

**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 САіУ
Мінєєв О.С.

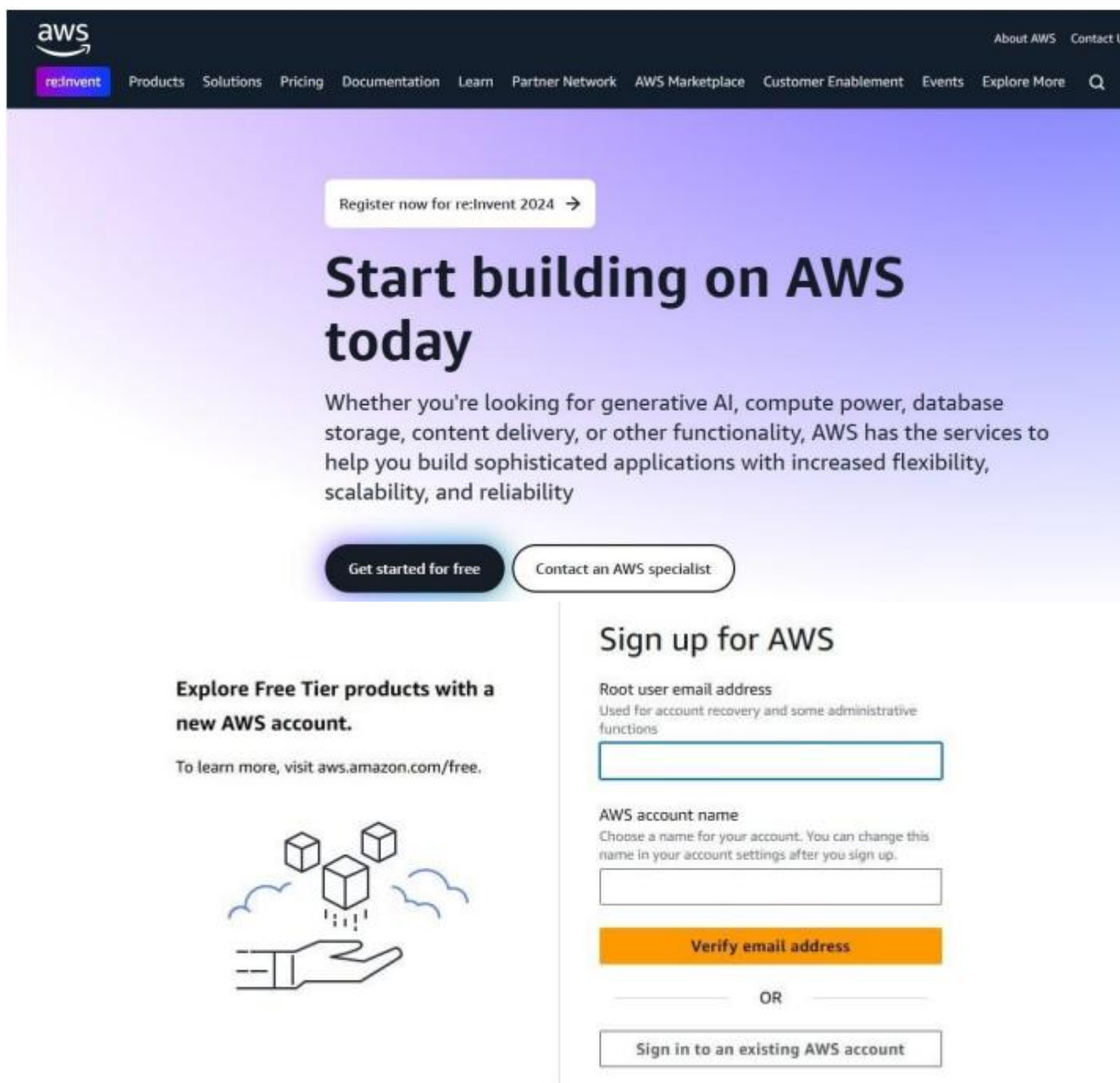
**Дніпро
2025**

Практична робота №4

AWS S3

Мета: Набування навичок у створення і розміщенні 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 AWS website homepage. At the top is the AWS logo and a navigation bar with links like 'redinvent', 'Products', 'Solutions', 'Pricing', 'Documentation', 'Learn', 'Partner Network', 'AWS Marketplace', 'Customer Enablement', 'Events', 'Explore More', and a search icon. Below the navigation bar is a large purple banner with the text 'Start building on AWS today'. Above this text is a button that says 'Register now for re:Invent 2024 →'. Below the banner text are two buttons: 'Get started for free' and 'Contact an AWS specialist'. To the left of the sign-up form is a section titled 'Explore Free Tier products with a new AWS account.' with a link to 'aws.amazon.com/free.' and an illustration of a hand holding three cubes. The sign-up form on the right is titled 'Sign up for AWS' and contains the following fields and buttons:

- Root user email address (Used for account recovery and some administrative functions) - input field
- AWS account name (Choose a name for your account. You can change this name in your account settings after you sign up.) - input field
- Verify email address - orange button
- OR - text separator
- Sign in to an existing AWS account - button

[Alt+S]

Europe (Frankfurt)
Account ID: 4836-4375-5933
Mykyta%20Tarasenko

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Frankfurt) eu-central-1

Bucket name Info
tarasenkorn-bucket-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 more](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

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 Info

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]

Europe (Frankfurt)

Account ID: 4836-4375-5933

Mykyta%20Tarasenko

Amazon S3

Buckets

tarasenkombucketapz

tarasenkombucketapz

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Name

Type

Last modified

Size

Storage class

Tarasenko Mykyta.124-22-2.A1T3.3ab4.html

html

November 3, 2025, 21:28:02 (UTC+02:00)

228.0 B

Standard

Files and folders (1 total, 228.0 B)

Remove

Add files

Add folder

Find by name

Name

Folder

Type

Size

Tarasenko Mykyta.124-22-2.A1T3.3ab4.html

-

text/html

228.0 B

Destination

Info

Destination

s3://tarasenkombucketapz

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]

Europe (Frankfurt)

Account ID: 4836-4375-5933

Mykyta%20Tarasenko

Amazon S3

Buckets

tarasenkombucketapz

tarasenkombucketapz

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)

Edit

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

Individual Block Public Access settings for this bucket

eu-central-1.console.aws.amazon.com/s3/bucket/taraskom-bucket-apz/property/bpa/edit?region=eu-central-1

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

Amazon S3 > Buckets > taraskom-bucket-apz > Edit Block public access (bucket settings)

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](#)

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

Amazon S3 > Buckets > taraskom-bucket-apz > Edit static website hosting

Edit static website hosting [info](#)

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

Static website hosting

☐ Disable
☒ Enable

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.

Taraskenko Микита.124-22-2.АП3.зав4.html

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

Static website hosting [Edit](#)

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://taraskom-bucket-apz.s3-website-eu-central-1.amazonaws.com>

Результат практичної роботи:

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



Тарасенко Микита Дмитрович

124-22-2