# КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ТАРАСА ШЕВЧЕНКА



## ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №5**

# з курсу

**«Безпека мереж і комп’ютерних систем»**

*Студента 2 курсу*

*групи ПП-21 спеціальності 122 «Комп'ютерні науки» ОП «Прикладне програмування»*

%username%

*Викладач:*

проф. Сайко В.Г.

## Київ – 202

**1.Назва роботи**

Вивчення брандмауерів, віртуальних приватних мереж і мережевих технологій

виявлення вторгнень і запобігання вторгнень

1. **Тема роботи**

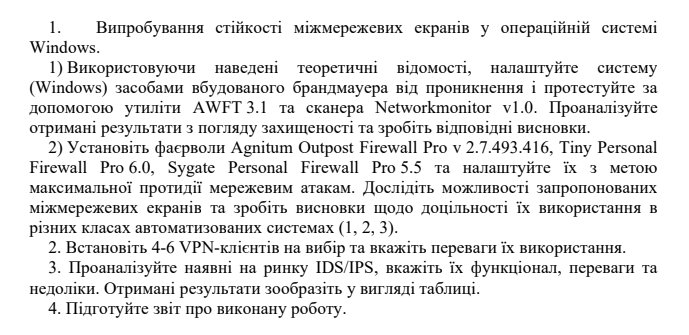
Вивчення брандмауерів, віртуальних приватних мереж і мережевих технологій

виявлення вторгнень і запобігання вторгнень

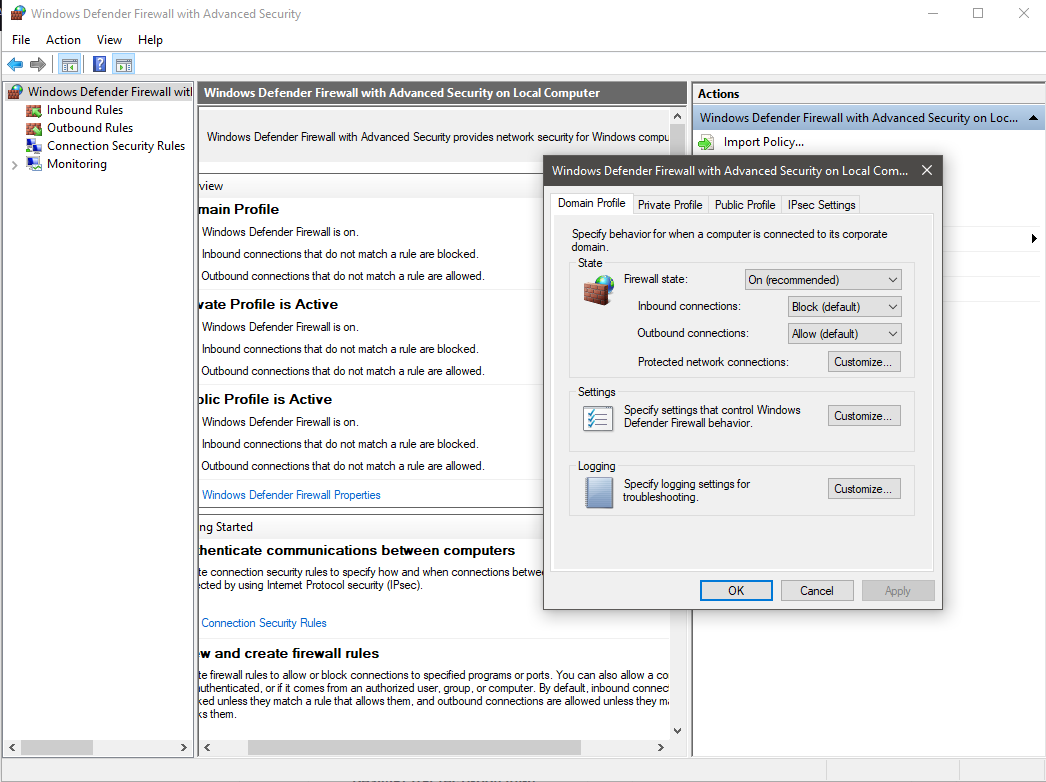
1. **Мета роботи**

За допомогою інтернет-ресурсів проаналізувати загрози мережевій безпеці.

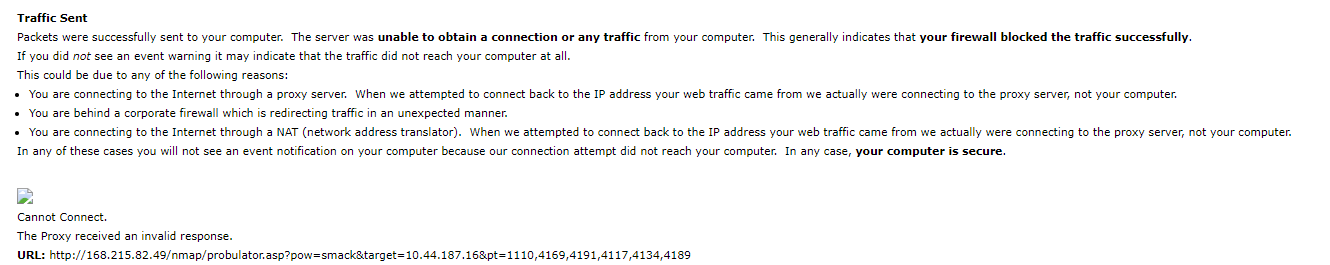
1. **Умова завдання**



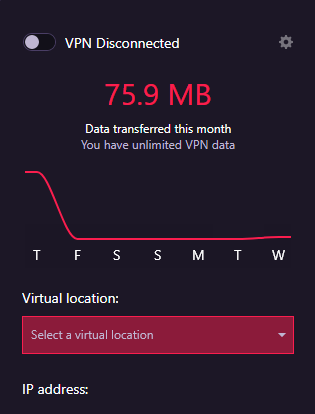
1. **Рішення**



Налаштовуємо вбудований файрволл

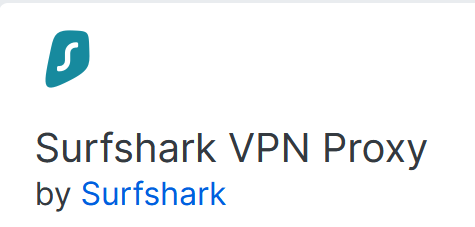


Перевіряємо його роботу: як бачимо, відповіді на запроси не надійшло, отже, файрволл працює як слід.

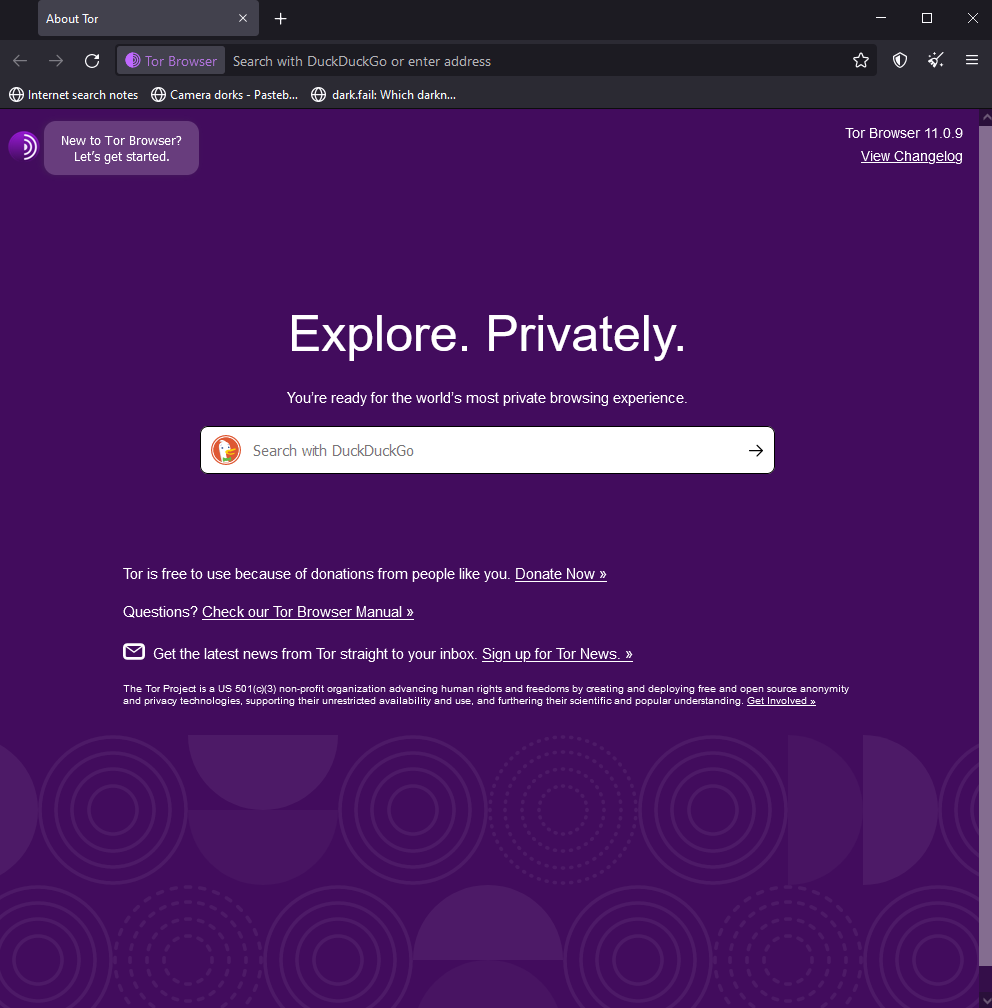


Перший VPN-клієнт: Opera GX (вбудований).

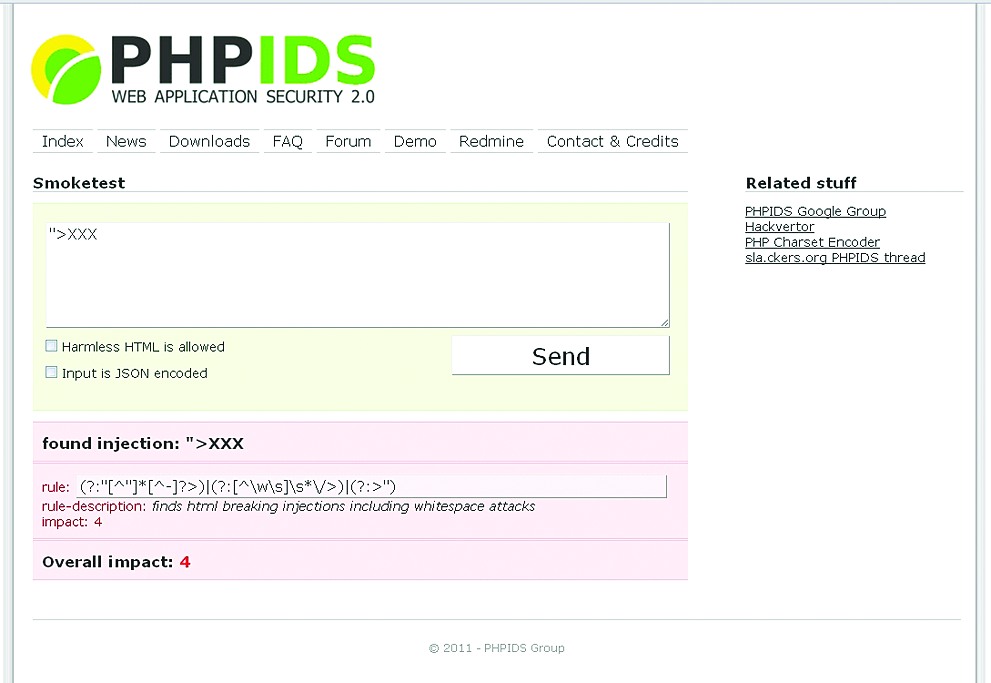
Дуже легкий у використанні, безкоштовний VPN. Скоріше за все, безкоштовність виправдовується збором та продажем даних користувачів, але через браузерну основу це не є великою проблемою.



Другий VPN-клієнт: Surfshark VPN Proxy. Чудовий інстальований платний клієнт.

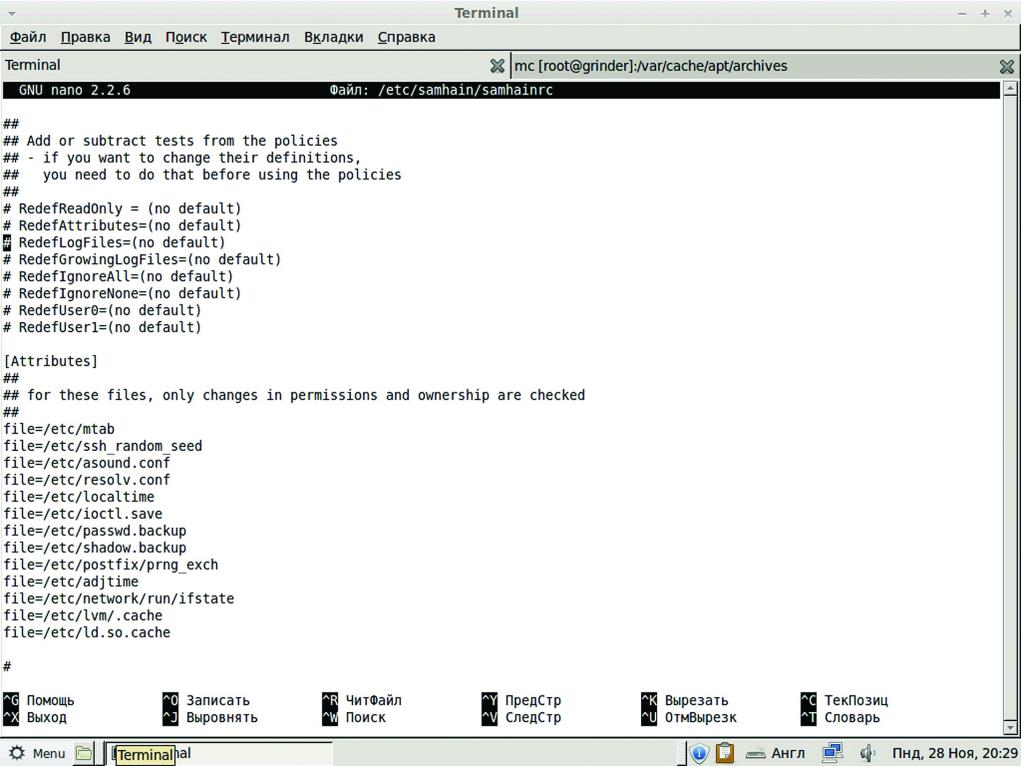


Третій (не VPN) клієнт - TOR Browser. Хоча технічно він не є VPN-сервісом, я використовую його саме так; головні причини - надійність, безпека та open-source код.

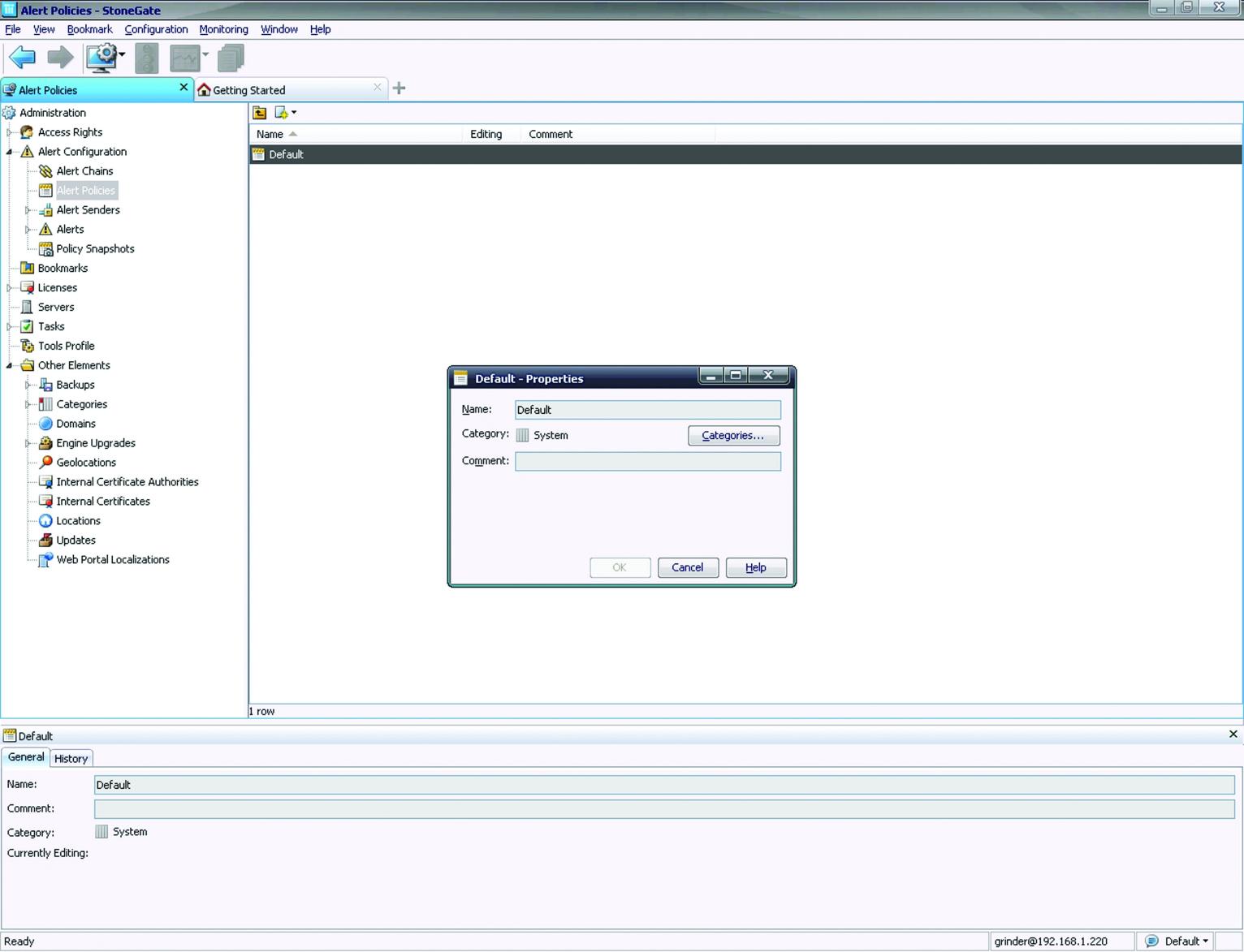


PHPIDS, IDS для аналізу запитів до PHP-додатків. Open-source застосунок, корисний для тих, хто працює з PHP.

Fwsnort - IDS/IPS, що використовує IP-таблиці для будування правил. Безкоштовний open-source проект, що до того ж має документацію.



Samhain - хостова IDS, що створює сигнатури файлів для подальшого порівняння зі станом системи, моніторить та аналізує записи в журналах, контролює вхід та вихід з системи, моніторить підключення до портів.



## StoneGate Intrusion Prevention System, комерційна программа для захисту від DDoS, 0day атак, що включає в себе функції веб-фільтрації, підтримку шифрованого трафіку, захист від систем AET.

**Контрольні запитання:**

1. Що таке брандмауер?

Брандмауер - міжмережевий екран, що запобігає проникненню на комп’ютер хакерів чи зловмисних програм.

1. Які три типи фаєрволів існують?

•фаєрвол мережного рівня представлений екрануючим маршрутизатором. Він

контролює лише дані мережевого і транспортного рівнів службової інформації

пакетів. Мінусом таких маршрутизаторів є те, що інші п’'ять рівнів залишаються

неконтрольованими. Адміністратори, які працюють з екрануючими

маршрутизаторами, повинні пам’ятати, що у більшості приладів, які фільтрують

пакети, немає механізмів аудиту та подачі сигналу тривоги. Іншими словами,

маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а

адміністратори навіть не будуть проінформовані;

•фаєрвол прикладного рівня, також відомий як проксі-сервер (proxy server,

сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний

поділ між локальною мережею та Інтернет, тому вони мають відповідати найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому в ролі якості сервера-посередника потрібно використовувати більш швидкі комп'ютери;

•фаєрвол рівня з’єднань схожий на фаєрвол прикладного рівня тим, що обидва є

серверами-посередниками. Відмінність полягає у тому, що фаєрволи прикладного

рівня вимагають спеціального програмного забезпечення для кожної мережевої

служби (на зразок FTP або HTTP). Натомість, фаєрволи рівня з’єднання

обслуговують велику кількість протоколів.

3. Що таке VPN?

Віртуальна приватна мережа, англ. Virtual Private Network – це логічна

мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передачі пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, в результаті чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об’єднати, наприклад, кілька географічно віддалених мереж організації в єдину мережу з використанням для зв’язку між ними незалежних каналів.

1. У чому особливість технології IPSec?

IPSec застосовується для створення VPN, підтримуваних провайдером. Тунелі в

них будуються на базі пристроїв клієнта, але конфігуруються вони віддалено, і керує провайдер. Технологія IPSec дозволяє вирішувати такі завдання щодо встановлення та підтримання захищеного каналу:

• аутентифікації користувачів або комп’ютерів при ініціалізації каналу;

• шифрування і аутентифікації переданих даних між кінцевими точками каналу;

• автоматичного постачання точок секретними ключами, потрібними для

роботи протоколів аутентифікації і шифрування даних.

Недоліком цієї технології є те, що з усіх властивостей віртуальної мережі

технологія IPSec реалізує лише захищеність та ізольованість адресного простору, а пропускну здатність та інші параметри QoS (Quality of Service) вона не підтримує. Крім того, серйозним мінусом протоколу IPSec є і його орієнтованість виключно на IP-протокол.

1. Назвіть особливості VPN із віддаленим доступом.

VPN із віддаленим доступом (Remote Access VPN). Використовують для

створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп’ютера, корпоративного ноутбука чи смартфона.

1. Що таке IDS/IPS?

(англ. Intrusion Detection System /Intrusion Prevention System, укр. Система

виявлення вторгнення (СВВ)/Система запобiгання вторгненню (СЗВ)). СВВ – програмний або апаратний засiб, призначений для виявлення фактiв несанкцiонованого доступу до комп’ютерної системи (мережі), або несанкцiонованого керування такою системою. СЗВ – програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разi їх виявлення.

1. Назвіть особливості статистичних СВВ.

Статистичні СВВ використовують статистичний пiдхiд, пiсля установки

«навчаються» адмiнiстратором, який задає полiтику СВВ, вiдповiдну нормальній активностi в мережi – типи трафiку, з’єднання мiж вузлами, використовуванi протоколи i порти. При виявленнi аномалiй у роботi мережi або статистично значущих вiдмiнностей трафiку вiд типового в цій мережi СВВ сповiщає про це адмiнiстратора. Основною проблемою такого пiдходу є складнiсть у налаштуваннi i велика кiлькiсть хибнопозитивних тривог у разi некоректно заданих правил;

1. Назвіть особливості ERIDS.

ERIDS (англ. External Routing Intrusion Detection System) - приклад

iнновацiйної та вузькоспецiалiзованої системи. Потреба її створення була

продиктована тим фактом, що крiм простого i розподiленого способу збору даних

про мережi iснують менш тривiальнi. Наприклад, зловмисник спочатку здiйснює

атаку на маршрутизатор, змiнює його налаштування так, що вiн направляє трафiк

через сегмент, який не контролюється i доступний атакуючому.

**Висновки**

В результаті виконання даної лабораторної роботи я оволодів практичними навичками використання вбудованого брандмауера системи Windows, користувався програмою Shields Up для перевірки параметрів налаштування вищевказаного файрволу. Налаштував декілька VPN-з’єднань, скориставшись різними клієнтами. Вважаю дану лабораторну роботу виконаною в повному обсязі.