# Дипломна робота

на тему:

***Порівняння шляхів проникнення стороннього програмного забезпечення на персональний комп'ютер те методи його захисту.***

Студент групи 44-ІС
Осташевський Адріан Ігорович

# Мета роботи

- Розглянути типи шкідливого програмного забезпечення
- Методи проникнення стороннього програмного забезпечення на персональний комп’ютер
- Антивірусні програми та інші методи захисту персонального комп’ютера

# Класифікація шкідливих програм

- ***За середовищем перебування:***
- *Завантажувальні* - проникають у завантажувальний сектор диска (Boot-сектор) або в сектор, що містить системний завантажник вінчестера (Master Boot Record);
- *Файлові* - впроваджуються у виконувані файли;
- *Файлово-завантажувальні* - заражають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи й часто застосовують оригінальні методи проникнення в систему;
- *Мережеві* - поширюються по комп'ютерній мережі;

## *За деструктивними можливостями:*

- *Нешкідливі* - вплив яких обмежується зменшенням вільної пам'яті на диску й графічними, звуковими ефектами;
- *Небезпечні* - ті, які можуть призвести до серйозних збоїв у роботі, або до втрати  інформації;
- *Дуже небезпечні* - ті, які можуть призвести до фізичного пошкодження обладнання (Виходу з ладу дискових пристроїв, пошкодження елементів материнської плати тощо);

***За способом зараження:***

- *Резидентні* - при інфікуванні комп'ютера залишають в оперативній пам'яті свою резидентну частину, що потім перехоплює звернення операційної системи до об'єктів зараження й впроваджується в них (перебувають у пам'яті і є активними аж до вимикання або перезавантаження комп'ютера);
- *Нерезидентні* - не заражають пам'ять комп'ютера і є активними обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус;

***За особливостями алгоритму:***

За особливостями алгоритму шкідливі програми важко класифікувати через велику різноманітність, нижче наведені деякі з них

- Стелс-програми
- Ботнет
- Трояни
- Backdoor
- Руткіти

# Основні ознаки зараження ПК:

- Непередбачені збої
- Уповільнення роботи комп'ютера
- Невідомі повідомлення
- Неправильна робота програм
- Повідомлення про помилки
- Зниження швидкості запуску операційної системи
- Подача невідомих звукових сигналів
- Зміна зовнішнього виду і розміру файлів
- Несподіване відключення антивіруса
- IP-адреса у чорному списку

# Основні шляхи проникнення шкідливого ПЗ

- Глобальна мережа інтернет
- Локальна мережа
- Електронна пошта
- Зовнішні накопичувачі
- Комп'ютери «загального призначення»
- Піратське програмне забезпечення
- Підроблене антивірусне забезпечення

# Антивірусні програми

Детектори

Фаги

Ревізори

Фільтри

Вакцини

# Основні антивірусні програми

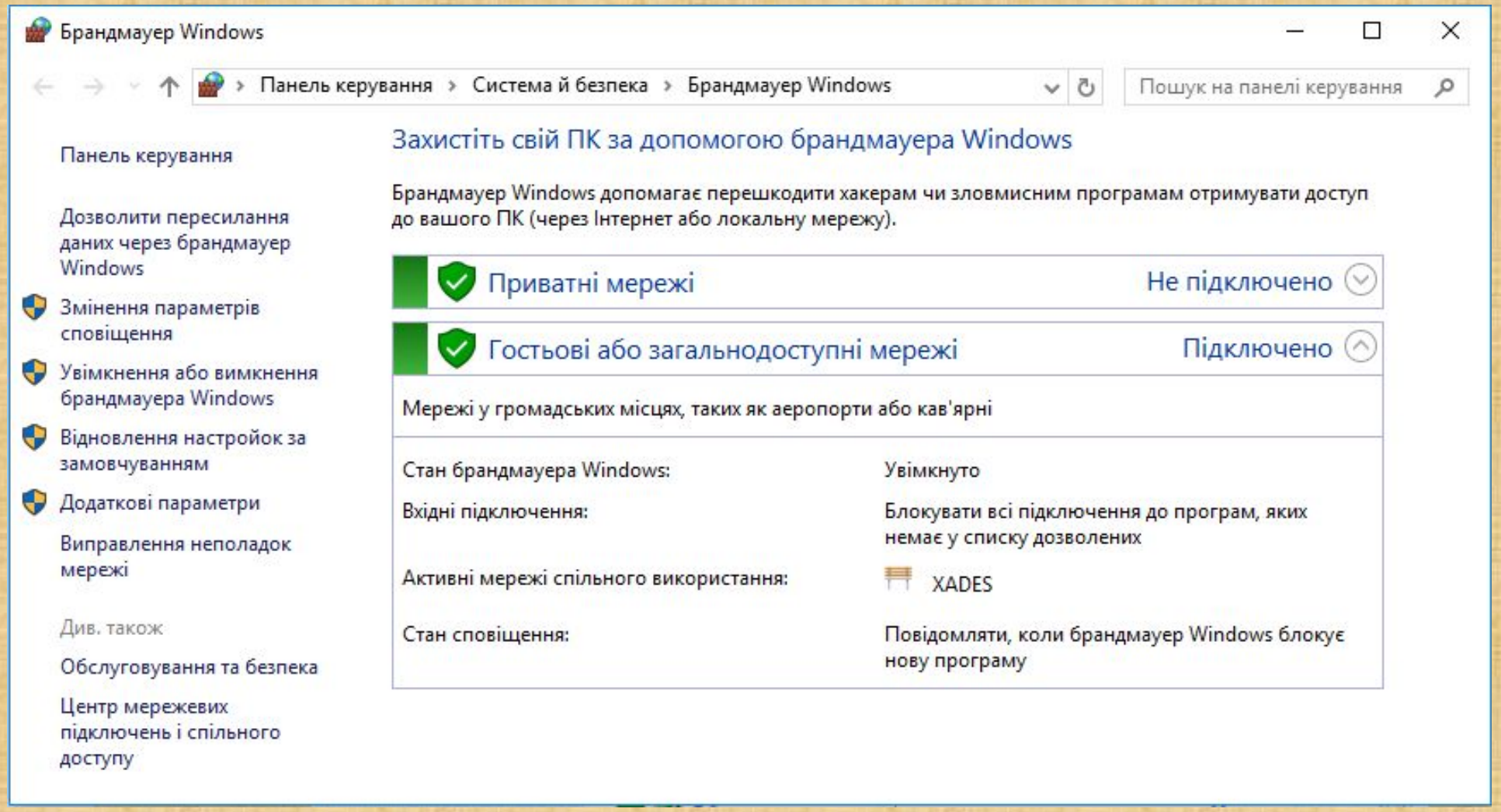




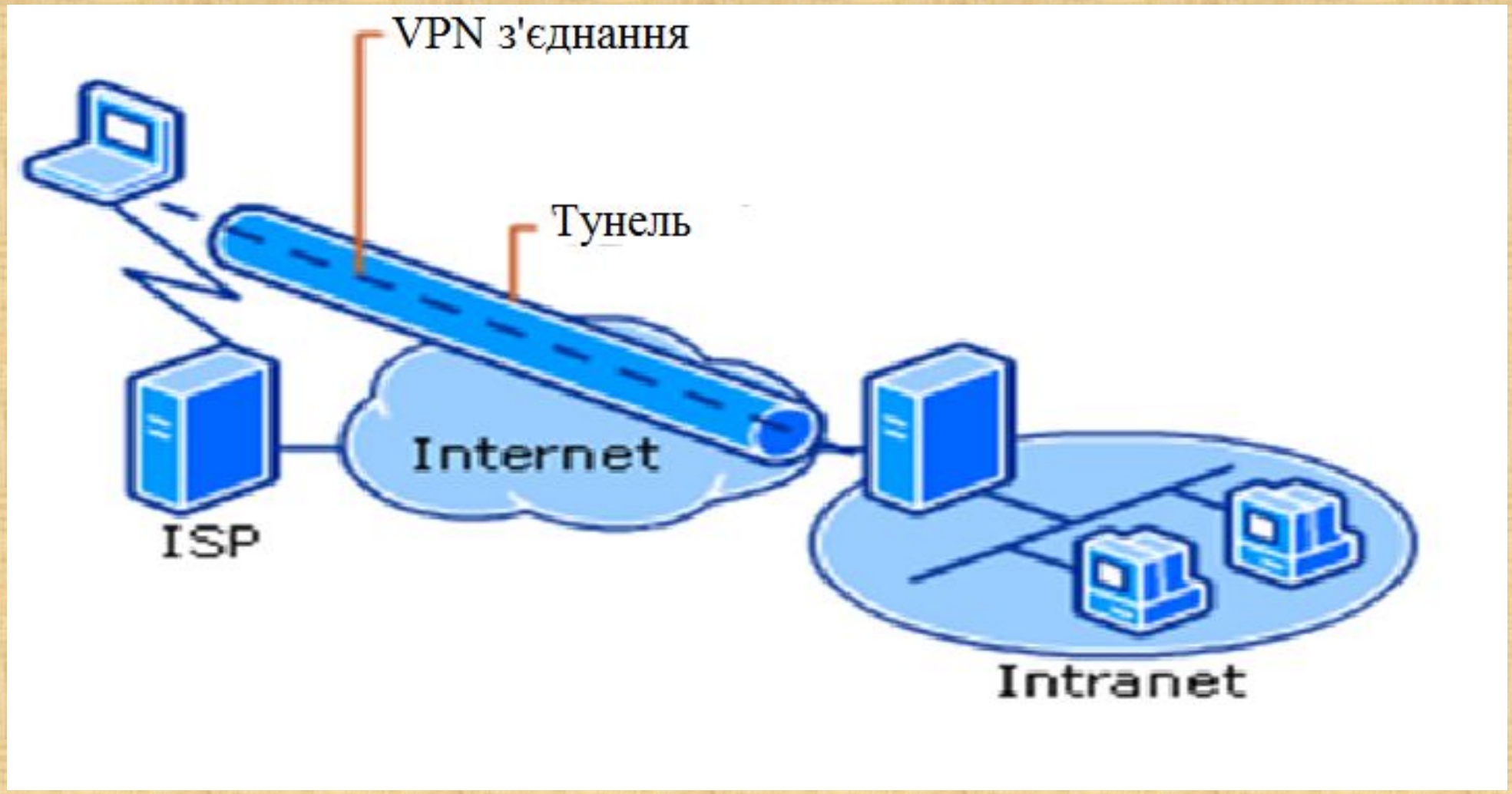




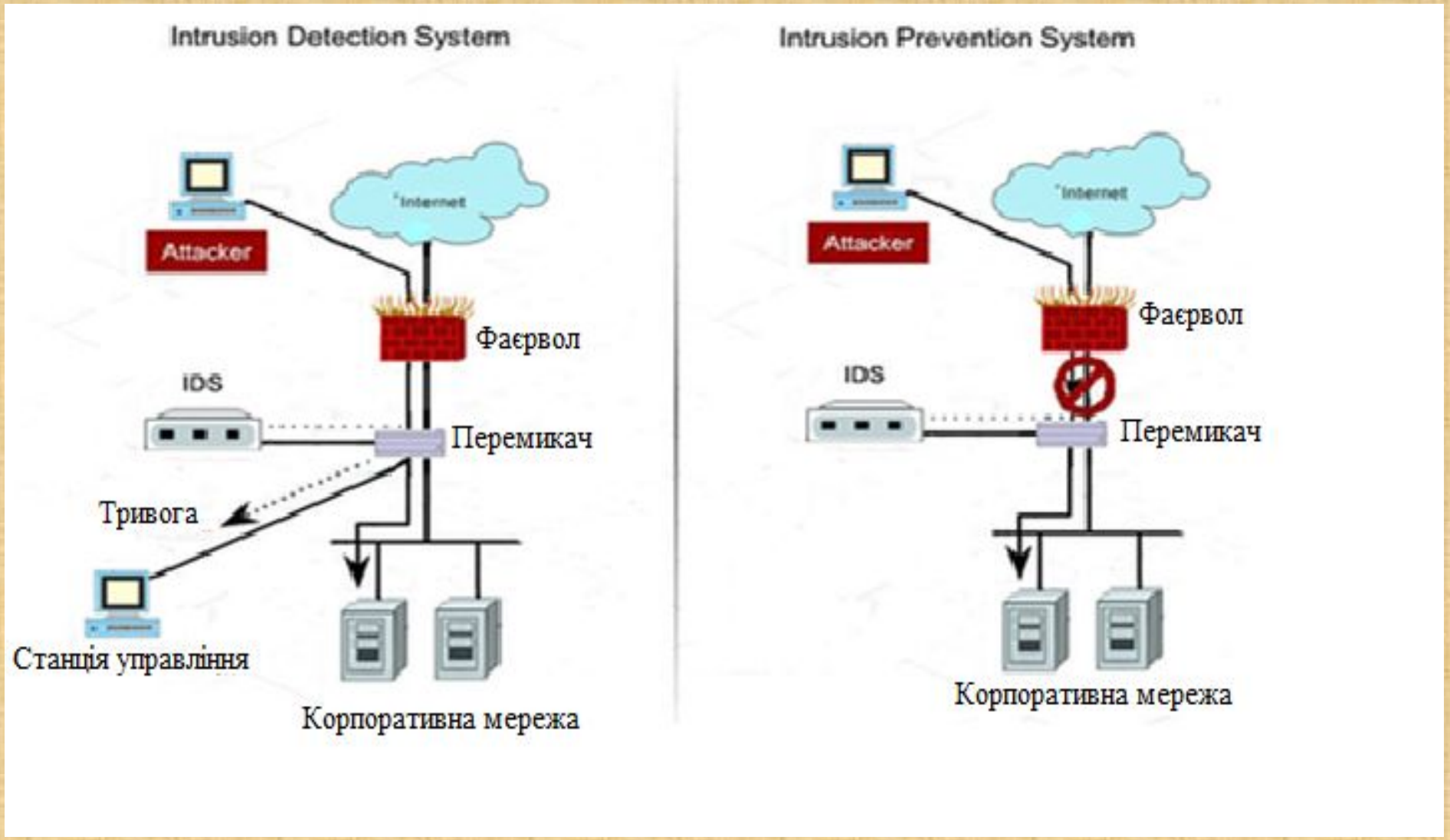

# Міжмережевий екран (Брандмауер)



# Віртуальні приватні мережі (VPN)



# Системи запобігання вторгнень IDS/IPS



# Висновки

- В даній роботі розглянуто, як і де саме у комп’ютер може проникнути шкідлива програма. Виведено класифікацію, яка визначає різновиди шкідливих програм і їх ступінь загрози.
- Приведені приклади антивірусних програм, проаналізований їх алгоритм роботи.

Жодна з антивірусних програм окремо не дає повного захисту від проникнення стороннього програмного забезпечення, тому найкращою стратегією захисту від шкідливих програм є багаторівнева «ешелонована» оборона.

# Дякую за увагу