**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

***Кафедра комп’ютерної інженерії***

**ЛАБОРАТОРНА РОБОТА № 6**

з курсу

***«Безпека програм та даних»***

**ТЕМА: Поширені види мережевих атак і способи захисту від них.**

**Студент : Трембіцький Нікіта**

**Група : 31ІПЗ**

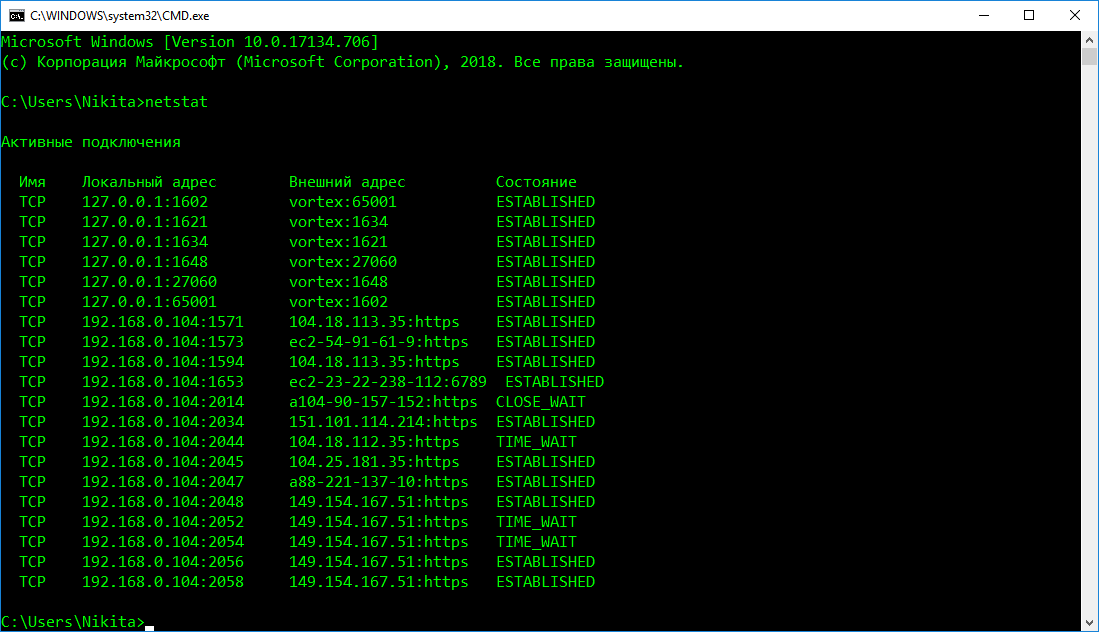
**Факультет : Інформатики**

**Викладач : Галицький О.В.**

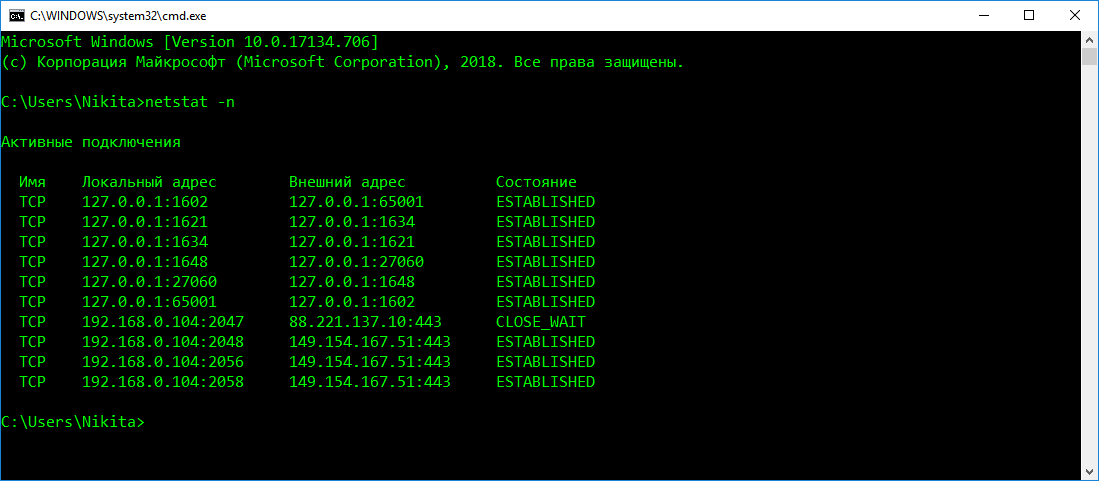
Київ 2019

1. **Завантажити командний рядок, з’ясувати призначення та дослідити статистику яку можна отримати за допомогою команди netstat.**

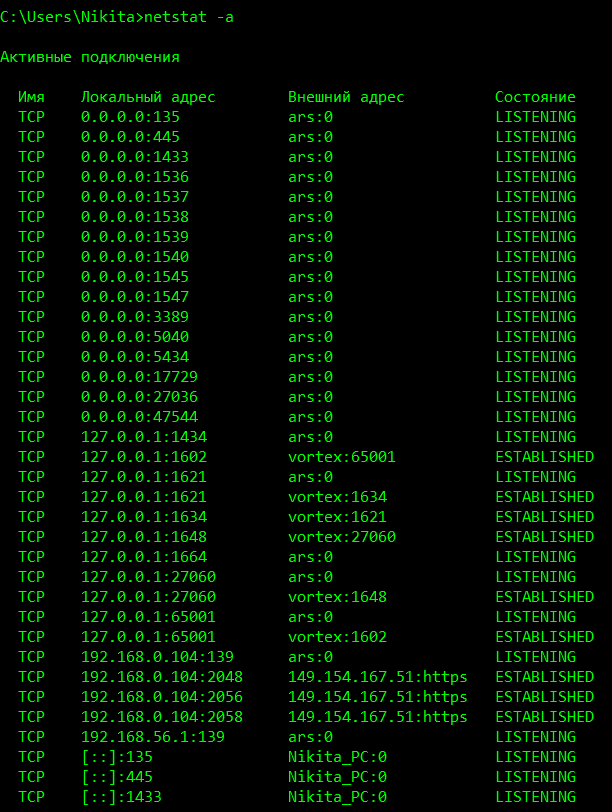
**Звичайний вивід**

****

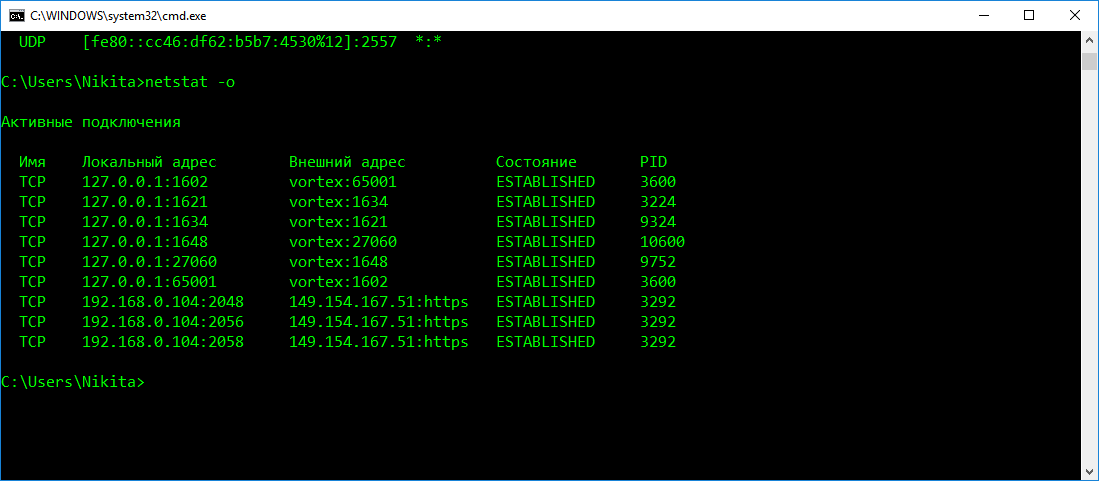
**Вивід без спроби дізнатись доменні імена(тільки айпі)**



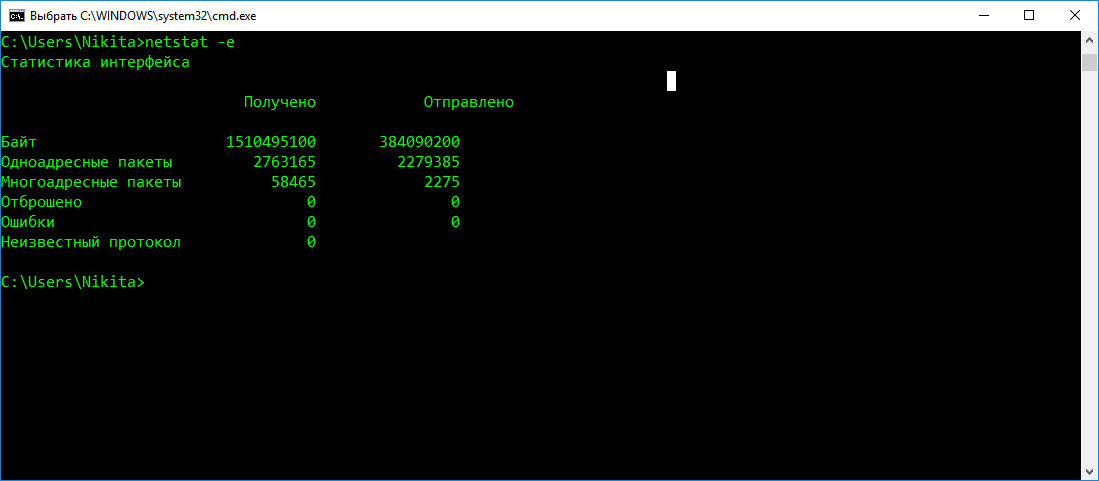
**Вивід всіх активних підключень (TCP і UDP)**



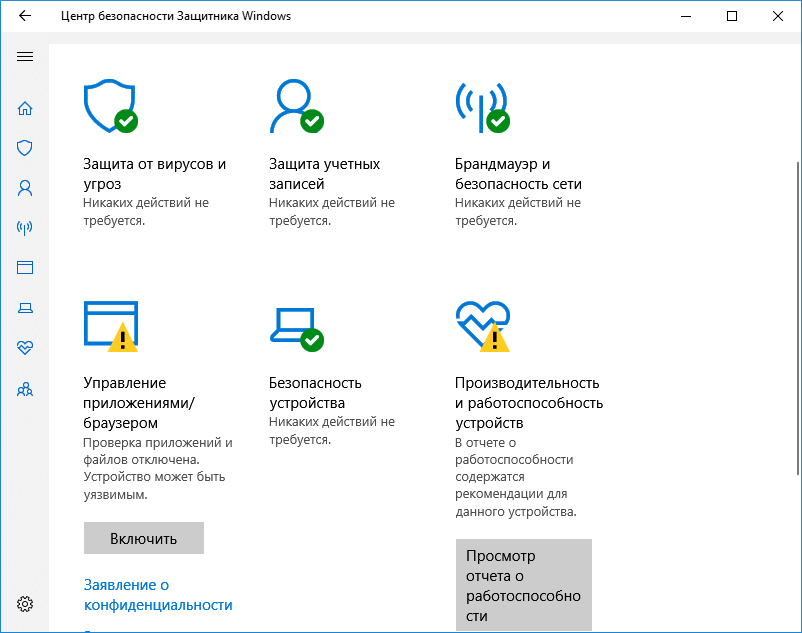
**Вивід з PID, який дозволяє ідентифікувати процес**

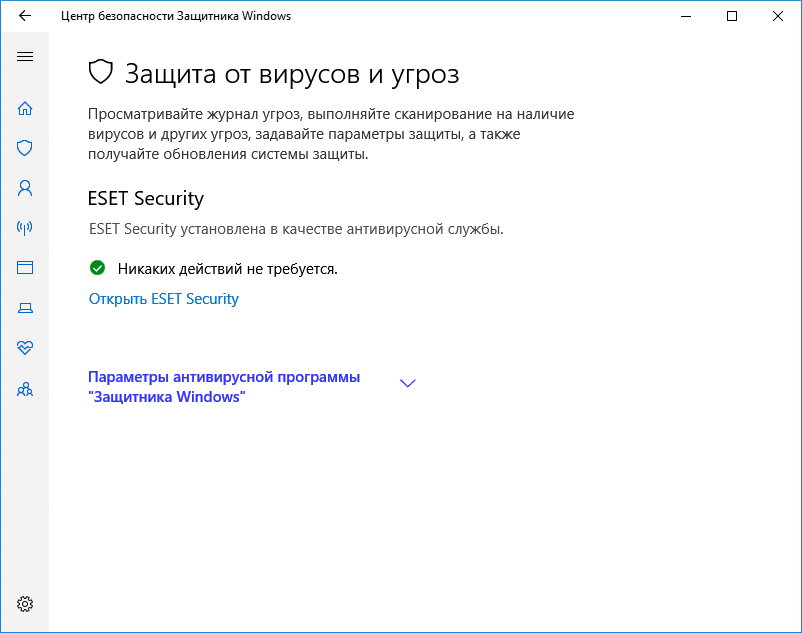


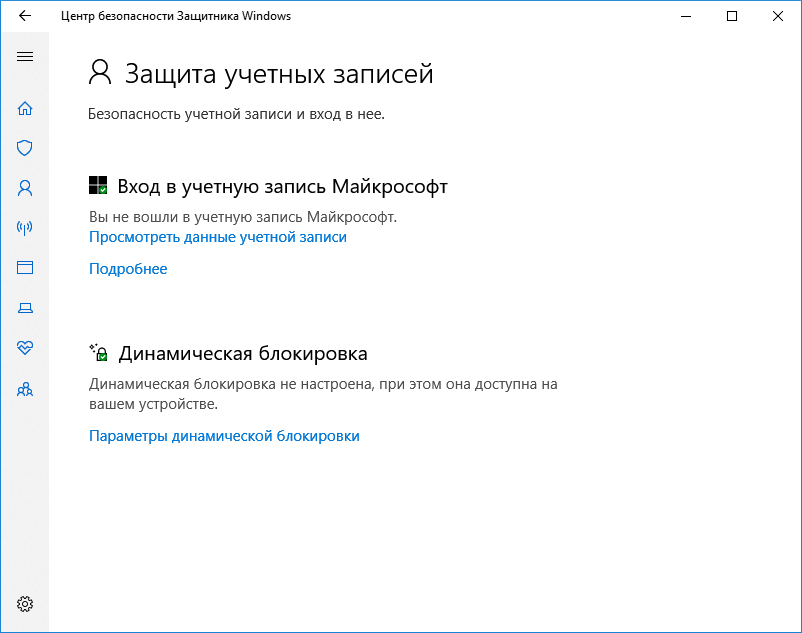
**Вивід статистики Ethernet**

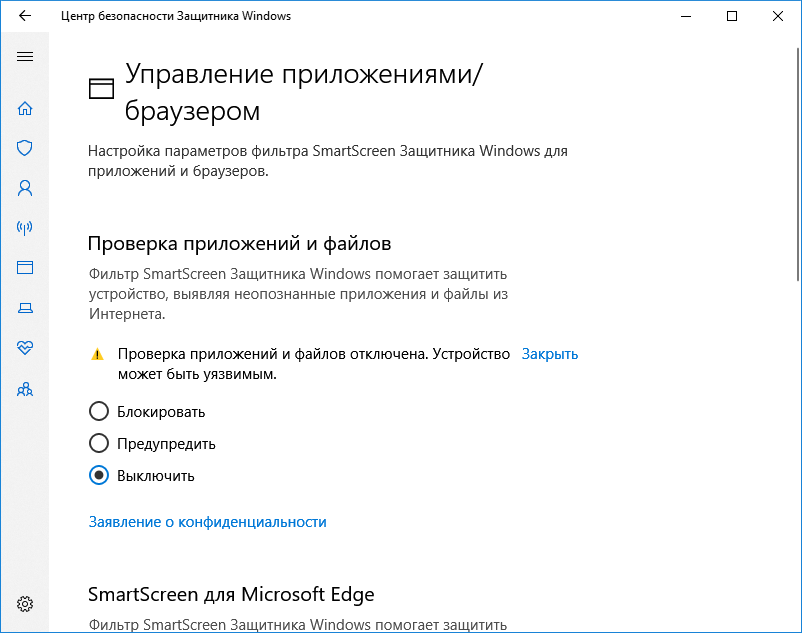


2. **Завантажити та з’ясувати призначення програмного додатку Центр безпеки (Панель керування) та компонентів, які входять до складу цього додатку.**

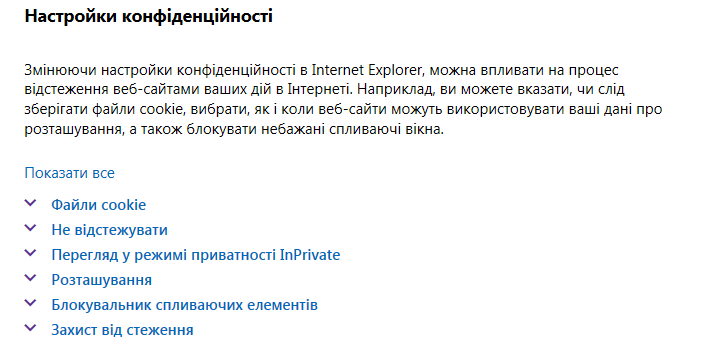


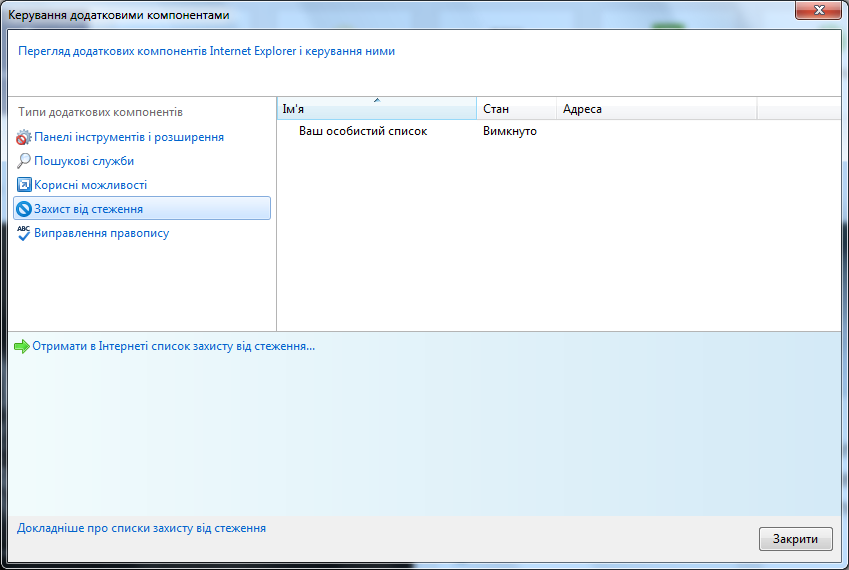




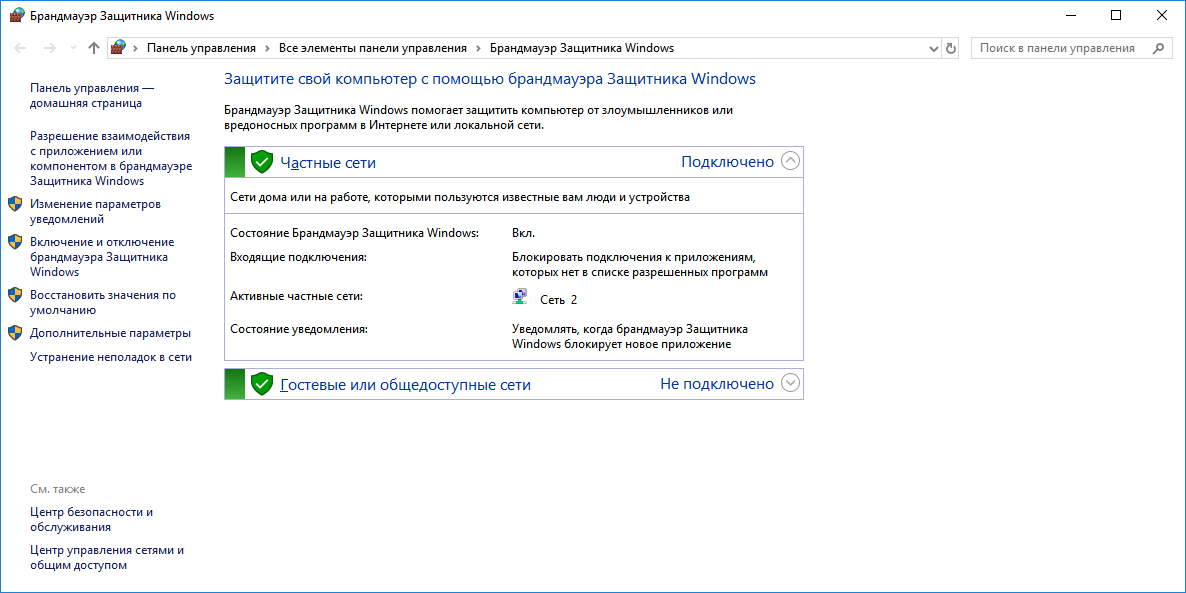


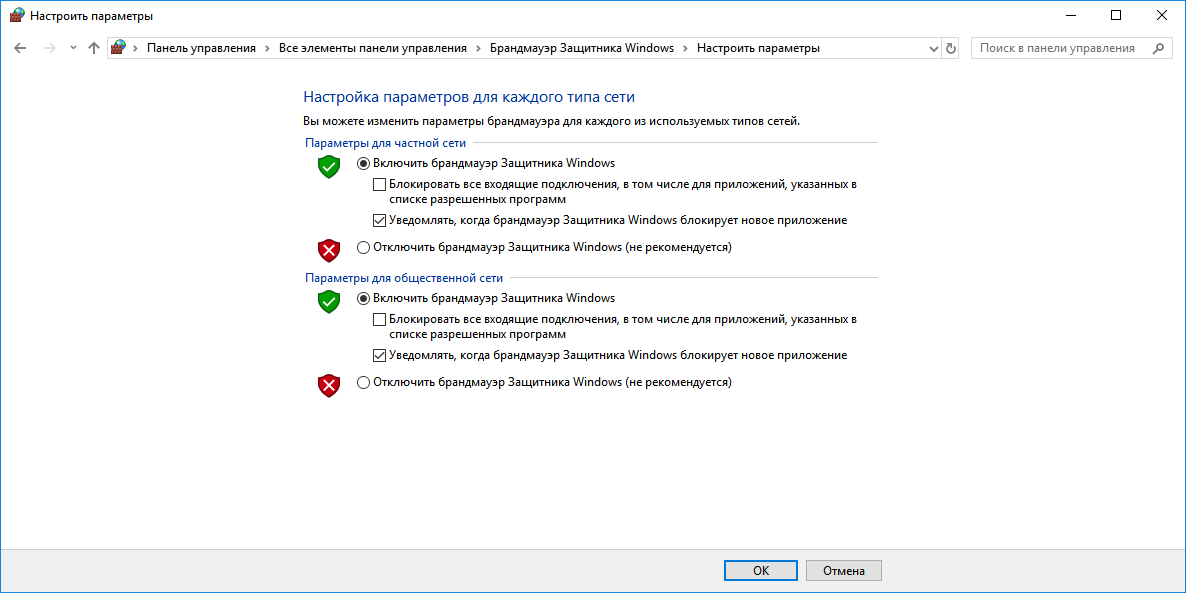
3. **Налаштувати параметри безпеки браузера Internet Explorer, з’ясувати які рівні безпеки найкраще використовувати для різних мережевих зон.**

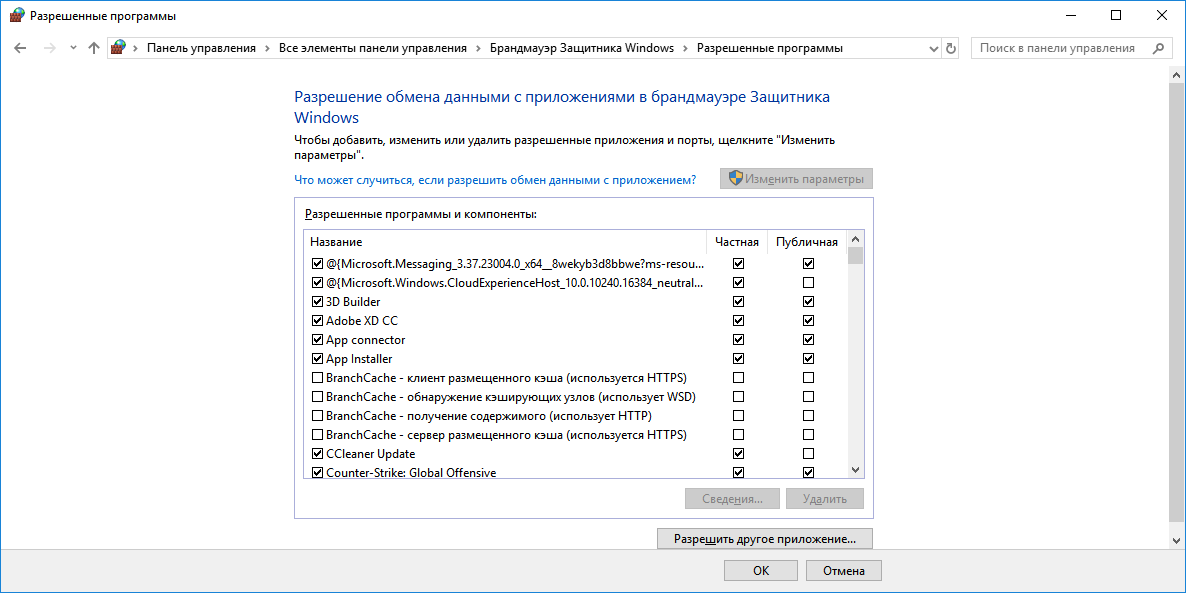
****

****

4. **Ознайомитися, налаштувати та продемонструвати роботу вбудованого брандмауера. Продемонструвати роботу брандмауера з окремими портами та програмами.**

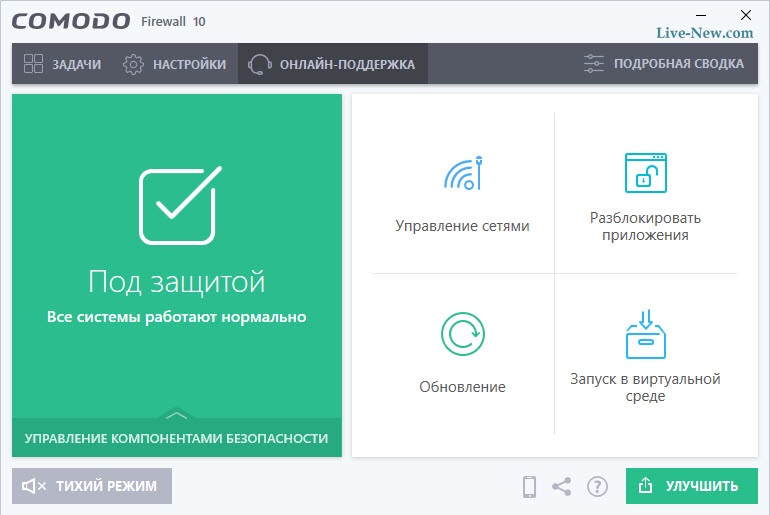






**5. За допомогою пошукової системи глобальної мережі Інтернет знайти та дослідити програмні засоби (брандмауери, файрволи) для забезпечення захисту комп’ютера від мережевих атак. Описати 2 програмних засоби за наступною схемою:**

# **Comodo Firewal**



**Comodo Firewall — один з найкращих безкоштовних файерволів, що нарівні конкурує з платними аналогами.** На відміну від інших, творці цього файервола пропонують нам повну версію програми для захисту комп’ютера від небажаної цікавості сусідів по Інтернету. Comodo Firewall орієнтований на простого, необізнаного в нетрях мережевих налаштувань, користувача.

Comodo Firewall допомагає зрозуміти, що відбувається при підключенні до Інтернету тієї чи іншої програми, аналізуючи кожне підозріле з’єднання. Про те що відбувається фаєрвол інформує користувача за допомогою спливаючих вікон, в яких відносно простою мовою пропонується «вирішити долю» того або іншого з’єднання.

#### Основні характеристики Comodo Firewall:

— Повний постійний контроль і захист персонального комп’ютера від інтернет-атак, троянів, хакерів, скриптів і інших невідомих загроз.

— Повний контроль за активністю програм в Інтернеті.

— Стеження за трафіком в режимі реального часу, що надає можливість миттєво реагувати на можливі загрози.

— Модуль захисту Comodo Defense+ (система запобігання вторгнення рівня хоста).

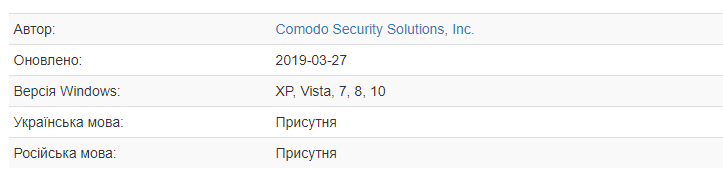
— Автоматична перевірка наявності оновлень Comodo Firewall.

— Контроль за оновленнями програмного забезпечення.

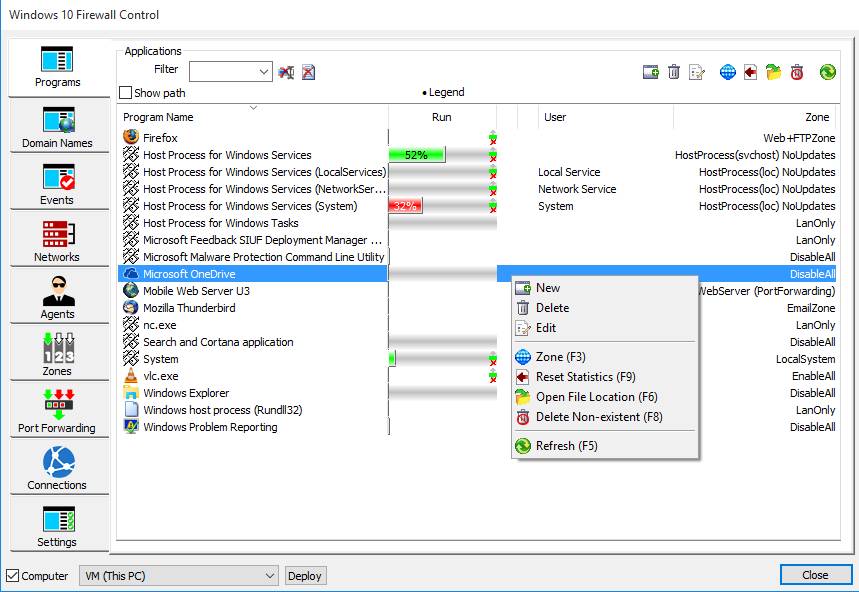
— Простий, інтуїтивно зрозумілий багатомовний інтерфейс.

**Недоліки даної програми.**

* Для простого обивателя складний в налаштуваннях;
* Знижує швидкість завантаження системи.



# **Windows 10 Firewall Control**



**Windows 10 Firewall Control – це фаєрвол від компанії Sphinx Software.** Версія Free продукту поширюється безкоштовно. Про неї мова і піде далі.

У своїй роботі програма знаходить на комп'ютері користувача активні програми та застосовує до них один з доступних наборів правил, які, в основному, стосуються отримання доступу до мережі Інтернет, з метою, наприклад, завантаження оновлень, відправки анонімної статистики та звіти про збої. Ці набори правил іменуються розробниками як зони (zones), яких в Windows 10 Firewall Control налічується чотири – дозволити вхідні/вихідні з'єднання або дозволити/заборонити вихід в мережу повністю. Таким чином, переміщаючись між додатками, встановленими в системі, і налаштовуючи для кожного з них політики безпеки, користувач може знизити ймовірність зараження ОС будь-яким шкідливим ПЗ, а також зменшити обсяг переданого в мережу трафіку. Останнє особливо актуально для власників 3G/4G модемів, що мають обмеження на кількість відправлених і прийнятих мегабайт згідно з тарифом.

Інструмент Windows 10 Firewall Control здатний працювати не тільки з окремими додатками. Так, в програмі є кілька режимів – Normal, при якому фільтрація трафіку здійснюється відповідно до встановлених для кожного додатка правил; EnableAll, який, по суті, відключає фаєрвол і надає доступ до мережі всім програмним продуктам; EnableUnknown, який зачіпає тільки відоме ПЗ і, відповідно, застосовується під час встановлення нових програм; DisableAll, при якому доступ закритий для всіх служб і процесів незалежно від прийнятих правил.

Ще однією корисною функцією цього фаервола є підтримка імпорту/експорту параметрів безпеки, що дозволяє експериментувати з поточною ОС, а також швидко налаштовувати політики доступу до мережі для додатків на інших пристроях.

Інтерфейс Windows 10 Firewall Control становить одне невелике вікно. Елементи керування досить численні і представлені всілякими кнопками-піктограмами, чекбоксами, полями введення і випадаючими списками. Перемикання між основними розділами програми здійснюється за допомогою механізму вкладок. Крім того, деякі дії можна зробити, клікнувши по іконці фаервола в треї Windows.

## **Переваги Windows 10 Firewall Control**

* Безкоштовне розповсюдження продукту.
* Наявність фірмового графічного інтерфейсу.
* Наявність звукового супроводу.
* Наявність декількох встановлених наборів правил – зон.
* Наявність декількох вбудованих режимів роботи.
* Підтримка імпорту і експорту параметрів безпеки.
* Наявність засобів самозахисту фаервола.
* Можливість ведення лог-файлу.

## **Недоліки Windows 10 Firewall Control**

* Відсутність підтримки інших мов, крім англійської.
* Дещо складний для розуміння інтерфейс програми з численними елементами керування і дрібними значками-кнопками.

## **Висновок**

Windows 10 Firewall Control працює коректно, без збоїв, не зависає. Зручності додає покрокове відкриття/закриття доступу до мережі для кожного встановленого додатка. Проте, щоб уникнути проблем з компонентами операційної системи, зокрема, зі службою оновлень, користуватися інструментом все ж варто з осторогою.

