

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



**ЗВІТ  
з виконання Практичної роботи  
з дисципліни  
«Аналіз програмного забезпечення»**

Виконав:  
студент гр. 124-22-2

Тарасенко Микита  
Дмитрович

Прийняв:

Доц. кафедри САiУ  
Мінєєв О.С.

**Дніпро  
2025**

## Практична робота №4

### AWS S3

**Мета:** Набування навичок у створення і розміщення статичної веб-сторінки на AWS S3.

**Очікувані результати навчання:** уміння створити і розмістити сторінку з власними даними на ресурсі AWS S3.

The screenshot shows the official AWS website homepage. At the top, there's a navigation bar with links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enablement, Events, Explore More, and a search icon. A purple banner for re:Invent 2024 is visible. Below the banner, a large call-to-action button says "Start building on AWS today". A descriptive text block explains that AWS offers services for generative AI, compute power, database storage, content delivery, and more, helping to build sophisticated applications with increased flexibility, scalability, and reliability. Two buttons below the text are "Get started for free" and "Contact an AWS specialist". To the right, a "Sign up for AWS" section includes fields for "Root user email address" and "AWS account name", both with explanatory text and input boxes. A yellow "Verify email address" button is present. At the bottom, there's a link to "Sign in to an existing AWS account". On the left side of the main content area, there's a small graphic of a hand holding three cubes.

Screenshot of the AWS S3 'Create bucket' configuration page.

### General configuration

**AWS Region:** Europe (Frankfurt) eu-central-1

**Bucket name:** tarasenkom-bucket-apz

**Copy settings from existing bucket - optional:** Only the bucket settings in the following configuration are copied. [Choose bucket](#)

Format: s3://bucket/prefix

### Object Ownership

**Object Ownership:**

- ACLs disabled (recommended)**: All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ACLs enabled**: Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

### 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.

### Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type:** [Info](#)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

- Server-side encryption with Amazon S3 managed keys (SSE-S3)**
- Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

**Bucket Key**: Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- Disable
- Enable

### Advanced settings

**After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.**

[Cancel](#) [Create bucket](#)

```
<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <title>Моя сторінка</title>
</head>
<body>
    <h1>Тарасенко Микита Дмитрович</h1><br/>
    <h2>124-22-2<h2>
</body>
</html>
```

aws | Search [Alt+S] Account ID: 4836-4375-5933 Europe (Frankfurt) Mykta%20Tarasenko

Amazon S3 > Buckets > tarasenkom-bucket-apz

## tarasenkom-bucket-apz Info

Objects Metadata Properties Permissions Metrics Management Access Points

Objects (1) Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
Тарасенко Микита.124-22-2.АП3.зав4.html	html	November 3, 2025, 21:28:02 (UTC+02:00)	228.0 B	Standard

aws | Search [Alt+S] Account ID: 4836-4375-5933 Europe (Frankfurt) Mykta%20Tarasenko

Amazon S3 > Buckets > tarasenkom-bucket-apz > Upload

### Files and folders (1 total, 228.0 B)

All files and folders in this table will be uploaded.

Find by name

Name	Folder	Type	Size
Тарасенко Микита.124-22-2.АП3.зав4.html	-	text/html	228.0 B

#### Destination Info

Destination <s3://tarasenkom-bucket-apz>

▶ Destination details Bucket settings that impact new objects stored in the specified destination.

#### Permissions

Grant public access and access to other AWS accounts.

#### Properties

Specify storage class, encryption settings, tags, and more.

Cancel Upload

aws | Search [Alt+S] Account ID: 4836-4375-5933 Europe (Frankfurt) Mykta%20Tarasenko

Amazon S3 > Buckets > tarasenkom-bucket-apz

## tarasenkom-bucket-apz Info

Objects Metadata Properties **Permissions** Metrics Management Access Points

### Permissions overview

**Access finding**  
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).  
[View analyzer for eu-central-1](#)

### Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access** Off Edit

▶ Individual Block Public Access settings for this bucket

**Edit Block public access (bucket settings)** Info

**Block public access (bucket settings)**

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 all your S3 buckets and 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 your buckets 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.

[Cancel](#) [Save changes](#)

**Edit static website hosting** Info

**Static website hosting**

Use this bucket to host a website or redirect requests. [Learn more ↗](#)

**Static website hosting**

Enable  
 Disable

**Hosting type**

Host a static website  
Use the bucket endpoint as the web address. [Learn more ↗](#)

Redirect requests for an object  
Redirect requests to another bucket or domain. [Learn more ↗](#)

ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#) ↗

**Index document**  
Specify the home or default page of the website.  
tarasenko.mikyta.124-22-2.ap3.зав4.html

**Error document - optional**  
This is returned when an error occurs

**Static website hosting**

Use this bucket to host a website or redirect requests. [Learn more ↗](#)

ⓘ We recommend using AWS Amplify Hosting for static website hosting  
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) ↗ or [View your existing Amplify apps](#) ↗

[Create Amplify app](#) ↗

**S3 static website hosting**  
Enabled

**Hosting type**  
Bucket hosting

**Bucket website endpoint**  
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more ↗](#)  
http://tarasenkom-bucket-apz.s3-website.eu-central-1.amazonaws.com

Результат практичної роботи:

<http://tarasenkom-bucket-apz.s3-website.eu-central-1.amazonaws.com>



**Тарасенко Микита Дмитрович**

**124-22-2**