**ВСП «Харківський фаховий коледж інформаційних технологій
Національного аерокосмічного університету ім. М.Є. Жуковського
«Харківський авіаційний інститут »**

ЗВІТ
про виконання лабораторної роботи

Лабораторна робота №4 Романенко Георгій гр. МЗ–31

Тема: ***Побудова захищених віртуальних мереж за допомогою міжмережевих екранів***

1. Що таке захищені віртуальні мережі та міжмережеві екрани

Захищені віртуальні мережі (ВМ) – це технологія, що дозволяє створювати ізольовані мережеві сегменти всередині фізичної мережі. ВМ використовуються для розділення мережевого трафіку на основі бізнес-вимог або рівнів безпеки, забезпечуючи таким чином ізоляцію між різними користувачами або групами користувачів. Використання ВМ може допомогти зменшити ризики безпеки, обмеживши потенційний доступ нелегітимних користувачів до чутливих ресурсів.

Міжмережеві екрани (файрволи) – це пристрої або програмні рішення, призначені для моніторингу та контролю вхідного і вихідного мережевого трафіку на основі заданих правил безпеки. Вони діють як бар'єр між ненадійною зовнішньою мережею, такою як Інтернет, і внутрішньою мережею організації, запобігаючи несанкціонованому доступу до мережевих ресурсів.

2. Приклади побудови захищених віртуальних мереж за допомогою міжмережевих екранів

Приклад 1: Корпоративна мережа

У корпоративній мережі файрвол встановлюється на межі мережі для захисту всієї мережевої інфраструктури. Віртуальні мережі створюються для розділення трафіку між різними відділами, наприклад, між відділом розробки та

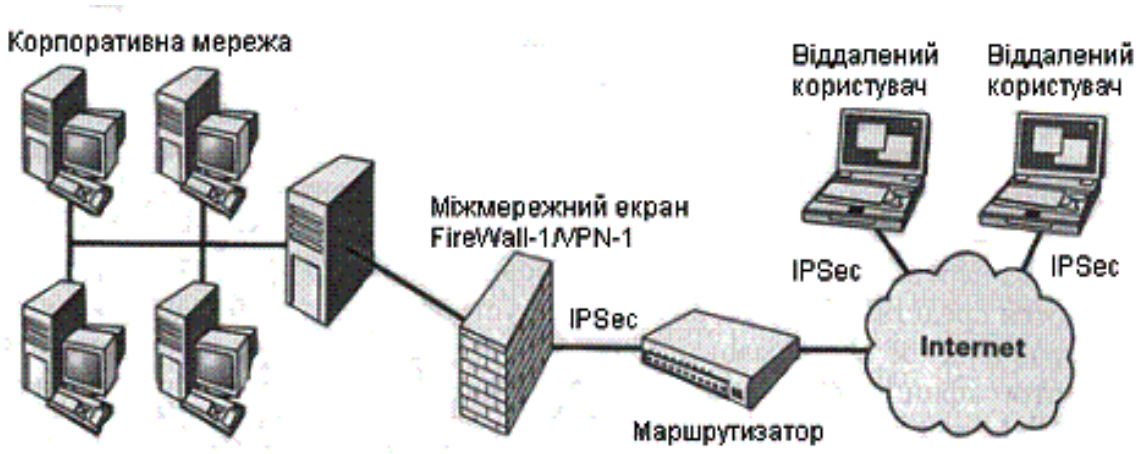
HR. Файрвол конфігурується так, щоб дозволяти співробітникам HR доступ тільки до необхідних їм ресурсів, а розробникам – до серверів розробки та тестування.

Приклад 2: Захист віддалених робочих місць

З використанням VPN (віртуальної приватної мережі) та файрволів, компанії можуть забезпечити безпечний віддалений доступ до своїх внутрішніх ресурсів. Віддалені співробітники підключаються через зашифрований VPN–тунель, а файрвол перевіряє трафік, що проходить через VPN, на відповідність політикам безпеки перед тим, як дозволити доступ до мережі.

Приклад 3: Ізоляція гостьового трафіку

Для ізоляції гостьового трафіку від корпоративних ресурсів можна використовувати окрему ВМ для гостей з окремим доступом до Інтернету. Файрвол налаштовується таким чином, щоб обмежити доступ гостей тільки до Інтернету, запобігаючи їхньому доступу до внутрішньої мережі компанії.



Малюнок 1.1 – схема побудови впн

Висновки: Побудова захищених віртуальних мереж за допомогою міжмережевих екранів є важливим елементом стратегії інформаційної безпеки будь-якої організації. Використання цих технологій дозволяє забезпечити захист від зовнішніх загроз, контролювати доступ до ресурсів та ефективно управляти мережевим трафіком.