів та їхніми правами доступу. В цьому випадку можлива інтеграція з різними системами та додатками для єдиного управління доступом. Переваги: підвищений рівень безпеки та зручність в управлінні. Недоліки: висока вартість впровадження та підтримки, а також можуть виникнути складнощі в інтеграції з існуючими системами.

Single Sign-On (SSO) - користувач вводить облікові дані один раз для доступу до всіх корпоративних систем. Переваги: зручність для користувачів та

зниження кількості паролів, які потрібно запам'ятовувати. Недоліки: підвищення ризику, якщо єдина точка входу буде скомпрометована. Також існує складність налаштування та інтеграції з усіма системами.

Підсумовуючи все вище розглянуте, можна обрати варіант, який задовільнить потреби та можливості кожного підприємства. На даний момент, ринок наповнений різноманітними продуктами, які можуть запропонувати різноманітність підходів до вирішення проблеми керування ідентифікацією та доступом для користувачів на підприємстві.

1.3 Аналіз існуючих рішень щодо керування ідентифікацією та доступом користувачів на підприємстві

Розглянемо найпопулярніші існуючі програмні забеспечення, що допоможуть з вирішенням проблеми ідентифікації:

Okta є хмарною IAM платформою, яка надає широкий спектр рішень для управління ідентифікацією та доступом. Вона підтримує аутентифікацію, авторизацію, управління користувачами, а також інтеграцію з іншими додатками та системами. Okta Single Sign-On надає безпечний і зручний доступ до додатків і сервісів. Це один із провідних постачальників рішень для єдиного входу, який спрощує управління ідентифікаційними даними користувачів для підприємств, як у локальних, так і у хмарних середовищах. Заснована в 2009 році зі штаб-квартирою в Сан-Франциско, Каліфорнія, США, Okta Single Sign-On є надійним і гнучким IAM SSO рішенням. Воно допомагає підприємствам підвищити ефективність, продуктивність і безпеку. Висока вартість продукту зумовлена різноманітними функціями, які він надає. Okta забезпечує політики паролів, синхронізацію паролів та самообслуговування для скидання паролів.

За допомогою Okta можна використовувати різні попередньо налаштовані шаблони та керувати доступом до Application programming interface(API). Ви також можете отримувати сповіщення про потенційні помилки входу.

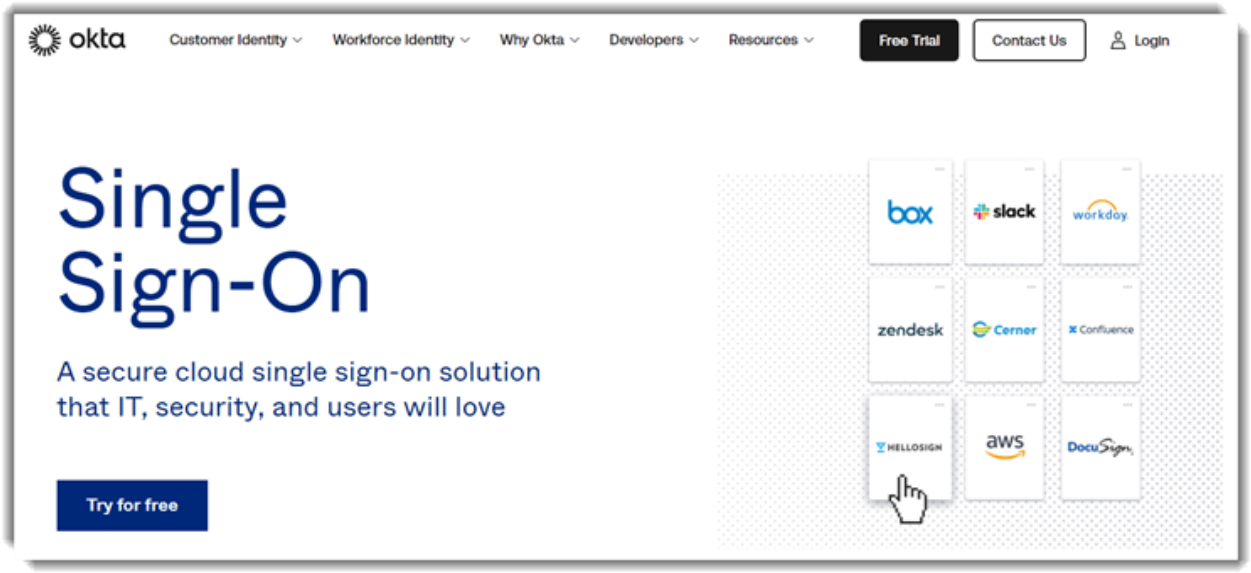

Рис. 1.1. Okta

Її переваги в легкій інтеграція з різними додатками, висока безпека, підтримка багатофакторної аутентифікації, зручний інтерфейс. Недоліки - висока вартість для великих підприємств, обмеження в налаштуваннях для складних сценаріїв.

Ping Identity надає комплексні IAM рішення, включаючи аутентифікацію, управління доступом, єдину аутентифікацію та API безпеку. Платформа підтримує як хмарні, так і локальні середовища. Він пропонує підприємствам розумні рішення для управління ідентифікацією. Це одне з провідних рішень, що дозволяє організаціям надійно контролювати та регулювати доступ користувачів до даних, API та програм у гібридних IT-середовищах. Його функціонал включає каталоги користувачів, управління ідентифікацією, єдиний вхід (SSO) та багатофакторну аутентифікацію (MFA). Ping Identity допомагає компаніям захищати свої цифрові ресурси, дотримуватися вимог законодавства та покращувати взаємодію з користувачами.

Рис. 1.2. Ping Identity

Переваги – це потужні функції управління доступом, висока масштабованість, підтримка різних аутентифікаційних методів. Недоліки - висока вартість, складність налаштування для малих підприємств.

LastPass Single Sign-On надає безпечний і зручний доступ до додатків і сервісів. Це один із провідних постачальників рішень для єдиного входу, який спрощує управління ідентифікаційними даними користувачів для підприємств, як у локальних, так і у хмарних середовищах. Заснований у 2008 році зі штаб-квартирою в Бостоні, Массачусетс, США, LastPass Single Sign-On є надійним і гнучким IAM SSO рішенням. Воно допомагає підприємствам підвищити ефективність, продуктивність і безпеку. Висока вартість продукту зумовлена різноманітними функціями, які він надає. LastPass забезпечує політики паролів, синхронізацію паролів та самообслуговування для скидання паролів. За допомогою LastPass можна використовувати різні попередньо налаштовані шаблони та керувати доступом до API. Ви також можете отримувати сповіщення про потенційні помилки входу.

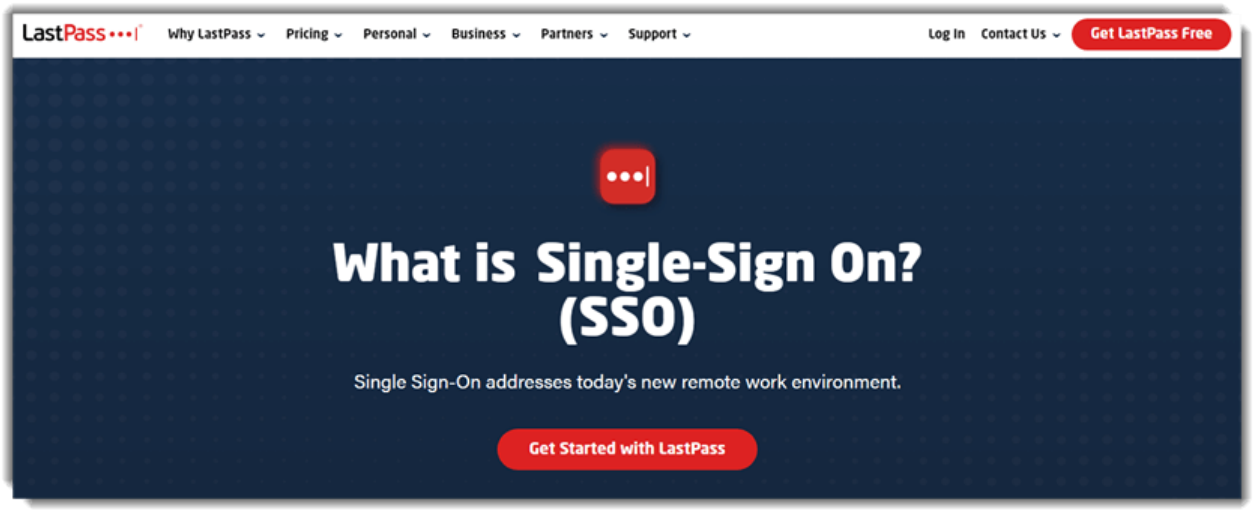

Рис. 1.3. LastPass Single Sign-On

Його переваги - зручність, високий рівень захисту, підтримка різних додатків. Недоліки - висока складність налаштування та вартість, постійна залежність від інтернету, були інциденти з безпекою в минулому.

AWS IAM Identity Center (раніше AWS Single Sign-On) є рішенням для управління ідентифікацією та доступом, яке надає функції єдиного входу (SSO) і централізованого управління доступом для користувачів, що використовують різні AWS акаунти та бізнес-додатки.

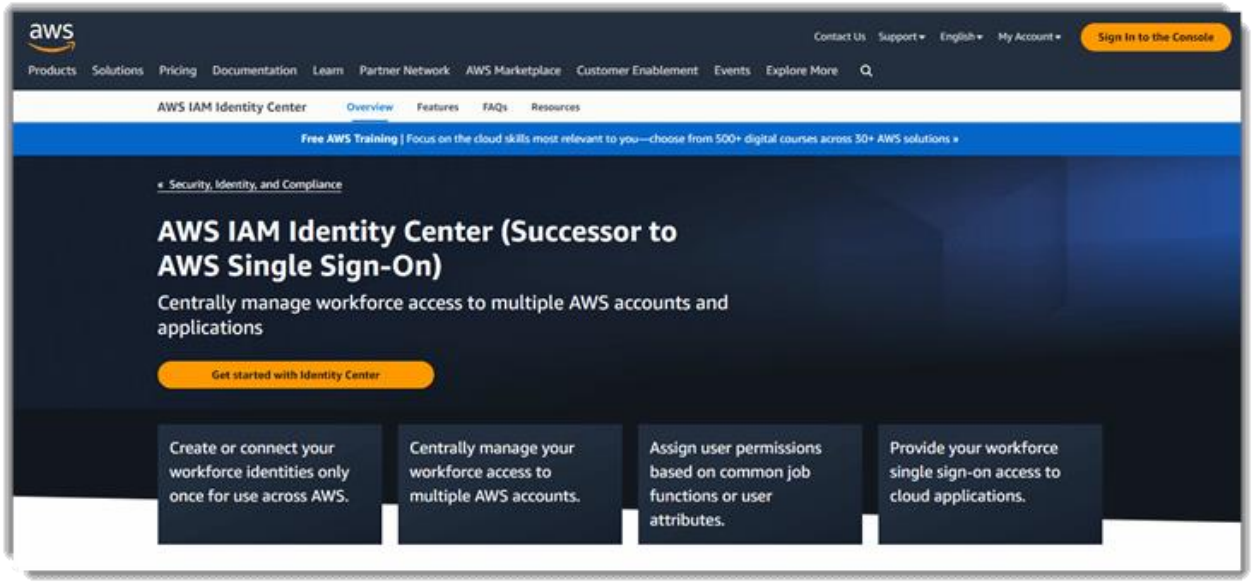

Рис. 1.4. AWS IAM Identity Center

Його переваги в спрощенні управління доступом до кількох AWS акаунтів і додатків з єдиного інтерфейсу, інтеграція з AWS сервісами, підтримка багатьох сторонніх додатків, підтримка багатофакторної аутентифікації (MFA) та політики безпеки на рівні підприємства. Недоліки в складності налаштування, залежності від AWS, високій вартості, користувачам може знадобитися час на навчання для повноцінного використання всіх функцій та можливостей AWS IAM Identity Center.

Microsoft Entra ID – це інтегроване хмарне рішення для керування ідентичностями й доступом. Воно є лідером ринку у сфері керування каталогами, надання доступу до програм і захисту ідентичностей. Воно забезпечує функції для єдиної аутентифікації, багатофакторної аутентифікації та управління доступом до додатків. Рішення Microsoft Entra ID дозволяє організаціям контролювати та захищати ідентичності працівників, партнерів і клієнтів, забезпечуючи їм доступ до необхідних додатків і сервісів. Microsoft Entra ID може інтегруватися з локальними застарілими програмами, тисячами передових SaaS-додатків та багатьма іншими ресурсами, що забезпечує зручну взаємодію з користувачами, а також покращену видимість і контроль.

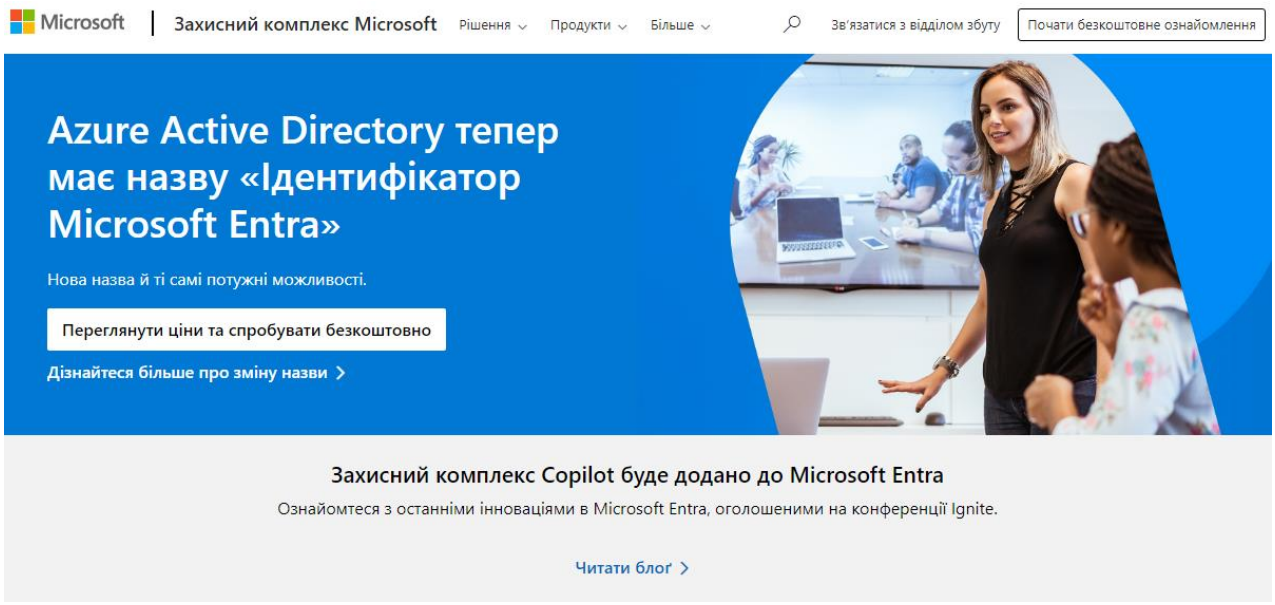

Рис. 1.5. Microsoft Entra ID

Переваги - глибока інтеграція з продуктами Microsoft, висока надійність, масштабованість, підтримка різних сценаріїв доступу. Недоліки - може бути складним для налаштування для невеликих організацій, залежність від хмарних сервісів Microsoft.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ КЕРУВАННЯ ІДЕНТИФІКАЦІЇ ТА ДОСТУПУ КОРИСТУВАЧІВ НА ПІДПРИЄМСТВІ НА БАЗІ MICROSOFT ENTRA ID

Microsoft Entra ID - це інноваційна хмарна служба, яка революціонізує спосіб, яким ваша команда отримує доступ до ресурсів та програм. Завдяки цій платформі керування ідентифікацією та доступом, ви можете легко контролювати та забезпечувати ідентифікацію вашого персоналу, партнерів і клієнтів, а також максимально ефективно використовувати широкий спектр програмних ресурсів.

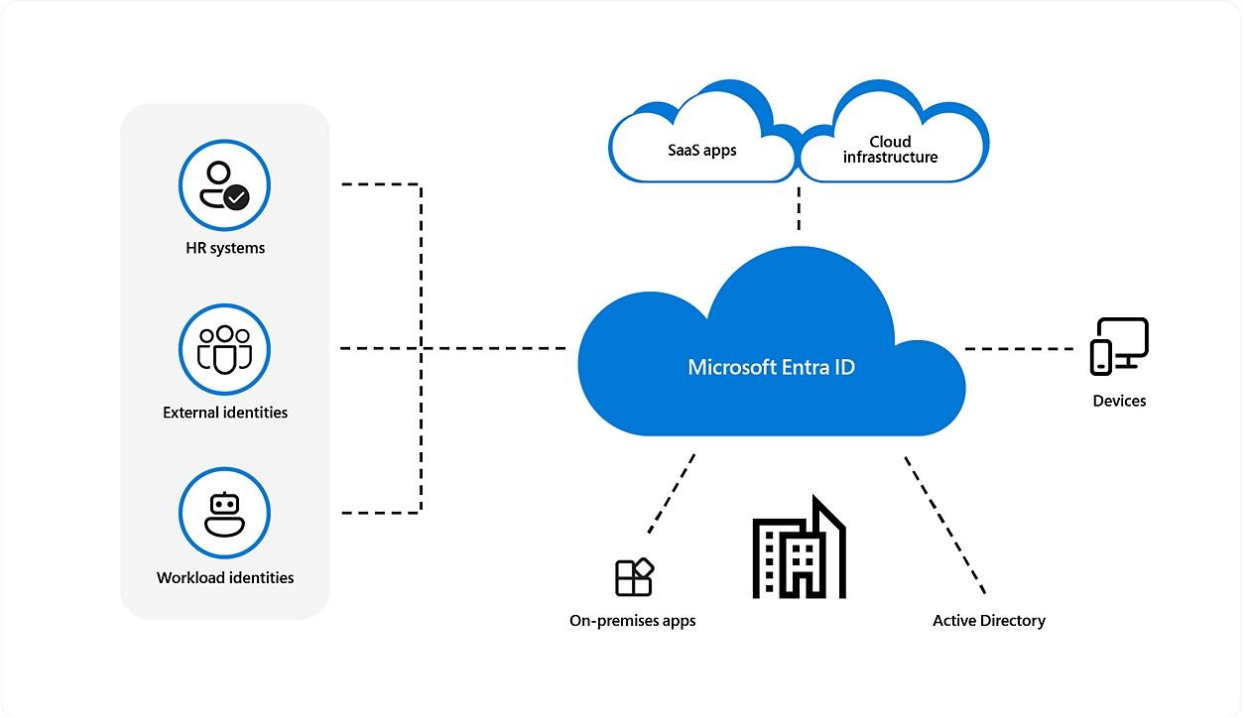

Рис. 2.1. Принцип роботи Microsoft Entra ID

Ця платформа призначена для різних категорій користувачів залежно від їх потреб та ролі, тому вона чудово підходить для підприємств різного розміру, направлення тощо.

IT-адміністратори, для яких Microsoft Entra ID стає потужним інструментом для IT-адміністраторів, які мають можливість контролювати доступ до різноманітних програм і ресурсів відповідно до бізнес-вимог. За допомогою цієї платформи, вони можуть вимагати багатофакторну аутентифікацію для доступу до важливих організаційних ресурсів та автоматизувати процеси налаштування користувачів.

Для *розробників програм* Microsoft Entra ID стає невід'ємною частиною, що надає можливість додавати систему єдиного входу до їх додатків та використовувати API для створення персоналізованого досвіду.

Абоненти Microsoft 365, Office 365, Azure або *Dynamics CRM Online* - кожен абонент однієї з цих платформ автоматично стає клієнтом Microsoft Entra, отримуючи доступ до всіх переваг цієї зручної та надійної хмарної служби.

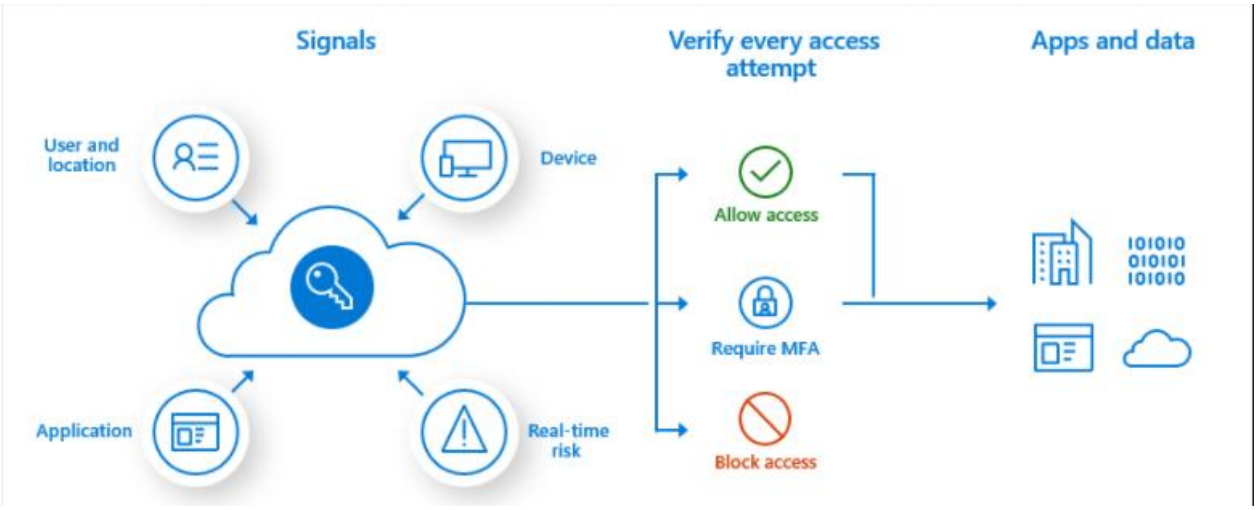

Рис. 2.2. Принцип надання доступу в Microsoft Entra ID

Microsoft Entra ID робить процес керування ідентифікацією та доступом простим і ефективним. З його допомогою ваша команда може отримати доступ до необхідних ресурсів та програм з будь-якого місця і в будь-який час, забезпечуючи безпеку та надійність даних.

2.1 Архітектура та компоненти рішення Microsoft Entra ID

Microsoft Entra ID - це ключовий інструмент для керування ідентифікацією та доступом до послуг корпоративного рівня, що пропонується Microsoft для підприємств. Географічно розподілена архітектура Microsoft Entra ID поєднує в собі масштабний моніторинг, автоматичне перенаправлення, відмовості, стійкість та можливості відновлення, що забезпечує клієнтам доступність і продуктивність по всій компанії. Розглянемо основні елементи архітектури.

Проектування архітектури служби є найпоширенішим способом побудови доступної та зручної, багатої на дані системи є використання незалежних блоків або одиниць масштабування. Для рівня даних Microsoft Entra одиниці масштабування називаються розділами.

Рівень даних має декілька служб front-end, які забезпечують можливість читання та запису. Наступна діаграма показує, як компоненти одного розділу каталогу розподіляються по географічно розподілених центрах обробки даних.

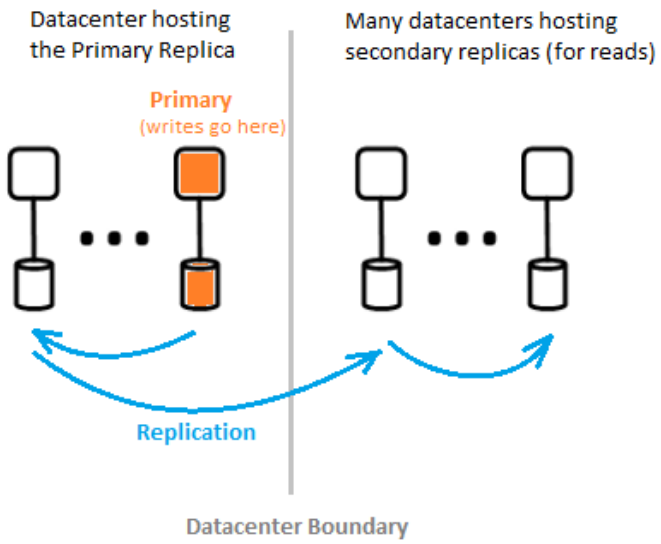

Рис. 2.3. Архітектура Microsoft Entra складається з *основної копії* та *допоміжних копій*.

Розглянемо детальніше *основну копію*:

Отримує всі записи (операції додавання чи змінення даних) для розділу, до якого вона належить;

Негайно реплікує (копіює) будь-яку операцію запису на допоміжну копію в іншому центрі обробки даних перед тим, як повідомити користувачу про успішне виконання операції;

Гарантує географічно розподілену стійкість записаних даних.

Наступний важливий елемент – це *допоміжні копії*:

Обслуговують всі читання з каталогу та розташовані у фізично віддалених один від одного центрах обробки даних;

Їх багато, адже дані реплікуються асинхронно (з певним запізненням);

Обслуговують запити на читання каталогів, наприклад, запити на автентифікацію, з центрів обробки даних, розташованих найближче до користувачів.

Другий пункт архітектури - *масштабованість*, тобто здатність служби розширюватися для того, щоб відповідати зростаючим потребам у продуктивності. Масштабованість запису досягається за допомогою партиціювання даних - процесу розділення даних на менші та більш керовані блоки. Масштабованість читання досягається шляхом реплікації даних з одного розділу на декілька допоміжних копій, розміщених по всьому світу. Реплікація – це створення копій даних.

Запити від програм, що використовують каталог, надсилаються до найближчого центру обробки даних. Записи прозоро перенаправляються до основної копії для забезпечення узгодженості читання та запису. Допоміжні копії значно розширюють масштаб розділів, оскільки більшу частину часу каталоги обробляють саме запити на читання.

Підвищення масштабу також можливе завдяки тому, що програми для роботи з каталогом підключаються до найближчих центрів обробки даних. Це покращує продуктивність. Оскільки один розділ каталогу може мати багато

допоміжних копій, їх можна розмістити ближче до клієнтів каталогу. Лише внутрішні компоненти служби каталогів, що активно здійснюють записи, напряму звертаються до головної, активної копії.

Безперервна доступність (або час безвідмовної роботи) визначає здатність системи працювати без перебоїв і є третім пунктом архітектури. Ключовим фактором високої доступності Microsoft Entra ID є можливість служб швидко перенаправляти трафік між кількома географічно розподіленими центрами обробки даних. Кожен центр обробки даних є незалежним, що дозволяє уникати каскадних відмов. Завдяки такій високодоступній архітектурі, Microsoft Entra ID не потребує простоїв для проведення технічного обслуговування.

Проектування розділів Microsoft Entra ID є більш простим порівняно з проектуванням локального Active Directory. Воно використовує модель з одним головним вузлом, що передбачає ретельно спланований та детермінований процес переходу на резервну копію у разі виходу з ладу основної.

Microsoft Entra ID підтримує нульовий показник RTO (Recovery Time Objective - Цільовий час відновлення), щоб не втрачати дані під час переходу на резервну копію. Це стосується видачі токенів та читання з каталогу, дозволяє лише близько 5 хвилин RTO для запису до каталогу

Центри обробки даних, що являються четвертим пунктом архітектури Microsoft Entra ID, мають такі характеристики:

Аутентифікація, Graph і інші служби AD розташовані за шлюзовою службою. Шлюзова служба керує балансуванням навантаження цих служб. Вона автоматично переключається у випадку виявлення несправних серверів за допомогою транзакційних зондів здоров'я. На основі цих зондів шлюз динамічно спрямовує трафік до здорових дата-центрів;

Для читання каталог має вторинні репліки та відповідні фронтальні служби в активній конфігурації, що працюють у кількох дата-центрах. Якщо

один з дата-центрів виходить з ладу, трафік автоматично перенаправляється до іншого дата-центру;

Для записів каталог переключає основну репліку між дата-центрами за допомогою планового (нова основна репліка синхронізується зі старою) або екстреного перемикання. Надійність даних досягається реплікацією будь-яких змін як мінімум у два дата-центри.

Модель каталогу базується на принципі кінцевої узгодженості. Однією з типових проблем у розподілених системах з асинхронною реплікацією є те, що дані, повернені з "певної" репліки, можуть бути неактуальними. Microsoft Entra ID забезпечує узгодженість записів і читань для застосунків, що орієнтовані на вторинну репліку, шляхом маршрутизації записів на основну репліку і синхронного повернення записів на вторинну репліку.

Записи застосунків, які використовують API Microsoft Graph у Microsoft Entra ID, абстраговані від підтримки зв'язку з реплікою каталогу для узгодженості читання-запису. Служба API Microsoft Graph підтримує логічну сесію, яка має зв'язок з вторинною реплікою, що використовується для читання; зв'язок зберігається в "токені репліки", який служба кешує, використовуючи розподілений кеш у дата-центрі вторинної репліки. Цей токен потім використовується для наступних операцій у тій самій логічній сесії. Щоб продовжити використання тієї самої логічної сесії, наступні запити повинні бути спрямовані до того ж дата-центру Microsoft Entra. Неможливо продовжити логічну сесію, якщо запити клієнта каталогу маршрутизуються до кількох дата-центрів Microsoft Entra; у такому випадку клієнт має кілька логічних сесій з незалежною узгодженістю читання-запису.

Розглянемо резервне копіювання на рівні служби. Microsoft Entra ID здійснює щоденне резервне копіювання даних каталогу і може використовувати ці резервні копії для відновлення даних у випадку загальної проблеми з обслуговуванням.

Каталог також реалізує м'яке видалення замість жорсткого видалення для обраних типів об'єктів. Адміністратор орендаря може скасувати будь-яке випадкове видалення цих об'єктів протягом 30 днів. Для отримання додаткової інформації дивіться API для відновлення видалених об'єктів.

Забезпечення високої доступності сервісу вимагає найкращих у своєму класі можливостей метрики та моніторингу. Microsoft Entra ID постійно аналізує і звітує ключові метрики здоров'я сервісу і критерії успішності для кожної зі своїх служб. Також здійснюється безперервна розробка і налаштування метрик, моніторингу і оповіщення для кожного сценарію, в межах кожної служби Microsoft Entra та серед усіх служб.

Розглянемо основні характеристики та можливості ліцензій Microsoft Entra ID.

Microsoft Entra ID Free - це безкоштовна ліцензія надає доступ до базових функцій керування користувачами та групами, синхронізації каталогів на місці, простих звітів та самообслуговування зміни пароля для хмарних користувачів. Також передбачено SSO для доступу до Azure, Microsoft 365 та популярних додатків SaaS.

Microsoft Entra ID P1 - доповнює функції безкоштовної версії, дозволяючи гібридним користувачам отримати доступ до ресурсів як в хмарі, так і на місці. Також підтримується розширене адміністрування, таке як динамічні групи, самообслуговування управління групами, Microsoft Identity Manager та можливості хмарного запису, які дозволяють самообслуговування скидання пароля для користувачів на місці.

Microsoft Entra ID P2 у додаток до функцій P1, P2 пропонує Microsoft Entra ID Protection для забезпечення умовного доступу на основі ризику до ваших додатків та важливих даних компанії, а також Privileged Identity Management для виявлення, обмеження та моніторингу адміністраторів та їх доступу до ресурсів.

Крім основних ліцензій, є можливість отримати додаткові можливості керування ідентифікацією з іншими продуктами Microsoft Entra:

Microsoft Entra ID Governance, де є розширені можливості управління ідентичністю для клієнтів P1 та P2;

Microsoft Entra Permissions Management - це рішення управління правами на основі хмарної інфраструктури, яке забезпечує повну видимість прав доступу до усіх ідентифікаторів, дій та ресурсів на хмарних інфраструктурах;

"Pay as you go" функціонал - це ліцензії для таких можливостей, як Microsoft Entra Domain Services та Microsoft Entra Business-to-Customer (B2C), які допомагають управляти доступом для зовнішніх користувачів.

Microsoft Entra ID - це потужний інструмент для організацій, який надає гнучкість та безпеку в управлінні ідентифікацією та доступом. Раніше він мав іншу назву - Azure Active Directory.

Компанія Microsoft перейменувала Azure Active Directory (Azure AD) на Microsoft Entra ID, щоб підкреслити багатохмарну та багатоплатформенну функціональність продуктів, усунути плутанину з Windows Server Active Directory та об'єднати продукти в сімействі Microsoft Entra. Усі функції та можливості продукту залишились доступними. Ліцензування, умови, угоди про рівень обслуговування, сертифікації продуктів, підтримка та ціни залишаються незмінними. Щоб забезпечити плавний перехід, всі існуючі URL-адреси для входу, API, командлети PowerShell та бібліотеки автентифікації Microsoft (MSAL) залишаються без змін.

Назви планів обслуговування змінилися 1 жовтня 2023 року. Нові назви окремих пропозицій: Microsoft Entra ID Free, Microsoft Entra ID P1 та Microsoft Entra ID P2. Усі можливості, включені до поточних планів Azure AD, залишаються такими ж. Microsoft Entra ID, раніше відомий як Azure AD,

продовжує входити до складу ліцензійних планів Microsoft 365, включаючи Microsoft 365 E3 та Microsoft 365 E5.

Microsoft Entra - це назва для сімейства продуктів і рішень для ідентифікації та доступу до мережі. Microsoft Entra ID є одним із продуктів у цьому сімействі.

Функції, раніше відомі як "Azure Active Directory <назва функції>" або "Azure AD <назва функції>", тепер відносяться до функцій сімейства продуктів Microsoft Entra. Наприклад, "Azure AD Conditional Access" тепер називається "Microsoft Entra Conditional Access". Назви Active Directory, інструментів розробників, Azure AD B2C, а також застарілі або виведені з експлуатації функції та служби залишаються незмінними.

Зміна назви у продуктах Microsoft розпочалася 15 серпня 2023 року. Назви SKU та планів обслуговування змінилися 1 жовтня 2023 року. Більшість змін текстових рядків у продуктах Microsoft та партнерських рішеннях було завершено до кінця 2023 року. Перейменування Azure AD на Microsoft Entra ID є частиною нашого прагнення спростити безпечний доступ для всіх. Нова назва точніше відображає багатохмарну та багатоплатформенну функціональність продукту, усуває плутанину з локальним рішенням для ідентифікації (Active Directory) та створює шлях для простішого захисту кожної ідентичності та кожної точки доступу. Зміни торкнулись, також, іконок додатків.

Рис. 2.4. Нові зображення іконок

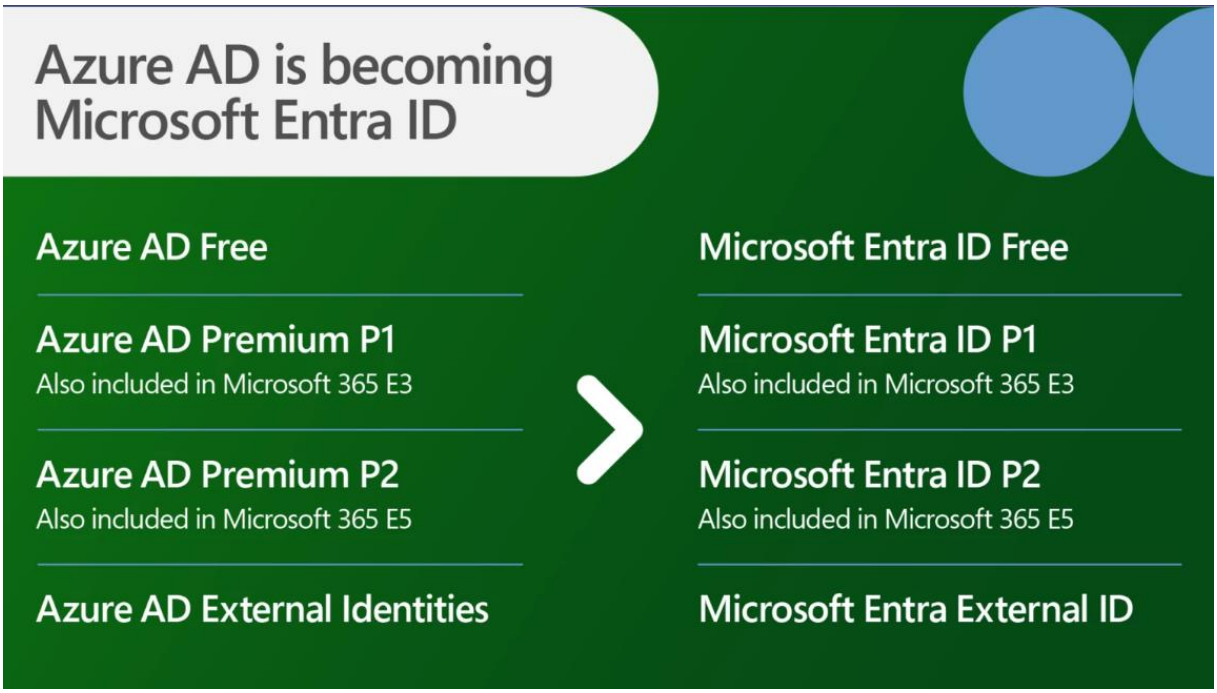

Рис. 2.5. Зі зміною імені на Microsoft Entra ID змінюються назви окремих ліцензій

2.2 Порівняння Microsoft Entra ID з іншими існуючими рішеннями

Візьмемо, для прикладу, рішення, які розглядали вище, а саме Okta, Ping Identity, LastPass Single Sign-On, AWS IAM Identity Center та порівняємо їх з Microsoft Entra ID. Порівняння буде сформоване на таких показниках, як управління ідентифікацією, централізоване керування доступом підтримка багатьох додатків, висока безпека та контроль доступу, простий та зручний інтерфейс, самообслуговування користувачів багатофакторна аутентифікація, інтеграція з іншими сервісами, вартість, складність налаштування та підтримка гібридних середовищ, що є найбільш важливими показниками для сучасних підприємств.

Таблиця 2.1.

Порівняння рішень для вирішення проблемі ідентифікації на підприємстві

Функція/Потреба користувача	*Okta*	*Ping Identity*	*LastPass Single Sign-On*	*AWS IAM Identity Center*	*Microsoft Entra ID*
Управління ідентифікацією	Так	Так	Так	Так	Так
Централізоване керування доступом	Так	Так	Так	Так	Так
Підтримка багатьох додатків	Так	Так	Так	Так	Так
Висока безпека та контроль доступу	Так	Так	Так	Так	Так
Простий та зручний інтерфейс	Так	Так	Так	Так	Так
Самообслуговування користувачів	Так	Так	Так	Так	Так
Багатофакторна аутентифікація	Так	Так	Так	Так	Так
Інтеграція з іншими сервісами	Так	Так	Так	Так	Так

Вартість	Висока	Висока	Середня	Середня	Середня
Складність налаштування	Помірна	Висока	Помірна	Висока	Помірна
Підтримка гібридних середовищ	Так	Так	Ні	Так	Так

Розглянемо оремо відмінності в рішенні кожної з програм:

Таблиця 2.2

Переваги кожного рішення

Okta	**Ping Identity**	**LastPass Single Sign-On**	**AWS IAM Identity Center**	**Microsoft Entra ID**
Велика кількість функцій та можливостей, гнучке налаштування та розширення.	Розширена підтримка протоколів та широкий спектр інтеграцій.	Зручний доступ до додатків на будь-яких пристроях.	Глибока інтеграція з AWS та іншими хмарними сервісами	Інтеграція з іншими продуктами Microsoft, зокрема з іншими хмарними послугами.

Звісно, всі рішення мають гарні показники та пропозиції, і це добре, що зараз клієнт може вибрати саме те, що подобається та підходить йому. Але зважаючи на різноманітність потреб користувачів у сфері керування ідентифікацією та доступом, Microsoft Entra ID вирізняється через декілька

ключових переваг порівняно з іншими рішеннями, такими як Okta, Ping Identity, LastPass Single Sign-On та AWS IAM Identity Center.

Microsoft Entra ID має глибоку інтеграцію з іншими продуктами Microsoft, такими як Office 365, Microsoft 365, Azure, Dynamics CRM та багатьма іншими. Це робить його ідеальним вибором для організацій, які вже використовують або планують використовувати продукти Microsoft.

Цей продукт надає гнучкість у конфігурації та масштабованості, що дозволяє підлаштовувати рішення під потреби різних типів організацій, від малих підприємств до великих корпорацій.

Microsoft Entra ID інтегрується з широким спектром хмарних послуг, не лише від Microsoft, але й від інших постачальників хмарних рішень, що дозволяє організаціям легко керувати доступом до різних хмарних ресурсів.

Microsoft Entra ID пропонує широкий набір інструментів для захисту ідентичності та доступу, включаючи багатофакторну аутентифікацію, управління привілеями, управління ризиками та аналіз активності.

Продукт Microsoft Entra ID надає підтримку гібридних середовищ, що дозволяє організаціям безпечно і ефективно керувати доступом до ресурсів як у хмарі, так і в локальних системах.

Загалом, Microsoft Entra ID вирізняється своєю глибокою інтеграцією з продуктами Microsoft, гнучкістю, масштабованістю та широким спектром інструментів для захисту ідентичності та доступу, що робить його привабливим вибором для багатьох організацій, особливо тих, які вже використовують екосистему Microsoft.

Одні з провідних компаній, закладів, підприємств та державних органів, що використовують Microsoft Entra, є Audi, UK Driver & Vehicle Standards Agency, Otto Group, Oregon State University, Domino’s Pizza Enterprises, LEGO House, Howard University, Dr. Oetker та Jacobs Solutions Inc. Всі вони дуже задоволені цим партнерством та вирішили не одну проблему завдяки сервісам Microsoft, серед яких є Microsoft Entra ID.

Компанія AUDI AG, відома своїми автомобілями та мотоциклами в преміум та люксових сегментах, а також своїм технологічним лідерством, розпочала трансформацію IT з Microsoft Intune для спрощення управління пристроями та підвищення безпеки. За допомогою Intune Audi прагнула спростити роботу користувачів, зменшити залежність від IT та забезпечити безпечний, безперебійний доступ до ресурсів.

Цей стратегічний крок дозволив мігрувати 40 000 пристроїв на єдину платформу управління, підвищуючи ефективність операцій та задоволеність користувачів без компромісів щодо персональних налаштувань. Ініціатива Audi демонструє її інноваційний підхід та встановлює стандарт для безпечної та ефективної трансформації робочого місця в автомобільній промисловості.

Microsoft Entra ID допоміг Audi, де IT-відділ прагнув покращити досвід співробітників, спростивши процеси управління пристроями, скоротивши витрати та підкресливши синергію, дотримуючись строгих політик безпеки Volkswagen Group. Audi шукала рішення для самоуправління пристроями, яке б підвищило автономію співробітників і зменшило потребу у втручанні IT, сприяючи культурі автономії, інновацій та ефективності.

Використовуючи Intune, співробітники Audi можуть самостійно «скидати» паролі та отримувати доступ до корпоративних додатків без затримок з боку IT-відділу. Сильні функції відповідності та звітності рішення відповідають моделі безпеки Zero Trust, забезпечуючи високий рівень захисту як корпоративних, так і приватних даних.

Ініціативи Audi в області IT, підтримувані продуктами Microsoft, значно підвищили ефективність операцій, зменшили витрати та покращили задоволеність співробітників. Використання рішень компанії Microsoft демонструє, як інновації та передові технології можуть сприяти розвитку та зміцненню лідерських позицій Audi в автомобільній промисловості.

Продукт Microsoft Entra ID допоміг Domino's Pizza Enterprises Ltd., глобальній мережа піцерій, що обслуговують клієнтів в Австралії, Новій Зеландії, Азії та Європі, які зіткнулись з викликом управління великою кількістю ідентифікаційних даних співробітників.

Для спрощення своєї IT-інфраструктури та зниження витрат компанія вирішила замінити свою попередню систему управління ідентифікацією Okta на Microsoft Entra ID. Це рішення мало великий вплив на ефективність роботи та безпеку компанії.

До липня 2023 року співробітники офісу підтримки використовували Microsoft Entra ID для доступу до додатків Microsoft 365, тоді як франчайзі та їхні команди в основному використовували Okta. Перехід на Microsoft Entra ID дозволив DPE уникнути витрат на ліцензування Okta, спростив управління IT-командою та забезпечив стандартизований і спрощений процес автентифікації для всіх співробітників.

Однією з ключових переваг використання Microsoft Entra ID стала можливість створення єдиної ідентичності для кожного співробітника, незалежно від кількості різних ролей чи локацій, де він працює. Це забезпечило точність даних та усунуло потребу в численних системах управління, які раніше використовувались для вирішення цієї проблеми.

Використовуючи Microsoft Entra ID, DPE запровадила функції єдиного входу (SSO), що дозволило співробітникам отримувати доступ до необхідних ресурсів з мінімальними зусиллями. Крім того, компанія використовує Conditional Access для підвищення безпеки, створюючи та впроваджуючи політики доступу залежно від ролей та потреб користувачів.

Перехід на Microsoft Entra ID допоміг Domino's Pizza Enterprises Ltd. скоротити витрати, підвищити продуктивність та забезпечити високий рівень безпеки даних. Використання єдиної платформи для управління ідентичностями співробітників дозволило компанії досягти нових висот у

ефективності та задоволеності співробітників, встановлюючи нові стандарти для IT-інфраструктури в галузі.

Microsoft Entra ID допоміг Howard University, ппровідному історично чорному навчальному закладі у Вашингтоні, який суттєво покращив свою безпеку завдяки розширеному використанню Microsoft Azure.

Після атаки програмного забезпечення-вимагача у 2021 році університет переглянув свою інфраструктуру та співпрацював з Cloudforce для оптимізації безпеки. Протягом трьох тижнів Howard відновив усі основні IT-сервіси, використовуючи рішення Microsoft.

Завдяки підтримці Microsoft та співпраці з Cloudforce, Howard University зміг модернізувати свою IT-інфраструктуру, підвищити безпеку, оптимізувати витрати та підтримати своїх студентів та співробітників.

2.3 Порядок функціонування рішення Microsoft Entra ID

Порядок функціонування складається з декількох етапів:

Запит користувача, де користувач звертається до програми або веб-сайту, який використовує Microsoft Entra ID для автентифікації та авторизації. Програма або веб-сайт надсилає запит до служби Microsoft Entra ID, щоб отримати токен доступу;

Автентифікація, коли Служба Microsoft Entra ID перевіряє ім'я користувача та пароль користувача і якщо ім'я користувача та пароль правильні, служба Microsoft Entra ID видає токен доступу користувачу;

В момент *авторизації*, програма або веб-сайт використовує токен доступу, щоб надати користувачеві доступ до ресурсів, а служба Microsoft Entra ID перевіряє токен доступу та права користувача. Якщо користувач має необхідні права, служба Microsoft Entra ID дозволяє програмі або веб-сайту надати користувачеві доступ до ресурсів;

Далі користувач отримує *доступ до ресурсів*, на які йому надано дозволи. Програма або веб-сайт використовує токен доступу для взаємодії з ресурсами;

Реєстрація та управління користувачами - адміністратори можуть створювати, видаляти та змінювати користувачів у Microsoft Entra ID. Адміністратори можуть призначати користувачам ролі та дозволи;

Microsoft Entra ID використовує різні методи для *захисту даних*, такі як шифрування, контроль доступу на основі ролей та аудиторський журнал;

Масштабованість та доступність, коли Microsoft Entra ID може масштабуватися, щоб підтримувати велику кількість користувачів і запитів. Microsoft Entra ID забезпечує високу доступність, щоб користувачі могли отримувати доступ до ресурсів цілодобово;

Microsoft Entra ID надає адміністраторам можливості для *моніторингу та звітування* про використання служби.

Також, Microsoft Entra ID підтримує багатофакторну аутентифікацію для підвищення безпеки, самообслуговування користувачів, щоб користувачі могли скидати паролі та оновлювати свою інформацію. Microsoft Entra ID інтегрується з іншими продуктами Microsoft, такими як Microsoft Teams та Microsoft 365.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО КЕРУВАННЯ ІДЕНТИФІКАЦІЇ ТА ДОСТУПУ КОРИСТУВАЧІВ НА ПІДПРИЄМСТВІ

3.1 Варіант розгортання системи ідентифікації на базі Microsoft Entra ID

Впровадження такого інструменту керування ідентифікацією та доступом, як Microsoft Entra ID, має вирішальне значення для забезпечення безпеки та ефективного управління доступом до ресурсів підприємства. Незалежно від розміру організації, метою рішення є централізоване керування ідентифікацією користувачів, захист ідентифікаційних даних, а також поліпшення безпеки і відповідальності у всьому бізнес-процесі.

Процес розгортання рішення Microsoft Entra ID розпочинається з детальної оцінки поточних практик керування ідентифікацією та доступом. Це дозволяє ідентифікувати ключові аспекти, де потрібно зосередити зусилля на покращенні. Аналізуючи існуючі стратегії, IT-фахівці можуть визначити найбільш вразливі області своєї інфраструктури.

Після оцінки настає етап планування, на якому формуються чіткі цілі та обираються методики їх досягнення. Важливо встановити реалістичні терміни та розрахувати необхідні ресурси, щоб забезпечити успішне впровадження платформи керування ідентифікацією, аби в подальшому не створити ще більше проблем.

Конфігурація є ключовим моментом у адаптації Microsoft Entra ID до специфічних потреб підприємства. Слідуючи детальним інструкціям, що знаходяться в вільному доступі на офіційному сайті, команди налаштовують інструментарій так, щоб він ефективно інтегрувався з існуючими робочими

процесами та забезпечував необхідний рівень безпеки. Підтримка Microsoft Entra ID завжди на зв’язку з користувачами, якщо виникла проблема з встановленням ПЗ на ПК.

На етапі розгортання команди впроваджують Microsoft Entra ID у свої процеси керування ідентифікацією та доступом. Це включає навчання IT-фахівців правильному використанню інструментів для забезпечення безпеки їхньої інфраструктури.

Розгортання в корпоративному середовищі може вимагати додаткових кроків для забезпечення масштабування та управління. Не менш важливим є проведення навчання для користувачів на підприємстві, щоб уникнути в подальшому проблем з роботою та розумінням ПЗ. Звісно, команда Microsoft Entra ID добре попрацювала над створенням максимально простого і зрозумілого інтерфейсу, але не можна виключати момент, описаний раніше.

Навчання IT-фахівців відіграє важливу роль у процесі розгортання, оскільки підвищує обізнаність команди щодо принципів безпеки та користування платформою Microsoft Entra ID. Ефективне використання інструментів значно зменшує ризики для підприємства. Підчас навчання, IT-фахівці можуть також отримати необхідні знання ля спрощення процесу налаштування та інтеграції ПЗ.

Завершує процес регулярний моніторинг та ітерації, які допомагають відслідковувати ефективність запроваджених змін і вносити корективи. Це зможе забезпечити постійне вдосконалення безпеки системи у відповідності до змінюваних вимог та загроз.

На офіційному сайті Microsoft Entra ID присутні декілька варіантів доступу до можливостей ПЗ. Azure Active Directory тепер має назву Microsoft Entra ID. Розглянемо основні можливості, щоб підібрати той варіант, який підходить певному підприємству.

Таблиця 3.1.

Порівняння тарифних планів

	Ідентифікатор Microsoft Entra Free	Azure Active Directory Premium P1	Azure Active Directory Premium P2	Microsoft Entra ID Governance
Ціна за одного користувача на місяць (без податку)	Безкоштовно	USD$6.00	USD$9.00	USD$7.00
Що входить в пакет	Включено в передплати на хмарні продукти корпорації Майкрософт, такі як Microsoft Azure, Microsoft 365 тощо.	Ідентифікатор Microsoft Entra (план 1) (попередня назва – Azure Active Directory (план 1)) доступний окремо або входить у Microsoft 365 E3 для корпоративних клієнтів і Microsoft 365 Business преміум для малого та середнього бізнесу, включно з версіями цих програмних комплексів, що не включають Microsoft Teams.	Ідентифікатор Microsoft Entra (план 2) (попередня назва – Azure Active Directory (план 2)) доступний окремо або входить у Microsoft 365 E5 для корпоративних клієнтів, включно з версіями цього програмного комплексу, що не включають Microsoft Teams.	Керування ідентифікатором Microsoft Entra – це розширений набір можливостей для керування ідентичностями, доступний для клієнтів з Ідентифікатором Microsoft Entra (план 1 і план 2). Для клієнтів Microsoft Entra P2 доступні спеціальні ціни.

Також на офіційному сайті детально розписано, що отримує користувач при підключенні одного з пакетів. Кожен пункт можна розгорнути та ознайомитись

Рис. 3.1. Що входить в кожен план. З ліва на право - Ідентифікатор Microsoft Entra Free, Azure Active Directory Premium P1, Azure Active Directory Premium P2, Microsoft Entra ID Governance

Для початку роботи з ПЗ Microsoft Entra ID, необхідно створити акаунт Microsoft Azure.

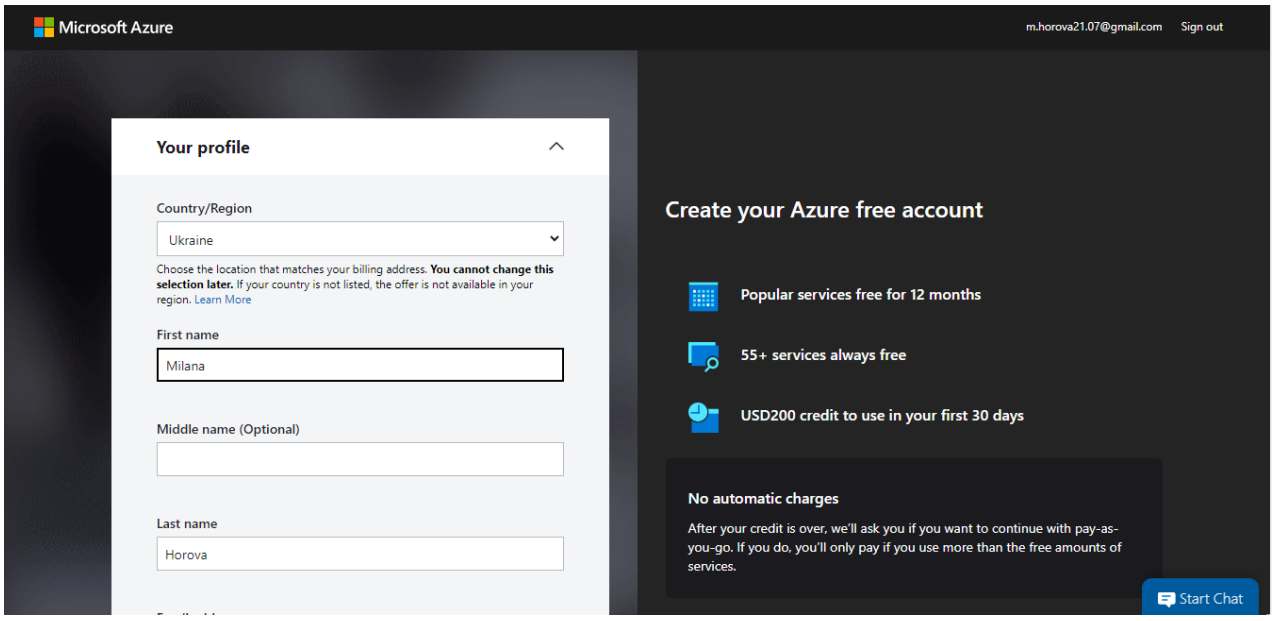

Рис. 3.2. Реєстрація акаунта Microsoft Azure

Після вдалої реєстрації чи входу, ми можемо потрапити в Центр адміністрування Microsoft Entra.

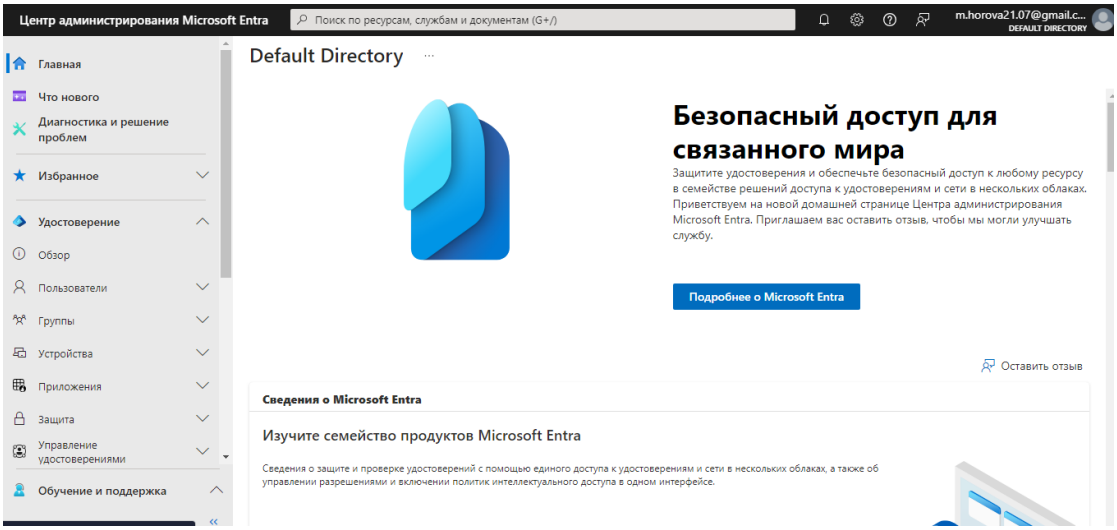

Рис. 3.3. Центр адміністрування Microsoft Entra

Це веб інтерфейс нашої програми. Тут ми можемо налаштовувати всю роботу, процеси, додавати нових користувачів, робити перевірки та аналізувати наявність проблем.

Дуже зручним моментом є те, що програма допомагає новим користувачам швидко зорієнтуватись та почати налаштування найбільш важливих моментів.

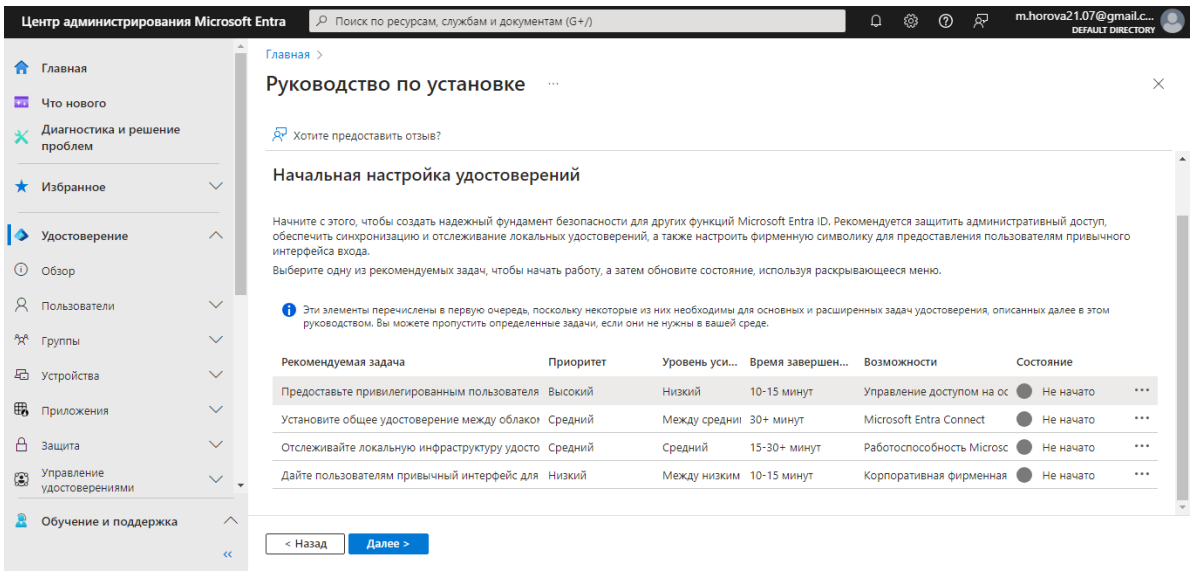

Рис. 3.4. Посібник зі встановлення

Якщо якийсь етап незрозумілий, можна завжди детальніше про нього дізнатись. Достатньо всього натиснути на нього, і меню з підказкою коротко розкаже про нього і необхідність налаштування.

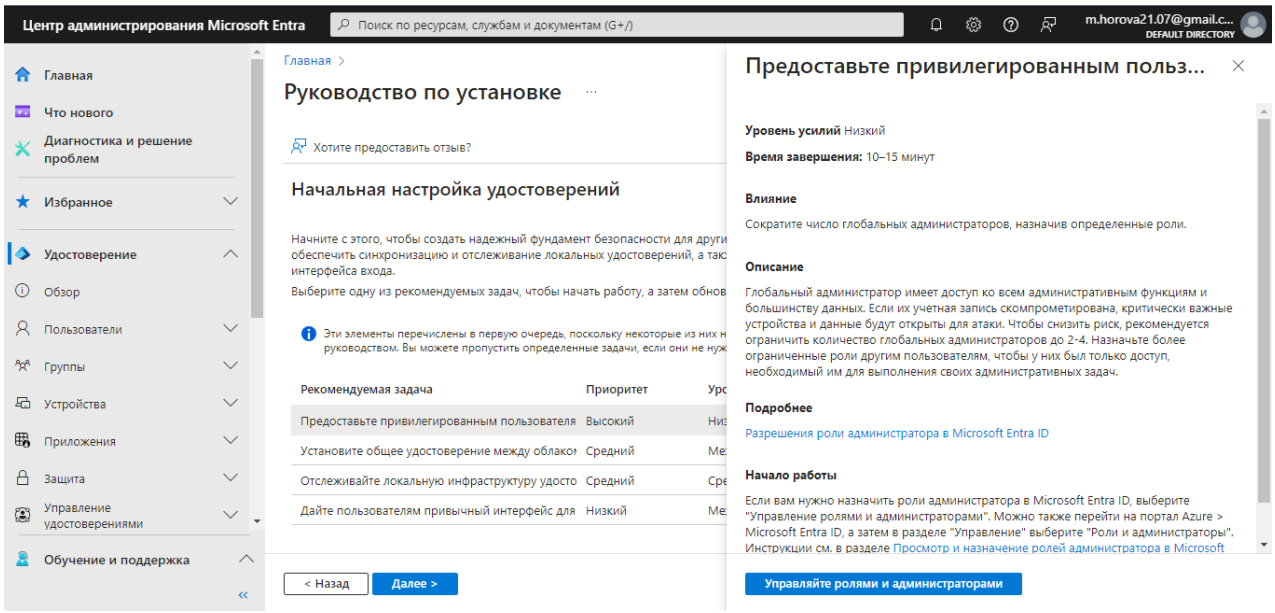

Рис. 3.5. Пояснення одного з етапів

Розглянемо інформацію, яку можна використовувати для планування розгортання єдиного входу (SSO) у Microsoft Entra ID. Коли ви плануєте розгортання системи єдиного входу за допомогою програм у Microsoft Entra ID, вам потрібно розглянути певні запитання. Які адміністративні ролі необхідні для керування програмою? Чи потрібно оновлювати сертифікат програми Security Assertion Markup Language (SAML)? Кого необхідно повідомляти про зміни, пов’язані із впровадженням CCO? Які ліцензії потрібні для ефективного керування програмою? Чи використовуються спільні та гостьові облікові записи користувачів для доступу до програми? Чи розумію я варіанти розгортання SSO?

Розглянемо адміністративні ролі. Завжди використовуйте роль із найменшою кількістю доступних дозволів для виконання необхідного завдання в Microsoft Entra ID. Ознайомтеся з різними доступними ролями та виберіть правильну, яка відповідає вашим потребам для кожної персони для програми.

Деякі ролі може знадобитися тимчасово застосувати та видалити після завершення розгортання.

Persona	Roles	Microsoft Entra role (if necessary)
Help desk admin	Tier 1 support view the sign-in logs to resolve issues.	None
Identity admin	Configure and debug when issues involve Microsoft Entra ID	Cloud Application Administrator
Application admin	User attestation in application, configuration on users with permissions	None
Infrastructure admins	Certificate rollover owner	Cloud Application Administrator
Business owner/stakeholder	User attestation in application, configuration on users with permissions	None

Рис. 3.6. Опис ролей

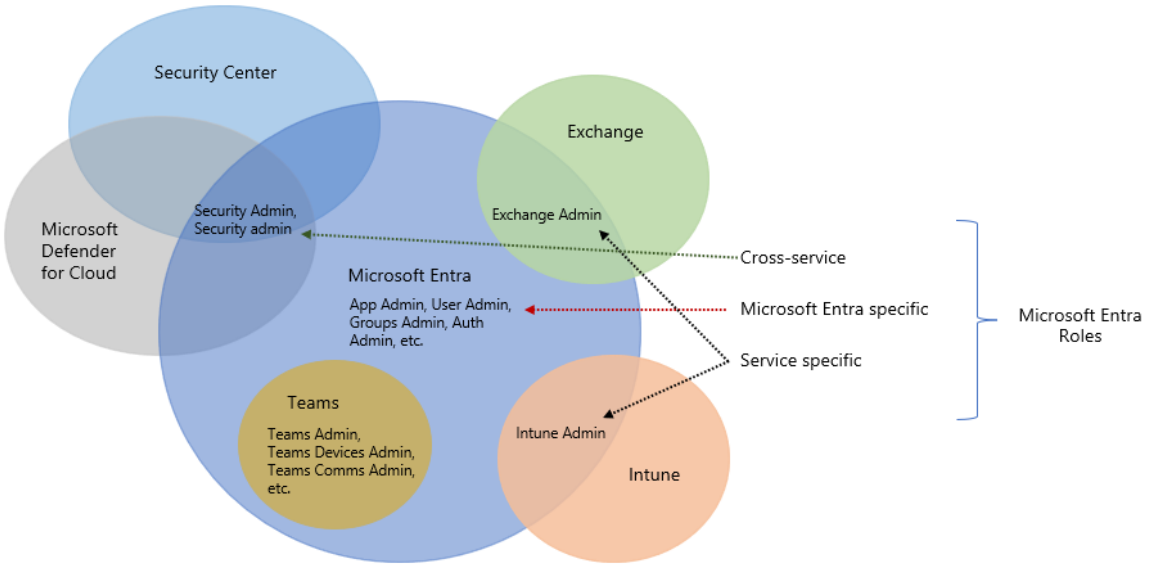

Рис. 3.7. Схематичне зображення доступу на основі ролей

Розглянемо сертифікати. Коли вмикається об’єднання в програмі SAML, Microsoft Entra ID створює сертифікат, який за замовчуванням дійсний протягом трьох років. За потреби ви можете налаштувати дату закінчення

терміну дії цього сертифіката. Переконайтеся, що у вас є процеси для оновлення сертифікатів до закінчення терміну їх дії.

Ми можемо змінити тривалість цього сертифіката в центрі адміністрування Microsoft Entra. Необхідно обов’язково задокументувати закінчення терміну дії. Важливо визначити правильні ролі та списки розсилки електронної пошти, пов’язані з керуванням життєвим циклом сертифіката підпису. Рекомендуються такі ролі:

власник для оновлення властивостей користувача в програмі;

власник за викликом для підтримки усунення несправностей програми.

3.2 Керування доступом до ресурсів в рішенні Microsoft Entra ID

Розглянемо детальніше облікові записи користувачів.

У Microsoft Entra ID всі облікові записи користувачів отримують набір стандартних дозволів. Доступ до облікового запису користувача визначається типом користувача, призначеними йому ролями та володінням окремими об'єктами.

У Microsoft Entra ID існують різні типи облікових записів користувачів. Кожен тип має рівень доступу, який відповідає обсягу роботи, що очікується від відповідного типу облікового запису. Адміністратори мають найвищий рівень доступу, за ними йдуть користувачі-члени організації Microsoft Entra. Гостьові користувачі мають найбільш обмежений рівень доступу.

Розглянемо інструкцію створення облікового запису користувача. Їх можна додавати через портал Azure, Azure PowerShell або Azure CLI. При використанні Azure CLI запускаємо такий командлет:

```
Azure CLI                                                    Copy

# create a new user
az ad user create
```

Рис. 3.8. Команда для створення нового облікового запису при використанні Azure CLI

Для Azure PowerShell запускаємо такий командлет:

```
PowerShell                                                   Copy

# create a new user
New-MgUser
```

Рис. 3.9. Команда для створення нового облікового запису при використанні Azure PowerShell

Ми можете масово створювати облікові записи учасників і гостей. На Рис. 3.10 показано, як масово запросити користувачів-гостей.

```
PowerShell                                                   Copy

$invitations = import-csv c:\bulkinvite\invitations.csv

$messageInfo = [Microsoft.Graph.PowerShell.Models.MicrosoftGraphInvitation]@{ `
   CustomizedMessageBody = "Hello. You are invited to the Contoso organization." }

foreach ($email in $invitations)
   {New-MgInvitation `
      -InviteRedirectUrl https://myapps.microsoft.com `
      -InvitedUserDisplayName $email.Name `
      -InvitedUserEmailAddress $email.InvitedUserEmailAddress `
      -InvitedUserMessageInfo $messageInfo `
      -SendInvitationMessage
   }
```

Рис. 3.10. Команда для створення масового запрошення колристувачів-гостей

Після додавання користувачів, необхідно створити організацію в Microsoft Entra. Для його необхідно виконати наступні кроки:

увійти в портал Azure;

на домашній сторінці порталу Azure у розділі «Служби Azure» виберіть «Створити ресурс»;

у розділі «Створити ресурс» у меню ліворуч у розділі «Категорії» виберіть «Ідентифікація». У розділі Популярні служби Azure виберіть Створити в розділі Microsoft Entra ID.

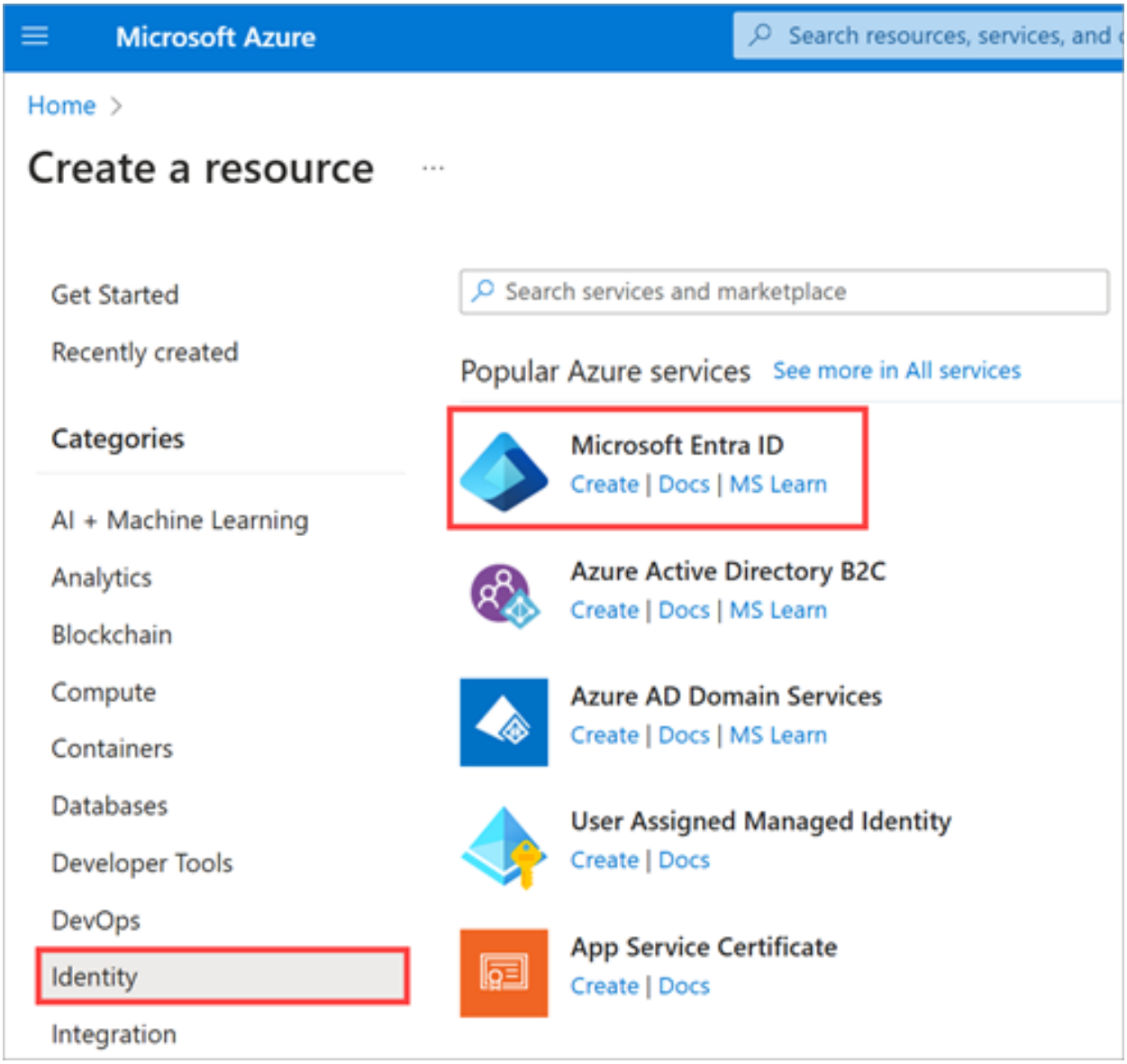

Рис. 3.11. Створення організації в Microsoft Entra ID

Після цього, у розділі «Створити клієнта» на вкладці «Основні» введіть таке значення параметра.

Таблиця 3.2.

Значення параметрів

Setting	**Value**
Tenant type	
Select a tenant type	Microsoft Entra ID

Виберіть «Далі: Конфігурація» та введіть наступні значення для кожного параметра.

Таблиця 3.3.

Введення значення параметрів

Setting	**Value**
Directory details	
Organization name	Enter *Contoso Marketing Company*
Initial domain name	Enter *contosomarketingXXXX* where you replace XXXX with numbers or letters to make your domain name unique

Вибераємо «Далі: переглянути + створити».

Після проходження перевірки вибераємо «Створити». Після цього, з’явиться панель «Допоможіть підтвердити, що ви не робот». Введимо відповідний код з капчі та вибираємо «Надіслати». Чекаємо завершення створення організації. На панелі «Допоможіть підтвердити, що ви не робот»,

виберіть посилання «Натисніть тут, щоб перейти до нового клієнта: маркетингова компанія Contoso».

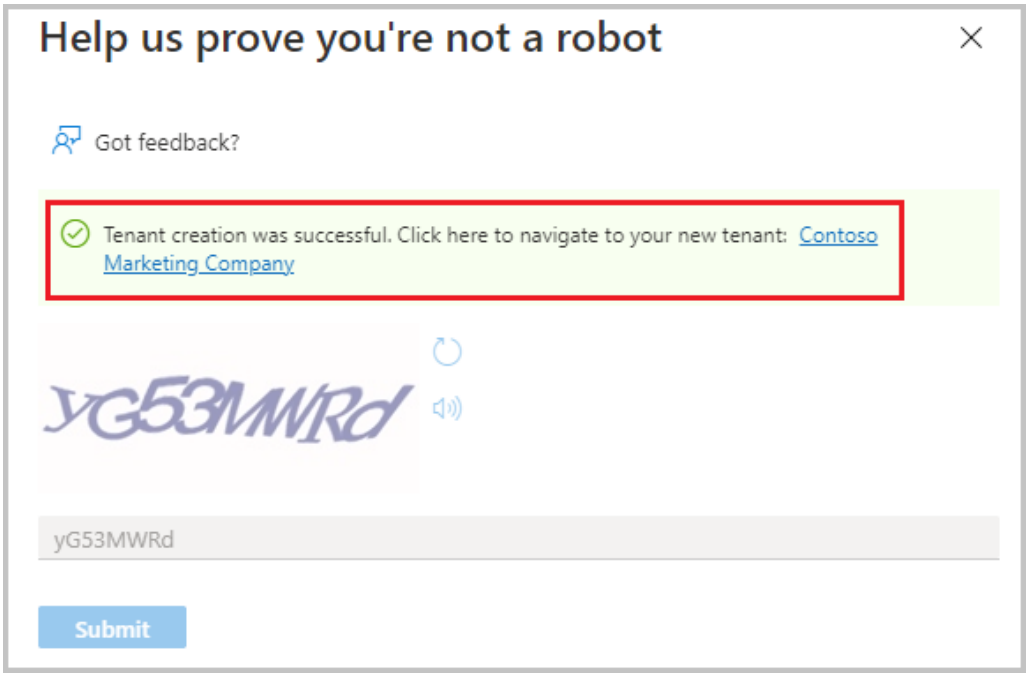

Рис. 3.12. Панель огляду для Contoso Marketing Company.

Тепер розглянемо додавання облікового запису користувача. У створеній раніше організації в Microsoft Entra, у лівій панелі меню, у розділі "Управління", вибераємо "Користувачі". Відкриється панель "Усі користувачі". У верхньому меню натискаємо "Новий користувач", а потім у випадаючому списку вибераємо "Створити нового користувача". Відкриється панель "Новий користувач" для компанії Contoso Marketing. Вводимо значення для кожного параметра.

Таблиця 3.4.

Дані про користувача

Ідентифікація
Ім'я користувача: chris@contosomarketingXXXXXX.onmicrosoft.com.
Ім'я: Chris Green

Звертаємо увагу, що доменне ім'я повинно відповідати основному домену, який скопіювали в попередньому розділі.

Переходимо до створення паролю. Після вдалого створення, натискаємо "Переглянути + Створити", потім вибераємо "Створити". Відкриється панель "Усі користувачі" для компанії Contoso Marketing - Microsoft Entra ID. Користувача створено та зареєстровано в організації.

Розглянемо управління доступом до додатків та ресурсів за допомогою груп. Microsoft Entra ID допомагає вам керувати ваших хмарних додатками, додатками на місці розташування та ресурсами за допомогою груп вашої організації. Ваші ресурси можуть бути частиною організації Microsoft Entra, наприклад, дозволи на управління об'єктами через ролі. Або ваші ресурси можуть бути зовнішніми для організації, як, наприклад, додатки як послуга (SaaS), служби Azure, сайти SharePoint та ресурси на місці розташування.

Використовуємо ролі Microsoft Entra для керування ресурсами, пов'язаними з Microsoft Entra ID, такими як користувачі, групи, розрахункові документи, ліцензування, реєстрація додатків та інше.

Також, використовуємо ролі RBAC для управління доступом до ресурсів Azure, таких як віртуальні машини, бази даних SQL або сховища. Наприклад, ми можемо призначити роль RBAC користувачу для керування та видалення баз даних SQL у певній групі ресурсів або передплаті.

Microsoft Entra ID допомагає нам надати права доступу або одному користувачеві, або цілій групі користувачів. Ми можемо призначити набір прав доступу всім членам групи. Права доступу можуть варіюватися від повного доступу до можливості створення або видалення ресурсів.

Існують різні способи призначення прав доступу, такі як:

пряме призначення, де користувачу призначаються потрібні права доступу, безпосередньо призначивши роль з необхідними правами доступу;

призначення групи, де ми призначаємо групі потрібні права доступу, і інші члени групи автоматично отримають ці права;

призначення на основі правил, де ми використовуємо правила для визначення членства у групі на основі властивостей користувача або пристрою. Для того щоб обліковий запис користувача або членство пристрою у групі було валідним, користувач або пристрій повинні відповідати правилам. Якщо правила не виконуються, членство облікового запису користувача або пристрою в групі більше не вважається валідним. Правила можуть бути простими. Ми можемо вибрати заздалегідь написані правила або написати свої власні розширені правила.

Розглянемо додавання користувачів до груп, що значно полегшить процес налаштування доступу. Ми можемо додавати користувачів і групи до кількох підписок. Це дозволяє користувачеві створювати, контролювати та отримувати доступ до ресурсів у підписці. Коли користувача додають до підписки, він має бути відомий пов'язаному каталогу, як показано на Рис. 3.13.

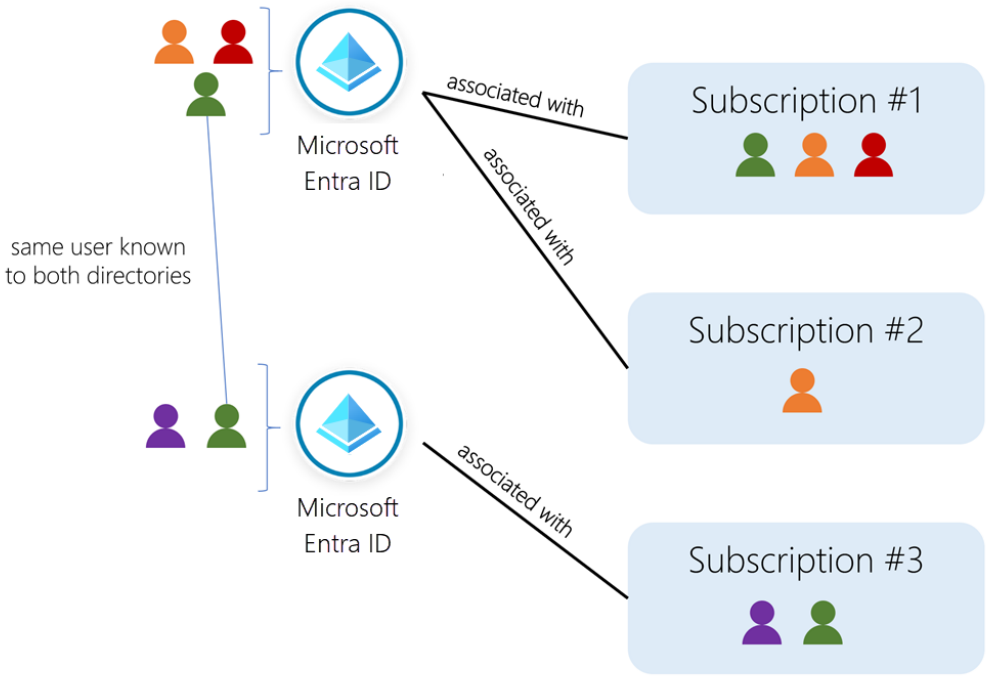

Рис. 3.13. Схема роботи груп користувачів та підписок

Для створення групи, переходимо до порталу Azure. Переходимо до Microsoft Entra ID. У лівій панелі меню, в розділі "Керувати", виберіть "Групи". З'явиться панель "Всі групи" для Microsoft Entra ID. На верхній панелі меню виберіть "Нова група". З'явиться панель "Нова група".

Вводимо наступні значення для кожного параметра.

Таблиця 3.5.

Значення параметрів для групи

Setting	**Value**
Group type	Security
Group name	Developer group
Group description	Developer team

Вибираємо «Створити». Панель «Групи | Усі групи» з’явиться, включаючи нову групу в списку. Можливо, для цього знадобиться оновити сторінку, щоб побачити нову групу. Тепер ми можемо призначити учасників до «групи розробників». Вибираємо «групу розробників». Після цього з’явиться «Панель групи розробників». На лівій панелі меню в розділі «Керування» вибираємо «Учасники». Для «групи розробників» з’явиться панель «Учасники». У верхній панелі меню вибираємо «Додати учасників».

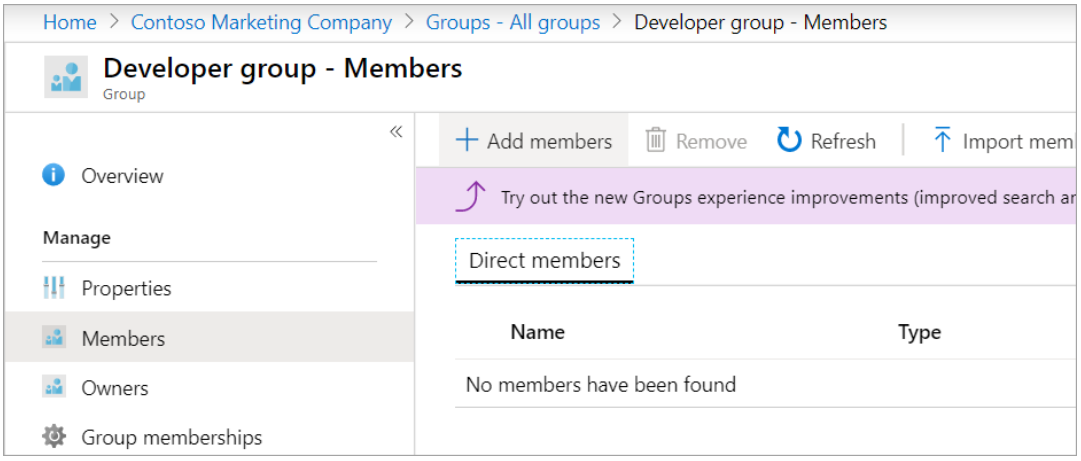

Рис. 3.14. Додавання учасників до групи

Знаходимо і вибираємо раніше створеного користувача, в нашому випадку Кріса Гріна. Натискаємо «Вибрати». Після цього ми побачимо цього користувача в списку безпосередніх учасників для групи «Розробники» на панелі «Учасники». Можливо, для цього знадобиться оновити сторінку, щоб побачити користувачів.

Розглянемо зміну групи для використання динамічного призначення. Членство в цьому випадку залежить від того, чи відповідає користувач правилам, які ви встановили для групи.

Якщо не використовується версія для Microsoft Entra ID P1 або P2, чи не активовано безкоштовний пробний період - ми не зможемо завершити цей етап.

У лівій панелі меню, в розділі "Керувати", вибираємо "Властивості". З'явиться панель "Властивості" для «групи розробників». Змінюємо тип «Членство» на «Динамічний користувач». Під «Динамічні користувачі» виберіть посилання «Додати динамічний запит».

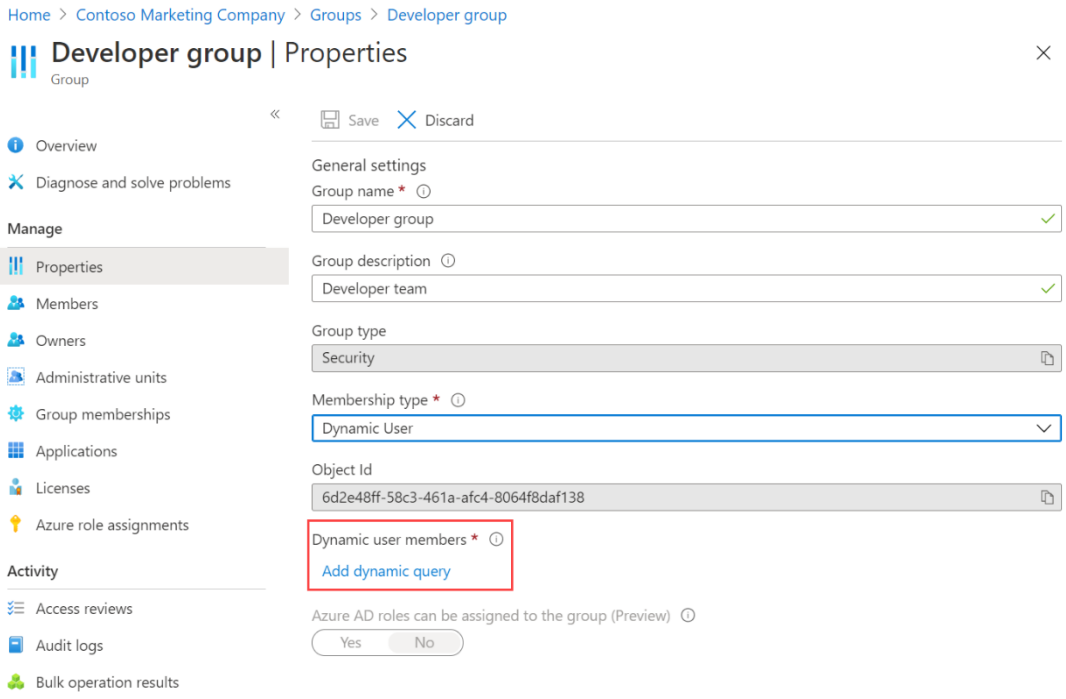

Рис. 3.15. Панель динамічного користувача

На вкладці «Налаштувати правила» вибираємо значення для правила.

Таблиця 3.6.

Значення для Динамічних користувачів

Setting	**Value**
Property	country
Operator	Equals
Value	United States

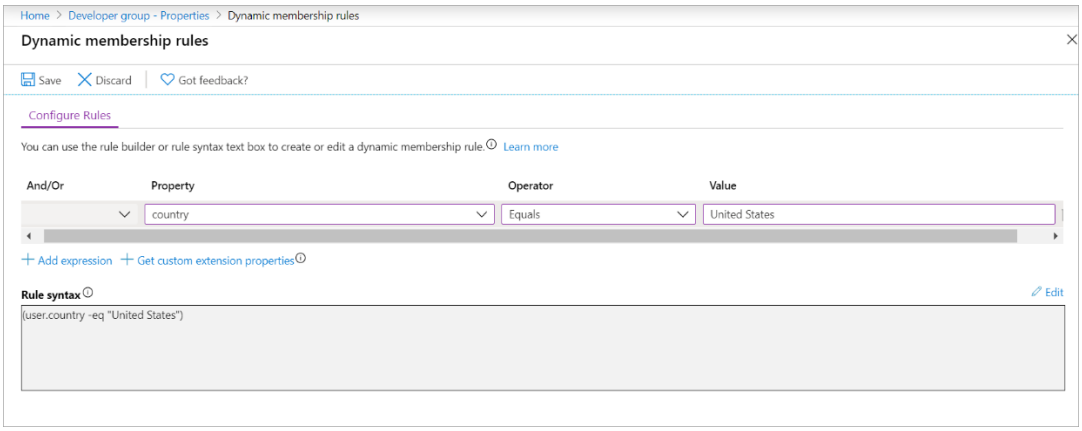

Рис. 3.16. Приклад, як членство в групі залежить від того, чи перебуває користувач у Сполучених Штатах.

Зберігаємо зміни, після чого для групи «Розробники» знову з’явиться панель властивостей.

3.3 Рекомендації щодо застосування керування ідентифікації та доступу користувачів на підприємстві

Керування ідентифікацією та доступом є критично важливим аспектом безпеки для будь-якого підприємства. Впровадження ефективної системи IAM

забезпечує надійний захист ресурсів компанії, одночасно забезпечуючи зручність доступу для користувачів.

Важливо вибрати платформу, яка відповідає потребам підприємства. Необхідно враховувати такі фактори, як масштабованість, сумісність з існуючими системами, можливості для інтеграції з хмарними та локальними ресурсами, а також підтримка багатофакторної аутентифікації.

Необхідно забезпечити, щоб користувачі мали лише ті права доступу, які необхідні для виконання їхніх службових обов'язків. Це зменшить ризик зловживання привілеями та підвищить загальну безпеку системи.

Бажано використовувати багатофакторну аутентифікацію для підвищення рівня безпеки. MFA вимагає від користувачів надання додаткового фактору аутентифікації, такого як одноразовий код, відбиток пальця або смарт-карта, що значно ускладнює несанкціонований доступ.

Важливим є регулярне проведення перевірки прав доступу користувачів та журналів активності. Це допоможе виявляти та реагувати на підозрілі дії та забезпечувати відповідність політикам безпеки.

Використання автоматизованих інструментів для управління ідентифікацією та доступом допоможе зменшити кількість помилок, прискорити процеси надання та відкликання доступу, а також покращити загальну ефективність управління IAM.

Використання підходу Role-Based Access Control для управління доступом, призначаючи користувачам ролі відповідно до їхніх службових обов'язків спрощує управління доступом і підвищує безпеку.

Особливо уважно треба підійти до захисту облікові записи адміністраторів та інших користувачів з підвищеними правами доступу. Використання додаткових заходів безпеки, такі як посилена аутентифікація та розширений моніторинг активності допоможуть в цьому.

Регулярне проведення тренінгів для співробітників щодо політик безпеки та найкращих практик управління ідентифікацією та доступом підвищить обізнаність користувачів та допоможе запобігти багатьом загрозам.

Інтегрування IAM-системи з іншими засобами кібербезпеки, такими як системи виявлення загроз, антивірусні програми та системи запобігання витоку даних, дозволить створити цілісну та узгоджену стратегію безпеки.

Застосування динамічних груп та правила призначення для автоматичного управління членством у групах на основі властивостей користувачів або пристроїв допоможе забезпечити актуальність і точність прав доступу.

Впровадження цих рекомендацій допоможе вашому підприємству побудувати ефективну систему управління ідентифікацією та доступом, що забезпечить високий рівень безпеки та зручність для користувачів.

ВИСНОВКИ

Проведено аналіз сучасних методів ідентифікації користувачів, що є критично важливим для забезпечення цілісності інформації та запобіганню несанкціонованого доступу.

Розглянуто шляхи інтеграції системи ідентифікації з використанням рішення Microsoft Entra ID, яке демонструє високу ефективність у в порівнянні з іншими рішеннями.

Встановлено значні переваги MFA для ідентифікації користувачів, а також важливість автоматизації процесів налаштування для спрощення управління доступом.

Рекомендації, розроблені на основі дослідження, спрямовані на підвищення ефективності процесів ідентифікації користувачів та забезпечення безпеки на підприємстві, включають необхідність впровадження надійних систем керування доступом, інтеграцію багатофакторної аутентифікації, а також використання можливостей платформи Microsoft Entra ID. Реалізація таких рекомендацій дозволить організаціям покращити свої стратегії управління ідентифікацією, мінімізувати ризики несанкціонованого доступу та ефективно реагувати на постійно змінювані загрози безпеці.

Здобуті результати дослідження вказують на ключові напрямки для вдосконалення систем ідентифікації користувачів, підкреслюючи значення впровадження передових технологій. Результати пропонують наукове та практичне використання, сприяючи розробці надійних систем управління ідентифікацією та доступом. Важливим фактором є імплементація сучасних методів аутентифікації та авторизації, що сприятиме підвищенню загального рівня безпеки підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 29.03.2006 р. № 373 : станом на 21 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 27.02.2024).

2. Role-Based Access Control. Access Control Systems. Boston. P. 190–251. URL: https://doi.org/10.1007/0-387-27716-1_8 (дата звернення: 28.02.2024).

3. Моделі та методи контролю доступу. Worldvision – інтернет магазин систем безпеки. URL: https://worldvision.com.ua/modeli-i-metody-kontrolya-dostupa-chto-vam-podkhodit/ (дата звернення: 01.03.2024).

4. 9 найкращих постачальників систем єдиного входу (система єдиного входу) 2024. Guru99. URL: https://www.guru99.com/uk/best-single-sign-on-sso-solution-providers.html#6-aws-iam-identity-center (дата звернення: 02.03.2024).

5. Ідентифікатор Microsoft Entra. Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/identity-access/microsoft-entra-id#overview (дата звернення: 03.03.2024).

6. What is Microsoft Entra ID? - Microsoft Entra. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/uk-ua/entra/fundamentals/whatis (date of access: 04.03.2024).

7. Okta - Управління Ідентифікацією | Офіційний Партнер - Cloudfresh. Cloudfresh. URL: https://cloudfresh.com/ua/produkty/okta/ (дата звернення: 04.03.2024).

8. Identity Security for the Digital Enterprise. Identity Security for the Digital Enterprise | Ping Identity. URL: https://www.pingidentity.com/en.html (дата звернення: 07.03.2024).

9. What is Single Sign-On?. Lastpass. URL: https://www.lastpass.com/products/sso (date of access: 09.03.2024).

10. Single-Sign On - AWS IAM Identity Center - AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/iam/identity-center/?nc1=h_ls (дата звернення: 10.03.2024).

11. How Identity Governance is Failing our Enterprises. YOUATTEST. URL: https://youattest.com/blog/identity-governance-is-failing-our-enterprises/ (дата звернення: 15.03.2024).

12. Microsoft Customer Stories. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/search?sq=Microsoft%20Entra&ff=language&%3EEnglish&p=7&so=story_publish_date%20desc (дата звернення: 18.03.2024).

13. Jacobs Solutions Inc. builds Alluvial Platform with Microsoft Fabric and Power BI. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1655187821653342085-jacobs-microsoft-fabric-power-bi-partner-professional-services-usa (дата звернення: 19.03.2024).

14. Audi is reimagining endpoint management and security with Microsoft Intune. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1746272734406517755-audi-microsoft-intune-automotive-en-germany (дата звернення: 20.03.2024).

15. A secure and compliant version of ChatGPT: Otto Group builds its own in-house AI solution using Azure OpenAI. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1741186295807491714-ottogroup-azure-openai-service-retailers-en-germany (дата звернення: 24.03.2024).

16. Oregon State University protects vital research and sensitive data with Microsoft Sentinel and Microsoft Defender. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1747330384796486050-oregon-state-university-microsoft-security-copilot-higher-education-en-united-states (дата звернення: 30.03.2024).

17. Domino’s Pizza Enterprises slices identity by role for seamless, highly secure access with Microsoft Entra ID. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1724197943143894881-dominos-microsoft-entra-id-australia (дата звернення: 02.04.2024).

18. Modernizing interactive experiences across LEGO House with Azure Kubernetes Service. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1703088157691224129-lego-house-azure-kubernetes-service-media-and-entertainment-denmark (дата звернення: 06.04.2024).

19. Howard University doubles security score and saves $1 million annually with Microsoft Azure. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1640097569557230568-howard-higher-education-azure-en-united-states (дата звернення: 10.04.2024).

20. Dashboard solutions from admins for admins: Dr. Oetker is continuously increasing the security of its IT infrastructure with Azure and Power BI. Microsoft Customers Stories. URL: https://customers.microsoft.com/en-us/story/1634950021614025445-droetker-powerbi-en (дата звернення: 15.04.2024).

21. Плани та ціни Microsoft Entra | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/uk-ua/security/business/microsoft-entra-pricing (дата звернення: 19.04.2024).

22. Plan a single sign-on deployment - Microsoft Entra ID. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/uk-ua/entra/identity/enterprise-apps/plan-sso-deployment (дата звернення: 22.04.2024).

23. Система єдиного входу Microsoft Entra | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/uk-ua/security/business/identity-access/microsoft-entra-single-sign-on (дата звернення: 27.04.2024).

24. Microsoft Entra expands into Security Service Edge and Azure AD becomes Microsoft Entra ID | Microsoft Security Blog. *Microsoft Security Blog*. URL: https://www.microsoft.com/en-us/security/blog/2023/07/11/microsoft-entra-expands-into-security-service-edge-and-azure-ad-becomes-microsoft-entra-id/?culture=uk-ua&country=ua (дата звернення: 30.04.2024).

25. Architecture overview - Microsoft Entra. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/uk-ua/entra/architecture/architecture (дата звернення: 05.05.2024).

26. Microsoft Entra ID documentation - Microsoft Entra ID. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/uk-ua/entra/identity/?culture=uk-ua&country=ua (дата звернення: 28.05.2024).