Практична робота №4

ОЗНАЙОМЛЕННЯ З ПРИНЦИПАМИ РОБОТИ ENTRA ID ТА ЙОГО ОСНОВНИМИ ФУНКЦІЯМИ

Мета: ознайомитися з принципами роботи Microsoft Entra ID (раніше – Azure Active Directory) та основними функціями, які використовуються в щоденній роботі адміністратора: керуванням тенантами, користувачами та групами, асоціюванням Subscription з тенантом, застосуванням Azure Policy, Resource locks та Azure RBAC для керування доступом і відповідністю ресурсів організаційним вимогам.

Теоретичні відомості

Microsoft Entra ID та тенанти

Microsoft Entra ID (до 2023 року – Azure Active Directory, Azure AD) – хмарна служба керування ідентифікаціями та доступом (Identity and Access Management, IAM) від Microsoft. Вона забезпечує автентифікацію та авторизацію користувачів, груп, застосунків і пристроїв під час доступу до Azure, Microsoft 365 та інших SaaS-застосунків, а також надає функції єдиного входу (Single Sign-On, SSO), багатофакторної автентифікації (Multi-Factor Authentication, MFA) та умовного доступу (Conditional Access).

Тенант (tenant) – виділений екземпляр Microsoft Entra ID, який належить одній організації та представляє її в хмарі Microsoft. Тенант містить користувачів, групи, реєстрації застосунків і налаштування безпеки. Кожен тенант має унікальний ідентифікатор (Tenant ID) та початковий домен формату `<назва>.onmicrosoft.com`, до якого згодом можна додати власні домени (custom domains). Користувач, який створює тенант, автоматично отримує в ньому роль Global Administrator.

Тенант може мати одну з двох конфігурацій. **Workforce** (в актуальному інтерфейсі – **Governed Workforce**) призначена для

співробітників, внутрішніх застосунків та ресурсів організації, а також для співпраці з партнерами через B2B collaboration. **External** призначена для сценаріїв Microsoft Entra External ID, тобто для публікації застосунків для споживачів і бізнес-клієнтів. Обидві конфігурації побудовані на одній платформі Microsoft Entra, проте мають відмінності у функціональності, наведені в офіційному порівнянні Microsoft. В актуальному інтерфейсі сторінка **Manage tenants** пропонує лише конфігурації Governed Workforce (потребує підписки Enterprise Agreement або Pay-As-You-Go) та External, проте форма створення звичайного workforce-тенанту Microsoft Entra ID залишається доступною в Azure Portal за прямим посиланням, яке використовується в практичній роботі.

Microsoft Entra ID доступний у кількох редакціях. Редакція Free включає керування користувачами та групами, SSO і базові звіти. Редакція P1 додає Conditional Access, динамічні групи та розширені можливості гібридної ідентифікації. Редакція P2 додатково містить Microsoft Entra ID Protection та Privileged Identity Management (PIM).

Керування Microsoft Entra ID виконується в Microsoft Entra admin center, в Azure Portal (сервіс Microsoft Entra ID), а також за допомогою Microsoft Graph PowerShell, Azure CLI та Microsoft Graph API.

Для нових тенантів за замовчуванням увімкнено **Security defaults** – набір базових налаштувань безпеки, який, зокрема, вимагає від усіх користувачів реєстрації MFA (як правило, у застосунку Microsoft Authenticator), вимагає MFA для адміністраторів та під час доступу до засобів керування Azure (Azure Portal, Azure CLI, Azure PowerShell), а також блокує застарілі протоколи автентифікації.

Користувачі та їх типи

Користувач у Microsoft Entra ID ідентифікується за допомогою User principal name (UPN) – імені формату `user@domain`, де domain – один із

доменів тенанту. Ключовою властивістю користувача є **User type** (Member або Guest), яка визначає рівень прав за замовчуванням: гості мають обмежений доступ до інформації в каталозі. Залежно від того, де відбувається автентифікація, у тенанті розрізняють типи користувачів, наведені в табл. 1.

Таблиця 1

Типи користувачів у тенанті Microsoft Entra ID

Тип користувача	Автентифікація та права	Типовий приклад
Internal member	Обліковий запис і пароль зберігаються в поточному тенанті, права члена організації	Співробітники організації
Internal guest	Обліковий запис у поточному тенанті, права гостя	Гостьові облікові записи, створені до появи B2B collaboration
External member	Автентифікація в домашньому тенанті користувача, права члена організації	Користувачі пов'язаних тенантів multitenant-організації
External guest	Автентифікація в домашньому тенанті, через обліковий запис Microsoft або одноразовий код на email, права гостя	Партнери, підрядники, запрошені через B2B collaboration

Створити користувачів можна вручну в Microsoft Entra admin center, масово з CSV-файлу (Bulk create), за допомогою Microsoft Graph PowerShell (`New-MgUser`) або Azure CLI (`az ad user create`), а також синхронізацією з локальною Active Directory через Microsoft Entra Connect чи Microsoft Entra Cloud Sync. Зовнішні користувачі додаються через механізм B2B collaboration: користувач отримує запрошення на email і після його прийняття отримує доступ до ресурсів тенанту.

Для доступу кінцевих користувачів до призначених їм застосунків використовується портал My Apps, на якому також доступні керування власним профілем, групами та налаштуваннями безпеки облікового запису.

Групи

Групи в Microsoft Entra ID використовуються для спільного керування доступом кількох користувачів. Існують два типи груп:

– **Security** – використовується для надання доступу до ресурсів, призначення ролей, ліцензій та політик;
– **Microsoft 365** – надає спільну поштову скриньку, календар, сайт SharePoint та команду Microsoft Teams.

Членство в групі може бути призначеним вручну (**Assigned**) або динамічним (**Dynamic User**, **Dynamic Device**), коли учасники автоматично додаються та видаляються за правилом на основі атрибутів (наприклад, `user.department -eq "IT"`). Динамічні групи потребують ліцензії Microsoft Entra ID P1. Кожна група має власників (Owners), які можуть керувати її членством, та учасників (Members). Призначення ролей і доступів групам, а не окремим користувачам, суттєво спрощує адміністрування.

Зв’язок Subscription і тенанта

Кожна Subscription має довірчі відносини (trust relationship) рівно з одним тенантом Microsoft Entra ID, тоді як один тенант може бути пов’язаний з багатьма Subscriptions. Тенант надає ідентичності (користувачів, групи, service principals), яким через Azure RBAC надається доступ до ресурсів Subscription.

Пов’язати Subscription з іншим тенантом можна за допомогою операції **Change directory**. Для її виконання користувач повинен мати роль Owner на рівні Subscription, призначену напряму, та обліковий запис як у поточному, так і в цільовому тенанті. Операція не підтримується для підписок Cloud Solution Provider (CSP) та Azure for Students Starter. Під час зміни тенанту:

– усі призначення ролей (role assignments) та custom roles Azure RBAC видаляються без можливості відновлення;
– об’єкти Azure Policy (визначення, призначення, винятки) не переносяться;

– system-assigned managed identities необхідно повторно увімкнути, а user-assigned – створити заново;
– для Key Vault необхідно оновити Tenant ID та політики доступу.

Тому зміну тенанту доцільно виконувати до налаштування ролей і політик. Відображення Subscription у новому тенанті може тривати до кількох годин; у разі затримки варто вийти з облікового запису та увійти повторно.

Важливо розрізняти **ролі Microsoft Entra** (Global Administrator, User Administrator тощо), які керують об'єктами каталогу (користувачами, групами, доменами), та **ролі Azure** (Owner, Contributor, Reader тощо), які керують доступом до ресурсів Azure. Зміна тенанту для Subscription не робить її власника Global Administrator у цільовому тенанті.

Azure Policy

Azure Policy – служба Azure для забезпечення відповідності ресурсів організаційним стандартам (governance). Політики оцінюють ресурси під час їх створення та зміни, а також періодично перевіряють наявні ресурси, а результати оцінювання відображаються в розділі Compliance. Основними поняттями Azure Policy є:

– **Policy definition** – JSON-опис політики, що містить режим (mode), параметри (parameters) та правило (policyRule) у формі «if – then» з ефектом;
– **Initiative definition** (policy set) – набір кількох policy definitions, які призначаються та відстежуються як єдине ціле;
– **Assignment** – призначення policy або initiative definition на певний scope (Management group, Subscription, Resource group або окремий ресурс) з конкретними значеннями параметрів;
– **Exemption** – виняток, що виключає певний scope з оцінювання призначення.

Ефект (effect) визначає дію політики у разі виконання умови: **Deny** блокує запит, **Audit** лише фіксує невідповідність, **Modify** та **Append** змінюють властивості ресурсу (наприклад, додають теги), **DeployIfNotExists** розгортає відсутні пов'язані ресурси, **Disabled** вимикає політику. Для політик з ефектами Modify і DeployIfNotExists призначення використовує managed identity, яку Azure Portal може створити автоматично.

Вбудовані (Built-in) політики змінювати не можна, проте їх можна скопіювати за допомогою операції **Duplicate definition** та змінити копію як власну (Custom) політику. У практичній роботі використовуються вбудовані політики **Allowed resource types** (ефект Deny; параметр – перелік дозволених типів ресурсів) та **Add a tag to resources** (ефект Modify; параметри – ім'я та значення тегу; тег додається до ресурсів під час їх створення або оновлення, а до наявних ресурсів – лише через remediation task; на Resource groups політика не поширюється). Нове призначення політики набуває чинності протягом приблизно 30 хвилин.

Resource locks

Resource lock – механізм захисту ресурсів від випадкового видалення або зміни. Блокування діє для всіх користувачів незалежно від їх ролей, зокрема й для Owner. Існують два рівні блокування:

- **CanNotDelete** (в Azure Portal – **Delete**) – авторизовані користувачі можуть читати та змінювати ресурс, але не можуть його видалити;
- **ReadOnly** (в Azure Portal – **Read-only**) – авторизовані користувачі можуть лише читати ресурс, що відповідає дії ролі Reader для всіх користувачів.

Блокування, встановлене на батьківському scope, успадковується всіма ресурсами всередині нього, а за наявності кількох блокувань діє найсуворіше. Resource locks застосовуються лише до операцій рівня керування (control plane), тобто запитів до `management.azure.com`, і не

впливають на операції рівня даних (data plane). Для створення та видалення блокувань необхідний доступ до дій `Microsoft.Authorization/locks/*`, який мають, наприклад, ролі Owner та User Access Administrator.

Azure RBAC

Azure role-based access control (Azure RBAC) – система авторизації, побудована на Azure Resource Manager, що забезпечує детальне керування доступом до ресурсів Azure. Доступ надається шляхом створення призначення ролі (role assignment), яке складається з трьох елементів:

- **security principal** – об'єкт, якому надається доступ: користувач, група, service principal або managed identity;
- **role definition** – набір дозволів (permissions), наприклад, читання, запис або видалення;
- **scope** – межі дії доступу: Management group, Subscription, Resource group або окремий ресурс.

Призначення ролей успадковуються дочірніми scope, а сукупні дозволи визначаються як об'єднання всіх призначених ролей. Основні вбудовані ролі Azure наведено в табл. 2.

Таблиця 2

Основні вбудовані ролі Azure

Роль	Опис
Owner	Повний доступ до керування ресурсами, включно з призначенням ролей іншим користувачам
Contributor	Повний доступ до керування ресурсами без права призначати ролі в Azure RBAC
Reader	Перегляд ресурсів без можливості їх змінювати
User Access Administrator	Керування доступом користувачів до ресурсів Azure
Role Based Access Control Administrator	Керування доступом шляхом призначення ролей Azure RBAC

В Azure Portal на сторінці Add role assignment ролі Owner, Contributor, User Access Administrator та Role Based Access Control Administrator розміщені на вкладці **Privileged administrator roles**, а решта вбудованих ролей – на вкладці **Job function roles**.

Якщо вбудовані ролі не відповідають потребам організації, створюються **custom roles**. Опис custom role містить властивості `Name`, `Description`, `Actions`, `NotActions`, `DataActions`, `NotDataActions` та `AssignableScopes`. Дозволи `Actions` стосуються операцій рівня керування (control plane), а `DataActions` – операцій з даними всередині ресурсу (data plane). Кожен дозвіл має формат `{Company}.{ProviderName}/{resourceType}/{action}`, наприклад, `Microsoft.Storage/storageAccounts/read`. Custom roles зберігаються в тенанті Microsoft Entra ID (до 5000 ролей на один тенант) і видаляються під час зміни тенанту для Subscription.

Azure RBAC, Azure Policy та Resource locks доповнюють один одного: Azure RBAC визначає, **хто** може виконувати дії над ресурсами, Azure Policy – **якими** мають бути ресурси та їх властивості, а Resource locks захищають критичні ресурси від видалення та змін незалежно від наданих ролей.

Хід роботи

У завданнях використовуються такі позначення: **yyy** – ініціали студента латинськими літерами, **zzz** – номер варіанту з трьох цифр (наприклад, для 15 варіанту – 015). Звіт має містити скріншоти, що підтверджують виконання кожного кроку.

1. Створити тенант Microsoft Entra ID.
   1.1. Увійти в Azure Portal під обліковим записом Azure for Students та відкрити сторінку Create a tenant. Сторінку необхідно відкривати саме за цим посиланням, оскільки в розділі **Manage tenants** доступні лише конфігурації Governed Workforce та External, створення яких з підпискою Azure for Students неможливе.
   1.2. На сторінці **Create a tenant** заповнити поля:
   – **Tenant Name** – `Lab4 yyy zzz`;

– **Domain Name** – `lab4yyyzzz` (лише латинські літери та цифри; домен `<domainname>.onmicrosoft.com` неможливо змінити чи видалити після створення, проте згодом можна додати власні домени; якщо ім'я зайняте, додати до нього довільну цифру);
– **Country/Region** – `Ukraine`. Під полем має з'явитися повідомлення **Geographic location – Europe**: обрана країна визначає, де Microsoft Entra зберігатиме основну копію даних каталогу.

1.3. Натиснути **Create**. На панелі **Help us prove you're not a robot** ввести символи із зображення в поле **Type the letters** та натиснути **Submit**.

1.4. Дочекатися завершення створення тенанту (може тривати кілька хвилин), перебіг операції відображається на панелі **Notifications**. Якщо під час створення виникає помилка, необхідно звернутися до викладача.

1.5. Перейти в новий тенант: у верхній панелі Azure Portal натиснути **Settings** (піктограма шестерні) > **Directories + subscriptions**, знайти створений тенант у списку **Directory name** та натиснути **Switch**.

1.6. У головному пошуку знайти **Microsoft Entra ID** та на сторінці **Overview** у розділі **Basic information** зафіксувати у звіті **Name**, **Tenant ID** та **Primary domain** тенанту. Усі подальші дії із завдань 2–4 виконуються в новому тенанті в Microsoft Entra admin center.

2. Створити користувачів у новому тенанті, дотримуючись кроків розділів «Create a new user» та «Invite an external user» офіційної документації Microsoft.

2.1. У Microsoft Entra admin center перейти в **Entra ID** > **Users** та обрати **New user** > **Create new user**. На вкладці **Basics** вказати:
   - **User principal name** – `user1-yyy`, домен – початковий домен тенанту (`lab4yyyzzz.onmicrosoft.com`);
   - **Display name** – `User1 yyy`;
   - **Password** – залишити опцію **Auto-generate password** та зберегти згенерований пароль, він знадобиться для першого входу;
   - **Account enabled** – залишити увімкненим.

2.2. Натиснути **Next: Properties** та переконатися, що в полі **User type** вказано **Member**. Натиснути **Review + create** та **Create**.

2.3. Запросити зовнішнього користувача: обрати **New user** > **Invite external user** та на вкладці **Basics** вказати:
   - **Email** – власна особиста поштова скринька (@gmail.com, @outlook.com тощо);
   - **Display name** – `Guest yyy`;
   - **Send invite message** – увімкнути та ввести довільний текст запрошення.

2.4. Натиснути **Review + invite** та **Invite**. Відкрити отриманий лист, прийняти запрошення та переконатися, що у властивостях користувача (**Users** > обраний користувач > **Properties**) поле **Invitation state** має значення **Accepted**.

2.5. Додати двох користувачів за допомогою Bulk create, дотримуючись кроків офіційної документації Microsoft: перейти в **Entra ID** > **Users** та обрати **Bulk operations** > **Bulk create**. Натиснути **Download** та завантажити шаблон CSV-файлу.

2.6. Відкрити шаблон у текстовому редакторі або Excel, видалити рядок-приклад (Chris Green) та всі необов’язкові стовпці, крім

`Account enabled (true/false) [accountEnabled]`, не змінюючи назв залишених стовпців. Додати двох користувачів, заповнивши стовпці `Name [displayName] Required`, `User name [userPrincipalName] Required`, `Initial password [passwordProfile] Required` та `Account enabled (true/false) [accountEnabled]` зі значенням `true`. Пароль має відповідати політиці паролів Microsoft Entra ID (щонайменше 8 символів, літери різного регістру, цифри та спеціальні символи). Приклад заповненого файлу:

```
Name [displayName] Required,User name [userPrincipalName]
Required,Initial password [passwordProfile] Required,Account enabled
(true/false) [accountEnabled]
User2 yyy,user2-yyy@lab4yyyzzz.onmicrosoft.com,Lab4-Passw0rd!2,true
User3 yyy,user3-yyy@lab4yyyzzz.onmicrosoft.com,Lab4-Passw0rd!3,true
```

2.7. Зберегти файл у форматі CSV, на сторінці **Bulk create user** обрати його в полі **Upload your csv file** та натиснути **Submit**. Після успішної перевірки файлу (повідомлення **File uploaded successfully**) підтвердити запуск операції. Статус виконання відображається на сторінці **Bulk operation results**, де в разі помилок можна завантажити файл з їх описом. Bulk create не надсилає користувачам запрошень, тому паролі передаються користувачам окремо.

2.8. Перейти в **Entra ID** > **Users** та додати до звіту скріншот зі списком чотирьох новостворених користувачів.

3. Увійти на портал My Apps від імені першого користувача.

3.1. Відкрити вікно браузера в режимі InPrivate/Incognito та перейти на My Apps.

3.2. Увійти, використовуючи UPN та згенерований пароль користувача `user1-yyy`. Під час першого входу необхідно змінити тимчасовий пароль. Якщо з’явиться повідомлення **More information required** (вимога Security defaults), необхідно

зареєструвати MFA за допомогою застосунку Microsoft Authenticator, дотримуючись інструкцій майстра.

3.3. Додати до звіту скріншот початкової сторінки **Apps dashboard**.

4. Створити дві Security groups з назвами **Developers** та **QA**.

4.1. Увійти в Microsoft Entra admin center у тенанті, створеному в завданні 1, та перейти в **Entra ID** > **Groups** > **All groups**.

4.2. Натиснути **New group** та заповнити поля:

- **Group type** – **Security**;
- **Group name** – `Developers`;
- **Group description** – довільний опис, наприклад, `Developers group, lab 4`;
- **Microsoft Entra roles can be assigned to the group** – **No**;
- **Membership type** – **Assigned**.

4.3. Під полем **Owners** натиснути **No owners selected**, обрати власний обліковий запис та натиснути **Select**.

4.4. Під полем **Members** натиснути **No members selected**, обрати двох із чотирьох користувачів, створених у завданні 2, та натиснути **Select**.

4.5. Натиснути **Create** та переконатися, що група з'явилася в списку **All groups**.

4.6. Повторити кроки 4.2–4.5 для групи `QA`, додавши до неї двох інших користувачів.

4.7. Відкрити кожну групу, перейти в розділ **Members** та додати до звіту скріншоти зі списками учасників обох груп.

5. Перемістити Subscription у створений тенант, дотримуючись кроків офіційної документації Microsoft, та створити ресурс.

5.1. В Azure Portal перейти в тенант, у якому розміщена Subscription Azure for Students (**Settings** > **Directories + subscriptions**). У

головному пошуку знайти **Subscriptions** та відкрити Subscription Azure for Students.

5.2. На сторінці Subscription натиснути **Change directory** та уважно ознайомитися з наслідками зміни тенанту. На запитання, чи буде запит у цільовому тенанті прийматися самостійно, обрати **Yes**, у випадному списку обрати Tenant ID тенанту, створеного в завданні 1, та натиснути **Continue**. На сторінці підтвердження продовжити операцію та натиснути **Accept**. Після завершення перейти в новий тенант (**Settings** > **Directories + subscriptions**). Відображення Subscription у новому тенанті може тривати до кількох годин; якщо Subscription не відображається або під час зміни тенанту виникає помилка, необхідно вийти з облікового запису та увійти повторно або повторити спробу пізніше.

5.3. Перед створенням ресурсу перевірити, чи зареєстровано в Subscription відповідний resource provider (`Microsoft.Network` – для Virtual Network, `Microsoft.Storage` – для Storage Account, `Microsoft.KeyVault` – для Key Vault). Azure Portal та розгортання ARM templates реєструють resource provider автоматично, проте Azure CLI та Azure PowerShell цього не роблять і повертають помилку `MissingSubscriptionRegistration`. Перевірити стан реєстрації можна в Subscription у розділі **Settings** > **Resource providers** або командами:

```
az provider show --namespace Microsoft.KeyVault --query
registrationState --output tsv
Get-AzResourceProvider -ProviderNamespace Microsoft.KeyVault |
Select-Object ProviderNamespace, RegistrationState
```

5.4. Якщо стан відрізняється від `Registered`, зареєструвати resource provider (у командах вказати простір імен, що відповідає ресурсу згідно з варіантом) та дочекатися стану `Registered` (зазвичай кілька хвилин):

```
az provider register --namespace Microsoft.KeyVault --wait
Register-AzResourceProvider -ProviderNamespace Microsoft.KeyVault
```

5.5. Створити Resource group та ресурс, вказаний у табл. 3 згідно з варіантом, використовуючи зазначений у таблиці метод (порядок роботи з Azure CLI, Azure PowerShell та ARM templates розглянуто в практичній роботі №3). Resource group називається `rg-aaa-xxx-yyy-zzz`, де **aaa** – скорочена назва типу ресурсу відповідно до офіційних рекомендацій щодо скорочень імен ресурсів (`vnet` – Virtual Network, `st` – Storage Account, `kv` – Key Vault), **xxx** – скорочена назва одного з регіонів, дозволених політикою Allowed resource deployment regions, відповідно до цього файлу, що містить відповідність між повною та скороченою назвою регіону. Ресурс створюється всередині цієї Resource group у тому самому регіоні та називається `aaaxxxyyyzzz` (значення aaa, xxx, yyy, zzz збігаються з використаними в імені Resource group).

6. Створити та застосувати Policy Initiative з копій вбудованих політик **Allowed resource types** та **Add a tag to resources**. Дозволеними типами ресурсів мають бути `Microsoft.Authorization/locks` та тип ресурсу, створеного в завданні 5 згідно з варіантом; до ресурсів має автоматично додаватися тег `Variant` зі значенням, що дорівнює номеру варіанту. Створення та призначення initiative definition детально описано в розділі «Create and assign an initiative definition» офіційної документації Microsoft.

6.1. Створити копію політики, яка обмежуватиме типи ресурсів. В Azure Portal у головному пошуку знайти **Policy** та перейти в **Authoring** > **Definitions**. Знайти вбудовану політику **Allowed resource types**, відкрити її та натиснути **Duplicate definition**. Вказати:

– **Definition location** – Subscription Azure for Students (обрати за допомогою кнопки «…»);
– **Name** – `[Custom] Allowed resource types`;
– **Description** – залишити опис, скопійований з вбудованої політики;
– **Category** – Use existing, General;
– **Policy rule** та параметри копії не змінювати.

6.2. Натиснути **Save**. Ця політика (ефект Deny) дозволятиме створювати в Subscription лише ресурси двох типів: `Microsoft.Authorization/locks` та тип ресурсу із завдання 5 згідно з варіантом (`Microsoft.Network/virtualNetworks`, `Microsoft.Storage/storageAccounts` або `Microsoft.KeyVault/vaults`). Сам перелік дозволених типів задається не в копії політики, а в параметрі **Allowed resource types** під час створення initiative definition (крок 6.7).

6.3. Створити копію політики, яка додаватиме тег до ресурсів. У **Authoring** > **Definitions** знайти вбудовану політику **Add a tag to resources**, відкрити її та натиснути **Duplicate definition**. Вказати:
– **Definition location** – Subscription Azure for Students;
– **Name** – `[Custom] Add a tag to resources`;
– **Description** – залишити опис, скопійований з вбудованої політики;
– **Category** – Use existing, Tags;
– **Policy rule** та параметри копії не змінювати;
– **Role definitions** – залишити **Contributor**. Це поле з’являється лише для політик з ефектами Modify та DeployIfNotExists і визначає роль, яку буде надано managed identity призначення політики, щоб вона могла змінювати ресурси (у цьому випадку

– додавати теги). Значення підставляється автоматично з властивості `roleDefinitionIds` у Policy rule (`b24988ac-6180-42a0-ab88-20f7382dd24c` – ідентифікатор вбудованої ролі Contributor).

6.4. Натиснути **Save**. Ця політика (ефект Modify) додаватиме до нових ресурсів тег з іменем `Variant` і значенням, що дорівнює номеру варіанту (наприклад, `15`). Ім’я та значення тегу задаються в параметрах **Tag Name** та **Tag Value** під час створення initiative definition (крок 6.7).

6.5. Перейти в **Authoring** > **Definitions** та натиснути + **Initiative definition**. На вкладці **Basics** вказати **Initiative location** – Subscription Azure for Students, **Name** – `[Custom] Policy Initiative definition - xxx, yyy, zzz` (значення xxx, yyy, zzz збігаються з використаними в імені Resource group із завдання 5), **Category** – Create new, `Custom`.

6.6. На вкладці **Policies** натиснути **Add policy definition(s)**, у фільтрі **Type** обрати **Custom**, позначити обидві створені політики та натиснути **Add**.

6.7. На вкладці **Policy parameters** задати значення параметрів:

– для політики `[Custom] Allowed resource types` у параметрі **Allowed resource types** обрати **Value type** – **Set value** та позначити два типи ресурсів: `Microsoft.Authorization/locks` і тип ресурсу із завдання 5 згідно з табл. 3 – `Microsoft.Network/virtualNetworks` (Azure Virtual Network), `Microsoft.Storage/storageAccounts` (Azure Storage Account) або `Microsoft.KeyVault/vaults` (Azure Key Vault);

– для політики `[Custom] Add a tag to resources` обрати **Set value** та вказати **Tag Name** – `Variant`, **Tag Value** – номер варіанту (наприклад, `15`).

6.8. Натиснути **Review + create** та **Create**.

6.9. Відкрити створену initiative definition та натиснути **Assign initiative**. Майстер призначення містить вкладки **Basics**, **Parameters**, **Remediation**, **Managed identity**, **Non-compliance messages** та **Review + create**:

– **Basics** – у полі **Scope** обрати Subscription Azure for Students, **Policy enforcement** – Enabled, решту полів залишити без змін;

– **Parameters** – значення параметрів уже задані під час створення initiative definition, тому їх не змінювати;

– **Remediation** – опцію **Create a remediation task** залишити непозначеною. За замовчуванням призначення діє лише на нові та змінені ресурси, а remediation task потрібен, щоб застосувати політику з ефектом Modify (у цьому випадку – додати тег) до вже наявних ресурсів;

– **Managed identity** – опція **Create a Managed Identity** позначена автоматично (її неможливо зняти, оскільки initiative містить політику з ефектом Modify); **Type of Managed Identity** – **System assigned managed identity**; **System assigned identity location** – регіон, використаний у завданні 5 (наприклад, (Europe) Germany West Central). У розділі **Permissions** відображається роль **Contributor**, яку буде надано цій identity на підставі поля Role definitions політики; саме від її імені додаватимуться теги;

– **Non-compliance messages** – залишити без змін.

6.10. Натиснути **Review + create** та **Create**. Без призначення initiative definition буде лише створена і не матиме жодного ефекту. Призначення набуває чинності протягом приблизно 30 хвилин.

6.11. Протестувати політики: у Resource group із завдання 5 створити ще один ресурс дозволеного типу (з іменем `aaaxxxyyyzzz2`) та переконатися, що його створено і що він має тег `Variant` (розділ **Tags** ресурсу). Спробувати створити в цій Resource group ресурс іншого типу, відсутнього в переліку дозволених (наприклад, Storage Account для варіантів з Virtual Network), та зафіксувати отриману помилку `RequestDisallowedByPolicy`. Пояснити, чому ресурс, створений у завданні 5, не має тегу `Variant`.

7. Дослідити роботу Resource locks (порядок налаштування блокувань описано в розділі «Configure locks» офіційної документації Microsoft). Після виконання завдань 5 та 6 у Resource group має бути два ресурси однакового типу.

7.1. Відкрити Resource group із завдання 5, перейти в **Settings** > **Locks** та натиснути **Add**. Вказати довільне **Lock name**, **Lock type** – **Read-only** та натиснути **OK**.

7.2. Спробувати виконати такі дії та зафіксувати результати:

- додати довільний тег до Resource group (розділ **Tags** Resource group);
- додати довільний тег до одного з ресурсів у Resource group;
- видалити один з ресурсів.

7.3. Видалити блокування Read-only (**Locks** > **Delete**), створити нове блокування з довільною назвою та типом **Delete** (CanNotDelete) і повторити попередні три дії. Зафіксувати результати та порівняти їх з результатами для Read-only.

8. Налаштувати доступ за допомогою Azure RBAC, дотримуючись кроків офіційної документації Microsoft щодо призначення ролей Azure та створення custom roles.
    8.1. Відкрити Resource group із завдання 5, перейти в **Access control (IAM)** та обрати **Add** > **Add role assignment**. На вкладці **Privileged administrator roles** обрати роль **Contributor** та натиснути **Next**. На вкладці **Members** обрати **Assign access to** – User, group, or service principal, натиснути **Select members**, обрати одного з користувачів, створених у завданні 2, та натиснути **Select**. Натиснути **Review + assign**.
    8.2. Аналогічно призначити іншому користувачеві роль **Reader** (вкладка **Job function roles**).
    8.3. У вікні браузера в режимі InPrivate/Incognito увійти в Azure Portal від імені користувача з роллю Contributor (за потреби – зареєструвавши MFA згідно з вимогами Security defaults). Створити в Resource group ресурс дозволеного політикою типу та переглянути перелік усіх ресурсів (**All resources**). Від імені користувача з роллю Reader спробувати створити ще один ресурс такого самого типу. Зафіксувати результати.
    8.4. Створити custom role: відкрити Subscription Azure for Students, перейти в **Access control (IAM)** та обрати **Add** > **Add custom role**. На вкладці **Basics** вказати **Custom role name** – `Technical Support`, довільний **Description** та **Baseline permissions** – Start from scratch.
    8.5. На вкладці **Permissions** натиснути **Add permissions**, знайти постачальників ресурсів **Microsoft Storage** та **Microsoft Key Vault** і позначити такі дозволи:
        – `Microsoft.Storage/storageAccounts/read`;
        – `Microsoft.Storage/storageAccounts/listKeys/action`;

- `Microsoft.Storage/storageAccounts/blobServices/containers/read`;
- `Microsoft.KeyVault/vaults/read`;
- `Microsoft.KeyVault/vaults/secrets/read`.

8.6. На вкладці **Assignable scopes** переконатися, що вказано Subscription Azure for Students, на вкладці **JSON** переглянути опис ролі та додати його до звіту. Натиснути **Review + create** та **Create**.

8.7. Призначити роль `Technical Support` одному з користувачів, створених у завданні 2, якому в кроці 8.1 та 8.2 не було надано ролей Contributor чи Reader (щоб результат перевірки дозволів цієї ролі не залежав від інших призначень): на рівні Subscription перейти в **Access control (IAM)** > **Add** > **Add role assignment**, на вкладці **Job function roles** знайти роль `Technical Support` (у фільтрі **Type** можна обрати **CustomRole**), на вкладці **Members** обрати користувача та натиснути **Review + assign**.

9. Видалити створені політики, призначення ролей, блокування, ресурси та тенант і повернути Subscription у домашній тенант «Державний університет «Житомирська політехніка»». Це завдання є обов'язковим: без його виконання політика `[Custom] Allowed resource types` блокуватиме створення ресурсів у наступних практичних роботах, а Subscription залишатиметься в тенанті, створеному в завданні 1.

9.1. Видалити призначення initiative: в Azure Portal перейти в **Policy** > **Authoring** > **Assignments**, знайти призначення `[Custom] Policy Initiative definition – xxx, yyy, zzz`, натиснути «…» > **Delete assignment** та підтвердити видалення.

9.2. Видалити initiative definition та копії політик: перейти в **Policy** > **Authoring** > **Definitions**, у фільтрі **Type** обрати **Custom**.

Відкрити `[Custom] Policy Initiative definition – xxx, yyy, zzz` та натиснути **Delete definition**. Аналогічно видалити `[Custom] Allowed resource types` та `[Custom] Add a tag to resources`. Initiative definition необхідно видаляти першою, оскільки політики, що входять до неї, видалити неможливо.

9.3. Видалити призначення ролей у Resource group із завдання 5: перейти в **Access control (IAM)** > **Role assignments**, позначити призначення ролей **Contributor** та **Reader** користувачам, а також призначення ролі **Contributor** для managed identity політики (після видалення призначення initiative воно може відображатися як **Identity not found**), натиснути **Delete** та підтвердити видалення.

9.4. Видалити custom role: відкрити Subscription Azure for Students, перейти в **Access control (IAM)** > **Role assignments**, видалити призначення ролі `Technical Support`. Далі перейти на вкладку **Roles**, у фільтрі **Type** обрати **CustomRole**, натиснути «…» навпроти ролі `Technical Support` > **Delete** та підтвердити видалення. Custom role неможливо видалити, доки існують її призначення.

9.5. Видалити блокування та всі ресурси, створені під час виконання практичної роботи:

- у Resource group із завдання 5 перейти в **Settings** > **Locks** та видалити блокування типу **Delete** (інакше видалити Resource group неможливо);
- видалити Resource group із завдання 5 разом з усіма ресурсами в ній (ресурсом із завдання 5, другим ресурсом із кроку 6.9 та ресурсом, створеним користувачем з роллю Contributor у кроці 8.3): на сторінці **Overview** Resource group натиснути **Delete**

resource group, ввести її ім’я для підтвердження та натиснути **Delete**;

- для варіантів з Azure Virtual Network видалити також Resource group `NetworkWatcherRG`, якщо її було автоматично створено разом із віртуальною мережею;
- видалити інші Resource groups, створені під час тестування політик чи ролей (якщо такі є);
- перейти в **Resource groups** та **All resources** і переконатися, що ресурсів, створених у практичній роботі, не залишилося.

9.6. Повернути Subscription у домашній тенант: перебуваючи в тенанті, створеному в завданні 1, відкрити Subscription Azure for Students, натиснути **Change directory**, ознайомитися з наслідками зміни тенанту, на запитання, чи буде запит у цільовому тенанті прийматися самостійно, обрати **Yes**, у випадному списку обрати тенант **Державний університет «Житомирська політехніка»** (домен `ztu.edu.ua`), натиснути **Continue**, а потім **Accept**.

9.7. Якщо зміну тенанту заблоковано політиками перенесення підписок, у тенанті із завдання 1 (у якому студент є Global Administrator) дозволити вихід підписок: у **Microsoft Entra ID** > **Properties** встановити **Access management for Azure resources** – **Yes** та натиснути **Save**, потім у **Subscriptions** натиснути **Manage Policies**, для **Subscriptions leaving a Microsoft Entra ID directory** обрати **Allow all users**, натиснути **Save changes** та повторити попередній крок.

9.8. Перейти в домашній тенант (**Settings** > **Directories + subscriptions** > **Switch** навпроти **Державний університет «Житомирська політехніка»**) та переконатися, що Subscription Azure for Students відображається в розділі **Subscriptions** з

роллю **Owner**. Відображення може тривати до кількох годин; за потреби вийти з облікового запису та увійти повторно.

9.9. Оновити контекст Azure CLI та Azure PowerShell у Cloud Shell, щоб команди виконувалися в домашньому тенанті (інакше вони повертатимуть помилку `SubscriptionNotFound`): у панелі Cloud Shell натиснути **Restart** або виконати команди:

```
az login --tenant ztu.edu.ua
az account set --subscription "Azure for Students"
Connect-AzAccount -Tenant ztu.edu.ua -UseDeviceAuthentication
Set-AzContext -Subscription "Azure for Students"
```

9.10. Видалити тенант, створений у завданні 1 (виконується лише після успішного повернення Subscription у домашній тенант): перейти в цей тенант (**Settings** > **Directories + subscriptions** > **Switch**), у Microsoft Entra admin center видалити всіх користувачів, крім власного облікового запису (**Entra ID** > **Users** – позначити користувачів > **Delete**), та остаточно видалити їх у розділі **Deleted users** (**Delete permanently**), а також видалити групи `Developers` і `QA` (**Entra ID** > **Groups** > **All groups**).

9.11. Перейти в **Entra ID** > **Overview** > **Manage tenants**, позначити тенант, створений у завданні 1, та натиснути **Delete**. Якщо на сторінці видалення відображаються невиконані вимоги (наприклад, наявні користувачі, застосунки чи Subscriptions), виконати зазначені дії та повторити видалення.

9.12. Додати до звіту скріншоти, що підтверджують видалення initiative definition, custom role, ресурсів і тенанту, а також повернення Subscription у домашній тенант.

Таблиця 3

Ресурси та метод їх створення згідно з варіантом

№ варіанту	Ресурс	Метод створення ресурсу
1	Azure Virtual Network	Azure CLI
2	Azure Storage Account	Azure PowerShell
3	Azure Key Vault	ARM Template
4	Azure Virtual Network	Azure PowerShell

№ варіанту	Ресурс	Метод створення ресурсу
5	Azure Storage Account	Azure CLI
6	Azure Key Vault	Azure CLI
7	Azure Virtual Network	ARM Template
8	Azure Storage Account	ARM Template
9	Azure Key Vault	Azure PowerShell
10	Azure Virtual Network	Azure CLI
11	Azure Storage Account	Azure PowerShell
12	Azure Key Vault	ARM Template
13	Azure Virtual Network	Azure PowerShell
14	Azure Storage Account	ARM Template
15	Azure Key Vault	Azure CLI
16	Azure Virtual Network	Azure CLI
17	Azure Storage Account	Azure PowerShell
18	Azure Key Vault	Azure PowerShell
19	Azure Virtual Network	ARM Template
20	Azure Storage Account	Azure CLI

Контрольні запитання

1. Що таке Microsoft Entra ID (раніше Azure Active Directory) і яку роль відіграє створення окремого тенанта у процесі керування доступом до ресурсів Azure?
2. У чому полягає різниця між внутрішнім користувачем тенанта та зовнішнім (external/guest user), і яким чином здійснюється їхнє додавання через портал Microsoft Entra?
3. Яке призначення мають Security Groups у Microsoft Entra ID і як вони можуть використовуватись для спрощення призначення ролей або політик у межах Azure?
4. Яким чином можна перемістити існуючу підписку (Subscription) до нового тенанта, і які обмеження або наслідки можуть виникнути після такого переміщення?
5. Поясніть логіку формування імен для ресурсів і груп ресурсів у завданні. Чому стандартизовані схеми найменування (наприклад, rg-aaa-xxx-yyy-zzz) є важливими для управління корпоративним середовищем Azure?
6. Яке призначення політик Allowed resource types та Add a tag to resources, і як їхнє дублювання з префіксом [Custom] допомагає у створенні власних ініціатив комплаєнсу (Policy Initiative Definition)?
7. Як працює Resource Lock у режимах ReadOnly та CanNotDelete? У чому полягає різниця між цими двома типами блокувань і які саме дії користувач не може виконати в кожному випадку?
8. Які відмінності у правах і можливостях мають користувачі з ролями Contributor і Reader у межах однієї Resource Group, і як це впливає на їхню здатність створювати або змінювати ресурси?

9. Яку роль виконує створена кастомна роль Technical Support, які дозволи вона надає користувачу та чому її призначення на рівні Scope Subscription є доцільним?
10. Як Azure RBAC, Azure Policy та Resource Locks взаємодіють між собою у забезпеченні цілісної системи контролю доступів, комплаєнсу та захисту ресурсів у середовищі Azure?