

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»



Національний
технічний університет
ДНІПРОВСЬКА
ПОЛІТЕХНІКА
1899



ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра системного аналізу та управління

Звіт з виконання практичних робіт

з дисципліни
«Аналіз програмного забезпечення»

Виконав:
студент групи 124-22-2
Марценюк Ганна

Перевірив:
Асистент кафедри САУ
Шевченко Ю. О.

Дніпро
2025

ПРАКТИЧНА РОБОТА №1

Тема: Створення ЕЦП

Мета: набуття навичок створення ЕЦП та підписання документів

1. Створення документу .pdf

Я студентка групи 124-22-2 Марценюк Ганна Сергіївна. Я 9 років професійно займалась плаванням, маю кішечку на ім'я Кассіонея. Вивчаю італійську мову.

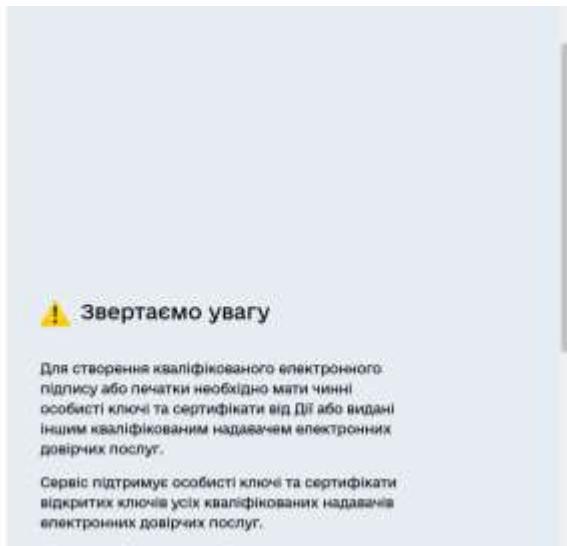
2. Підписання за допомогою застосунку Дія

Підписати документ

Підписати файл за допомогою

- Електронного підпису →
- Дія.Підпис - UA →
- Дія.Підпис - EU →

Версія від 2025.08.25 13:00



Обираємо Дія.Підпис – UA

Перевірте дані

Що таке сертифікат?

Марценюк Ганна Сергіївна

РНOKLP
3835210640

УНЗР
20050101-05145

Сертифікати

ЕЦП (ДСТУ 4145), Неспростовність (ДСТУ 4145) *

EJ-3E2367105294AF70400000E10270013906CF04.cer

Назад

Далі

Що таке ASiC?

👉 Рекомендуємо підписувати документи у форматі ASiC-E.

Це уніфікований формат електронного документообігу, який гарантує, що ваші документи прийматимуть всі держоргани.

Так, підписати в форматі ASiC-E

Ні, обрати інший формат

Версія від 2025.08.25 13:00

Що таке ASiC?

👉 Рекомендуємо підписувати документи у форматі ASiC-E.

Це уніфікований формат електронного документообігу, який гарантує, що ваші документи прийматимуть всі держоргани.

Файл(и) для підпису:

- Марценюк_124-22-2_АПЗ№1.pdf

Змінити

Підписати в форматі ASiC-E

Назад



Накладання підпису на файл



Натисніть або зчитайте QR-код сканером у застосунку
ДіЯ та дотримуйтесь інструкцій
QR-код буде дійсним ще 02:50

×

Запит на підпис документа через Дія.Підпис

ID.GOV.UA

м. Київ, вул. Ділова, 24

Підпис у застосунку через Дія.Підпис

Необхідно підписати:

- Марценюк_124-22-2_АПЗ№1.pdf.asice



Підтвірджую запит на вебресурсі.

Надіслати

Відхилити запит

3. Нарешті отримуємо підписаний файл

Підписати документ



Документ підписано

⬇ Завантажити все архівом

⬇ Файл з підписом

Марценюк_124-22-2_АПЗN°1.pdf.asice

77.7 КБ



⬇ Файл(и) без підпису

Марценюк_124-22-2_АПЗN°1.pdf

76.0 КБ



⬇ Протокол створення та перевірки кваліфіков...

Марценюк_124-22-2_АПЗN°1_Validation_Report.pdf

50.4 КБ



ПРАКТИЧНА РОБОТА №2

Тема: Знайомство з GitHub

Мета: набути базових навичок взаємодії із системою контролю версій Git на базі GitHub.

1. Заходимо на GitHub і проводимо авторизацію

The screenshot shows the GitHub homepage with a dark background. At the top, there is a navigation bar with links for Platform, Solutions, Resources, Open Source, Enterprise, and Pricing. On the right side of the header are search, sign-in, and sign-up buttons. Below the header, a large blue button with a yellow octocat icon and the text "Explore the latest tools from Universe '25" is visible. The main headline reads "The future of building happens together". A subtext below it says "Tools and trends evolve, but collaboration endures. With GitHub, developers, agents, and code come together on one platform." At the bottom of the page, there are three buttons: "Enter your email", "Sign up for GitHub" (in green), and "Try GitHub Copilot free".

The screenshot shows the GitHub sign-up form. On the left, there is a section titled "Create your free account" with a subtext "Explore GitHub's core features for individuals and organizations." and a "See what's included" link. Below this is a dark background featuring three cartoonish, colorful characters (a purple blob-like character, a yellow bird-like character, and a blue cube-like character) floating in space. On the right, the sign-up form is displayed. It includes fields for "Email" (with placeholder "Email"), "Password" (with placeholder "Password" and a note about length and complexity), "Username" (with placeholder "Username" and a note about allowed characters), "Your Country/Region" (a dropdown menu with "Ukraine" selected), and "Email preferences". There are also "Continue with Google" and "Continue with Apple" buttons at the top of the form area. A link "Already have an account? Sign in" is located at the top right of the form area.

2. Провівши авторизацію створюємо репозиторій

Create a new repository

Repositories contain a project's files and version history. Have a project elsewhere? [Import a repository](#).
Required fields are marked with an asterisk (*).

1 General

Owner * Repository name *

hmartseniuk /

Great repository names are short and memorable. How about [miniature-waddle](#)?

Description

0 / 350 characters

2 Configuration

Choose visibility * Public

Choose who can see and commit to this repository

Add README Off

READMEs can be used as longer descriptions. [About READMEs](#)

Add .gitignore No .gitignore

.gitignore tells git which files not to track. [About ignoring files](#)

Add license No license

Licenses explain how others can use your code. [About licenses](#)

Create repository

ПРАКТИЧНА РОБОТА №3

Приклад Test Case: «Успішна реєстрація нового користувача»

Загальні відомості

- Назва: Перевірка успішної реєстрації користувача з валідними даними.
- Pre-condition:
 1. Користувач перебуває на сторінці реєстрації.
 2. Користувач має доступний унікальний email, який ще не використовувався в системі.
 3. Пароль відповідає всім вимогам системи (наприклад, містить мінімум 8 символів, велику літеру та цифру).
 4. Підключення до Інтернету стабільне та активне.
- Steps:
 1. У полі "Email" ввести валідну, унікальну електронну адресу.
 2. У полі "Пароль" ввести вимогам відповідаючий пароль.
 3. У полі "Повторити пароль" ввести той самий пароль.
 4. Натиснути на праپорець (чекбокс) "Я згоден з умовами користування".
 5. Натиснути кнопку "Зареєструватися".
- Expected Result:
 1. Система відображає повідомлення про успішну реєстрацію.
 2. Користувач автоматично перенаправляється на сторінку підтвердження email або на головну сторінку, вже як залогінений користувач.
 3. У базі даних створюється новий запис користувача з наданими даними.
- Post-condition: новий користувач успішно створений у системі, і він/вона має доступ до функціоналу, доступного лише для авторизованих користувачів.

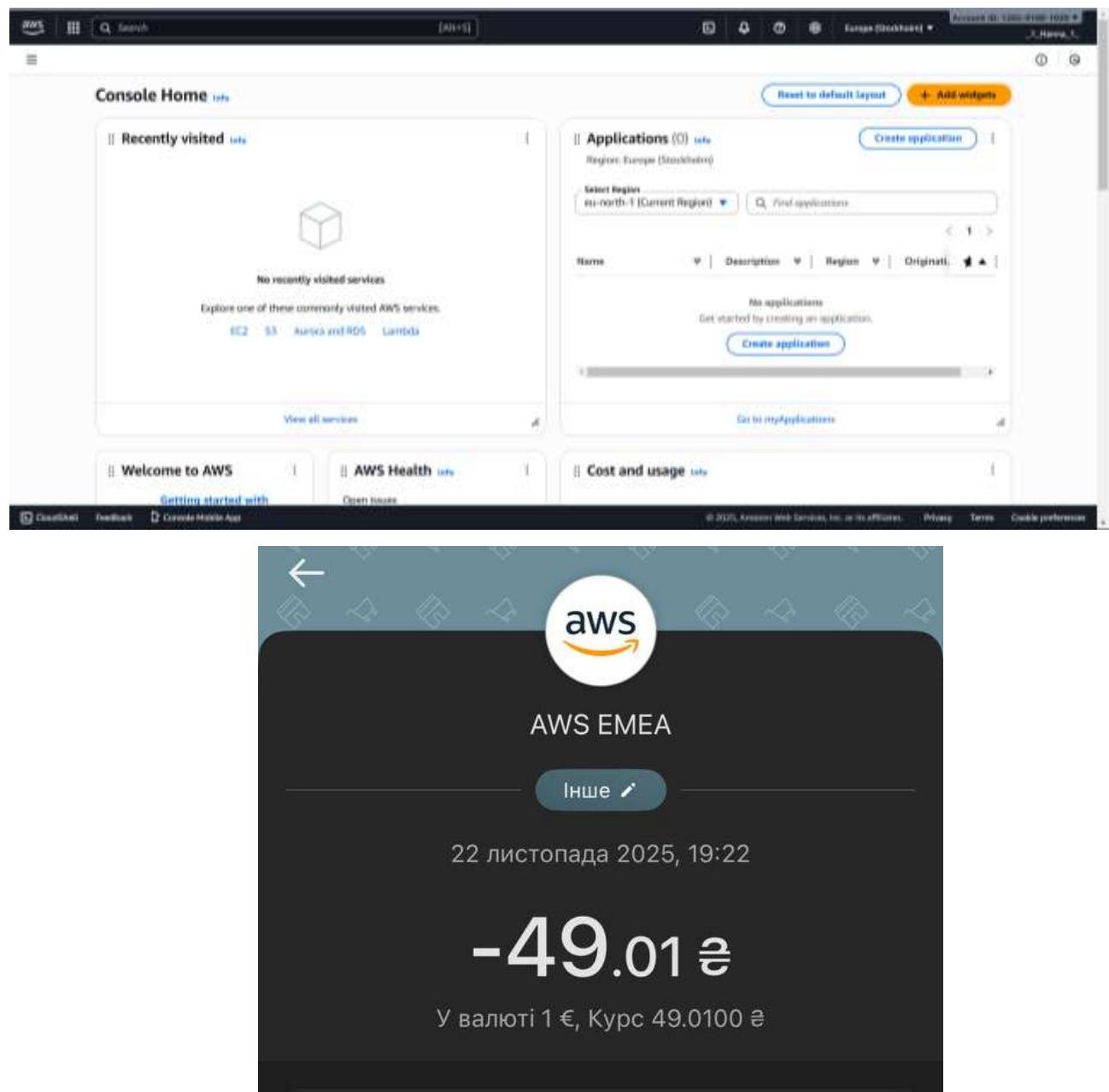
ПРАКТИЧНА РОБОТА №4

Тема: AWS S3

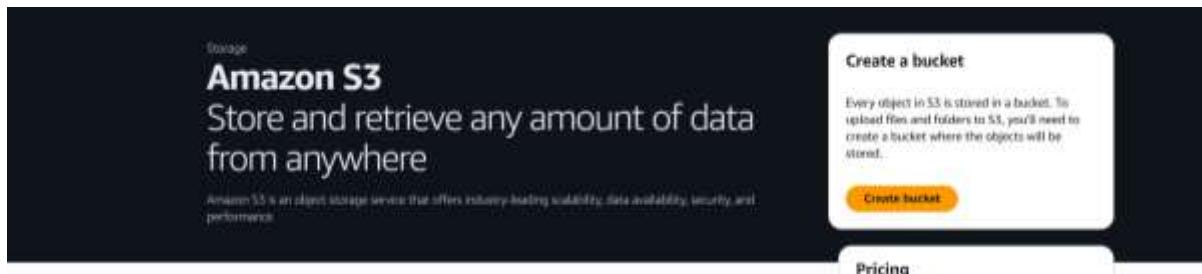
Мета: Набування навичок у створення і розміщенні статичної веб-сторінки на AWS S3.

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

1. Проведено реєстрацію на сайті та створено акаунт



2. Створимо перший Bucket



The screenshot shows the 'Create a bucket' page for Amazon S3. At the top, there's a header with the Amazon logo and the text 'Amazon S3' and 'Store and retrieve any amount of data from anywhere'. Below the header, a sub-header says 'Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.' To the right, there's a 'Create a bucket' button. Further down, there's a 'Pricing' section.

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 IAM 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.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

Bucket owner preferred

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object owner.

Object owner

The object owner retains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more ↗](#)

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 off 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](#). [Learn more ↗](#)

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

3. Завантаження html

4. Налаштуємо доступ

Object Ownership

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.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

⚠️ Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

I acknowledge that ACLs will be restored.

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the `bucket-owner-full-control` canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

💡 If you want to enforce object ownership for new objects only, your bucket policy must specify that the `bucket-owner-full-control` canned ACL is required for object uploads. [Learn more ↗](#)

Grantee	Objects	Object ACL
Object owner (your AWS account)	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Canonical ID: 45bed8b8330e8f2c163c57e9d1ca8a307084e080a5b1e381337375767231b		
Everyone (public access)	<input checked="" type="checkbox"/>   Read	<input checked="" type="checkbox"/>   Read <input type="checkbox"/> Write
Group: http://acs.amazonaws.com/groups/global/AllUsers		
Authenticated users group (anyone with an AWS account)	<input checked="" type="checkbox"/>   Read	<input checked="" type="checkbox"/>   Read <input type="checkbox"/> Write
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers		

Позиции:

<https://banne-first-bucket.s3.eu-north-1.amazonaws.com/>

1.amazonaws.com/%D0%9C%D0%B0%D1%80%D1%86%D0%B5%D0%BD%D1%8E%D0%BA.html

ПРАКТИЧНА РОБОТА № 5

Тема: Знайомство з EC2

Мета: набуття базових навичок взаємодії із сервісами AWS у вигляді EC2, налаштування та відкриття доступу до підключення до віддаленого робочого столу по IP.

1. Створення нового EC2

The screenshot shows the AWS EC2 console interface. On the left, there's a sidebar with 'Resources' and 'Launch instance' sections. The main area has 'Service health', 'Zones', and 'Scheduled events'. On the right, there are sections for 'EC2 cost', 'Account attributes', and 'Explore AWS'. A large central window is titled 'Create New Instance' with tabs for 'Amazon Machine Image (AMI)', 'Instance Type', 'Configure Security Group', 'Configure Network', 'Configure Volume', and 'Review and Launch'. The 'Amazon Machine Image (AMI)' tab is active, showing options like 'Microsoft Windows Server 2025 Base' and 'Amazon Linux 2'. The 'Instance Type' tab shows 't2.micro' selected. The 'Configure Security Group' tab shows 'New security group' named 'NewSecurityGroup'. The 'Configure Network' tab shows 'New subnet' selected. The 'Configure Volume' tab shows '1 volume(s) - 10 GB'. The 'Review and Launch' tab shows 'Launch' and 'Preview code' buttons.

Instance type [Info](#) | [Get advice](#)

Instance type

m7s-flex-large	Free tier eligible
Family: m7s-fx Large 2 vCPU 8 GiB Memory Current generation true On-Demand Linux base pricing: 0.01716 USD per Hour On-Demand Ubuntu Pro base pricing: 0.01294 USD per Hour On-Demand RHEL base pricing: 0.01934 USD per Hour On-Demand Windows base pricing: 0.08911 USD per Hour On-Demand SUSE base pricing: 0.02055 USD per Hour	

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

For Windows instances, you can use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

[Create new key pair](#)

Network settings [Info](#)

Network [Info](#)
ipn-00bf49673375e17ca0

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Firewall (security group) [Info](#)
A security group is a set of Network rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Will create a new security group called "Launch-wizard-1" with the following rules:

Allow RDP traffic from Anywhere Helps you connect to your instance

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Software Image (AMI)
Microsoft Windows Server 2025 ... [read more](#)
ami-01fa40ca0127403388

Virtual server type (instance type)
m7s-flex-large

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

[Cancel](#) [Launch instance](#) [Preview code](#)

Success
Successfully initiated launch of instance ([i-0bf49673375e17ca0](#))

2. Створення ключа доступу

~\$рценюк_124-22-2_АПЗ№5.docx	C6 22.11.25 21:22	Документ Microsoft Word	1 КБ
pckey.pem	C6 22.11.25 21:32	Файл PEM	2 КБ
Марценюк_124-22-2_АПЗ№5.docx	C6 22.11.25 21:22	Документ Microsoft Word	0 КБ

3. Підключення створеного ключа

[Get Windows password](#)

Use your private key to retrieve and decrypt the initial Windows administrative password for this instance.

Instance ID
[i-0bf49673375e17ca0](#) (MyPCHartsenuk)

Key pair associated with this instance
[pckey](#)

Private key
Enter, upload your private key file or copy and paste its contents into the field below.

[Upload private key file](#)

`pkkey.pem`

Private key contents

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQDAnwCAnQ5kXQJ70LqRHPHyMP60OMQ5n3Jh4KwUDfHtLc
wppL1Z2AKGFLtOw8CgYIwJn0D4H5Ctg0d4ufk5J2MHMNg46n7wp+9bgi+k
J1fM8-H0wepWtCp0t1p45cf17+4kaQJUbaevRaE1P9+H2a3U7Wk3QKkiknD
lfFwdbmfl-k47NuB23neBHCtunQXUAvr19wjLJMhYiU2zGFCBHMqQH
d1hPFT24iLV3jw5DnreMsfrmgC19wjqhdDeQJTwtyQXtE1700G2AMP
kJ6/sqf/YH02TCmJrVgfu8f8h1PTTfLJdyQDwDRQMaRbME+csbkX10C9Vw
mhsKtYwHo/RPzxaRylyFvA4r5/13ckRfQDFlwA&YH02SMWCHQhN00KVb/P52P
-----END RSA PRIVATE KEY-----
```

4. Отримання інформації про машину

Get Windows password X

Connect to your Windows instance using Remote Desktop with this information.

Instance ID
 i-0bf49673375e17ca0 (MyPCMartseniuk)

Private IP address
 172.31.43.49

Username
 Administrator

Password
 cly(kl*Z9s9El&%esvW0\$5ukOR\$rSdE

i **Password change recommended**
We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved using this tool. It is important that you change your password to one that you will remember.

Cancel OK

 Підключення до віддаленого робочого стола — □ X

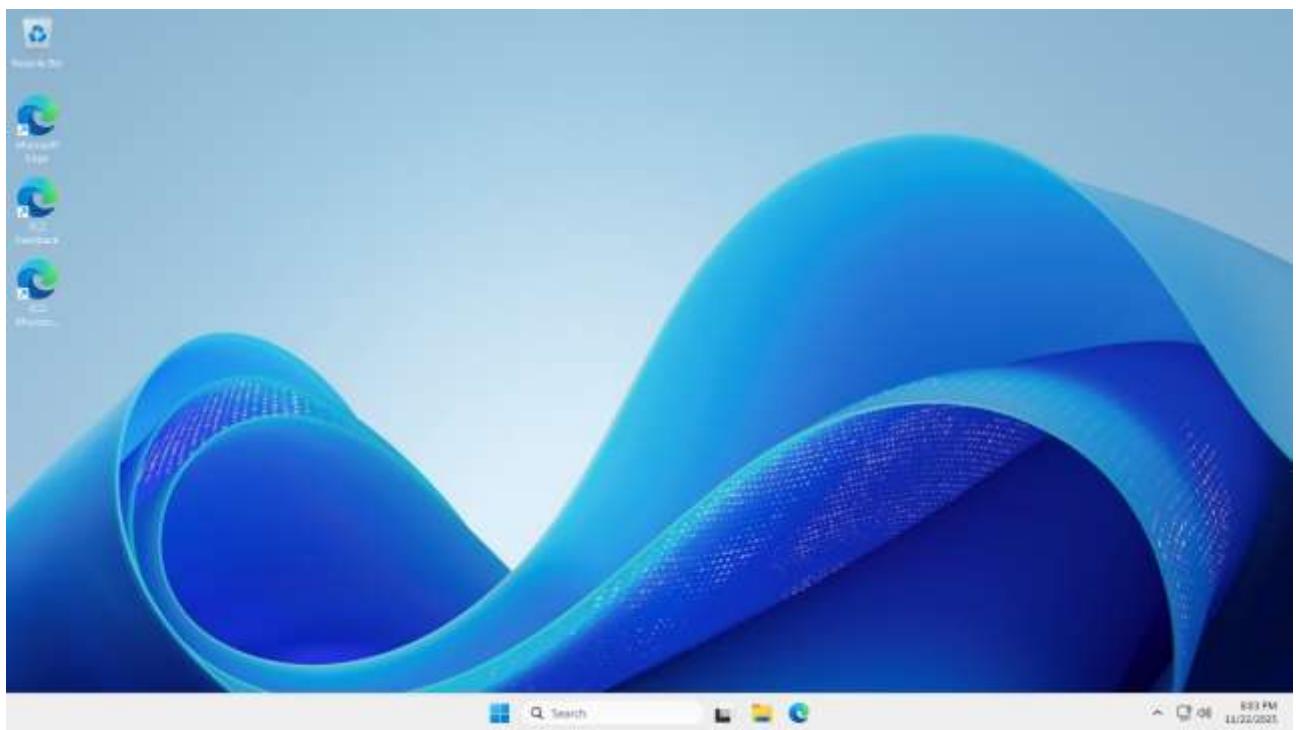
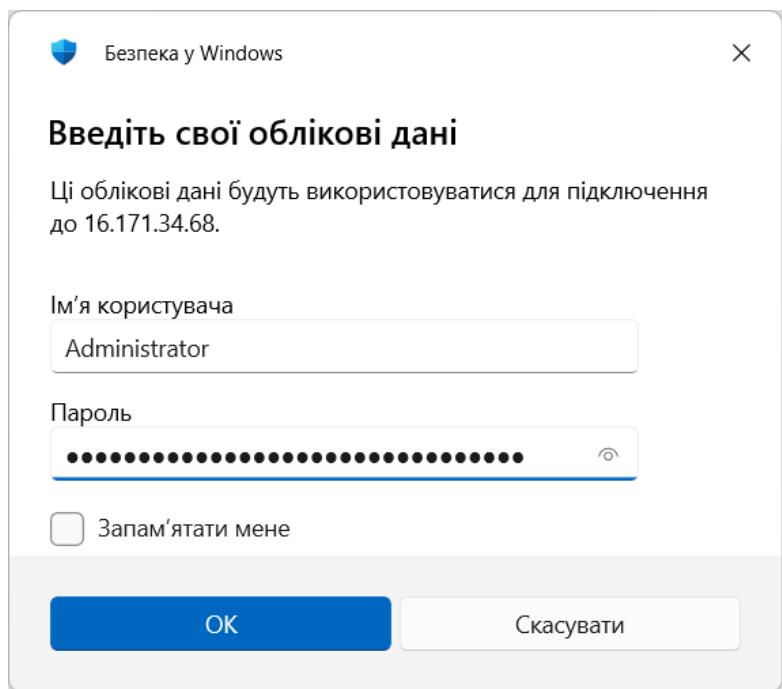
 **Підключення до віддаленого робочого стола**

Комп'ютер:

Ім'я користувача:

Під час підключення буде здійснено запит ваших облікових даних.

Показати параметри Підключитися Довідка





Public IP	16.171.34.68
Private IP	172.31.43.49
Username	Administrator
Instance ID	i-0bf49673375e17ca0
Password	cIy(kI*Z9s9EId&%esvW0\$5ukOR\$rSdE