

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



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 Кассіопея. 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

⚠ Звертаємо увагу

Для створення кваліфікованого електронного підпису або печатки необхідно мати чинні особисті ключі та сертифікати від Дії або видані іншим кваліфікованим надавачем електронних довірчих послуг.

Сервіс підтримує особисті ключі та сертифікати відкритих ключів усіх кваліфікованих надавачів електронних довірчих послуг.

Обираємо Дія.Підпис – UA

Перевірте дані

Що таке сертифікат?

Марценюк Ганна Сергіївна

РНОКПП
3835210640

УНЗР
20050101-05145

Сертифікати

ЕЦП (ДСТУ 4145), Неспростовність (ДСТУ 4145) ⬇
EU-382367185294AF5701000000E10270003F06CF04.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



☒ Підтверджую 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_АПЗН[№]1.pdf.asice

77.7 КБ



Файл(и) без підпису



Марценюк_124-22-2_АПЗН[№]1.pdf

76.0 КБ



Протокол створення та перевірки кваліфіков... ⬇

Марценюк_124-22-2_АПЗН[№]1_Validation_Report.pdf

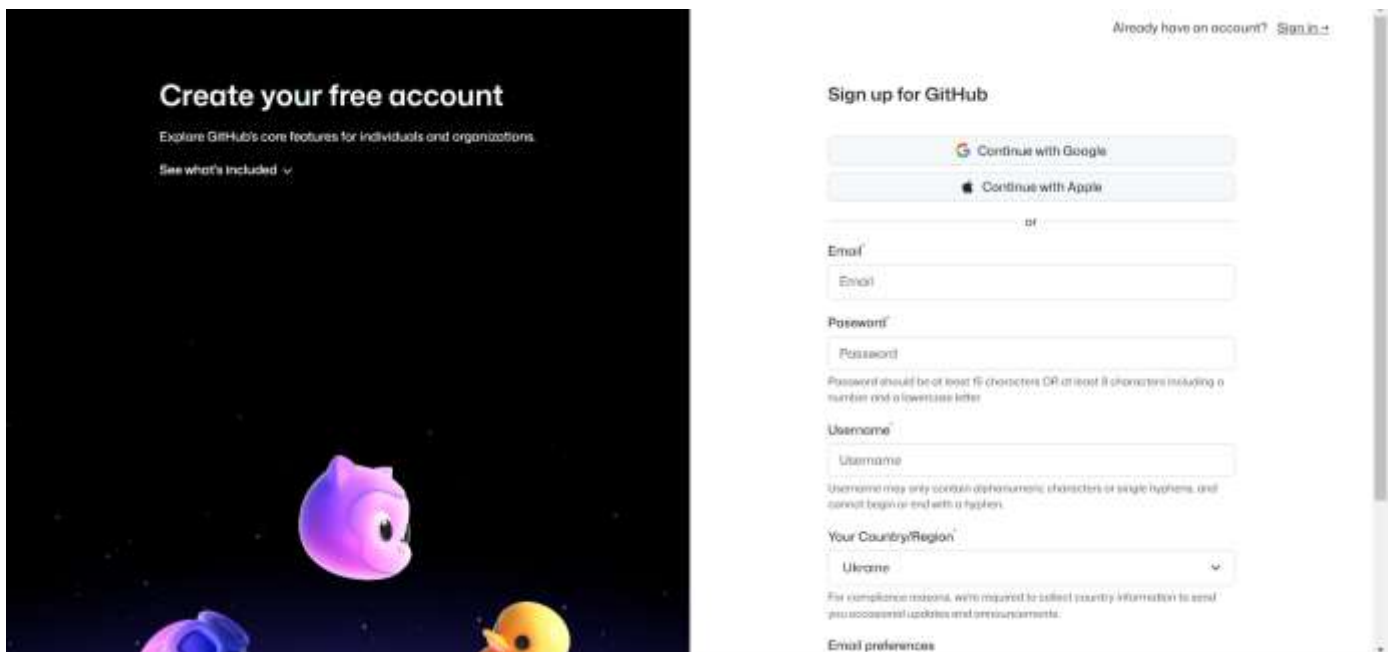
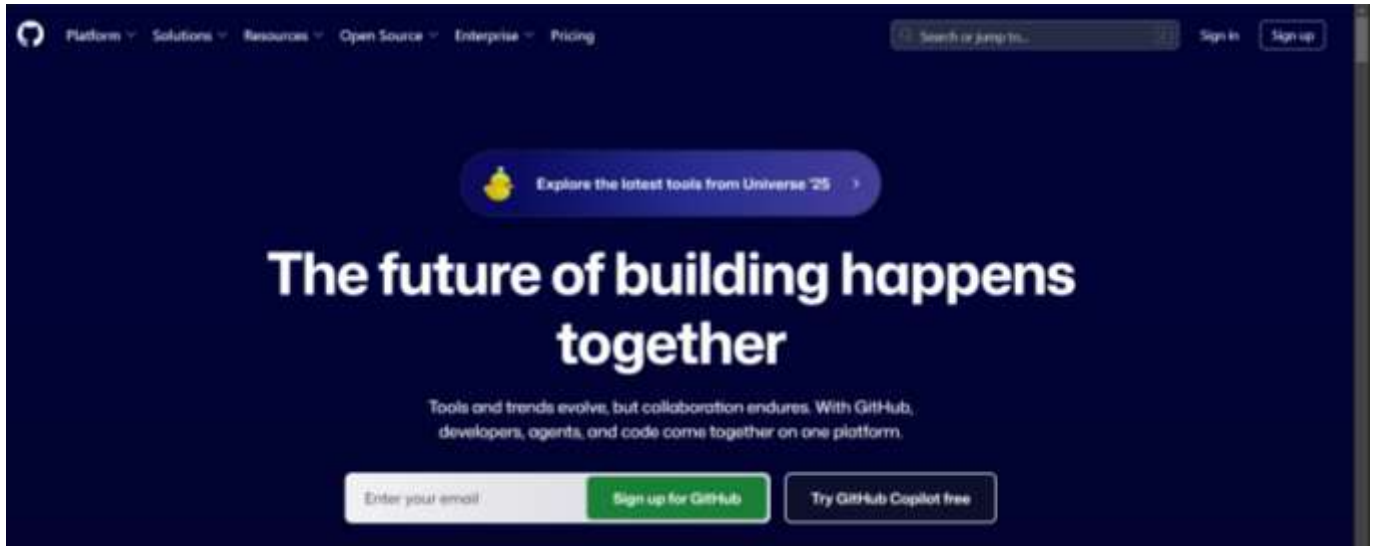
50.4 КБ

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



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 *


Choose who can see and commit to this repository

 Public ▾

Add README

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

Off ☐



Add .gitignore

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

No .gitignore ▾

Add license

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

No license ▾

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 вимогамний пароль.
 3. У полі "Повторити пароль" ввести той самий пароль.
 4. Натиснути на прапорець (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 зареєстрований 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.

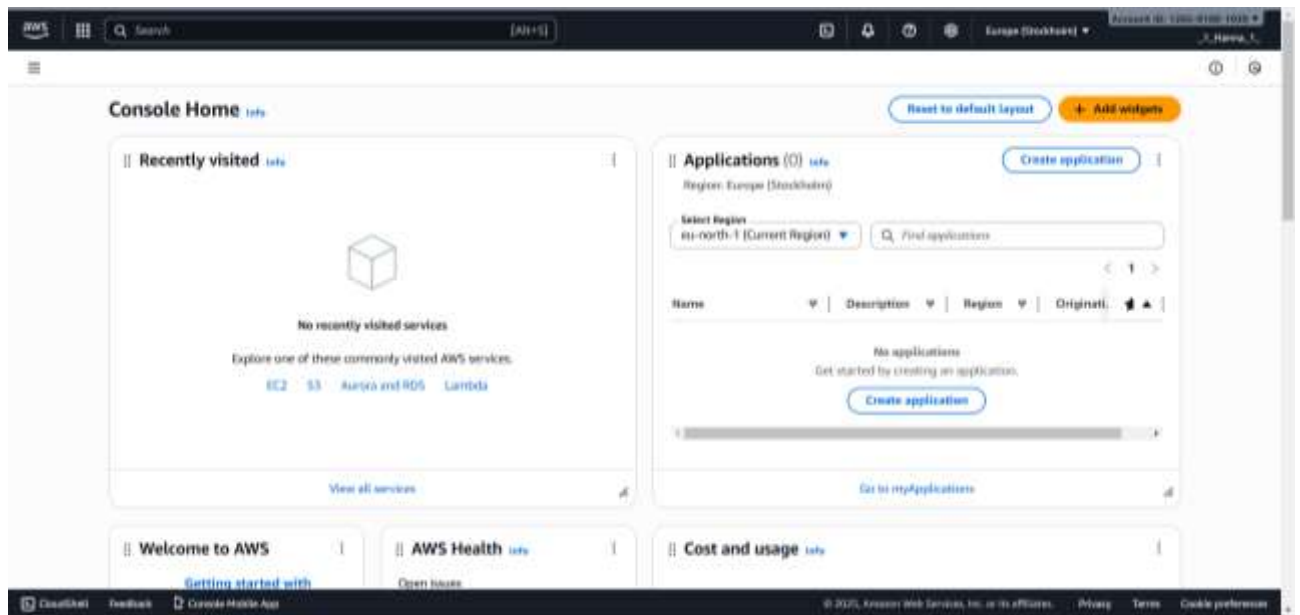
ПРАКТИЧНА РОБОТА №4

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

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

Pricing

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.

⚠ 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 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](#)

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](#). [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

Files and folders (1 total, 119.0 B)

All files and folders in this table will be uploaded.

Find by name

Name

Folder

Type

Size

Mapageweb.html

-

text/html

119.0 B

Destination

Destination

s3://hanna-first-bucket

Destination details

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

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](#)

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee

Object

Object ACL

Object owner (your AWS account)

☒ Read

☒ Read

☒ Write

Everyone (public access)

☒ ☒ Read

☒ ☒ Read

☒ ☒ Write

Authenticated users group (anyone with an AWS account)

☒ ☒ Read

☒ ☒ Read

☒ ☒ Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more](#)

☒ I understand the effects of these changes on this object.

Access for other AWS accounts

No other AWS accounts associated with the resource.

Add grantee

Посилання:

[https://hanna-first-bucket.s3.eu-north-](https://hanna-first-bucket.s3.eu-north-1.amazonaws.com/%D0%9C%D0%B0%D1%80%D1%86%D0%B5%D0%BD%D1%8E%D0%BA.html)

[1.amazonaws.com/%D0%9C%D0%B0%D1%80%D1%86%D0%B5%D0%BD%D1%8E%D0%BA.html](https://hanna-first-bucket.s3.eu-north-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 displays the AWS Management Console interface. The top section shows the 'Resources' dashboard for the Europe (Stockholm) Region, listing various EC2 resources like Instances, Auto Scaling Groups, and Capacity Reservations. The 'Launch instance' section is active, showing a 'Launch instance' button and a 'Migrate a server' link. Below this, there are sections for 'Instance alarms', 'Scheduled events', and 'Service health'. The 'Service health' section indicates that the service is operating normally. The 'Account attributes' section shows the default VPC and settings. The 'Explore AWS' section offers a discount on EC2 Spot Instances.

The bottom section shows the 'Launch instance' wizard. The 'Name and tags' section has a name 'MyPCWorkbook' and a tag 'Add additional tags'. The 'Application and OS Images (Amazon Machine Image)' section shows a search bar and a 'Quick Start' section with various AMIs. The 'Summary' section on the right shows the number of instances (1), the software image (Microsoft Windows Server 2025 Base), the virtual server type (m7i-flex.large), the firewall (New security group), and the storage (1 volume(s) - 50 GB). The 'Launch instance' button is highlighted.

Instance type

Info

Get advice

Instance type

m7i-flex.large

Free tier eligible

Family: m7i-flex

2 vCPU

8 GB Memory

Current generation: true

On-Demand Linux base pricing: \$105.75 USD per Hour

On-Demand Ubuntu Pro base pricing: \$105.24 USD per Hour

On-Demand SUSE base pricing: \$116.05 USD per Hour

All generations

Compare instance types

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

pckey

Create new key pair

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

Software Image (AMI)

Microsoft Windows Server 2025

ami-01b4d0c327403883

Virtual server type (instance type)

m7i-flex.large

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

Cancel

Launch instance

Preview code

Network settings

Info

Edit

Network

Info

sgp-00a000b42ef7e0a2

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Firewall (security group)

Info

Create security group

Select existing security group

We'll create a new security group called "launch-wizard-1" with the following rules:

Allow RDP traffic from

Anywhere

0.0.0.0/0

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.

Number of instances

Info

1

Software Image (AMI)

Microsoft Windows Server 2025

ami-01b4d0c327403883

Virtual server type (instance type)

m7i-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_АПЗН№5.docx	C6 22.11.25 21:22	Документ Microso...	1 КБ
	pckey.pem	C6 22.11.25 21:32	Файл PEM	2 КБ
	Марценюк_124-22-2_АПЗН№5.docx	C6 22.11.25 21:22	Документ Microso...	0 КБ

3. Підключення створеного ключа

Get Windows password

Info

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

Instance ID

i-0bf49673375e17ca0 (myPCHarbenuk)

Key pair associated with this instance

pckey

Private key

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

Upload private key file

pckey.pem

1.57 KB

Private key contents

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQAwKxH5j6X0070LJ9HPhyMP60uMCOjvUj8gWu0c5PLe
wpyL12ZAG6wL0v8k5gUj0Dn45Ctp04uM9Sj3HMyg8Kz7pge+8tgle+8
J1uM8+8wipW6Cp01p45e5P7+4uQ1L8bave8du8B8+P5u3U7W43QUkkk0
Mfue8u8+47u8Q2Fue04Ctu0P9U4u0U8e8JL8V8U2u3uFC3HMyQH
61uFTT24LY3p5CNewM45rmyS79eJh8d0Q37u+Q0M8U6fT000JAMP
kL8/qg/YV07TC8u8Vufu8B88TTFUJ8y8Ow8G8Q8A8u8AE+c88kX10C3Vw
888u8Y8u8u8P2u88y8u8V8L4u8U88u8u8Y8u8Y8u8Y8u8Y8u8Y8u8Y8u8
-----END RSA PRIVATE KEY-----
```


4. Отримання інформації про машину

Get Windows password ✕

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*Z9s9Eld&%esvW0\$5ukOR\$rSdE

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

 Підключення до віддаленого робочого стола

Комп'ютер: 16.171.34.68

Ім'я користувача: Не вказано

Під час підключення буде здійснено запит ваших облікових даних.

Показати параметри Підключитися Довідка



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