

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



Факультет інформаційних технологій
Кафедра системного аналізу та управління

Звіт
з практичних робіт з дисципліни
«Аналіз програмного забезпечення»

Виконав:

студент групи 121-21-1

Киричок В.А

Перевірили:

доц. Мінєєв О.С.

ас. Шевченко Ю.О.

Дніпро
2025

Лабораторна 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.

Хід роботи

1. Створення нового EC2

2. Обрання необхідної конфігурації машини:

The screenshot shows the AWS EC2 'Launch an instance' wizard. The first step, 'Instance type', is selected. It shows a t3.large instance type (2 vCPU, 8 GiB Memory) and provides options to view all generations or compare with other types. The second step, 'Key pair (login)', is shown with a dropdown for selecting a key pair and a link to create a new one. The third step, 'Network settings', is shown with network and subnet configurations. The fourth step, 'Summary', shows the final configuration: Microsoft Windows Server 2025 AMI, t3.large instance type, and 30 GiB storage. Buttons for 'Cancel', 'Launch instance', and 'Preview code' are at the bottom.

3. Створення ключа доступу:

The screenshot shows the 'Create key pair' dialog box. It asks for a 'Key pair name' (set to 'mykey') and 'Key pair type' (set to 'RSA'). It also asks for a 'Private key file format' (set to '.pem'). A note at the bottom says: '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.' Buttons for 'Cancel' and 'Create key pair' are at the bottom.

mykey.pem 12.11.2025 10:18 Файл PEM 2 КБ

4. Надання дозволу підключення (0.0.0.0) :

Network settings

- Network: vpc-0e9d95de0916d66b5
- Subnet: No preference (Default subnet in any availability zone)
- Auto-assign public IP: Enable
- Firewall (security groups):
 - Create security group (selected)
 - Select existing security group

We'll 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.

Summary

- Number of instances: 1
- Software Image (AMI): Microsoft Windows Server 2022; ami-08d8e0922f4f41d4c
- Virtual server type (instance type): t3.large
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 30 GiB

Cancel

▼ Configure storage [Info](#)

[Advanced](#)

5. Повідомлення про успішне створення

Success
Successfully initiated launch of instance i-041c7203eaf154f74

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"?

Next Steps

- Create billing usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy
- Manage detailed monitoring
- Create Load Balancer
- Create AWS budget
- Manage CloudWatch alarms
- Disaster recovery for your instances
- Monitor for suspicious runtime activities
- Get instance screenshot
- Get system log

6. Підключення створеного ключа:

Get Windows password

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

Instance ID: i-041c7203eaf154f74 (Kirichok-lv5-instance)

Key pair associated with this instance: mykey

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

Upload private key file

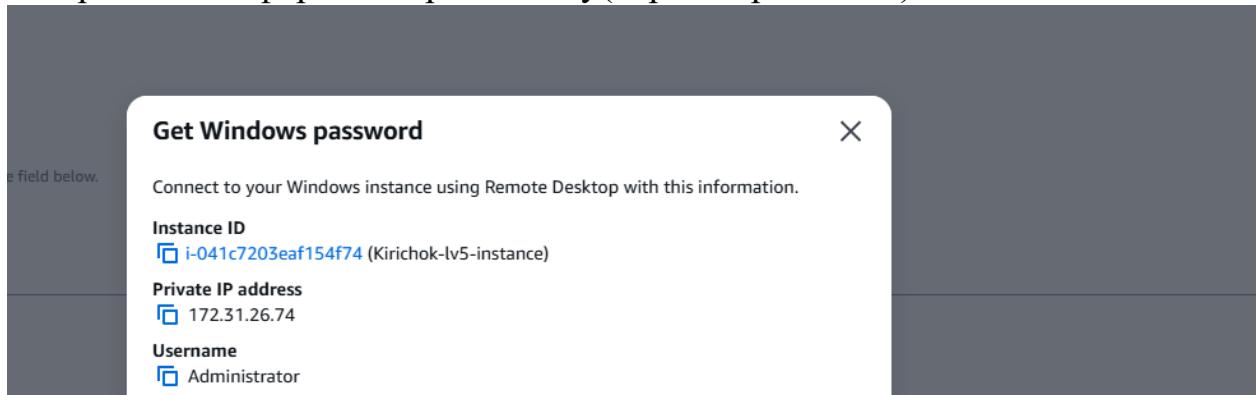
mykey.pem
1.67 kB

Private key contents:

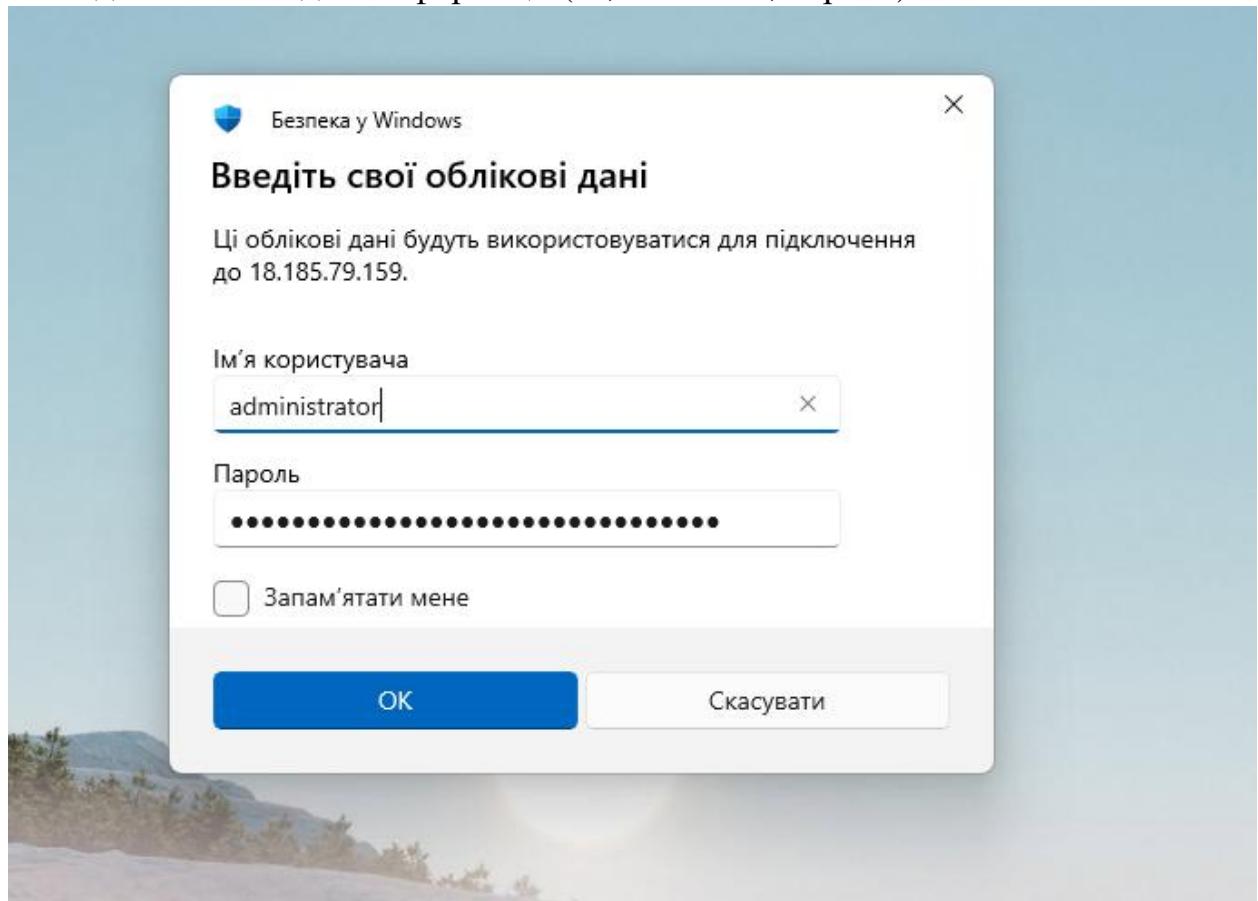
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwPrRumvcAkgMxm1Ipo5nP0UHTEp0hRqlLineQvNO3YRby
ZAVX2qjPm+mAmgkK9mDodalZyJnDmDmWzqf43pmh243hBm
-----END RSA PRIVATE KEY-----
```

Decrypt password

7.Отримання інформації про машину(пароль приховано)



8.Уведення необхідної інформації (IP, username, пароль):



Дані для входу:

Administrator

18.185.79.159

rvkg0l;g*pe)hzGdy0wWOXoQs6RFp(Zy

9. Встановлення нової заставки на в якості фону робочого столу:

