

Міністерство освіти і науки України  
НТУУ «КПІ ім. Ігоря Сікорського»  
Навчально-науковий інститут атомної та теплової енергетики  
Кафедра цифрових технологій в енергетиці

Лабораторна робота №4  
з дисципліни  
«Інформаційне забезпечення безпеки комп'ютерних систем»  
Тема «Захист даних в комп'ютерних мережах»  
Варіант №18

Студента 4-го курсу НН ІАТЕ гр. ТР-12

Ковальова Олександра

Перевірив: доцент, Онисько А. І.

КИЇВ 2024

**Мета роботи.** Ознайомитися з основними поняттями комп'ютерних мереж, навчитися використовувати програмні засоби для захисту даних в комп'ютерних мережах.

**Завдання:**

1. На віртуальному комп'ютері завантажити та з'ясувати призначення програмного додатку Центр безпеки (Панель керування) та компонентів, які входять до складу цього додатку.
2. Ознайомитися, налаштувати та продемонструвати роботу вбудованого брандмауера.
3. Продемонструвати увімкнення або вимкнення брандмауера Windows. Пояснити чим може загрозовувати вимкнення брандмауера.
4. Перевірити проходження пакетів ICMP між комп'ютерами до і після відключення брандмауера (за допомогою команди ping).
5. Продемонструвати налаштування брандмауера Windows для різних типів мереж (приватна мережа, мережа спільного використання або мережа з доменами).
6. Продемонструвати надання програмі (будь-якій) дозволу на отримання даних через брандмауер.
7. Продемонструвати відкриття порту у брандмауері Windows.

**Хід роботи**

Робота буде проводитись з використанням операційної системи Windows 10 Pro. «Чиста» система була встановлена на віртуальну машину за допомогою гіпервізора VirtualBox. Характеристики машини продемонстровані на скріншоті:

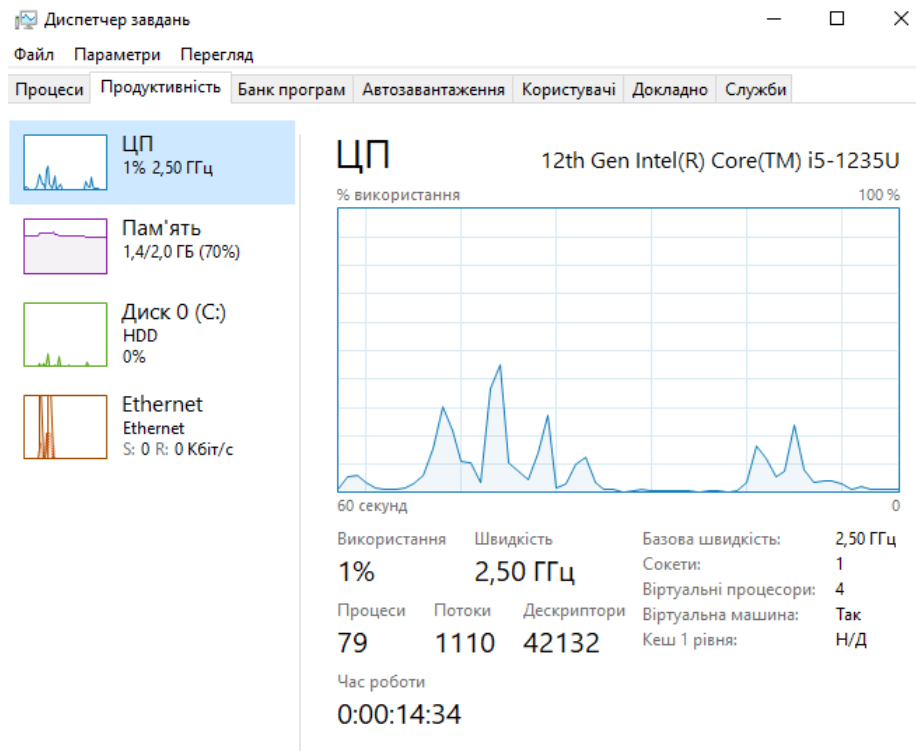
Специфікації Windows

Випуск	Windows 10 Pro
Версія	22H2
Дата інсталяції	20.11.2024
Збірка ОС	19045.3803
Взаємодія	Windows Feature Experience Pack 1000.19053.1000.0

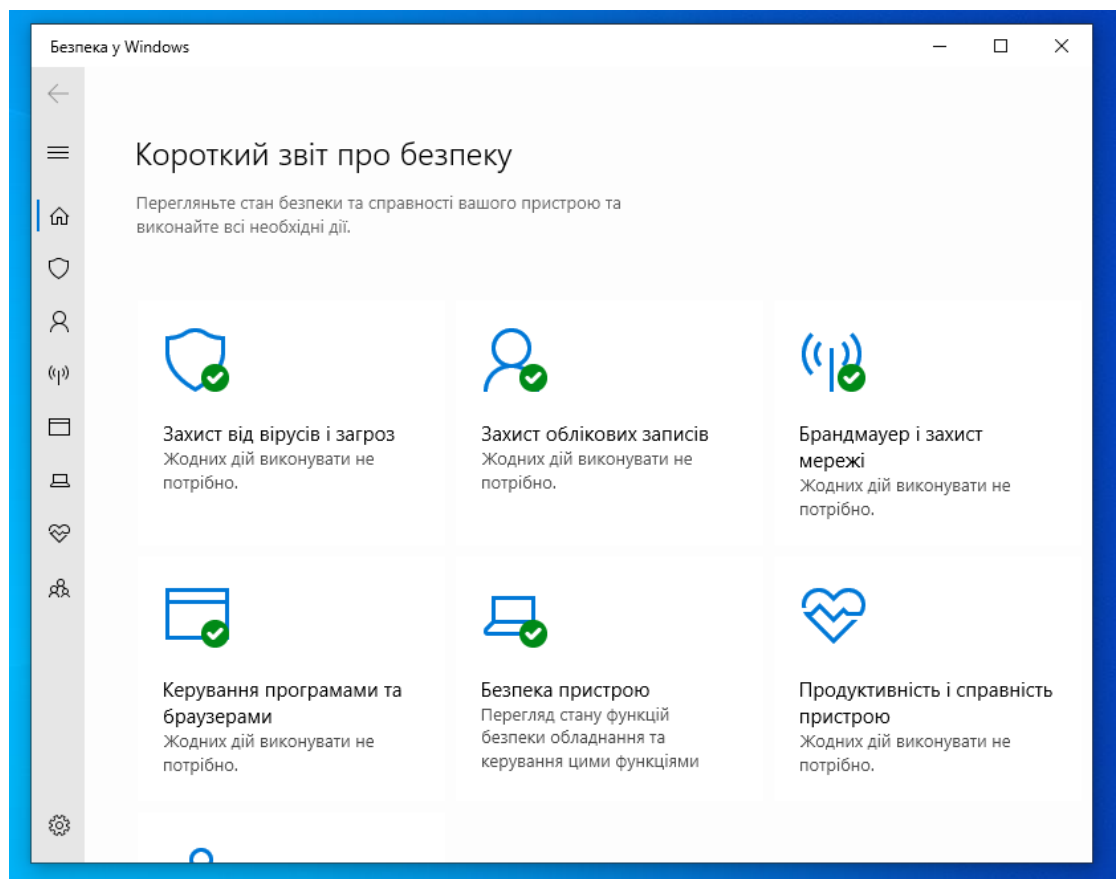


**ALEXKOVALOV**

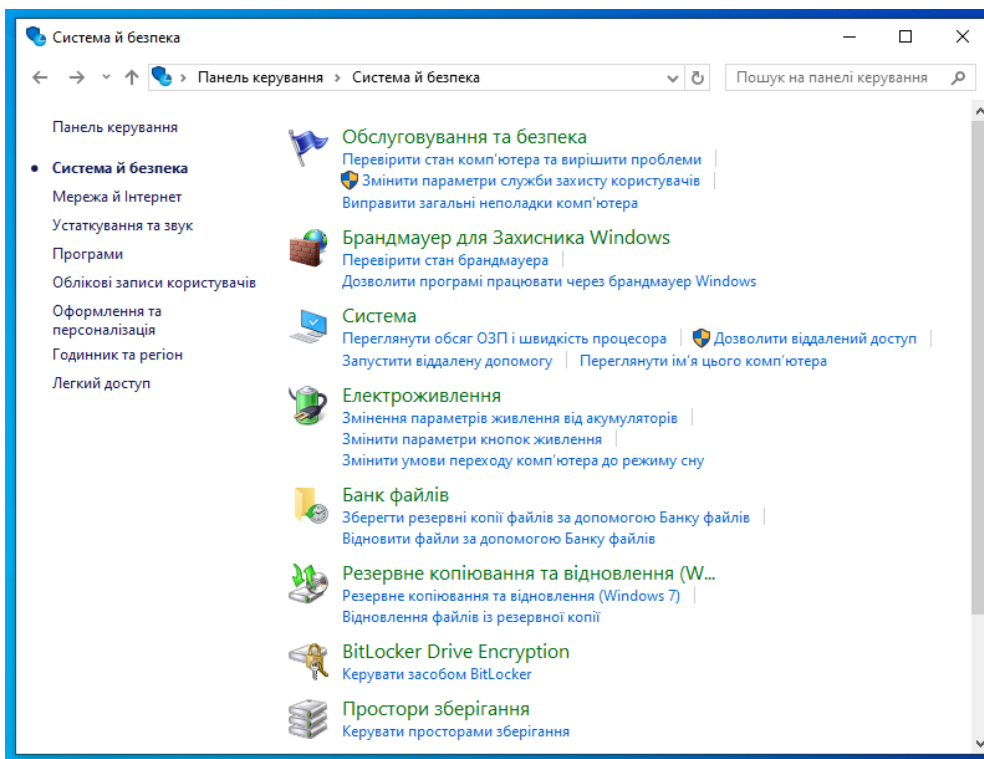
Локальний обліковий запис  
Адміністратор



Програмний додаток «Центр безпеки» вже завантажений за замовчуванням, але починаючи з оновлення «Windows 10 Creators Update» він знаходиться не в Панелі Керування, а в налаштуваннях, і називається Windows Defender Security Center (WDSC), або у перекладі на українську «Безпека у Windows»:



Але, у панелі керування є окремий пункт «Система й безпека», де знаходяться певні налаштування безпеки, такі як, наприклад, брандмауер, який розглядається в даній роботі:



Щодо центру безпеки, він складається з таких підзастосунків:

- «Захист від вірусів та загроз». Антивірус, його налаштування, оновлення, історія загроз.
- «Захист облікових записів». Встановлення паролю, тощо.
- «Брандмауер і захист мережі». Налаштування, хто й що може отримати доступ до мережі: домену, приватної, загальнодоступної.
- «Керування програмами і браузерами». Захист на основі репутації, запобігання експлойтам.
- «Безпека пристрою». Ізоляція ядра, віртуалізація. Модуль TPM 2.0 (який також називається процесором безпеки), безпечне завантаження, DEP, UEFI MAT.
- «Продуктивність і справність пристрою». Звіт про справність системи (Служба часу Windows, обсяг пам'яті, час роботи акумулятору, програми та ПЗ). Чистий запуск.
- «Параметри сім'ї». Батьківський контроль.

Пункт «Система й безпека» в панелі керування складається з:

- «Обслуговування та безпека». Перевірка стану комп'ютера, виправлення загальних неполадок, зміна параметрів служби захисту користувачів.
- Брандмауер.
- Резервне копіювання та відновлення.
- BitLocker.
- Адміністрування.

## Загальні налаштування брандмауера:

### Захистіть свій ПК за допомогою Брандмауера для Захисника Windows

Брандмауер для Захисника Windows допомагає перешкодити хакерам чи зловмисним програмам в отриманні доступу до вашого ПК (через Інтернет або локальну мережу).

✓ Приватні мережі

Не підключено

Мережі вдома або на роботі, де ви знаєте користувачів і пристрої і довіряєте їм

Стан Брандмауера для Захисника Windows:

Увімкнено

Вхідні підключення:

Блокувати всі підключення до програм, яких немає у списку дозволених

Активні приватні мережі:

Немає

Стан сповіщення:

Повідомляти, коли Брандмауер для Захисника Windows блокує нову програму

✓ Гостьові або загальнодоступні мережі

Підключено

Мережі у громадських місцях, таких як аеропорти або кав'ярні

Стан Брандмауера для Захисника Windows:

Увімкнено

Вхідні підключення:

Блокувати всі підключення до програм, яких немає у списку дозволених

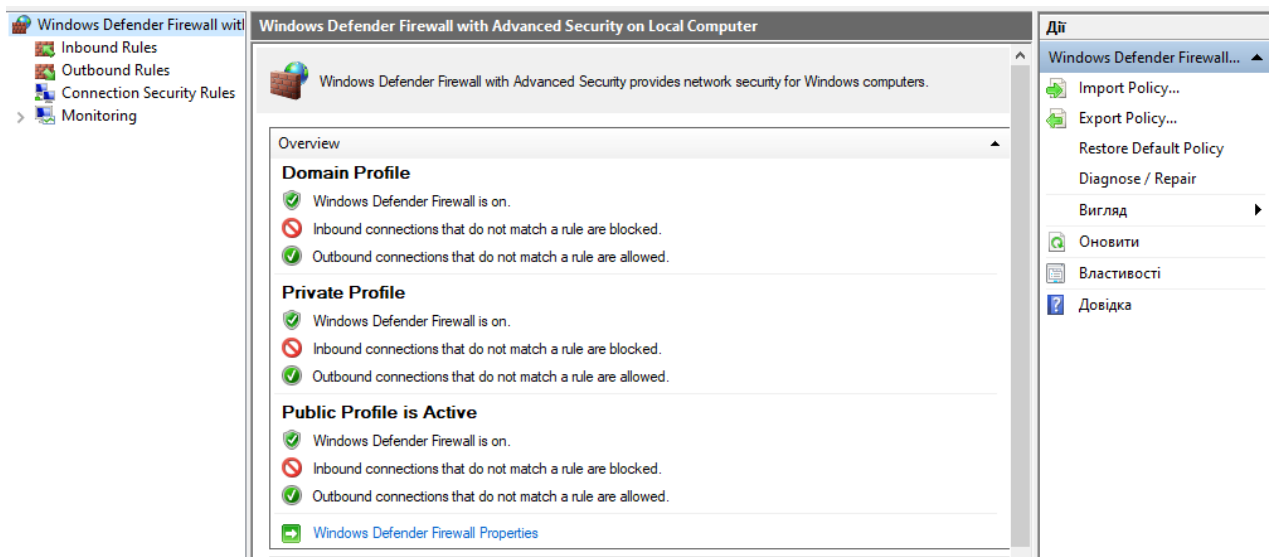
Активні мережі спільного використання:

Мережа

Стан сповіщення:

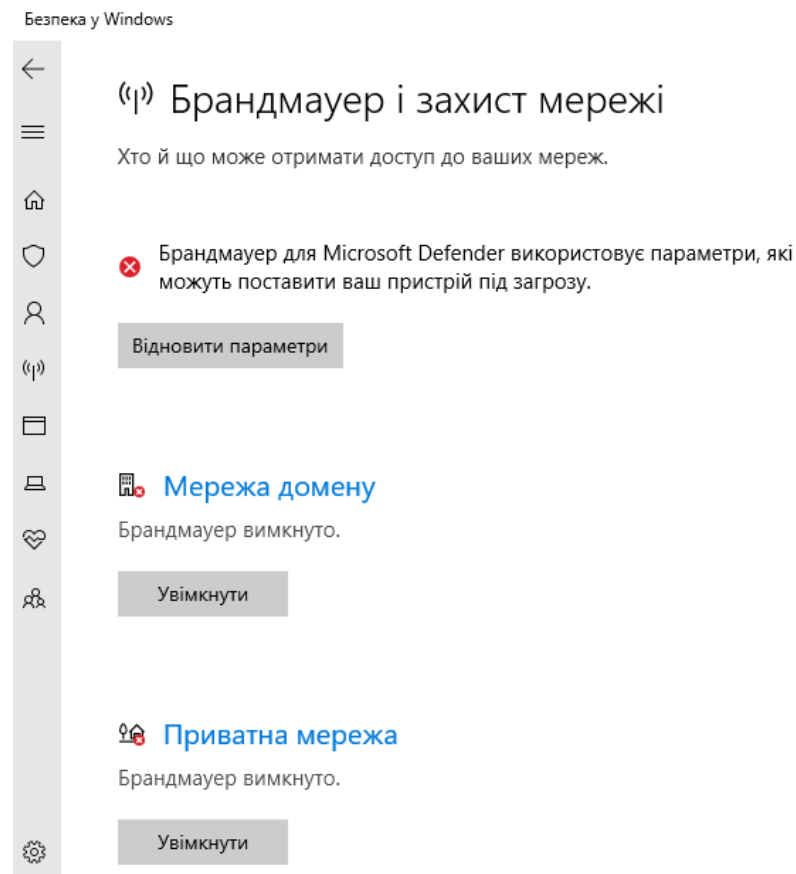
Повідомляти, коли Брандмауер для Захисника Windows блокує нову програму

## Додаткові налаштування:

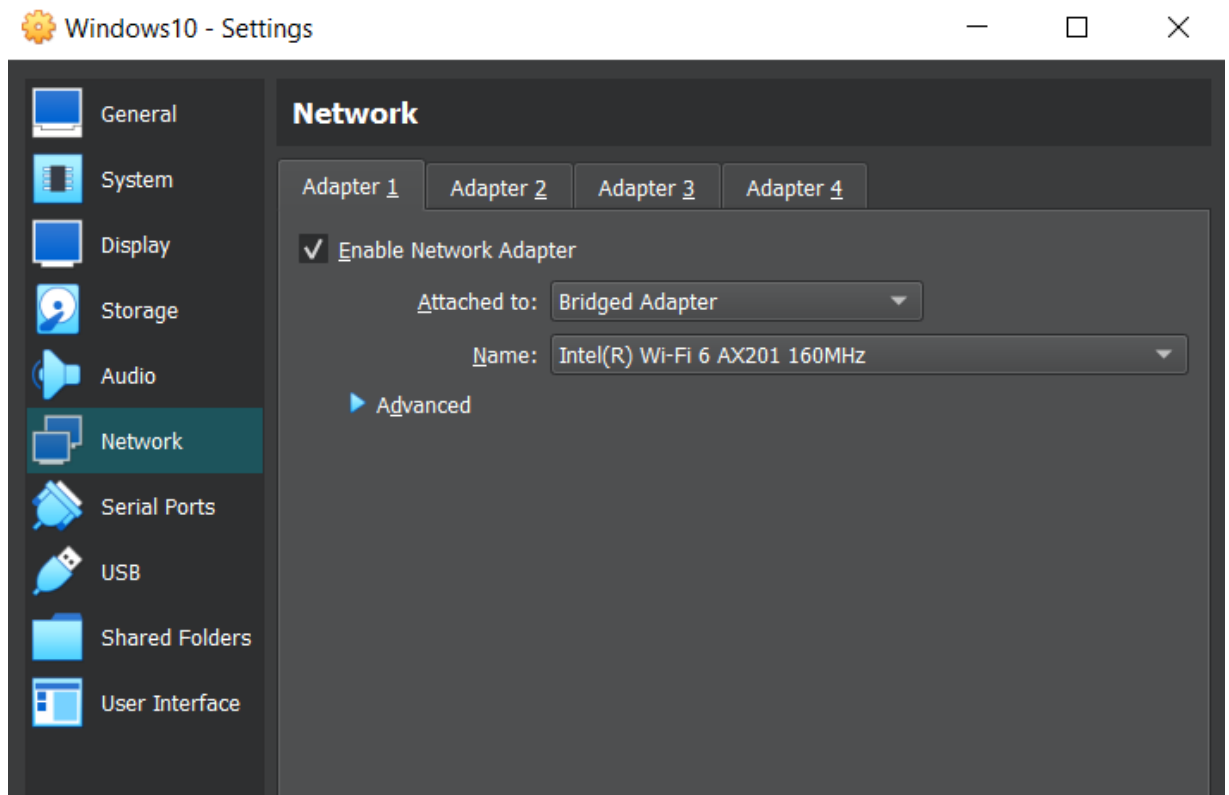


Вимкнення брандмауера створює серйозні ризики для безпеки системи. Це відкриває пристрій для несанкціонованого доступу з боку зловмисників, які можуть використовувати відкриті порти для проникнення в мережу. Відсутність фільтрації трафіку дозволяє шкідливому програмному забезпеченню або атакам типу «man-in-the-middle» отримувати доступ до конфіденційної інформації, перехоплювати трафік або викрадати дані. Такий стан також збільшує ймовірність зараження вірусами, виконання DoS-атак та експлуатації вразливостей у службах, доступних через Інтернет.

Вимкнений брандмауер:



Для того, щоб була можливість пропінгувати машину, додамо брідж адаптер:



IP адреса машини:

```
Командний рядок
Microsoft Windows [Version 10.0.19045.3803]
(с) Корпорація Майкрософт. Усі права захищені.

C:\Users\AlexKovalov>ipconfig


Windows IP Configuration


Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::cbd1:7b3:dbbb:fb61%5
    IPv4 Address. . . . . : 192.168.0.104
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

C:\Users\AlexKovalov>
```

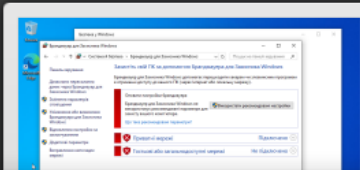
Пінг з хостової машини (при вимкненому брандмауері на «гостьовій»):

**Oracle-Linux**  
Powered Off

**Windows10**  
Running

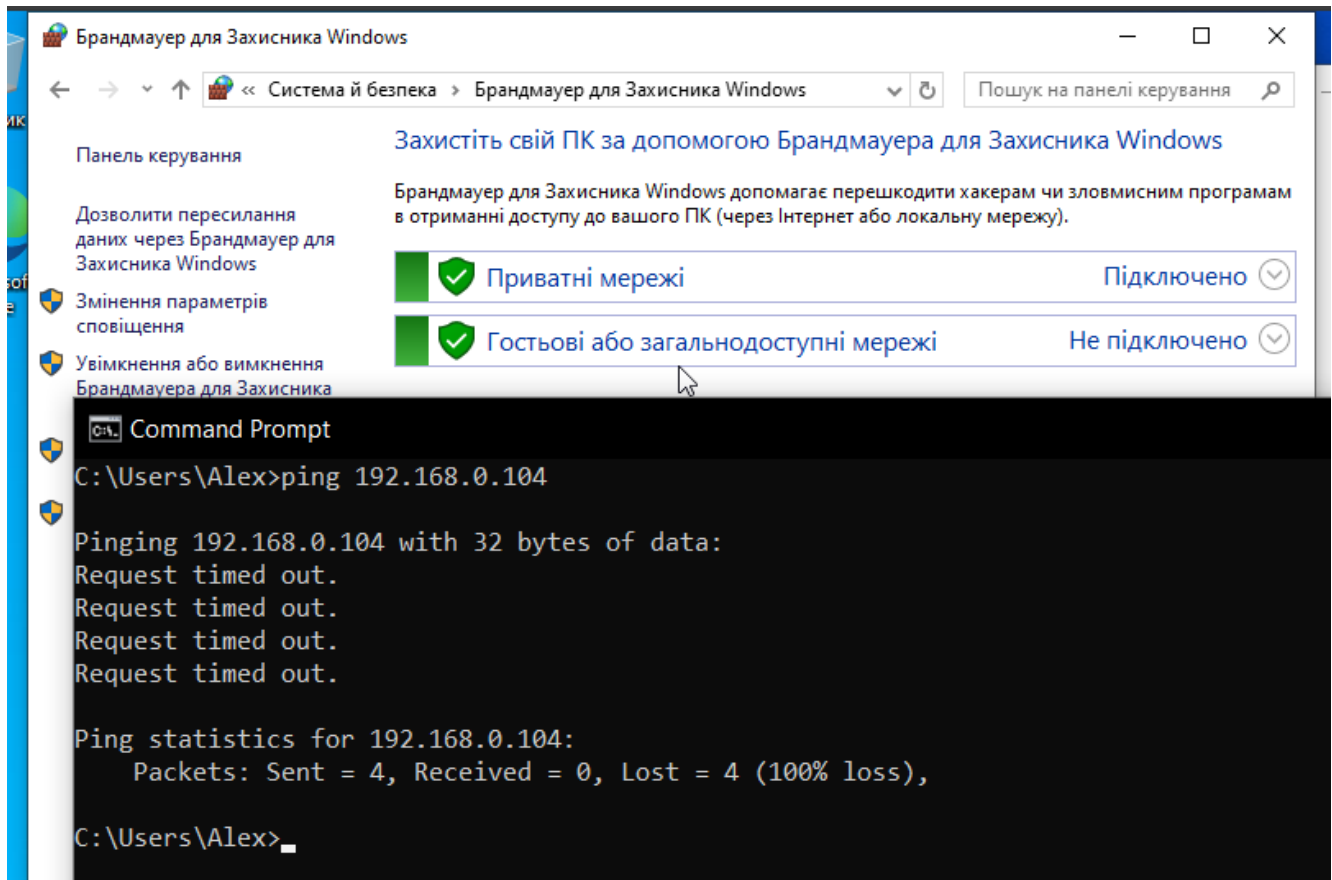
**General**  
Name: Windows10  
Operating System: Windows 10 (64-bit)

**System**  
Base Memory: 2048 MB  
Processors: 4  
Boot Order: Floppy, Optical, Hard Disk  
Acceleration: Nested Paging, Hyper-V

**Preview**  


**Command Prompt**  
Wireless LAN adapter Wi-Fi:  
  
 Connection-specific DNS Suffix . :  
 Link-local IPv6 Address . . . . . : fe80::3fd7:e186:95fb:7bad%15  
 IPv4 Address. . . . . : 192.168.0.100  
 Subnet Mask . . . . . : 255.255.255.0  
 Default Gateway . . . . . : 192.168.0.1  
  
C:\Users\Alex>ping 192.168.0.104  
  
Pinging 192.168.0.104 with 32 bytes of data:  
Reply from 192.168.0.104: bytes=32 time<1ms TTL=128  
Reply from 192.168.0.104: bytes=32 time<1ms TTL=128  
Reply from 192.168.0.104: bytes=32 time<1ms TTL=128  
Reply from 192.168.0.104: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.0.104:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
 Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\Alex>

Знову увімкнемо брандмауер на гостьовій машині, стандартні налаштування. Спробуємо пропінгувати з хосту:



Результат: Request Timed Out. Причиною є саме брандмауер. Це означає, що гостьова машина просто не відповідає на ICMP пакети, не надсилає ECHO REPLY. Якщо б це була помилка в роутінгу або ще якась інша проблема, то не проходили б пінги при вимкненому брандмауері, і при цьому результатом була б помилка Destination Host Unreachable.

Приклад помилки (спробуємо пропінгувати хост з адресою, якої немає в мережі):

```
C:\Users\Alex>ping 192.168.0.4

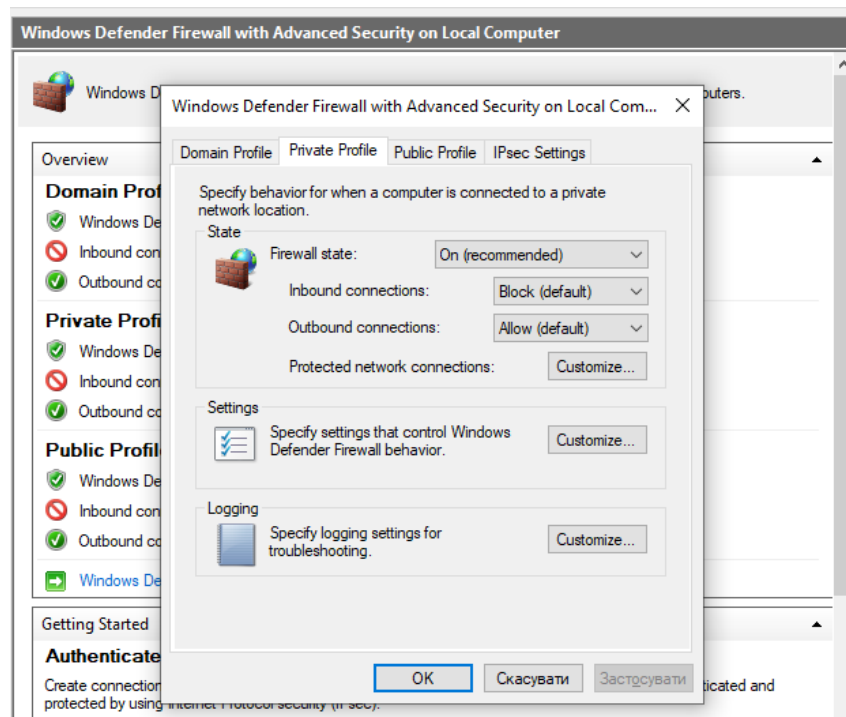
Pinging 192.168.0.4 with 32 bytes of data:
Reply from 192.168.0.100: Destination host unreachable.
Reply from 192.168.0.100: Destination host unreachable.
Reply from 192.168.0.100: Destination host unreachable.
Reply from 192.168.0.100: Destination host unreachable.

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

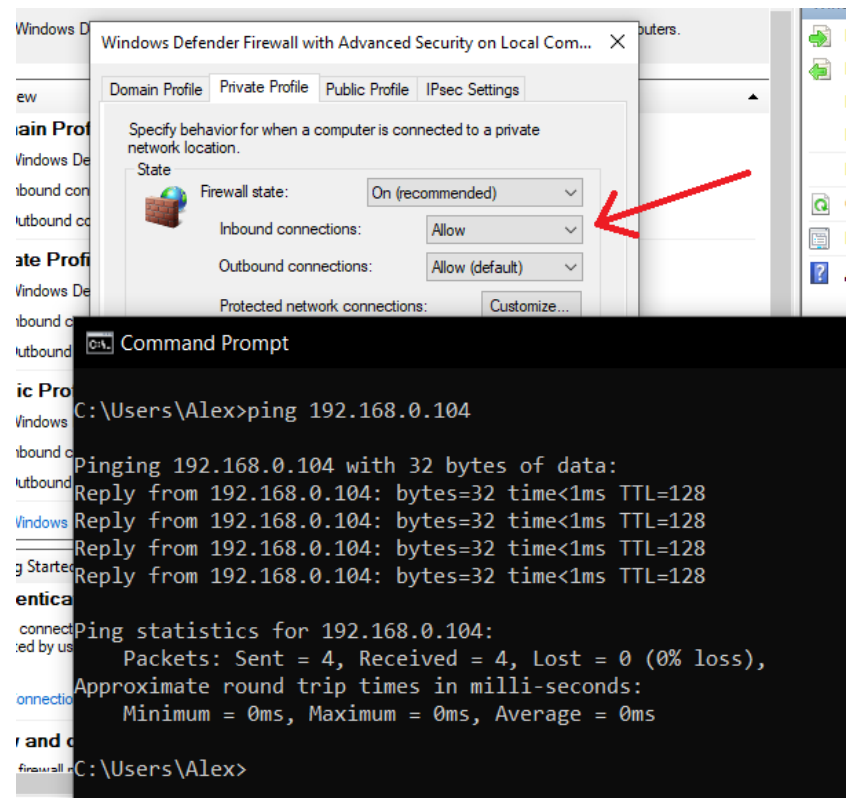
C:\Users\Alex>
```



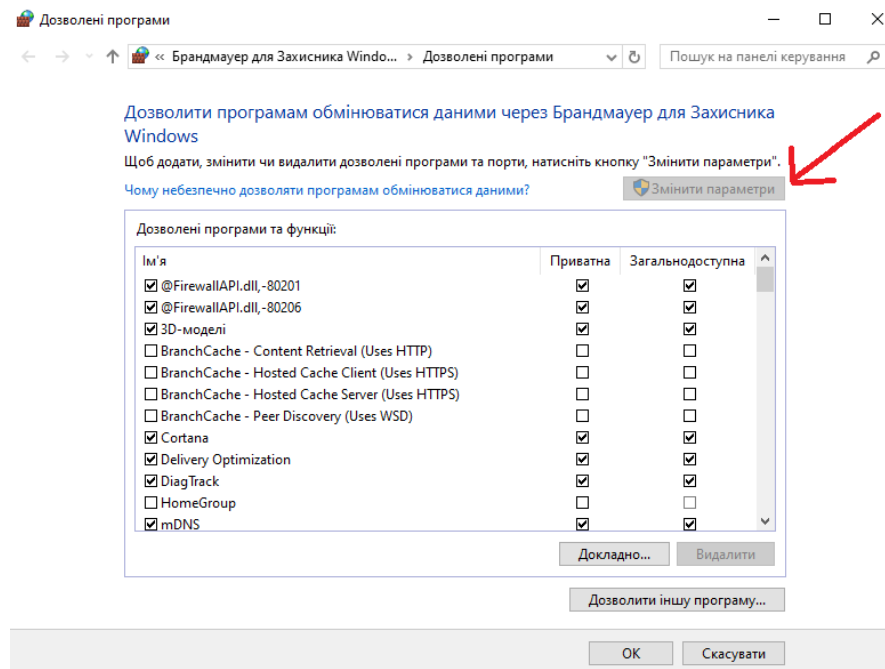
Може з'явиться питання, а яке саме налаштування викликає таку поведінку (відсутність відповіді на ECHO REQUEST)? Для цього потрібно перейти в налаштування профілів брандмауеру.



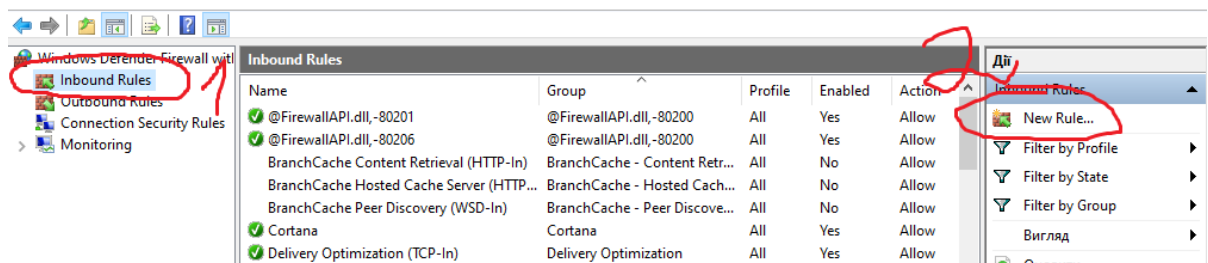
Для всіх профілів (приватна мережа, загальнодоступна, доменна) за замовчуванням встановлено блокування вхідних з'єднань. Змінимо це налаштування на Allow і спробуємо зробити пінг (не вимикаючи брандмауер):



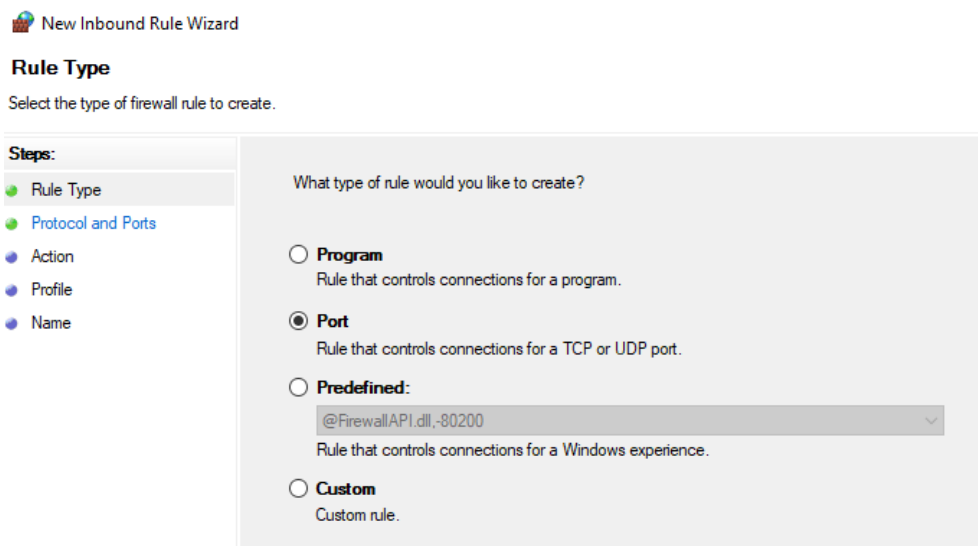
Дозвіл на роботу програм відбувається через налаштування брандмауеру:



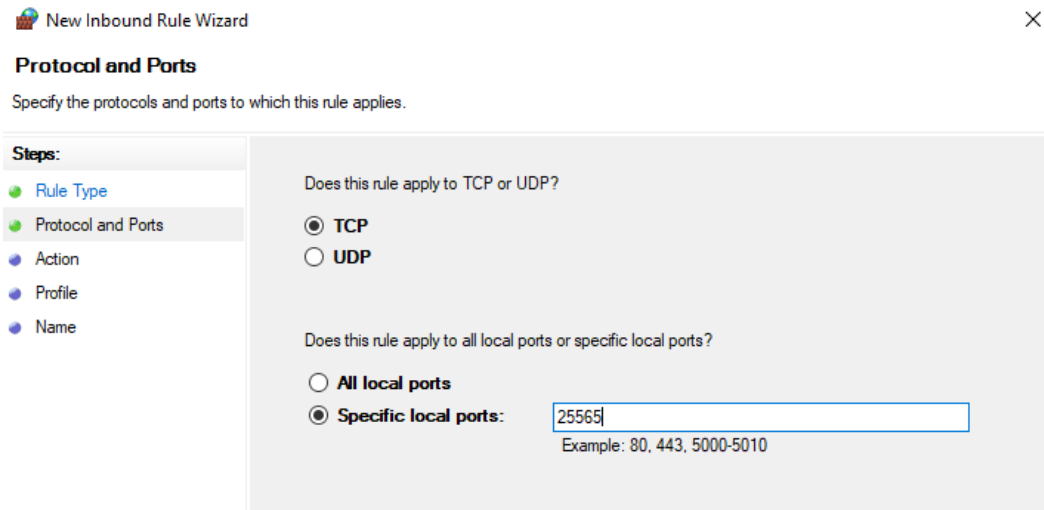
Для того щоб відкрити порт, спочатку треба зайти в додаткові налаштування фаєрволу, обрати потрібний пункт (Inbound/Outbound Rules), та натиснути на "New Rule".



Обираємо тип правила — порт.

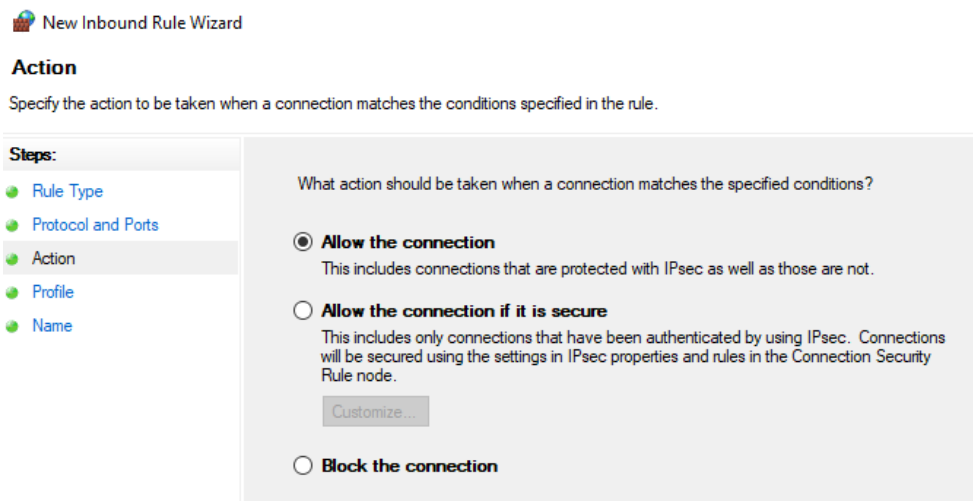


Обираємо протокол: TCP або UDP. Різниця в цьому пункті впливає з сутності самих протоколів (з'єднання або «точкове» надсилання пакетів), також вказуємо порт, наприклад, 25565 (на ньому працюють деякі сервери які використовують OpenJDK, приклад з робочої практики).



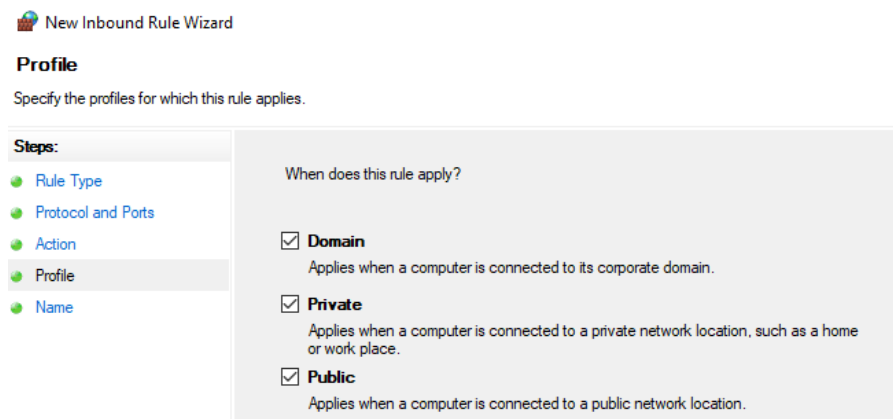
The screenshot shows the 'New Inbound Rule Wizard' window with the 'Protocol and Ports' step selected in the left sidebar. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' (selected) and 'UDP'; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports' (selected). A text box next to 'Specific local ports' contains the value '25565', with an example '80, 443, 5000-5010' shown below it.

Далі, обираємо, власне, дію – блокувати чи дорішити з'єднання.



The screenshot shows the 'New Inbound Rule Wizard' window with the 'Action' step selected in the left sidebar. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. Descriptive text is provided for each option, and a 'Customize...' button is visible under the 'Allow the connection if it is secure' option.

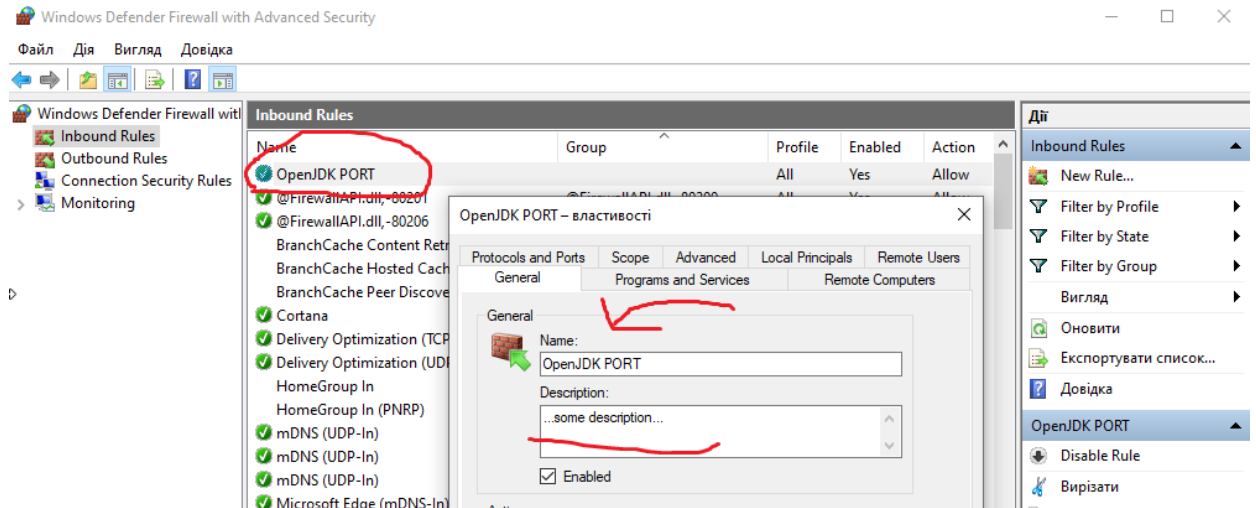
Вибір профілю:



The screenshot shows the 'New Inbound Rule Wizard' window with the 'Profile' step selected in the left sidebar. The main area contains the question 'When does this rule apply?' with three checked checkboxes: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.).

Вказуємо назву та опис правила. Натискаємо «Ок».

Правило відображається в списку всіх правил фаєрволу:



### Контрольні запитання:

- 1. Наведіть приклади класів електронної комерції і основні засоби їх безпеки.*  
Класи електронної комерції включають B2B (бізнес для бізнесу), B2C (бізнес для споживача), C2C (споживач для споживача), G2C (уряд для споживача). Основні засоби їх безпеки включають шифрування даних, використання SSL/TLS для захищених з'єднань, багаторівневу аутентифікацію, захист від атак DDoS, системи запобігання вторгнень (IPS) та застосування політик конфіденційності.
- 2. Наведіть приклади основних сервісів, що забезпечуються зв'язком з мережею Інтернет, і засоби їх безпеки.*  
Основні сервіси включають електронну пошту, веб-сайти, хмарні сервіси, онлайн-банкінг, відеоконференції. Засоби їх безпеки передбачають використання антивірусів, міжмережевих екранів, шифрування даних, аутентифікацію користувачів, захист від спаму, резервне копіювання та моніторинг трафіку.
- 3. Надайте ваше розуміння брандмауера.*  
Брандмауер (фаєрвол) – це програмне або апаратне рішення для забезпечення безпеки мережі шляхом фільтрації вхідного та вихідного трафіку на основі визначених правил. Він контролює доступ до ресурсів, запобігає несанкціонованим з'єднанням, протоколює мережеву активність і може виконувати функції антивірусного сканування, контент-контролю та захисту від атак.
- 4. Які основні різновиди заміни мережевої адреси використовуються в брандмауерах?*  
Основними різновидами заміни мережевої адреси є NAT (трансляція мережевих адрес), яка дозволяє використовувати приватні IP-адреси для

доступу до Інтернету через спільну публічну IP-адресу, та PAT (трансляція портів), що дозволяє відображати кілька приватних IP-адрес через один публічний IP за допомогою унікальних портів.

**Висновок:** У ході виконання лабораторної роботи було досліджено основи захисту даних у комп'ютерних мережах, зокрема налаштування брандмауера в операційній системі Windows 10. Вивчено ключові аспекти функціонування програми "Центр безпеки" (Windows Defender Security Center), що включає налаштування для захисту від вірусів, безпеки мережі та захисту пристроїв. Окрему увагу було приділено налаштуванню брандмауера для різних типів мереж, а також забезпеченню доступу програм до мережі через брандмауер.

У процесі роботи було продемонстровано, як вимикання брандмауера збільшує ризики несанкціонованого доступу та можливі наслідки для безпеки системи, зокрема перехоплення даних та зараження шкідливим програмним забезпеченням. Було перевірено, як зміни в налаштуваннях брандмауера впливають на мережеву взаємодію між комп'ютерами, а також продемонстровано створення правил для відкриття портів і дозволу програмам доступу до мережі.

Загалом, лабораторна робота дозволила набути практичних навичок у налаштуванні брандмауера, що є важливою складовою частиною системи безпеки комп'ютерних мереж.