

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



Національний
технічний університет
ДНІПРОВСЬКА
ПОЛІТЕХНІКА
1899

Звіт

Лабораторна робота №5
З дисципліни «Аналіз програмного забезпечення»

Виконала:

студентка групи 122-22-5

Алексєєнко Є.Д.

Перевірив:

Мінєєв Олександр Сергійович

Юлія Олексandrівна Шевченко

м. Дніпро

2025 рік

Мета роботи: набування навичок створення та розміщення віртуального сервера за допомогою AWS EC2.

Створюємо Instance. Для цього перейшла на [AWS Management Console](#) та увійшла за своїм обліковим записом AWS. У рядку пошуку консолі ввела EC2:

The screenshot shows the AWS Management Console interface. At the top, there's a search bar with 'EC2' and a navigation menu. Below it, the 'Services' section is open, with 'EC2' highlighted. A 'Top features' card includes links for Dashboard, Launch templates, Instances, Spot Instance requests, and Savings plans. The main content area is titled 'Launch instance' with the sub-instruction: 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' It features two buttons: 'Launch instance' (orange) and 'Migrate a server' (blue). A note below says: 'Note: Your instances will launch in the Europe (Stockholm) Region'. The next section, 'Name and tags', has a 'Name' field containing 'APZ-YELYZAVETA-ALEKSIEENKO' and a 'Add additional tags' button. The 'Quick Start' section shows icons for various AMIs: Amazon Linux, macOS, Ubuntu, Windows (selected), Red Hat, SUSE Linux, and Debian. To the right is a link to 'Browse more AMIs'. The 'Amazon Machine Image (AMI)' section details the selected Windows Server 2025 Base AMI (ami-010e40c6557403885). The 'Description' section provides the AMI's full details: Microsoft Windows Server 2025 Datacenter edition. [English], 64-bit (x86), Microsoft Windows Server 2025 Full Locale English AMI provided by Amazon. The final table shows provider details: Architecture (64-bit (x86)), AMI ID (ami-010e40c6557403885), Publish Date (2025-11-12), Username (Administrator), and a green 'Verified provider' badge.

Створюємо key pair:

Create key pair



Key pair name

Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA

RSA encrypted private and public key pair

ED25519

ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

.pem

For use with OpenSSH

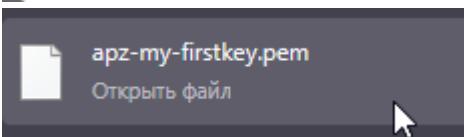
.ppk

For use with PuTTY

When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more ↗](#)

Cancel

Create key pair



Далі налаштовуємо Configure storage:

▼ Configure storage [Info](#)

Advanced

1x GiB Root volume, 3000 IOPS, Not encrypted

[Add new volume](#)

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance

Click refresh to view backup information



The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Edit

▼ Summary

Number of instances | [Info](#)

1



Software Image (AMI)

Microsoft Windows Server 2025 ...[read more](#)

ami-010e40c6557403885

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

[Cancel](#)

[Launch instance](#)

 [Preview code](#)

Instance був успішно створений:



Success

Successfully initiated launch of instance ([i-0aeaaf1fe5fde6e8f](#))

Наступний крок - це отримання паролю Windows:

Get Windows password

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

[Get Windows password](#) 

Get Windows password Info

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

Instance ID
 i-0aeaaf1fe5fde6e8f (APZ-YELYZAVETA-ALEKSIEIENKO)

Key pair associated with this instance
 apz-my-firstkey

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

apz-my-firstkey.pem

1.67 KB

Private key contents

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAs6sh0BwMVRspXqldij4v5Ln9p/dDVa7qOHY3n1/rmQ+7jifj  
vApLN2z5h8gqpPTqdy4TtpqYufWFCqrEd91dgJbhg62v8LpHz5zVApLPFDrmgPDG  
pUVbSXF+rnu9UfVPC/5mFE84yFnuiuBM2DhB2djk2dVj4M45fU13Gr78hBy  
HCqhdFc7CBERaYdPgxxliblDrACLO7Migm41gBiNE3f/E2E4AymkALMpJrySKv  
GxJ3Jte8c7BRWIRtgK4TC6W96JW+G27WsIBNOCPic1q1puqEsam6MdvEM+Bx  
Ra926reB1G2ria1XsKKmGDlu5M36k4kgK5QlDAQABAoIBAA/Bb/ffbdgZ8BQB  
MdcRj6FNLL6G21/uowO8byiRT86TQ27Ol.r65uiMgLN+t0RFwzfvsJWBXD4i+7
```

Get Windows password

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

Instance ID
 i-0aeaaf1fe5fde6e8f (APZ-YELYZAVETA-ALEKSIEIENKO)

Private IP address

Username
 Administrator

Password

ⓘ 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.

Password decryption successful	
The password for instance i-0aeaaf1fe5fde6e8f was successfully decrypted.	
Instances (1) <small>Info</small>	<input type="button" value="Connect"/> <input type="button" value="Instance state"/> <input type="button" value="Actions"/> <input type="button" value="Launch instances"/>
<input type="button" value="Find instance by attribute or tag (case-sensitive)"/>	<input type="button" value="All states"/>
<input checked="" type="checkbox"/> Name <input type="text" value="i-0aeaaf1fe5fde6e8f"/> <input type="checkbox"/> Instance ID <input type="text" value="i-0aeaaf1fe5fde6e8f"/> <input type="checkbox"/> Instance state <input type="text" value="Running"/> <input type="checkbox"/> Instance type <input type="text" value="t3.micro"/> <input type="checkbox"/> Status check <input type="text" value="2/3 checks passed"/> <input type="checkbox"/> Alarm status <input type="text" value="None"/> <input type="checkbox"/> Availability Zone <input type="text" value="eu-north-1b"/> <input type="checkbox"/> Public IPv4 DNS <input type="text" value="ec2-13-53-129-43.eu-n..."/> <input type="checkbox"/> Public IPv4 IP <input type="text" value="13.53.129.43"/> <input type="checkbox"/> Elastic IP <input type="text" value="None"/> <input type="checkbox"/> IPv6 IPs <input type="text" value="None"/> <input type="checkbox"/> Monitoring <input type="text" value="disabled"/> <input type="checkbox"/> Security group name <input type="text" value="launch-wizard-1"/> <input type="checkbox"/> Key name <input type="text" value="api-firstkey"/>	<input type="button" value="View alarms"/> <input type="button" value="Launch instance"/>

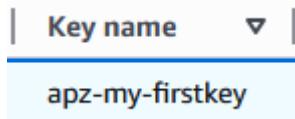
Підключення до віддаленого комп'ютера (Windows EC2 Instance):

Після успішного створення віртуального сервера на AWS EC2 я виконала підключення до нього за допомогою віддаленого робочого столу (RDP).

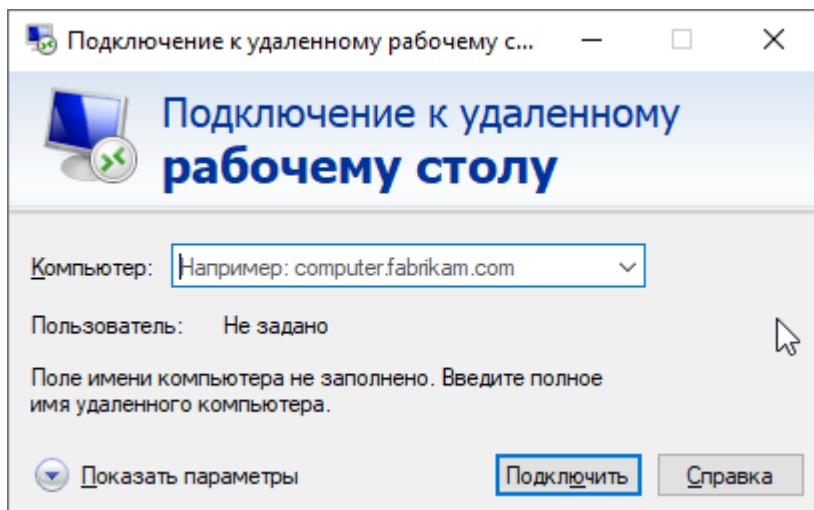
1. Спочатку я отримала Public IP-адресу свого Instance у консолі AWS EC2.

Public IPv4 address
13.53.129.43 | [open address](#)

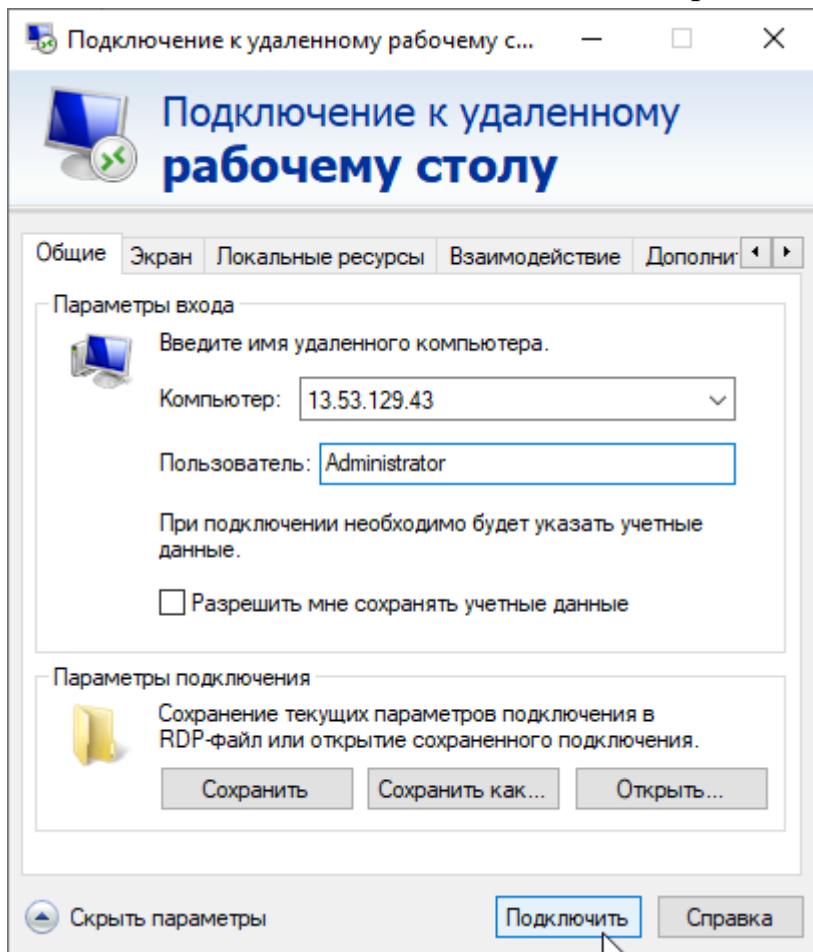
2. Далі натиснула Connect → RDP client → Get password, використавши свій Key Pair (.pem) для розшифрування паролю адміністратора.



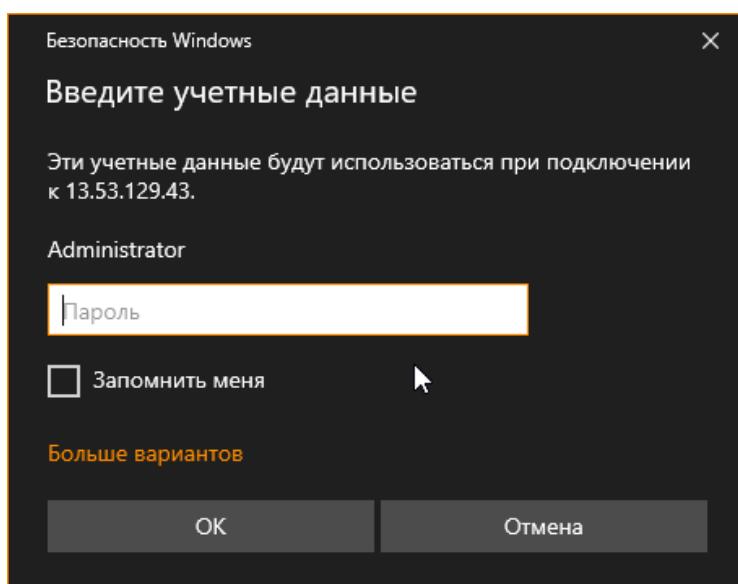
3. На своєму комп'ютері відкрила програму Підключення до віддаленого робочого столу (mstsc).

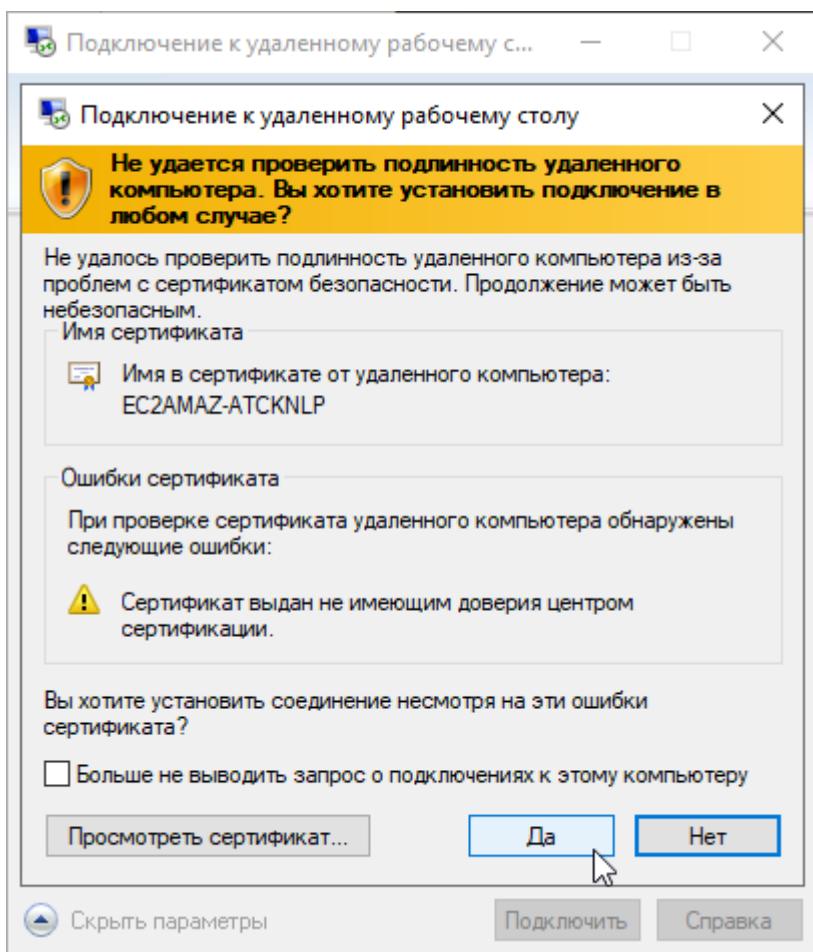
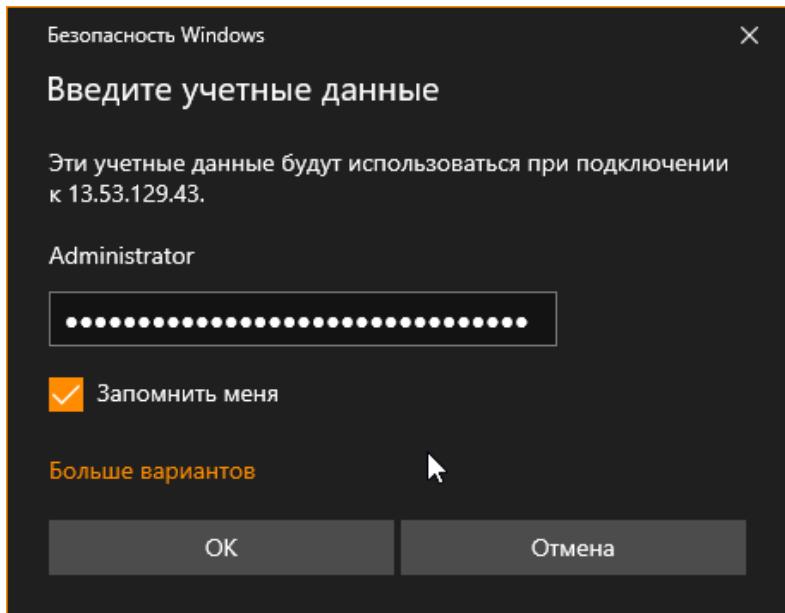


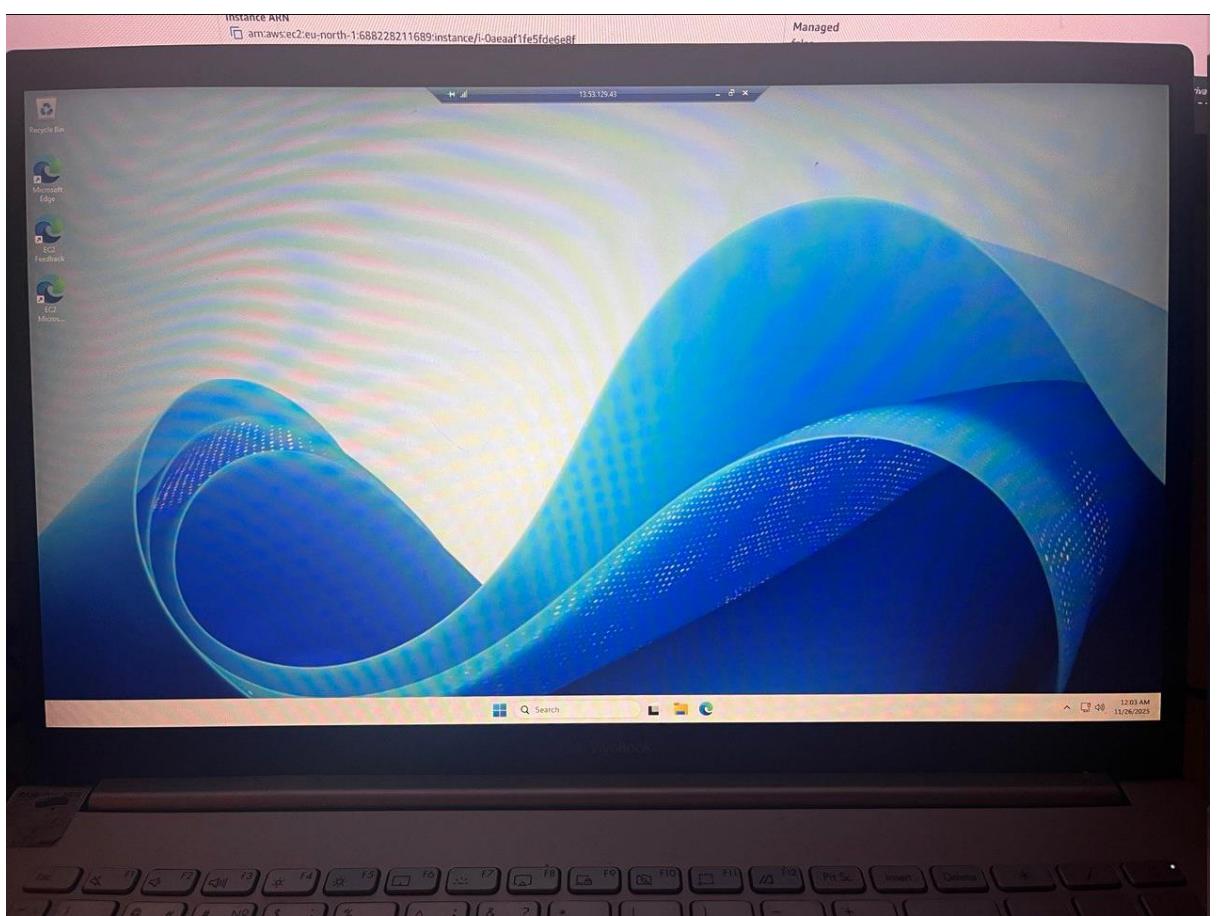
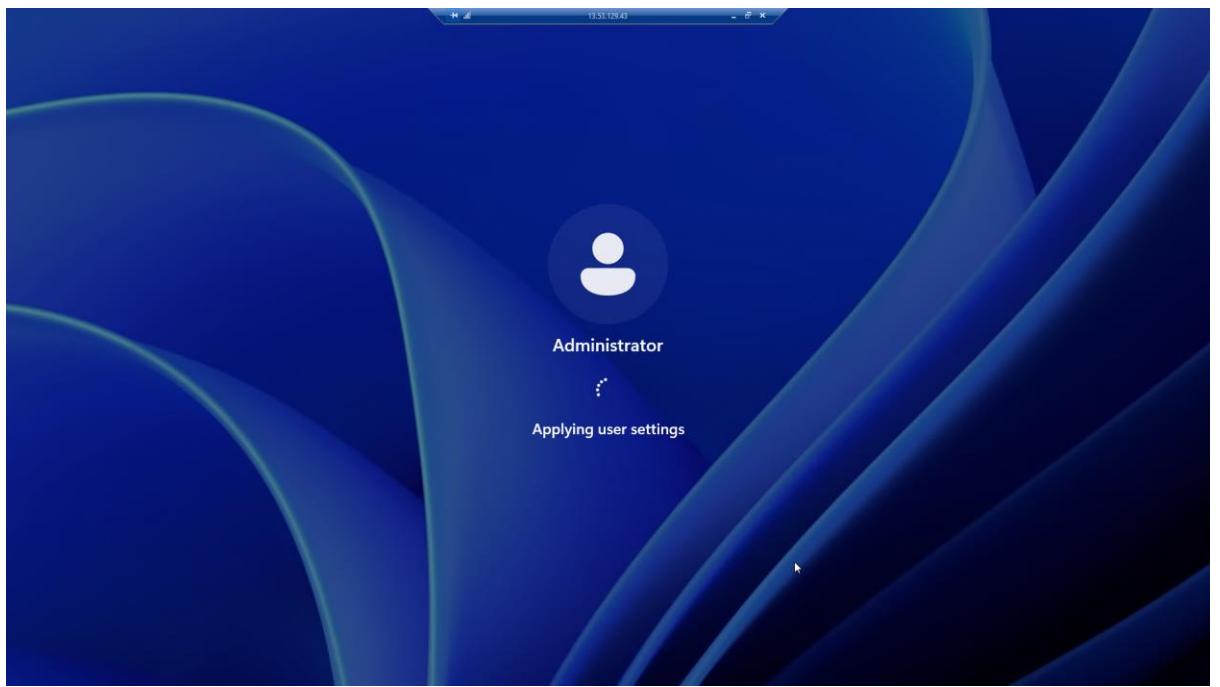
4. В полі Computer ввела Public IP свого сервера, а в полі Username — Administrator. У поле Password вставила пароль, отриманий на AWS.



5. Натиснула Connect і підтвердила сертифікат безпеки, після чого відбулося успішне підключення до віддаленого робочого столу Windows.







Таким чином я змогла отримати доступ до свого EC2 Instance і готова виконувати подальші дії на сервері.

Висновок:

Під час виконання лабораторної роботи я ознайомилася з процесом створення та налаштування віртуального сервера на AWS EC2, включаючи створення key pair, налаштування сховища та отримання паролю адміністратора для Windows. Я успішно підключилася до віддаленого робочого столу та отримала доступ до сервера, що дозволяє виконувати подальші операції та тестування програмного забезпечення. Робота допомогла набути практичних навичок роботи з хмарними сервісами та віддаленими серверами.