

**Міністерство освіти і науки України
Національний технічний університет «Дніпровська
політехніка»**



**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ Кафедра
програмного забезпечення комп'ютерних систем**

**Звіт з практичної роботи №4
З дисципліни
«Аналіз програмного забезпечення»**

**Виконала студентка: гр. 122-23ск-1
Колдун Ярослава Віталіївна
Прийняв:**

**Дніпро
2025**

ПРАКТИЧНА РОБОТА № 4

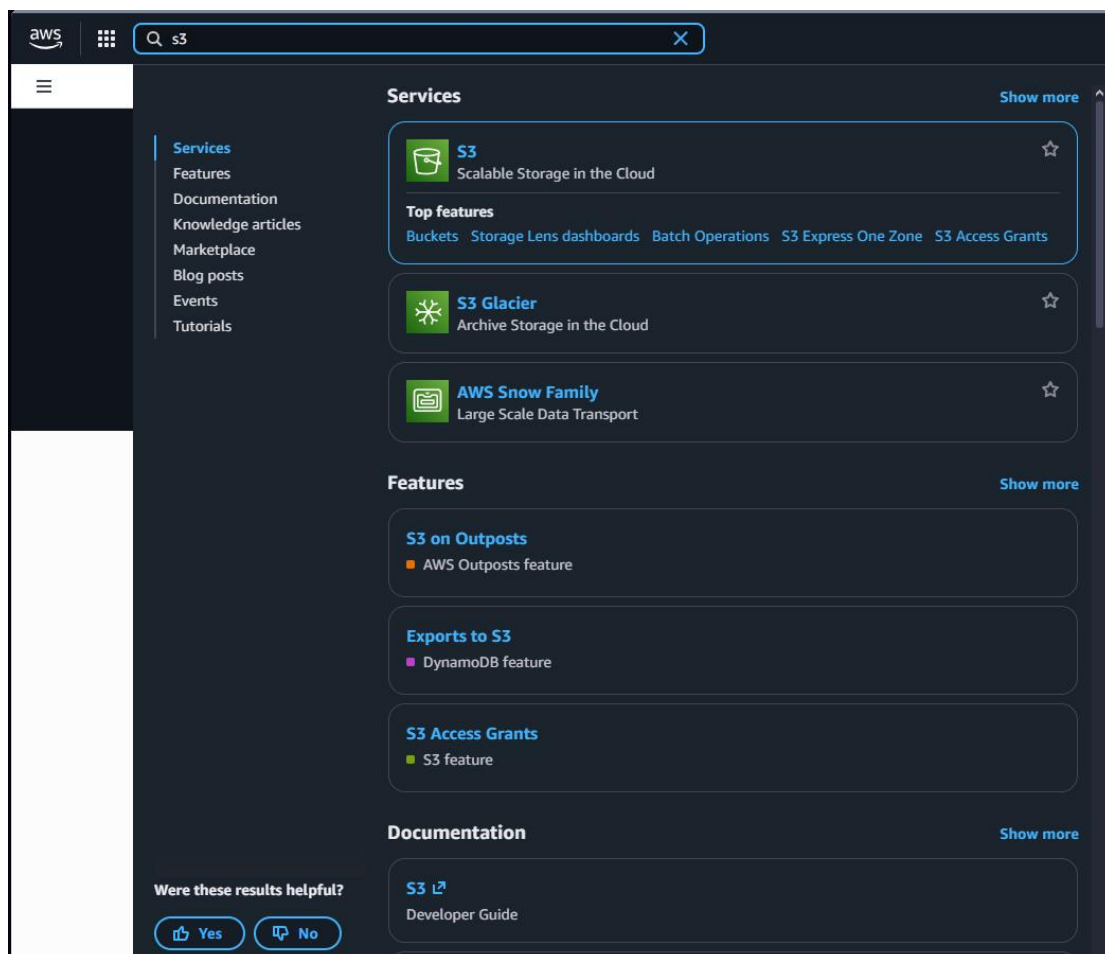
Основні кроки виконання:

Крок 1. Зареєструватися в системі AWS.



The image shows the AWS sign-up page. On the left, there is a section titled "Explore Free Tier products with a new AWS account." with a link to "To learn more, visit aws.amazon.com/free." and an illustration of a hand holding a cube. On the right, the "Sign up for AWS" section contains a form with the following fields: "Root user email address" (with a note "Used for account recovery and some administrative functions"), "AWS account name" (with a note "Choose a name for your account. You can change this name in your account settings after you sign up."), and a "Verify email address" button. Below the form, there is an "OR" separator and a "Sign in to an existing AWS account" link.

Крок 2. Створити бакет у S3 з вашим прізвищем та іменем.



Крок 3. Розмістити на S3 статичну веб-сторінку, яка містить ваше ПІБ та Вашу академічну групу.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ Directory

Recommended for low-latency use cases. These buckets us processing of data within a single Availability Zone.

Bucket name [Info](#)

Yaroslava-Koldun-apz

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Крок 4. Налаштування хостингу і отримання публічної адреси сторінки, наприклад: <https://kbaleiko-bucket-apz.s3-website.eu-north-1.amazonaws.com/>

