Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Особливості налаштування міжмережевих екранів"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Стецик Сергій Сергійович
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Стецику Сергію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Особливості налаштування міжмережевих екранів

Керівник роботи Лечаченко Тарас Анатолійович, PhD доктор філософії., асистент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 14.06.2024

3. Вихідні дані до роботи Літературні джерела та мережа Інтернет

4. Зміст роботи (перелік питань, які потрібно розробити)
Дати визначення міжмережевих екранів, описати їх призначення та принцип роботи.
Розглянути функції міжмережевих екранів на різних рівнях моделі OSI.
Викласти способи класифікації міжмережевих екранів, їх види і компоненти.
Проаналізувати переваги і недоліки різних видів міжмережевих екранів.
Описати проблему політики міжмережевої взаємодії.
Розглянути основні схеми організації міжмережевих екранів та особливості їх налаштування.
Продемонструвати налаштування міжмережевого екрану на обладнанні Cisco.
Надати рекомендації по ефективному використанню міжмережевих екранів.
Безпека життєдіяльності, основи охорони праці
Проаналізувати ергономічні проблеми безпеки життєдіяльності. Розглянути вимоги ергономіки до організації робочого місця оператора ПК, агрегата.
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Основні схеми підключення міжмережевих екранів. Топологія комп'ютерної мережі. Результати налаштування міжмережевого екрана на обладнанні Cisco. Результати перевірок пінгу. Ергономічні вимоги до організації трудових процесів та робочих місць. Робоче місце і робоча поза користувача комп'ютера. Блок-схема організації робіт на ПК.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С.Ю., кандидат технічних наук, доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.01 – 23.01	Виконано
2.	Підбір джерел для огляду міжмережевих екранів	25.01 – 05.02	Виконано
3.	Опрацювання джерел в галузі дослідження	06.02 – 20.02	Виконано
4.	Розглянути схеми підключення міжмережевих екранів	22.02 – 12.03	Виконано
5.	Опрацювати налаштування міжмережевого екрана на обладнанні Cisco	15.03-25.03	Виконано
6.	Вивчити способи класифікації міжмережевих екранів	25.02 – 10.04	Виконано
7.	Оформлення розділу «Міжмережеві екрани як засіб захисту інформаційних мереж»	10.02 – 05.03	Виконано
8.	Оформлення розділу «Особливості впровадження технологій міжмережевих екранів»	26.03 – 04.05	Виконано
9.	Оформлення розділу «Налаштування міжмережевого екрана на обладнанні Cisco»	12.04-20.04	
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	25.04 – 10.05	Виконано
11.	Оформлення кваліфікаційної роботи	23.05 – 08.06	Виконано
12.	Нормоконтроль	10.06 – 15.06	Виконано
13.	Перевірка на плагіат	20.06 – 22.06	Виконано
14.	Попередній захист кваліфікаційної роботи	17.06 – 19.06	Виконано
15.	Захист кваліфікаційної роботи	27.06.2024	

Студент _____ Стецик С.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Особливості налаштування міжмережевих екранів // Кваліфікаційна робота ОР «Бакалавр» // Стецик Сергій Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2024 // С. 55 , рис. – 24, додат. – 1.

КЛЮЧОВІ СЛОВА: Міжмережевий екран, протокол, мережа, доступ, пакет, фільтрація, списки ACL, Stateful.

Кваліфікаційна робота присвячена дослідженню міжмережевих екранів та їх ролі у захисті комп'ютерних мереж від несанкціонованого доступу. У роботі розглянуті призначення та принцип роботи міжмережевих екранів, основні види їх класифікації. Аналізуються переваги і недоліки різних видів міжмережевих екранів. Описані сегментація мереж та основні схеми підключення міжмережевих екранів.

Викладені особливості налаштування міжмережевих екранів на обладнанні Cisco. Результати роботи дозволять підвищити рівень безпеки комп'ютерних мереж.

Кваліфікаційна робота також може бути використана в навчанні.

ABSTRACT

Features of setting up firewalls // Thesis for bachelor's degree // Stetsyk Serhii Serhiiovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Cybersecurity, group SBs-42 // Ternopil, 2024 // P. 55, fig. 24, supplementary material -1.

KEYWORDS: firewall, protocol, network, access, packet, filtering, ACLs, Stateful.

The qualification work is devoted to the study of firewalls and their role in protecting computer networks from unauthorized access. The paper considers the purpose and principle of operation of firewalls, the main types of their classification. The advantages and disadvantages of different types of firewalls are analyzed. Network segmentation and basic firewall connection schemes are described.

The features of configuring firewalls on Cisco equipment are outlined. The results of the work will increase the level of security of computer networks.

The qualification work can also be used in training.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AAA	—	Authentication, Authorization, Accounting
ACE	—	Access Control Entries
ACL	—	Access Control List
DLP	—	Data loss prevention
DMZ	—	Demilitarized zone
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
DPI	—	Deep Packet Inspection
FTP	—	File Transfer Protocol
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
NAT	—	Network Address Translation
SNMP	—	Simple Network Management Protocol
SQL	—	Structured Query Language
TCP	—	Transmission Control Protocol
URL	—	Uniform Resource Locator
UTM	—	Unified threat management
VLAN	—	Virtual Local Area Network
VPN	—	Virtual Private Network
XSS	—	Cross-Site Scripting
ЕОМ	—	електронно-обчислювальна машина
ІКС	—	інформаційно-комунікаційна система
КС	—	комп’ютерна система
МЕ	—	міжмережевий екран
ОС	—	операційна система
ПЗ	—	програмне забезпечення
ПК	—	персональний комп’ютер

ВСТУП

У 21 столітті, на відміну від попередніх етапів розвитку суспільства, все більш домінуючу позицію займає інформаційна сфера. Формуються і стрімко масштабуються як територіально, так і за глибиною проникнення в усі економічні і соціальні сфери інформаційно-обчислювальні системи і мережі та технології збирання, накопичення, пошуку, зберігання, передачі та обміну інформацією. Від їх стану залежать не лише окремі користувачі чи представники від дрібного до транснаціонального бізнесу, а й економічна та політична безпека сучасних держав.

Проте, надаючи нові, набагато ширші можливості з обробки, передачі та зберігання інформації, сучасні інформаційні технології можуть нести потенційну небезпеку втрати, зміни чи блокування доступу до інформації.

Висока значимість і комерційна вартість сучасної ділової та приватної інформації та щодня зростаючі обсяги оброблюваної інформації визначають актуальність проблеми забезпечення її захисту від несанкціонованого доступу та атак зловмисників, кількість та різноманітність яких з часом тільки зростає.

Ця кваліфікаційна робота має на меті розглянути призначення та принцип роботи міжмережевих екранів, їх основні функції, а також політики безпеки. Буде здійснено огляд різних типів міжмережевих екранів, їх переваги та недоліки. До завдань роботи належить також вивчення основних схем підключення міжмережевих екранів та особливостей налаштування даних пристроїв.

На підставі опрацьованого матеріалу буде виконане налаштування міжмережевого екрану в мережі умовного невеликого підприємства з використання Cisco Packet Tracer, сформовані рекомендації з ефективного застосування міжмережевих екранів.

Напрацювання кваліфікаційної роботи сприятимуть покращенню обізнаності в галузі міжмережевої безпеки і можуть бути використані для підвищення рівня безпеки ІКС.

1 МІЖМЕРЕЖЕВІ ЕКРАНИ ЯК ЗАСІБ ЗАХИСТУ ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1 Призначення та принцип роботи МЕ

Глибоко аналізуючи проблему захищеності інформації, можна прийти до висновку, що найбільш захищеною є інформація, яка не поширюється взагалі, тобто до якої повністю відсутній доступ. На практиці це може бути реалізовано шляхом фізичного або логічного переривання каналу зв’язку. Цей принцип ліг в основу роботи міжмережевих екранів (далі - МЕ) - одного з основних компонентів захисту мереж. Інші їх назви – брандмауер та фаєрвол - були запозичені відповідно з німецької та англійської мов. Це термін з будівельної сфери, що перекладається як вогнестійка або протипожежна стіна із негорючого матеріалу – каменю або металу, яка розділяє суміжні будівлі. Під час пожежі в одному з будинків брандмауер перешкоджає поширенню вогню на інші та пом'якшує шкідливий вплив на людину [4, с.8].

Аналогічним чином МЕ відокремлюють мережі організацій від Інтернету або мереж інших організацій для запобігання поширенню шкідливого впливу. У сфері комп'ютерних мереж фаєрвол, брандмауер, або МЕ відокремлює захищені області від незахищених і таким чином блокує доступ до захищених ресурсів користувачам без відповідних прав. Це спеціалізоване програмне або апаратне забезпечення, яке виконує контроль мережевих пакетів: відстежує, блокує їх або пропускає. Воно дозволяє поділити одну мережу на дві і більше частин і реалізувати набір правил для проходження даних з однієї частини в іншу. Основне призначення МЕ – практичне втілення політики безпеки, прийнятої в організації стосовно обміну інформацією з зовнішньою мережею - обмеження транзиту трафіку і встановлення небажаних з'єднань тощо за допомогою інструментів фільтрації та аутентифікації [23, с.56].

Можна сказати, що МЕ – це свого роду бар’єр у вигляді напівпроникної «мембрани» між особливо вразливим внутрішнім сегментом мережі і зовнішньою мережею Інтернет, що відстежує і контролює інформаційний трафік

в обидві сторони [7, с.17]. Зазвичай він розміщується на периферії мережі. Кордоном є межа розділення між внутрішньою корпоративною мережею і зовнішньою мережею Інтернет або різними частинами розподіленої мережі.

Екран фільтрує інформаційні пакети, пропускаючи одні та блокуючи інші. МЕ надає захист від спроб зловмисників втрутитися у внутрішню мережу з метою копіювання, зміни або знищення інформації, блокування доступу до неї або використання пам'яті чи обчислювальної потужності комп'ютерів мережі. Він відслідковує і блокує спроби підключень, що загрожують безпеці пристроїв, забезпечує надійне зберігання і захист персональної інформації користувачів. МЕ безперервно спостерігає за портами комп’ютерів, щоб вчасно виявити момент спроби підключення шкідливого програмного забезпечення, вірусів, хробаків тощо.

1.2 Функції МЕ

МЕ розрізняють і класифікують за різними параметрами, але всі вони мають такі загальні властивості:

- протидіють атакам зловмисників;
- є єдиними транзитними точками між мережами, так як через них проходить весь трафік;
- забезпечують реалізацію політики управління доступом;

Функціональні вимоги до МЕ стосуються таких аспектів захисту:

- фільтрація пакетів (на мережевому та прикладному рівні);
- налаштування правил фільтрації й адміністрування;
- шифрування, тобто створення VPN;
- трансляція адрес;
- аутентифікація користувачів;
- впровадження журналів і обліку.

МЕ базуються на різних рівнях протоколів моделі OSI. На першому, фізичному рівні їх функціями є:

- Відділення серверів та робочих станцій внутрішнього сегмента мережі від зовнішніх каналів зв’язку;
- Забезпечення фізичної ізоляції мережевих компонентів.

На канальному рівні до функцій МЕ належать:

- Використання інформації про MAC-адреси для фільтрації пакетів;
- Перевірка прав доступу користувачів до ресурсів мережі.

На мережевому рівні виконуються:

- Фільтрація пакетів на основі IP-адрес (наприклад, не пропускає пакети з Інтернету до захищених серверів, пакети з IP адресами з «чорного списку» та з фальшивими зворотними адресами);
- Реєстрація всіх запитів до компонентів внутрішньої підмережі ззовні.

На транспортному рівні:

- Контроль доступу до ресурсів на основі портів та протоколів;
- Відстеження стану з'єднань та контроль потоку даних (фільтрація здійснюється номерами TCP-портів і прапорців, що містяться в пакетах).

На сеансовому рівні МЕ здійснюють:

- Управління сеансами зв'язку між різними системами;
- Встановлення, підтримку та завершення сеансів.

На рівні представлення функціями МЕ є:

- Кодування та декодування даних;
- Забезпечення сумісності між різними форматами даних.

На прикладному рівні може виконуватися:

- Фільтрація пакетів на основі конкретних додатків та послуг;
- Забезпечення безпеки на рівні додатків, тобто аналіз прикладних протоколів (FTP, HTTP, SMTP та ін.) і контроль вмісту потоків даних (заборона внутрішнім абонентам на отримання певних типів файлів, наприклад реклами або виконуваних програмних модулів) [14, с.56].

Ці функції допомагають забезпечити безпеку мережі та ефективно управляти комунікацією між різними системами. Таким чином, на кожному рівні МЕ виконують специфічні завдання, що сприяє забезпеченню цілісності та конфіденційності даних.

1.3 Основні види класифікації МЕ, їх види і компоненти

1.3.1 Класифікація МЕ за способом реалізації

Відповідно до способу реалізації виділяють апаратні та програмні МЕ. Апаратний МЕ – це пристрій з встановленою спеціалізованою ОС, який підключається до мережі і призначений ефективно обробляти мережеві взаємодії, застосовувати до них правила та забезпечувати високу швидкість цих операцій. Як правило, потужні апаратні МЕ, спроможні якісно і надійно виконувати свої функції, мають високу вартість та складніші у налаштуванні і обслуговуванні; у дешевих варіантів значно нижча швидкість взаємодії з вбудованим інтерфейсом, слабший функціонал, пріоритет віддається обробці мережевої активності. Прикладом апаратного МЕ в його найпростішій реалізації є домашній роутер, що з'єднує користувача через провайдера з мережею інтернет і володіє лише базовим функціоналом – обробляє мережеві з'єднання, фільтрує трафік, забезпечує обмежений режим доступу [20, с.83].

Програмний МЕ – це спеціалізоване програмне забезпечення, яке може бути розгорнуте як на певному обладнанні (комп'ютері, системному блоці, сервері і т. д.), так і у віртуальному режимі, тобто у вигляді віртуальної машини, розгорнутої в хмарі чи інфраструктурі. Для надійного захисту потрібно всі звернення мережі направити на опрацювання через МЕ. Дана опція МЕ дешевша, гнучкіша, проста в розгортанні, і, хоча швидкість і продуктивність поступаються апаратному МЕ, у переважній більшості є достатньо ефективною. Інтерфейс адміністрування в такому випадку реагує краще, ніж в апаратних МЕ найнижчого і середнього цінового сегмента. Якщо МЕ виконує контроль сеансів, то він може аналізувати трафік не тільки на підставі заданих адміністратором правил фільтрації, але й в «розумному» режимі, і здатний в поєднанні з правилами виявляти і блокувати аномальну активність.

1.3.2 Класифікація МЕ за об’єктом захисту

За об’єктом захисту можна виділити такі види МЕ:

- персональні або рівня окремого вузла, які захищають один ПК або вузол мережі;
- сегментні або рівня мережі, які захищають мережу або сегмент мережі;
- розподілені - захищають кілька мереж або сегментів мережі з допомогою окремих сегментних МЕ, об’єднаних в одну систему з допомогою єдиного центру управління [25, с.117].

1.3.3 Класифікація МЕ за рівнем роботи

За рівнем роботи виділяють МЕ:

- мережевого рівня;
- сеансового і прикладного рівня;
- рівня з'єднання.

1.3.4 Класифікація МЕ за способом фільтрації

За способом фільтрації, а саме ця функція і розглядається зазвичай як МЕ, розрізняють:

- МЕ з фільтрацією пакетів;
- шлюз рівня сеансу;
- МЕ зі збереженням стану;
- шлюз прикладного рівня (проксі-сервер).

1.4 Переваги і недоліки різних видів міжмережевих екранів.

Найпростішим в реалізації і найшвидшим МЕ є фільтруючий маршрутизатор або пакетний фільтр, зображений на рисунку 1.1 [7, с.90]. Це розташований між мережею Інтернет та внутрішньою мережею маршрутизатор

або працююча на сервері програма, налаштовані таким чином, щоб вхідні і вихідні пакети, порівнюючи кожен пакет даних з набором правил. Фільтрація пакетів здійснюється на підставі аналізу їх адрес, портів і протоколів. Таким чином, комп'ютери мережі під захистом МЕ отримують вільний доступ в Інтернет, проте основна частина доступу до них з Інтернету блокується.

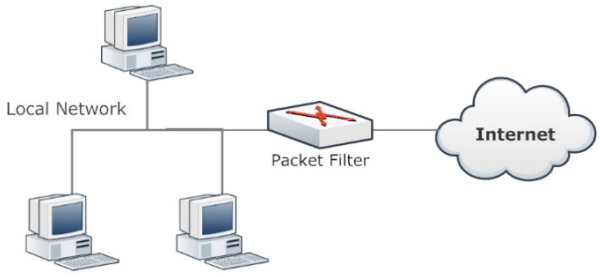


Рисунок. 1.1 - Фільтруючий маршрутизатор

В процесі фільтрації аналізуються такі поля заголовка пакету:

- IP-адреса відправника;
- IP-адреса одержувача;
- порт відправника (вихідний порт);
- порт одержувача (порт призначення);
- протокол, який використовується.

Фільтрація може бути реалізована по-різному для блокування з'єднання з певними хостами або портами. Є можливість блокувати з'єднання з конкретних адрес підозрілих або небезпечних хостів і мереж; деякі маршрутизатори як додатковий критерій фільтрації контролюють, з якого мережевого інтерфейсу маршрутизатора прийшов пакет.

Оскільки цей тип пристроїв підключається до кінцевих систем, вони спроможні захистити лише систему, в якій підключені, а не мережу загалом. Цей тип МЕ працює на мережному рівні моделі OSI. Оскільки він не враховує контекст або стан з’єднання, тому може бути схильний до атак типу IP-спуфінгу або фрагментації [1, с.106].

Пакетні фільтри можуть бути реалізовані в таких пристроях інфраструктури мереж:

- прикордонні маршрутизатори;
- операційні системи;
- персональні МЕ.

Перевагами фільтруючих маршрутизаторів є:

- незначний вплив на швидкість роботи мережі;
- застосування простого набору дозволяючих або забороняючих правил;
- підтримка більшістю маршрутизаторів;
- порівняно невисока вартість.

Пакетні фільтри забезпечують початковий ступінь безпеки на мережевому рівні. Вони дозволяють вирішувати значну частину проблем безпеки, як і багатофункціональні МЕ, але при значно менших витратах. Не в змозі забезпечити весь функціонал МЕ, пакетні фільтри є для останніх засобом реалізації корпоративних політик безпеки. Вбудовані в прикордонні маршрутизатори пакетні фільтри ефективні для розміщення на кордоні з частково довіреною мережею. За рахунок фільтрації небажаних протоколів через контроль доступу на рівні сесій і наступну передачу трафіка іншим МЕ для опрацювання даних на вищих рівнях стека протоколів вони спроможні заблокувати основні атаки.

На практиці пакетні фільтри в чистому вигляді зустрічаються рідко. До їх недоліків відносять:

- відсутність аутентифікації на рівні користувача;
- повна втрата захисту і доступу до комп’ютерів мережі при порушеннях в роботі пакетного фільтра;
- можливість обходу аутентифікації по IP-адресі шляхом її підміни;
- пакетні фільтри безсилі перед атаками авторизованих користувачів або запущеними в обхід екрану атаками;
- погано справляються з фрагментованими пакетами, оскільки у фрагментованих IP-пакетів заголовок TCP передається в першому

фрагменті, а пакетні фільтри обробляють тільки інформацію з заголовка TCP, всі фрагменти, які йдуть за першим, проходять без обмежень;

- вразливість для спуфінгу IP-адрес, тобто через фільтр зможуть пройти пакети, які відповідають критеріям зі списку ACL;
- не зберігають стан, а перевіряють кожен пакет окремо, при цьому стан з'єднання не враховується.

Шлюзи рівня сеансу моніторять TCP-з’єднання між мережами на рівні сеансу моделі OSI. Він перевіряє, чи є з’єднання довіреним, виходячи з рукостискання TCP, і відповідно або дозволяє, або блокує трафік на підставі цього. Оскільки не проводиться аналіз вмісту пакетів або програм, деякі види атак можуть пройти непоміченими.

МЕ з технологією SPI (інспекція пакетів зі збереженням стану) є найбільш універсальним і широко застосовуваним та додає у пакетний фільтр розуміння логіки протоколу транспортного рівня. Він переглядає стан, порт і протокол кожного з’єднання та фіксує інформацію про попередні пакети того ж самого з’єднання. Перевіряє на відповідність правилам безпеки заголовки та вміст пакетів. Для кожного отриманого пакета розшукується запис у таблиці станів і звіряється відповідність прапорців у заголовках пакета очікуваному стану. Зловмисник, наприклад, може створити пакет, у заголовку якого імітує належність до встановленого з'єднання. МЕ з відстеженням станів не знайде відповідний запис у таблиці і не пропустить його. Цей тип МЕ ефективніший у блокуванні складних DoS та DDoS атак [20, с.149].

Розділяючи слабкі й сильні сторони пакетних фільтрів, МЕ з аналізом стану вважаються більш безпечними, оскільки:

- пропускають пакети тільки зі встановленими з'єднаннями;
- не розривають TCP-з'єднання і є прозорими для клієнтів і серверів.

Шлюз мережевого рівня можна вважати системою трансляції адрес, оскільки він виключає пряму взаємодію між авторизованим користувачем і зовнішнім хостом. Після перевірки допустимості запитаного довіреним клієнтом сеансу він встановлює з'єднання та дублює пакети без фільтрації в обох напрямках. Шлюз очікує підтвердження зв'язку між користувачем і зовнішнім

хостом, перевіряючи запитуваний сеанс зв'язку на допустимість. Він може також підтримувати VPN-з'єднання для безпечного доступу до внутрішньої мережі зовнішніх користувачів.

Він виконує ще одну важливу функцію захисту, виступаючи як сервер-посередник, і здійснює трансляцію адрес, при якій відбувається перетворення внутрішніх IP-адрес в одну "надійну" IP-адресу. Ця адреса асоціюється з МЕ, з якого передаються всі вихідні пакети. У результаті виключається прямий контакт між внутрішньою (авторизованою) мережею і потенційно небезпечною зовнішньою мережею. IP-адреса МЕ стає єдино активною IP-адресою, яка потрапляє в зовнішню мережу, захищаючи таким чином внутрішні мережі від нападів типу підміни адрес [12, с.58].

На практиці більшість шлюзів мережевого рівня не є самостійними продуктами, а комбінуються зі шлюзами прикладного рівня.

На рисунку 1.2 [7, с.92] зображено МЕ прикладного рівня.

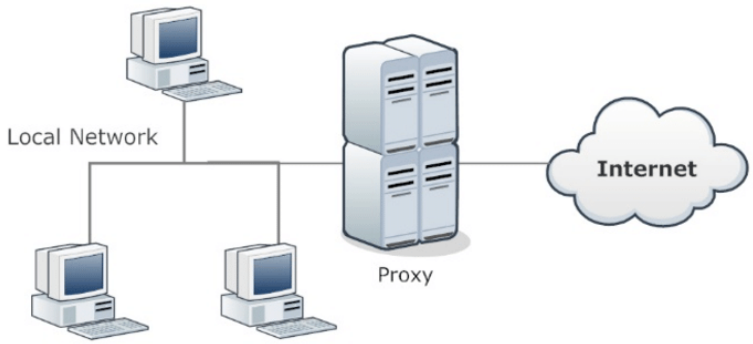


Рисунок 1.2 - МЕ прикладного рівня

МЕ сеансового і прикладного рівнів включають пакетну фільтрацію і, крім адресної інформації, можуть аналізувати дані пакетів на наявність потенційно небезпечних або атакуючих команд, структур, сигнатур. Завдяки чому їх можливості розширюються, наприклад, до фільтрації вірусних атак на етапі входу в систему на підставі БД сигнатур вірусів. Використовуючи БД сигнатур віддалених хакерських атак, можна відповідно відфільтровувати пакети.

Аналізуючи структуру даних пакета, можна застосовувати евристичні методи фільтрації на віруси.

Шлюз прикладного рівня (проксі-сервер) фільтрує інформацію на рівнях 3, 4, 5 і 7 базової моделі OSI. Більшість операцій з управління та фільтрації виконується програмами. Для отримання доступу до віддаленого сервера клієнт підключається до проксі-сервера, який і з'єднується з віддаленим сервером. Тому сервер бачить тільки з'єднання від проксі-сервера.

Одним з важливих компонентів концепції МЕ є аутентифікація - процес перевірки та підтвердження ідентичності користувача перед наданням йому доступу до певного ресурсу або сервісу. МЕ можуть вимагати від користувачів підтвердження своєї ідентичності перед отриманням доступу до ресурсів мережі. Це допомагає забезпечити безпеку та обмежити доступ до конфіденційної інформації.

Оскільки МЕ можуть централізовано керувати доступом в мережі, вони добре підходять для підключення програм або пристроїв посиленої аутентифікації. В мережі без МЕ із засобами посиленої аутентифікації небезпечний трафік TELNET або FTP може дістатися до систем. Без застосування хост-комп'ютерами заходів посиленої аутентифікації зловмисник може перехопити паролі та мережевий трафік з метою їх отримання.

Вищий рівень захисту можуть забезпечити шлюзи прикладного рівня, оскільки взаємодія із зовнішнім світом реалізується через прикладні повноважні програми-посередники, що повністю контролюють весь вхідний і вихідний трафік. Вони використовуються також для електронної пошти, Windows і деяких інших служб. Важливими їх перевагами є:

- невидимість структури мережі з глобальної мережі Інтернет;
- надійна аутентифікація та реєстрація;
- оптимальне співвідношення між ціною і ефективністю;
- прості правила фільтрації;
- можливість організації великого числа перевірок на рівні додатків, що знижує ймовірність злому з використанням "дірок" у програмному забезпеченні [5, с.133].

Недоліками шлюзів прикладного рівня є:

- нижча продуктивність у порівнянні з пакетними фільтрами (при використанні клієнт-серверних протоколів, як TELNET, використовується двокрокова процедура для вхідних та вихідних з'єднань);
- вища вартість.

МЕ із уніфікованим управлінням загрозами (UTM) поєднує функції МЕ зі станом з іншими службами безпеки, серед яких антивірус, IDS, IPS, фільтрація URL, VPN і хмарне управління. UTM позиціонується як зручне нескладне рішення для малого та середнього бізнесу.

Шлюзи наступного покоління NGFW можуть працювати не тільки на підставі протоколів і портів, але й на рівні додатків і функцій цих додатків і виходячи з аналізу цих показників, здійснювати фільтрацію трафіка, забезпечуючи високий рівень безпеки. У них є можливість більш гнучкого налаштування політики безпеки користувачів та налаштування кластеризації, важливих для захисту мереж великого бізнесу. Крім стандартних для МЕ модулів, вони містять додаткові модулі, призначені для налаштування міжмережевої взаємодії, серед яких контроль додатків, сервер точного часу, DPI, DLP, IPS, фільтрація URL та інші. Деякі МЕ надають технології систем виявлення вторгнень IDS, які можуть реагувати на атаки. Додатково в ПЗ МЕ можуть використовуватися технології нейромереж, здатні навчатися на певних типах інформації в процесі фільтрації для самостійного прийняття рішень щодо блокування/ пропуску пакетів або повідомлення адміністратора мережі [24, с.78].

МЕ нового покоління перевершують міжмережеві екрани зі збереженням станів за кількома важливими аспектами:

- точна ідентифікація, моніторинг і контроль поведінки в рамках програм;
- обмеження веб-трафіку і веб-додатків на основі репутації сайту;
- проактивний захист від інтернет-загроз;
- впровадження політик на основі користувача, пристрою, типу програми і профілю загроз;
- покращена продуктивність NAT, VPN і процесу контролю протоколу станів;

– використання інтегрованої системи запобігання вторгненням (IPS).

В даний час більшість компаній використовують МЕ наступного покоління (NGFW), щоб убезпечити себе від сучасного шкідливого ПЗ та атак на рівні додатків. Вважається, що шлюз NGFW має включати:

– інтелектуальний контроль доступу на основі стану;
– інтегровану систему запобігання вторгненням (IPS);
– поінформованість та контроль додатків, щоб бачити та блокувати ризиковані додатки;
– шляхи оновлення, щоб включати майбутні інформаційні потоки;
– методи для вирішення проблем безпеки, що еволюціонують;
– фільтрування URL на основі геолокації та репутації.

Орієнтовані на загрози МЕ поєднують всі можливості NGFW з технологіями просунутого виявлення та усунення загроз. Вони можуть:

– в режимі реального часу виявляти та нейтралізувати відомі та невідомі загрози;
– автоматично корелювати події безпеки та мережеву активність;
– використовувати глобальну розвідку щодо загроз для оновлення правил та політик;
– ізолювати заражені системи та відновлювати нормальну роботу [8, с.97].

2 ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ МЕ

2.1. Політика міжмережевої взаємодії

Політика міжмережевої взаємодії, поряд з іншими спеціалізованими політиками безпеки, такими, як політика віддаленого доступу, політика захисту паролів та інші є важливим інструментом побудови системи інформаційного захисту. Вона визначає основні аспекти обміну інформацією з іншими суб'єктами інформаційної діяльності, зокрема політику роботи МЕ та політику доступу до мережевих сервісів.

Відповідно повинні бути чітко ідентифіковані всі сервіси інформаційно-комунікаційної мережі, розписані їх допустимі адреси та правила функціонування. Потрібно також сформувати і довести до користувачів правила та процедури використання всіх сервісів.

Слід зазначити, що прийнята в організації політика міжмережевої взаємодії повинна бути реалістичною, тобто оптимальним співвідношенням між потребами користувачів у доступі для виконання їх завдань та забезпеченням достатнього рівня безпеки.

При формуванні політики роботи МЕ за основу слід взяти один з двох принципів:

- дозволено все, що явно не заборонено;
- заборонено все, що явно не дозволено [20, с.129].

Відповідно до цього вибору вибудовується логіка і реалізація МЕ та інших засобів захисту мережі.

2.2. Сегментація мереж

При під'єднанні внутрішніх мереж до глобальних перед адміністратором мережеві постають такі виклики:

- спроби несанкціонованого доступу з мережі Інтернет;

- необхідність приховати структуру мережі та її компонентів від зовнішніх користувачів та розмежувати доступ в обидві сторони.

Важливим засобом зменшення шкоди від вторгнення зловмисника в корпоративну IT-інфраструктуру є сегментація, тобто поділ мережі на менші сегменти, що діють як менші незалежні мережі. Вона базується на відокремленні користувачів і ресурсів мережі в ізольовані одна від одної групи. Доступ користувачам надається до окремих сегментів, а не до мережі в цілому. Обмін даними між цими групами контролюється або взагалі блокується відповідно до вимог політики безпеки організації. Якщо хакер зламав одну частину мережі, він не повинен автоматично мати доступ до всієї мережі. Сегментація мережі також може захистити від внутрішніх загроз.

Сегментація мережі може здійснюватися як фізично, так і логічно. Фізична сегментація передбачає поділ мережі на різні підмережі. Потім підмережі розділяються за допомогою фізичних або віртуальних МЕ. Логічна сегментація також передбачає поділ мережі на підмережі, але доступ до неї контролюється за допомогою VLAN або схем мережевої адресації. Фізичну сегментацію легше реалізувати, але зазвичай це дорожче, оскільки вимагає нової проводки та обладнання. Логічна сегментація є більш гнучкою та дозволяє вносити налаштування без зміни апаратного забезпечення.

Сегментація мережі є важливою частиною впровадження політики найменших привілеїв, відповідно до якої всім користувачам надається лише рівень доступу або привілеїв, необхідний для виконання їхньої роботи. Вона полегшує моніторинг мережі та відстеження користувачів під час їх доступу до різних областей, що також може допомогти виявити підозрілу поведінку законних користувачів.

Перед впровадженням сегментації мережі всі бізнес-активи класифікують за цінністю та ризиком. Активи з найбільш цінними даними, наприклад інформація про клієнтів, повинні зберігатися окремо і доступ до цього сегмента має бути під жорстким контролем. Активи, схожі за рівнем ризику та до яких часто звертаються ті самі користувачі, розміщують у тому ж сегменті. Це зменшує складність мережі та полегшує користувачам доступ до необхідних

даних, а також дозволяє масово оновлювати політики безпеки для подібних активів.

Основні сегменти підмереж такі:

- Відкритий (публічний сегмент), тобто сегмент з вільним доступом - доступні усім зовнішні мережі, що належать до глобального Інтернету;
- Закритий сегмент - внутрішні приватні мережі - домашня мережа, корпоративні та інші закриті мережі;
- Сегмент з обмеженим доступом - периметральні мережі, які з допомогою бастіонних хостів з посиленою безпекою протистоять атакам ззовні. Виконуючи роль своєрідного буфера між внутрішніми та зовнішніми мережами, вони також можуть вміщати захищені сервіси внутрішньої мережі, наприклад, web- та email-сервери, FTP, VoIP тощо. Таким чином можна отримати зони, безпечніші за зовнішні мережі, але менш безпечні, ніж внутрішні.

Розміщений на межі між довіреною та недовіреною мережею, МЕ створює точку проходження трафіку. Він опрацьовує дані на підставі спеціального набору правил. Перш ніж будь-який пакет досягне свого пункту призначення, він перевіряється МЕ. Якщо пакет відповідає набору правил, він досягає пункту призначення; інакше МЕ відкидає пакет.

2.3. Брандмауер Windows

У домашніх мережах, яким загрожують шкідливе ПЗ та злом даних, використовують вбудований у маршрутизатор апаратний МЕ. Додатково можна використовувати програмний МЕ на кожному пристрої, який підключається до домашньої мережі.

Брандмауер Windows - Microsoft Defender - це вбудований МЕ в Microsoft Windows. Він з’явився в Windows XP SP21. Попередньо інстальований й автоматично активований, він надає такі можливості захисту:

– Блокування небезпечних з'єднань: перевіряє вхідні та вихідні з'єднання і блокує небезпечний трафік. Правила для дозволу або блокування певних програм і портів можна налаштувати під свої потреби;
– Захист від несанкціонованого доступу: брандмауер контролює доступ до пристрою через мережу. Можна встановити правила для дозволу або блокування певних IP-адрес або діапазонів IP;
– Захист від атак на рівні мережі: брандмауер виявляє та блокує спроби атак на рівні мережі, такі як сканування портів або відправка шкідливого трафіку;
– Захист від шкідливих програм: брандмауер може блокувати спроби шкідливих програм встановити з'єднання з Інтернетом або взаємодіяти з іншими програмами;
– Захист від внутрішніх загроз: брандмауер контролює з'єднання між програмами на пристрої, щоб запобігти внутрішнім загрозам.

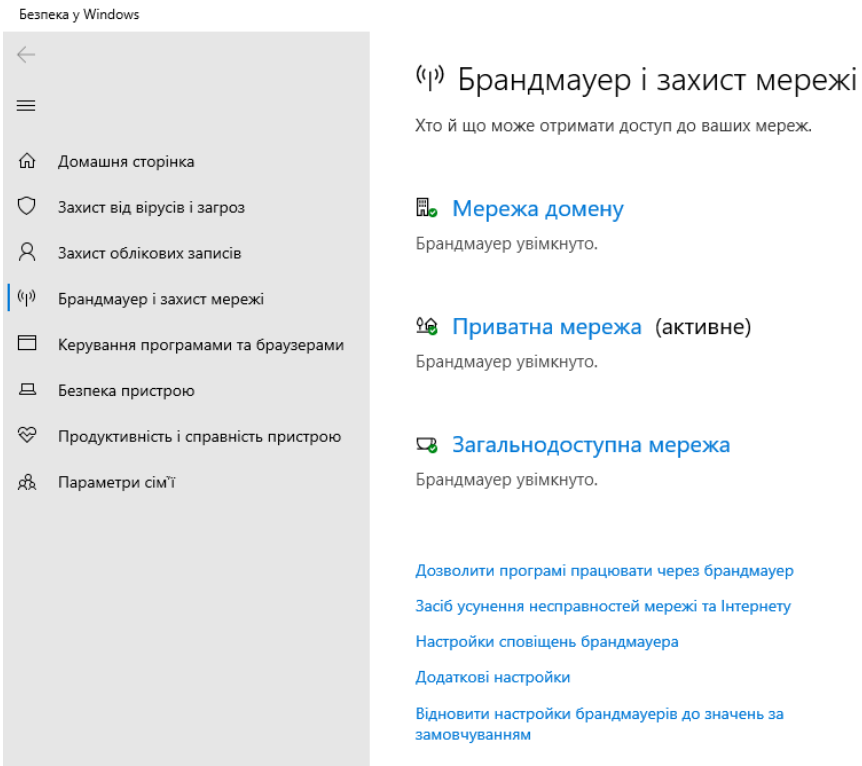


Рисунок 2.1 - Налаштування брандмауера Windows

Щоб увімкнути або вимкнути брандмауер Microsoft Defender, необхідно

– натиснути кнопку “Пуск” і вибрати “Параметри";

– у розділі “Конфіденційність і захист” обрати “Безпека Windows” > “Брандмауер і захист мережі”;
– обрати профіль мережі: “Мережа домена”, “Приватна мережа” або “Загальнодоступна мережа”;
– в розділі “Брандмауер Microsoft Defender” встановити параметр в режим "Вкл."

Вікно налаштування брандмауера Windows зображене на рисунку 2.1.

2.4 Основні схеми організації МЕ

Якщо припустити, що локальна мережа має чіткі кордони, то про будь-який хост можна сказати, перебуває він у локальній мережі чи ні. Ці кордони називають мережевим периметром. Також вважається, що існують явні точки входу в локальну мережу. Оскільки МЕ зазвичай розміщують на кордоні мережі, вважається, що МЕ має зовнішній і внутрішній, або ж відповідно незахищений і захищений інтерфейси. Однак стверджувати, що один інтерфейс є захищеним, а інший - ні, не зовсім коректно, адже політика МЕ може бути визначена в обох напрямках. Наприклад, вона може забороняти пересилати файли певного типу зсередини назовні мережевого периметра.

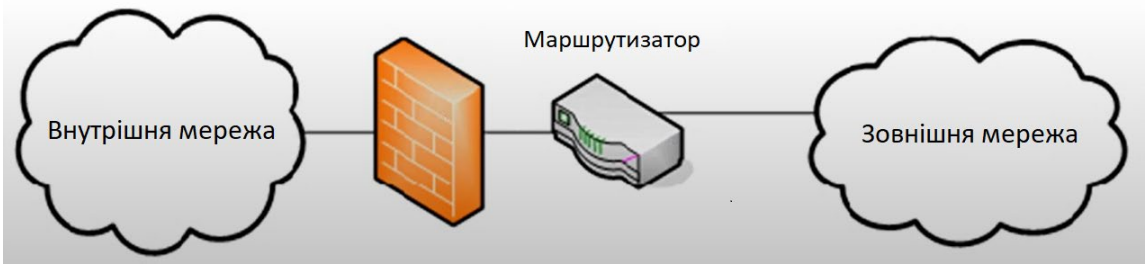


Рисунок 2.2 - Підключення МЕ з двома мережевими інтерфейсами

На рисунку 2.2 зображена найпростіша схема підключення МЕ з двома мережевими інтерфейсами, при якій МЕ встановлений перед внутрішньою інформаційною мережею і фільтрує всі пакети, що приходять із зовнішньої

мережі (наприклад, мережі Інтернет) та виходять з внутрішньої мережі, згідно встановлених правил.

Така схема підключення використовується найчастіше тоді, коли внутрішня мережа є однорідною. Для забезпечення додаткового захисту між прикладним шлюзом та мережею Інтернет зазвичай розміщують фільтруючий маршрутизатор. У результаті між прикладним шлюзом та маршрутизатором утворюється внутрішня екранована підмережа. Цю підмережу можна використовувати для розміщення доступних ззовні інформаційних серверів [22, с.149].

Якщо в інформаційній мережі є публічні ресурси, наприклад, поштовий сервер, веб-сервер чи інший публічний ресурс з базами даних і окрема внутрішня мережа, доцільно застосувати показану на рисунку 2.3 схему підключення МЕ з двома мережевими інтерфейсами при виділенні відкритого сегмента внутрішньої мережі:

Рисунок 2.3 - Схема підключення МЕ з двома мережевими інтерфейсами при виділенні відкритого сегмента внутрішньої мережі

У внутрішній мережі, захищеній МЕ, зосереджують офісну техніку, внутрішні бізнес-процеси тощо, відділивши її від відкритого сегмента з публічними ресурсами, який такого суворого захисту не потребує.

Найчастіше на практиці використовується схема, зображена на рисунку 2.4, при якій використовують додатково третій інтерфейс – так звану демілітаризовану зону (ДМЗ), в якій розміщені загальнодоступні сервіси, (web-сервер, email-сервер, ftp – сервер тощо), відділені таким чином від закритих, і до якої можуть застосовуватися певні фільтри. Завдяки цьому, порівняно з

попередньою схемою, відкритий сегмент мережі є більш захищеним. Потенційним недоліком даної схеми є те, що, якщо атакуючий пакет фізично потрапляє у менш захищений сегмент, залишається загроза потрапляння його у внутрішню мережу через наявність фізичного каналу зв'язку.

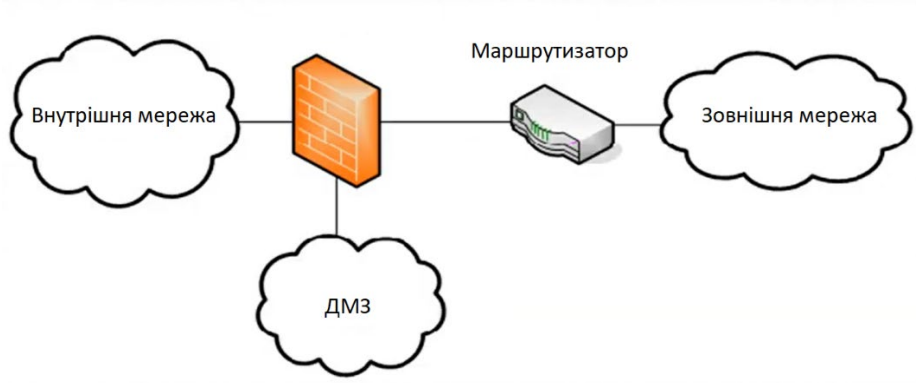


Рисунок 2.4 - Схема підключення МЕ з трьома мережевими інтерфейсами для захисту внутрішньої мережі і її відкритого сегмента

Отримати доступ до ресурсів ДМЗ можна з мереж різного рівня довіри - як з внутрішньої мережі, так і з зовнішньої. Логічно такі загальнодоступні сервіси відділяти в окремий сегмент від внутрішніх з можливістю вільного доступу з мережі Інтернет. Ідея такої структури побудови - з відокремленням ДМЗ в окрему частину мережі – полягає в тому, що навіть при проникненні зловмисника на сервер, локальна мережа, котра з нею з'єднується, залишається захищеною. Таким чином збитки від можливого злому будуть найменшими порівняно з іншими варіантами структури.

Для забезпечення повного захисту та підвищення рівня безпеки слід враховувати певні правила та вимоги:

- сервіси за межами ДМЗ повинні встановлювати з'єднання тільки до самої ДМЗ;
- сервіси всередині DMZ повинні підключатися до Інтернету лише з використанням проксі-сервера;
- більш захищені сервіси повинні виступати в ролі клієнта при здійсненні запиту з менш захищених зон.

Для забезпечення надійнішого захисту від несанкціонованого доступу обов’язковим є використання МЕ, зазвичай двох: перший використовується на зовнішньому периметрі та фільтрує трафік, який надходить виключно на ДМЗ, другий – на внутрішньому і фільтрує трафік із ДМЗ до внутрішньої мережі.

Ще вищий рівень захисту забезпечує розміщена на рисунку 2.5 схема підключення двох МЕ для захисту внутрішньої мережі і її відкритого сегмента, при якій ДМЗ захищена додатковим МЕ, який фільтрує направлені до неї пакети. Дана схема вимагає більших фінансових затрат, іншим її недоліком є ризик накладення правил фільтрації. При невірній конфігурації та наявності суперечностей між деякими правилами фільтрації двох МЕ можуть виникати колізії. Тому дуже важливим є узгодження правил фільтрації обох МЕ між собою.

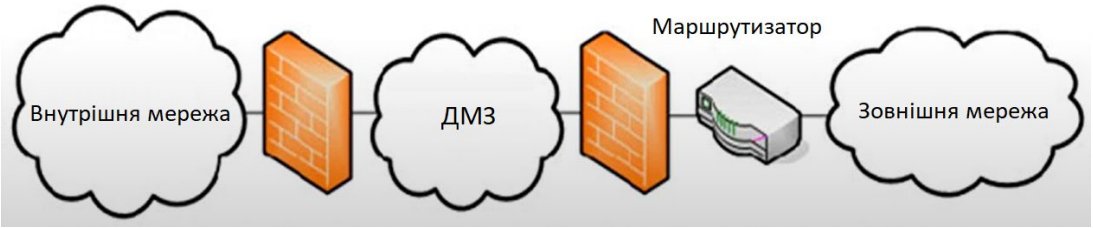


Рисунок 2.5 - Схема підключення двох МЕ для захисту внутрішньої мережі і її відкритого сегмента

Таким чином, топологія використання МЕ може бути різною – від одного до кількох МЕ в одній мережі, коли, наприклад, є основний МЕ, який захищає всю мережу від зовнішніх впливів, і додаткові форпости захисту, які знаходяться всередині мережі і захищають окремі спеціально виділені сегменти мережі, застосовуючи інший набір правил, більш суворих або ж детальніше налаштованих під конкретні задачі. Схема з виділенням ДМЗ і основної мережі може бути налаштована і всередині одного МЕ, тобто фізичне розділення мережі не є обов’язковим. Чим більше перешкод на шляху зловмисника і чим майстерніше вони налаштовані, тим важче буде йому проникнути і тим відповідно вищим буде рівень безпеки мережі.

2.5 Списки контролю доступу

Список контролю доступу (ACL) є важливим інструментом забезпечення роботи комп'ютерних мереж і мережевої безпеки з метою запобігання атак і управління трафіком. У ньому зафіксовано, хто саме може отримати доступ до об’єкта (файлу, програми, процесу), а також які операції дозволено або заборонено виконувати суб’єкту (користувачеві або групі користувачів). Це в основному набір правил, які спостерігають за вхідним і вихідним трафіком.

ACL і ME без збереження стану — це в основному однакові речі в тому сенсі, що вони лише обмежують, блокують або дозволяють усі пакети, які надходять від джерела до кінцевого призначення. Списки контролю доступу налаштовують в мережевих пристроях для управління доступом до ресурсів, таких як порти, IP-адреси, протоколи та служби. Якщо ACL не ввімкнено, то будь-якій формі трафіку дозволено входити або виходити, таким чином відкритий доступ для небажаного і небезпечного трафіку.

ACL встановлюються на інтерфейсах маршрутизаторів та комутаторів для фільтрації трафіку. Наприклад, можна дозволити або заборонити певні IP-адреси або порти. Вони також використовуються для захисту від атак, таких як DDoS або переповнення буфера. В ME ACL використовуються для контролю трафіку між мережами. Вони дозволяють або блокують певні типи з’єднань (наприклад, HTTP, SSH, SMTP). Можна налаштувати фаєрвол так, щоб дозволити доступ лише від певних IP-адрес або мереж. Вони визначають, хто може підключатися до VPN і які ресурси вони можуть використовувати, а також можуть бути налаштовані на серверах для обмеження доступу до файлів, баз даних або веб-сервісів. Наприклад, можна дозволити доступ до веб-сайту лише з певних IP-адрес. Загалом, ACL допомагають забезпечити безпеку, контроль та ефективне використання ресурсів в мережах.

Розрізняють такі види ACL:

- Стандартні:
  1. Визначають доступ на основі джерела (IP-адреси);
  2. Зазвичай використовуються для фільтрації трафіку на роутерах;

3. Нумеруються від 1 до 99 або від 1300 до 1999.

- Розширені:
  1. Визначають доступ на основі джерела та призначення (IP-адреси, порти, протоколи);
  2. Використовуються для більш детальної фільтрації трафіку;
  3. Нумеруються від 100 до 199 або від 2000 до 2699.
- Іменовані:
  1. Можуть мати власні назви замість номерів;
  2. Використовуються на комутаторах та фаєрволах.
- ACL для керування VTY-лініями: використовуються для обмеження доступу до консольних та Telnet-сесій на маршрутизаторах;
- ACL для керування SNMP: використовуються для обмеження доступу до SNMP-запитів.

Список ACL є послідовним переліком правил, які щось дозволяють або забороняють, відомих як записи контролю доступу (ACE). Записи ACE також називаються операторами списків управління доступу ACL. Записи ACE можна створювати для виконання фільтрації трафіку на основі певного критерію, наприклад адреси джерела або адреси призначення, протоколу і номера порту.

Стандартні списки ACL обробляють пакети, перевіряючи поле IP-адреси джерела і IP-заголовок. Такі списки ACL використовуються для фільтрації пакетів тільки на підставі інформації про джерело.

В розширених списках ACL пакети перевіряються на основі інформації про джерело та адресу призначення. У порівнянні зі стандартними розширені списки ACL надають більш гнучкі можливості по управлінню доступом до мережі.

2.6 Налаштування ACL у Windows Defender Firewall

Windows Defender Firewall (WDF) — це безпековий модуль, включений до складу операційної системи Windows, який допомагає захистити комп'ютер від небажаного мережевого трафіку. Його можливості такі:

– Фільтрація мережевого трафіку за допомогою правил, які можуть бути налаштовані користувачем. Це дозволяє заборонити або дозволити доступ до певних мережевих ресурсів або додатків;
– Заборона або дозвіл доступу до мережі для певних додатків або користувачів;
– Фільтрація трафіку за протоколами TCP, UDP, ICMP та ін;
– Виявлення та блокування шкідливих програм (віруси, троянці та ін.);
– Моніторинг та звітність про мережевий трафік, що допомагає виявляти та аналізувати потенційні загрози;
– Інтеграція з іншими безпековими інструментами, такими як Windows Defender для більш ефективного захисту комп'ютера;
– Підтримка різних мережевих інтерфейсів (Ethernet, Wi-Fi та ін.);
– Регулярні оновлення та коригування з метою виявленню нових загроз та покращення безпеки комп'ютера;

У цілому, Windows Defender Firewall є важливим інструментом для захисту комп'ютера від несанкціонованих доступів та шкідливих програм, і його налаштування та коригування можуть бути корисними для забезпечення високого рівня безпеки. На рисунку 2.6 зображено вікно налаштування типу правила списку контролю доступу. Обрано спеціальний тип правила.

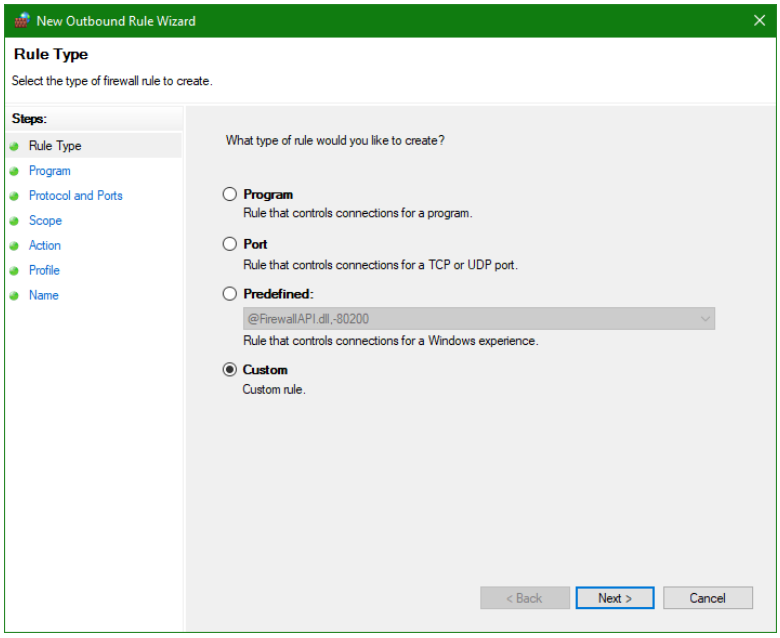


Рисунок 2.6 - Вікно налаштування типу правила

Рисунок 2.7 показує наступну дію – налаштування діапазону IP-адрес, з’єднання з якими буде заборонено.

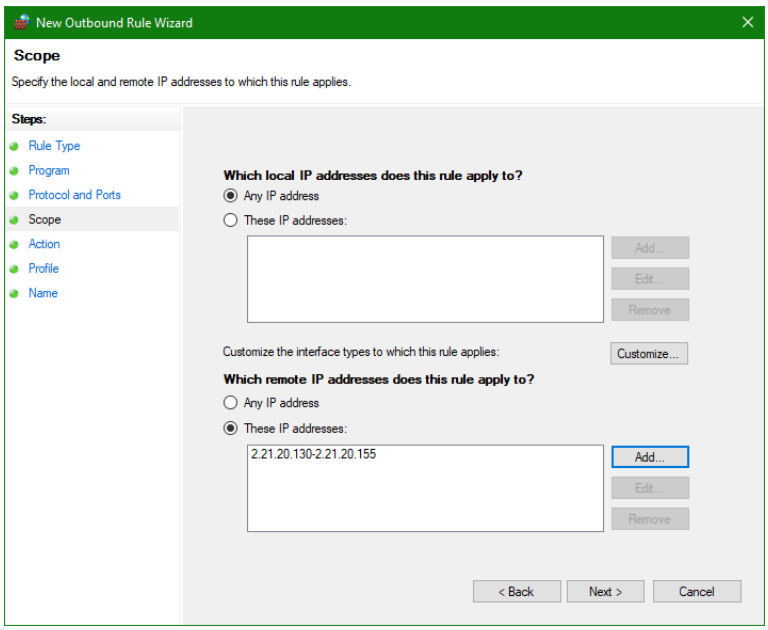


Рисунок 2.7 – Вікно налаштування правила для програми

На рисунку 2.8 відображено вибір однієї з трьох дій для правила – блокувати з’єднання. Інші дві дії – дозволяти з’єднання без винятків або дозволяти лише тоді, коли воно безпечне.

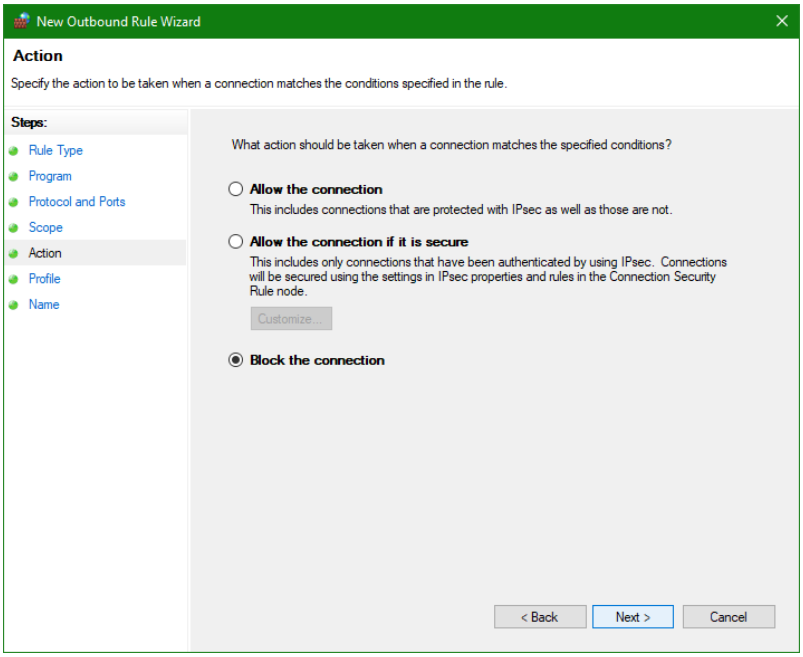


Рисунок 2.8 – Вікно вибору дії для правила

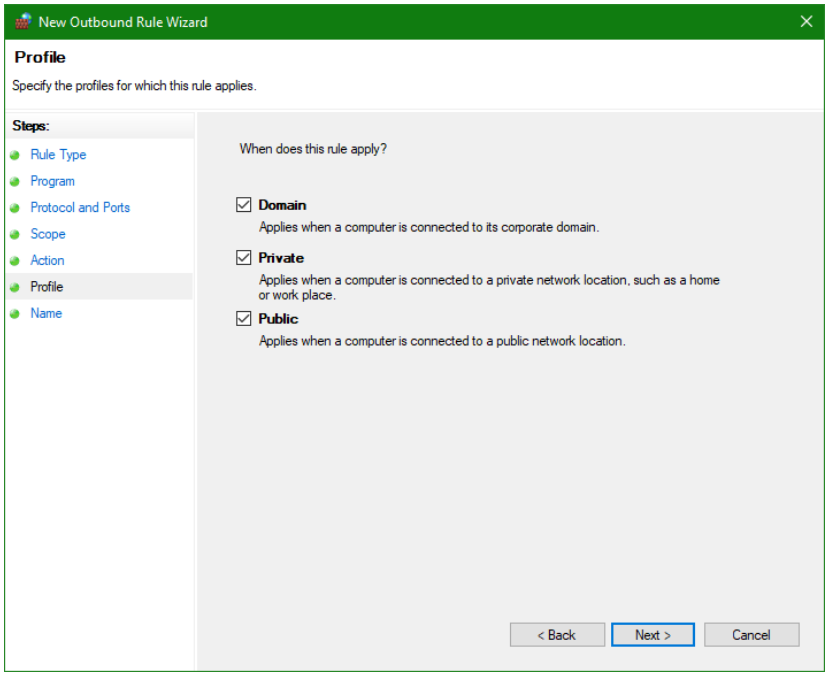


Рисунок 2.9 – Вікно вибору профілю застосування правила

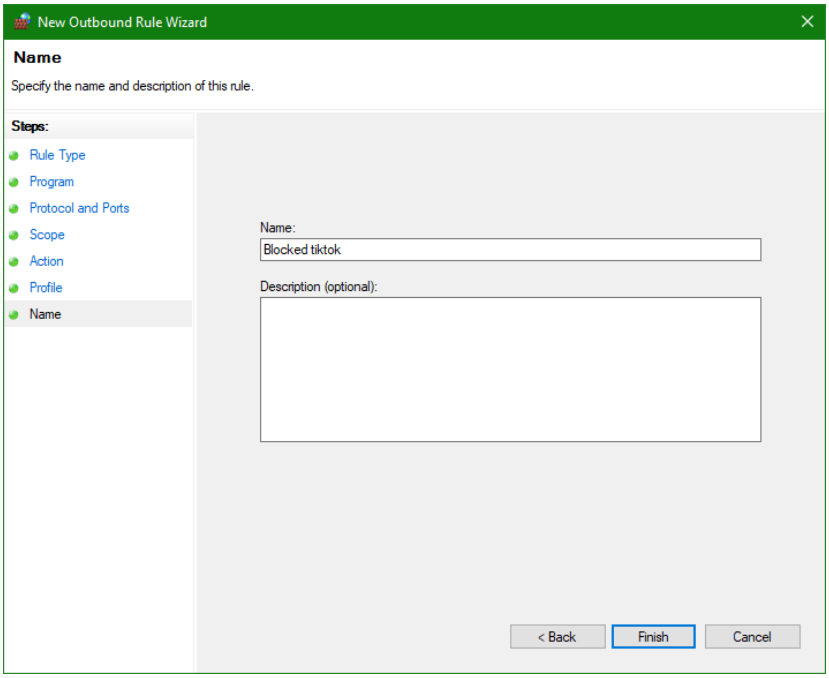


Рисунок 2.10 – Вікно найменування та опису правила

На рисунку 2.9 відображено вибір усіх можливих профілів застосування правила - домену, приватної та публічної мережі. Рисунок 2.10 показує вікно найменування та опису правила, а рисунок 2.11 – список правил контролю доступу з новоствореним правилом.

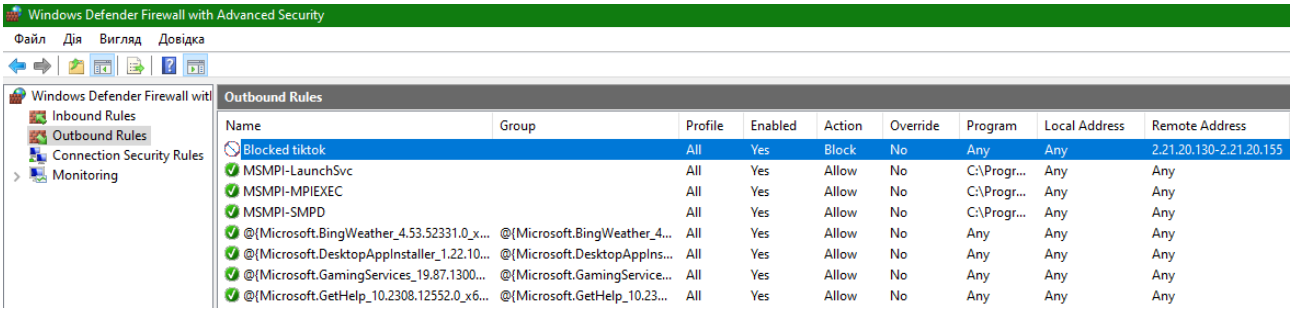


Рисунок 2.11 – Список правил контролю доступу

На рисунку 2.12 відображено результат практичного застосування щойно створеного правила блокування з’єднання з веб-сайтом TikTok – повідомлення про блокування підключення:

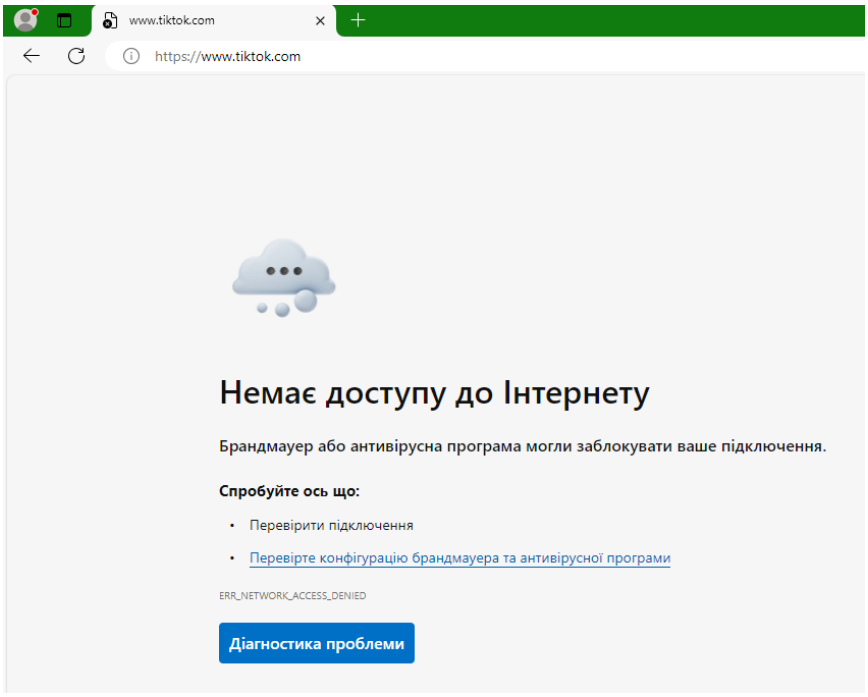


Рисунок 2.12 – Повідомлення про блокування підключення

3 НАЛАШТУВАННЯ МЕ НА ОБЛАДНАННІ CISCO

3.1 Вибір засобу реалізації

Для демонстрації особливостей налаштування МЕ типового невеликого підприємства прийнято рішення використати симулятор Cisco Packet Tracer. Це створена компанією Cisco програма для відтворення роботи комп'ютерних мереж і відповідного обладнання: роутерів, комутаторів, серверів, ПК та ін. З його допомогою можна отримати досвід в налаштуванні реальної мережі з необмеженою кількістю пристроїв. Для налаштування обладнання виконується внесення команд в операційну систему Cisco IOS, графічний веб-інтерфейс, команди та графічне меню операційної системи. В Packet Tracer режим віртуалізації дає можливість користувачу відстежити переміщення пакетів даних та отримати повну інформацію про них на всіх пристроях мережі. За допомогою симулятора можна виявити слабкі місця, несправності та надійність мережі.

До переваг симулятора відносять:

- можливість моделювання фізичної і логічної топології;
- зрозумілий графічний інтерфейс;
- наглядне зображення всіх пристроїв і процесів у мережі;
- інтерактивність;
- можливість налаштовувати та тестувати різноманітні аспекти мережевого середовища.

Хоча Cisco Packet Tracer підтримує імітацію лише власного обладнання та доступний для завантаження лише для інструкторів, студентів та адміністраторів Мережевої академії Cisco, його можливостей цілком достатньо для побудови топології мережі умовного невеликого підприємства, демонстрації особливостей налаштування МЕ та досягнення поставленої мети кваліфікаційної роботи.

3.2 Побудова топології мережі

На підставі аналізу основних схем організації інформаційних мереж була побудована логічна схема комп'ютерної мережі невеликого підприємства, наведена на рисунку 3.1.

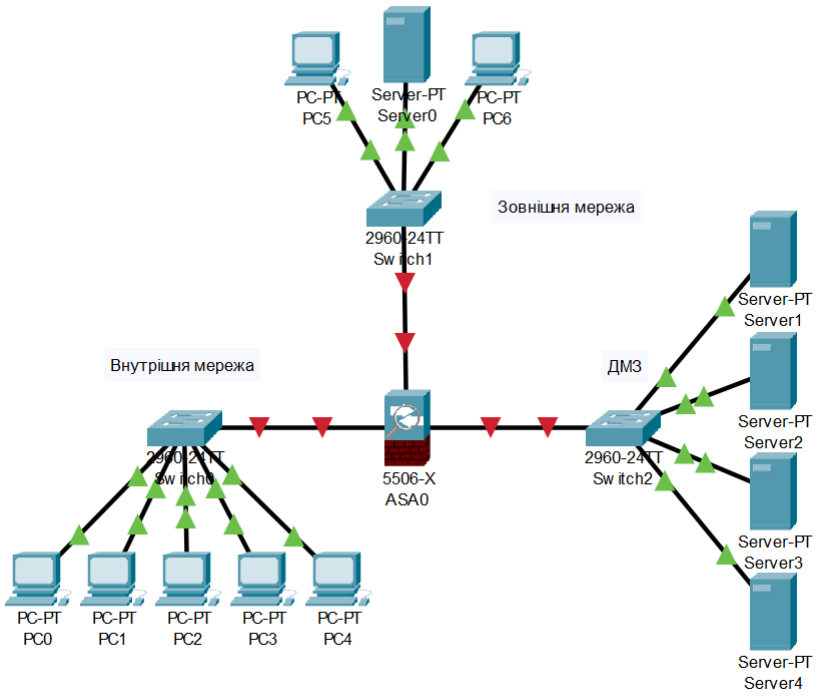


Рисунок 3.1 – Топологія мережі підприємства

Як видно з рисунка, уся мережа розділена на три підмережі – зовнішню, внутрішню та демілітаризовану зону. Найбільш захищеною, або довіреною є внутрішня (приватна) мережа, тоді як зовнішня (публічна) мережа є недовіреною. Статус демілітаризованої зони, так званої серверної ферми, є проміжним – вона лише частково довірена. Відповідно до дизайну мережі МЕ буде мати три інтерфейси.

Трафік з внутрішньої мережі дозволений без обмежень або з мінімальними обмеженнями. Інспектований трафік, що повертається з мережі ДМЗ або зовнішньої мережі у внутрішню мережу, теж дозволений. Якщо трафік з ДМЗ у внутрішню мережу зазвичай блокується, то у зовнішню мережу він дозволяється вибірково, відповідно до вимог. Трафік із зовнішньої мережі у ДМЗ, а тут

розміщені сервери DNS, DHCP, а також web- та email-сервери, дозволяється вибірково і інспектується. Зворотній трафік з ДМЗ у зовнішню мережу дозволяється динамічно. Трафік із зовнішньої мережі у внутрішню мережу блокується.

Оскільки для проектування мережі використовується симулятор Cisco Packet Tracer, для формування інформаційної мережі було обране обладнання Cisco Systems на підставі його характеристик. З метою організації безпечного доступу в Інтернет було прийнято рішення встановити ME Cisco ASA 5506-X, зображений на рисунку 3.2. Він забезпечує високий рівень захисту від мережевих загроз завдяки таким можливостям, як:

- глибока перевірка мережі;
- аналіз окремих потоків;
- безпека підключень за рахунок оцінки захищеності кінцевих пристроїв;
- підтримка передачі голосових і відеоданих через VPN.

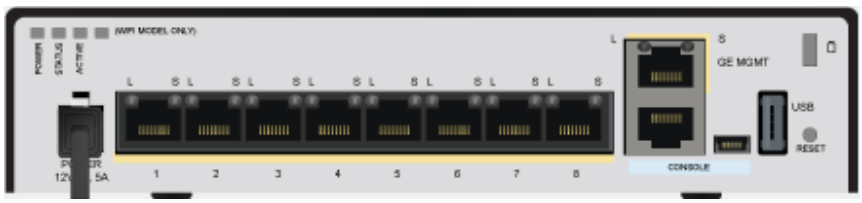


Рисунок 3.2 – Маршрутизатор Cisco ASA 5506-X

Мережа підприємства включає також робочі станції PC-PT, сервери, комутатори та лінії зв’язку.

3.3. Налаштування конфігурації ME Cisco ASA 5506-X

Для виконання функцій захисту мережі пристрій Cisco ASA 5506-X потрібно налаштувати за допомогою таких основних команд, як interface, nameif, security-level, ip address.

Для ідентифікації типу апаратних засобів, встановлення параметрів продуктивності та ініціалізації інтерфейсів використовується команда interface.

Для присвоєння імені інтерфейсам ASA використовується команда nameif. Команда ip address присвоїє ip-адресу кожному з інтерфейсів ME.

Рівень безпеки інтерфейсу прописують з допомогою команди security-level. Найнижчий рівень безпеки 0, найвищий – 100, а для частково довіреної мережі його встановлюють на рівні від 50 до 70.

На рисунку 3.3 показано результат базового налаштування зовнішнього («outside»), внутрішнього («inside») та інтерфейсу демілітаризованої зони («dmz»). Зокрема, було сконфігуровано назву, логін і пароль, назви інтерфейсів, ip-адреси та рівень безпеки.

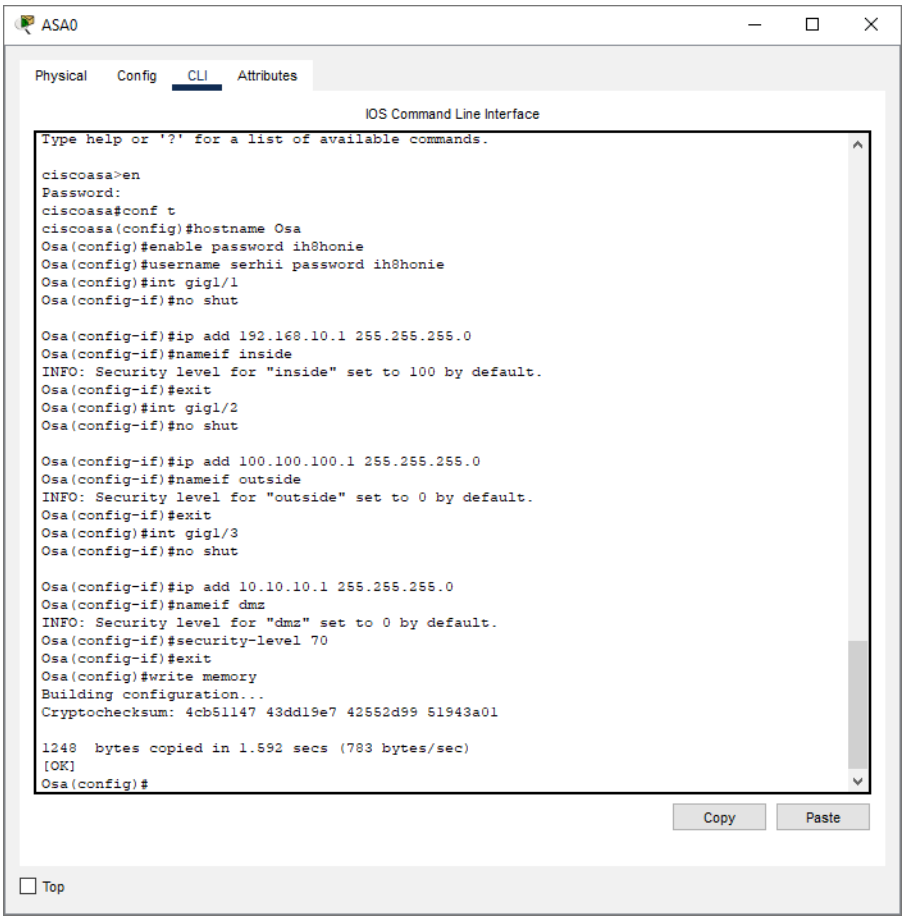


Рисунок 3.3 – Налаштування інтерфейсів

Наступним кроком є налаштування DHCP-сервера для внутрішньої мережі, зокрема діапазону ip-адрес, а також DNS-сервера. Результат наведено на рисунку 3.4.

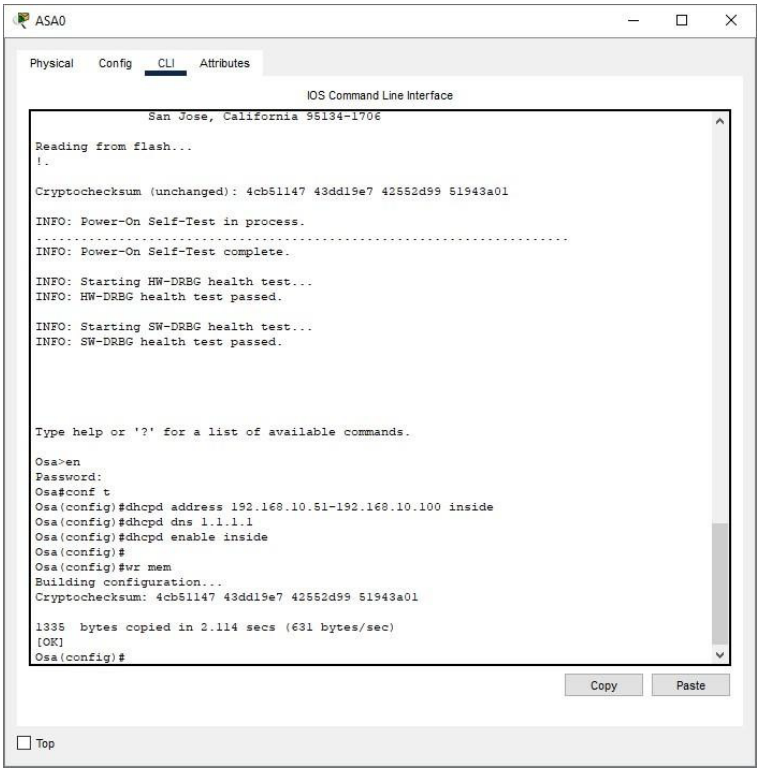


Рисунок 3.4 - Налаштування DHCP-сервера

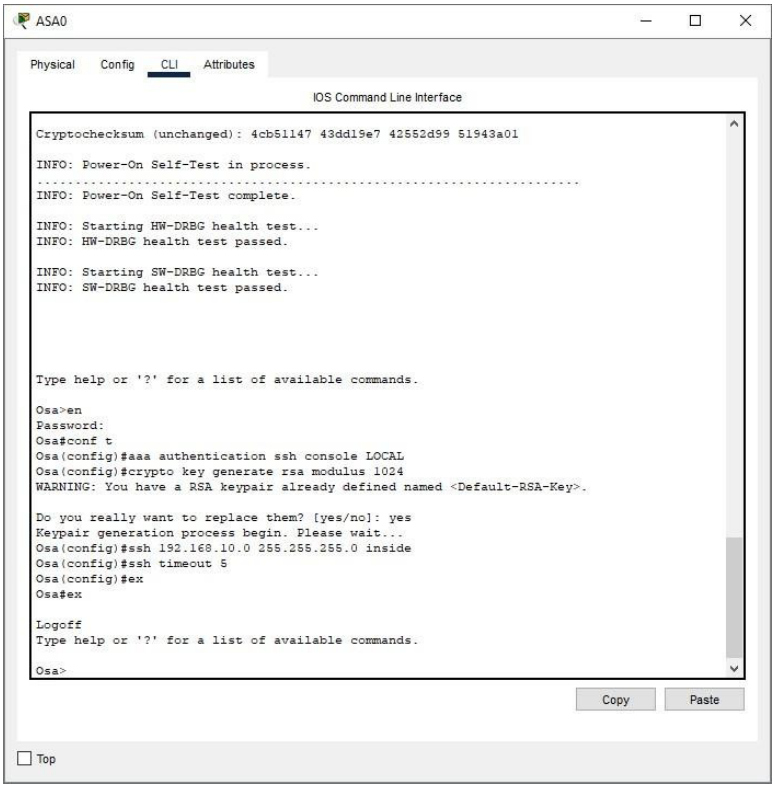


Рисунок 3.5 - Налаштування протоколу SSH

На рисунку 3.5 відображене налаштування локальної аутентифікації та необхідного для надання віддаленого доступу комп’ютерам внутрішньої мережі

протоколу SSH. Після цього було налаштовано трансляцію мережевих адрес (NAT), результат показано на рисунку 3.6:

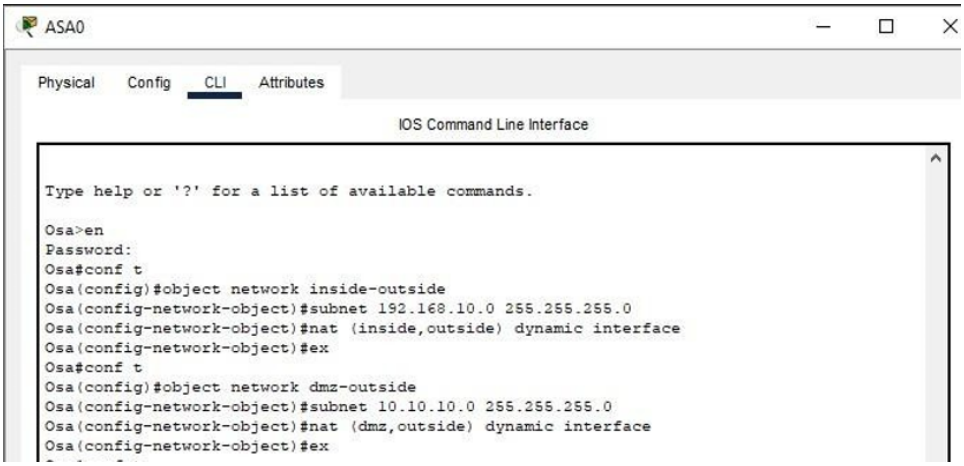


Рисунок 3.6 - Налаштування трансляції мережевих адрес

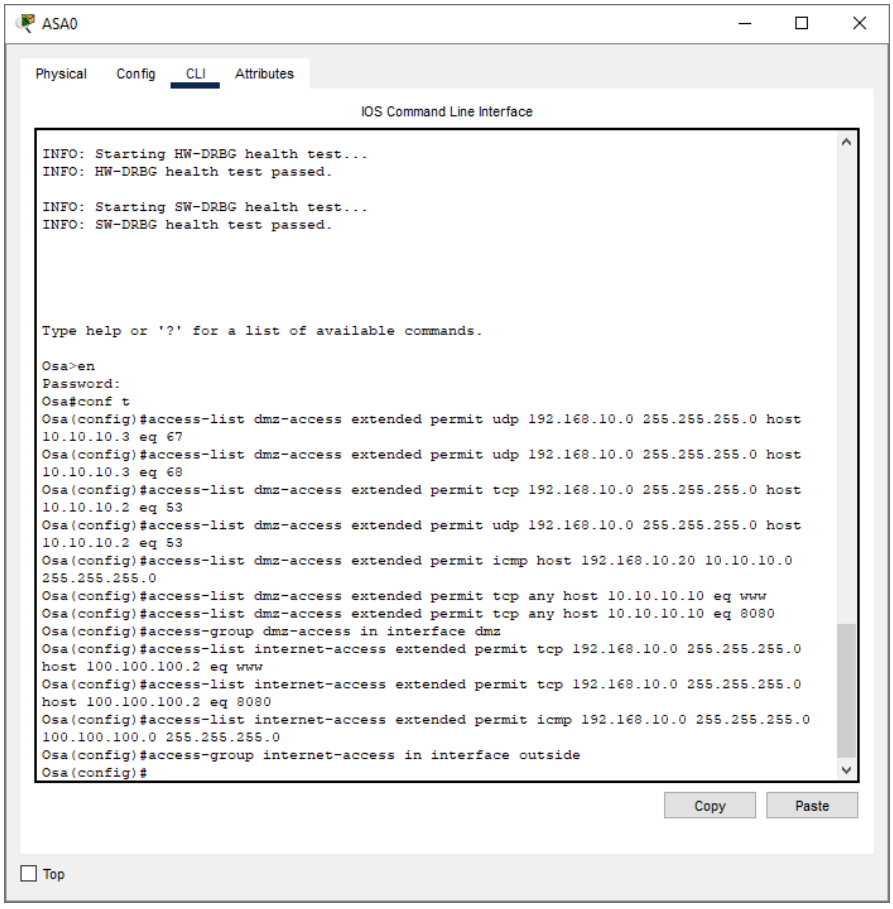


Рисунок 3.7 – Налаштування списків контролю доступу

На рисунку 3.7 відображена налаштування списків контролю доступу, зокрема надано доступ з внутрішньої зони до DHCP та DNS-серверів зони ДМЗ. Дозвіл виконувати перевірку пінгу зони ДМЗ надано виключно робочій станції адміністратора мережі PC-4. Всім станціям надано доступ до сервера зовнішньої мережі, а також до web-сервера.

Для перевірки налаштування проведені перевірки пінгу, результат яких відображений на рисунку 3.8.

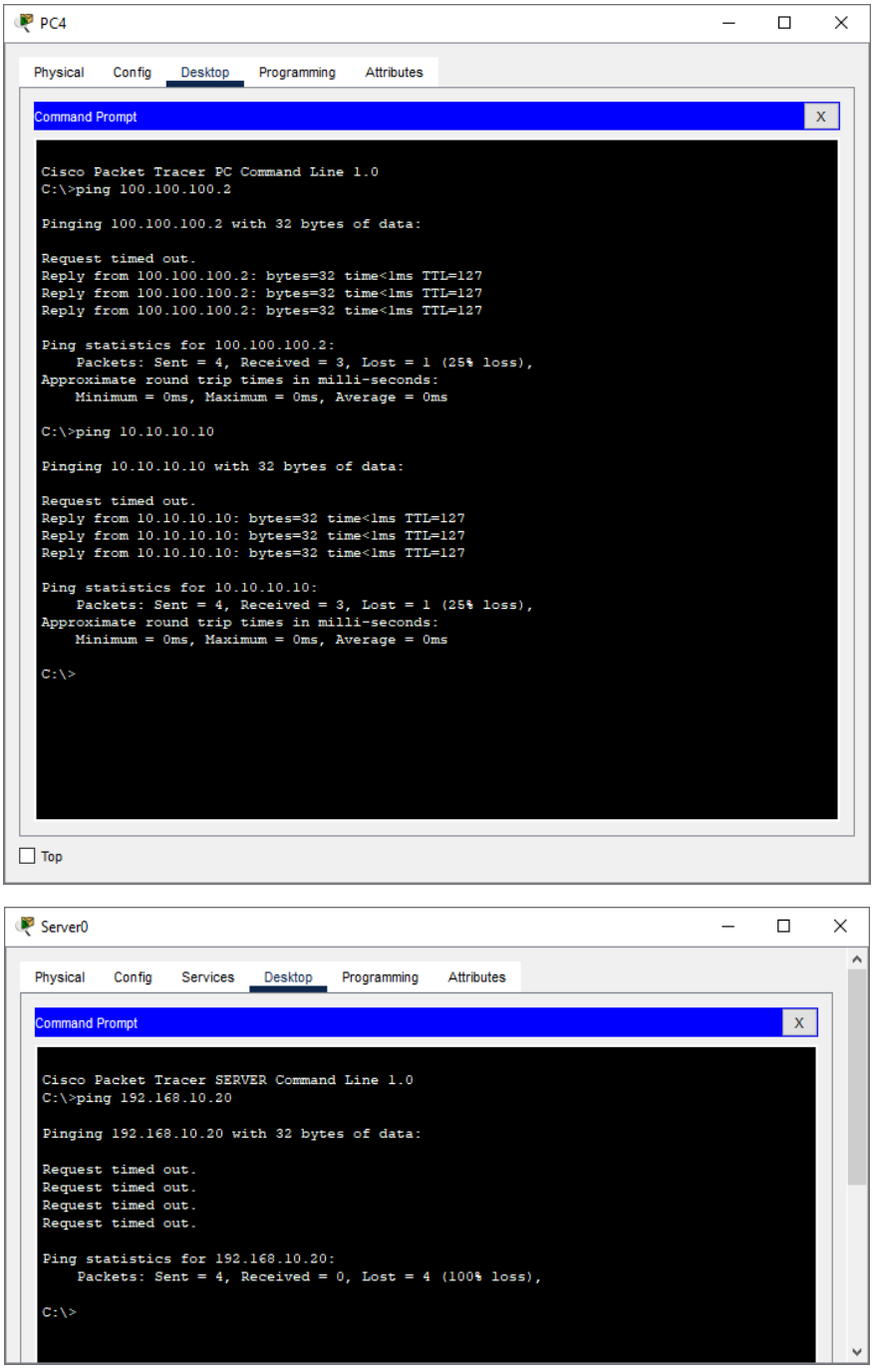


Рисунок 3.8 – Результати перевірок пінгу

3.4 Рекомендації по застосуванню МЕ

Незважаючи на те, що МЕ не в змозі убезпечити в повному обсязі сучасні ІКС, вони є важливою частиною архітектури інформаційної безпеки. Сучасні МЕ відрізняються за можливостями фільтрації трафіку, охоплення рівнів моделі OSI та використанням супутніх безпекових технологій. Залежно від топології, масштабу та потреб користувачів мережі або пристрою, найкраще спрацює різний тип або поєднання МЕ та інших мережевих пристроїв.

Для найбільш ефективного використання МЕ важливо:

- провести аналіз усіх ризиків і потреб користувачів;
- розробити оптимальні політики МЕ та міжмережевої взаємодії;
- розуміти і враховувати специфіку різних типів та технологій МЕ;
- сформувати відповідну до потреб безпеки топологію мережі;
- розробити оптимальний набір правил;
- налаштувати МЕ як інтегрований елемент безпекової інфраструктури;
- відслідковувати ефективність МЕ і при потребі вносити зміни в набір правил;
- регулярно оновлювати ПЗ або прошивку МЕ;
- постійно моніторити звіти і журнали МЕ в пошуках порушень та аномалій.

Таким чином, в сучасних умовах важливо постійно керувати політиками, архітектурою та іншими компонентами МЕ.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1. Ергономічні проблеми безпеки життєдіяльності.

Забезпечення безпеки життєдіяльності людини - складна науково-технічна, політична, економічна та соціальна проблема. Це одна з найголовніших потреб людини, необхідна умова повноцінного існування особи, суспільства, держави. В умовах високого рівня інформатизації суспільства та технічного оснащення праці, комплексної механізації та автоматизації виробництва актуальною є проблема найбільш доцільного поєднання живої праці та засобів виробництва, їх найефективніше застосування за умови збереження здоров’я та високої працездатності працівників.

Оптимізацією взаємовідносин в системі «людина - машина - середовище» (далі – ЛМС) займається ергономіка - комплексна наука, що вивчає людину в конкретних умовах її життєдіяльності з метою забезпечення максимальної ефективності цієї діяльності, безпеки та комфорту людини [10, с.147]. Також це набір міжнародних стандартів щодо умов праці. Поняття "ергономіка" походить від грецьких слів "ергон" (робота) і "номос" (закон), що можна перекласти як "закони роботи". Основна мета ергономіки - створити умови, в яких людина відчуватиме себе комфортно і зможе працювати без зайвого напруження та ризику для здоров'я.

Ергономіст вивчає проблеми оптимального розподілу та узгодженості функцій між людиною, машиною й виробничим середовищем, проектує процес діяльності людини, обґрунтовує оптимальні вимоги до засобів та умов праці, розробляє методи їх урахування при створенні та експлуатації техніки, яка обслуговується людиною. Раціональне поєднання можливостей людини, характеристик машин і відповідний розподіл функцій всередині системи суттєво підвищує її ефективність, обумовлює оптимальне використання людиною технічних засобів за їх призначенням.

Основними завданнями ергономіки є:

- вивчення умов праці;

- виявлення конструктивних недоліків виробничого обладнання;
- оцінка організації робочих місць з точки зору забезпечення нормальної робочої зони, допустимих швидкостей, траєкторій, кількості рухів і зусиль, необхідних для обслуговування виробничого обладнання;
- вивчення інформаційної взаємодії оператора й машини.

Ергономіка є складним симбіозом фізіології, гігієни, психології, антропології, біомеханіки та технічних наук, які вирішують конкретні проблеми для підвищення якості та надійності характеристики системи ЛМС.

Ергономіка вивчає людину в конкретних умовах її діяльності на виробництві, щоб виявити можливі шляхи вдосконалення знарядь, умов та процесу праці і має на меті якнайповніше врахувати можливості й особливості людини при експлуатації нею машин і механізмів. Основа ергономіки — це комплексний системний підхід з дослідження того чи іншого об'єкта, тому й методи ергономічних досліджень мають комплексний системний характер. Специфічним предметом ергономічних досліджень є не відокремлена техніка, не тільки людина як суб'єкт виробництва, не окреме середовище, а система ЛМС, всі елементи якої розглядаються в єдності й взаємодії з кінцевою метою узгодженості фізичних і психічних можливостей людини, її естетичних смаків та інших якісних показників з параметрами сучасних технічних засобів і виробничого середовища.

Види ергономічних вимог до організації трудових процесів та робочих місць представлені на рисунку 4.1 [22, с.77].

Економічні вимоги ергономіки передбачають підвищення технічного оснащення праці, вибір оптимальної технології, найповніше використання технологічного обладнання, обґрунтування оптимального ритму і темпу праці та раціональну організацію робочого місця.

Психофізіологічні вимоги ергономіки передбачають встановлення відповідності між енергетичними, швидкісними, зоровими та іншими фізіологічними особливостями людини та елементами технологічного процесу виробництва, зниження нервово-емоційних напружень та фізичних навантажень, обґрунтування оптимальних режимів праці та відпочинку.

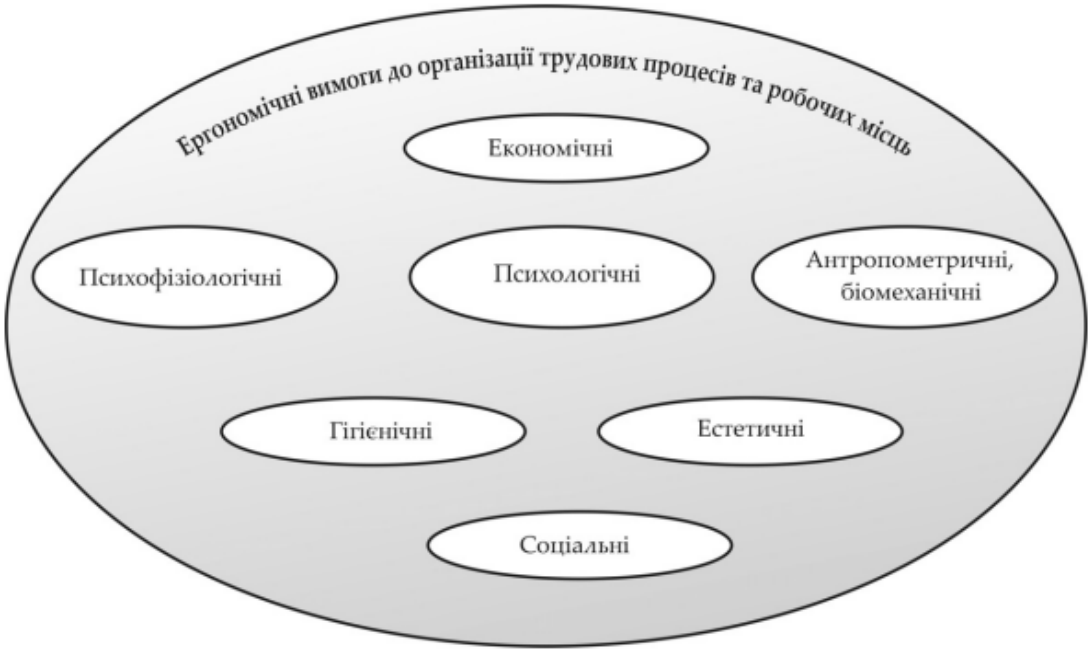


Рисунок 4.1 – Ергономічні вимоги до організації трудових процесів та робочих місць

Психологічні вимоги ергономіки передбачають встановлення відповідності між спадковими і набутими рефлексами, можливостями пам'яті і мислення та елементами технологічного процесу виробництва.

Антропометричні та біомеханічні вимоги ергономіки передбачають встановлення відповідності між знаряддями праці та розмірами та масою тіла людини, силою і напрямком рухів.

Гігієнічні вимоги ергономіки передбачають забезпечення комфортних метеорологічних умов середовища, оптимального фізико-хімічного складу повітря, належних рівнів освітленості, виробничого випромінювання, шуму та вібрації.

Естетичні вимоги ергономіки передбачають встановлення відповідності між естетичними потребами людини та художньо-конструкторським оформленням робочих місць та виробничого середовища.

Соціальні вимоги ергономіки передбачають підвищення змісту праці, творчої активності працівника, ефективності управління виробничими процесами та персоналом [21, с.62].

4.2. Вимоги ергономіки до організації робочого місця оператора ПК, агрегата.

Використання у різноманітних сферах діяльності людини персональних комп'ютерів (ПК) має супроводжуватися урахуванням норм ергономічної безпеки користувачів ПК, яку регламентують такі нормативні документи:

- Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями, затверджені Наказом Міністерства соціальної політики України № 207 14.02.2018р.;
- ДСанПІН 3.3.2-007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно обчислювальних машин, затверджені Постановою Головного державного санітарного лікаря України № 7 10.12.1998р.;
- ДСТУ 7234:2011. Дизайн і ергономіка. Обладнання виробниче. Загальні вимоги дизайну та ергономіки, затверджені наказом Держспоживстандарту України від 02.02.2011 р. № 37;
- ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги, затверджені наказом ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» 21.12.2015 № 204;
- ГОСТ 22269-76. Система «людина - машина». Робоче місце оператора. Взаємне розміщення елементів робочого місця. Загальні ергономічні вимоги.

Найменшою одиницею, де наявні усі елементи системи ЛМС (предмет праці, засоби праці та суб'єкт праці) є робоче місце - це зона простору, де відбувається трудова діяльність одного працівника чи групи працівників, що оснащена необхідним устаткуванням: засобами відображення інформації, органами керування та допоміжним обладнанням.

До робочого місця ставляться такі вимоги:

- достатній робочий простір, який дає змогу працюючій людині здійснювати необхідні рухи та переміщення;

- достатні фізичні, зорові та слухові зв'язки між людиною та обладнанням, а також між людьми під час виконання спільного трудового завдання;

- необхідний рівень освітлення;

- допустимий рівень шуму, і вібрацій та інших шкідливих факторів, які генерує обладнання місця праці та інші джерела;

- наявність необхідних засобів захисту;

- оптимальне розташування робочих місць, а також безпечні та достатні проходи для працюючих людей [18].

Організація робочого місця передбачає:

- правильне розміщення робочого місця у виробничому приміщенні;
- вибір ергономічно обгрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;
- раціональне компонування обладнання на робочих місцях;
- урахування характеру та особливостей трудової діяльності.

Раціональне планування робочого місця має забезпечувати найкраще розміщення знарядь і предметів праці, сприяти усуненню загального дискомфорту, зменшенню втомлюваності працівника, підвищенню його продуктивності праці. Площа робочого місця має бути такою, щоб працівник не робив зайвих рухів і не відчував незручності підчас виконання роботи. Важливо мати також можливість змінити робочу позу, тобто положення корпуса, рук, ніг. Проте слід виключати або мінімізувати всі фізіологічно неприродні і незручні положення тіла [15, 16].

Проведені дослідження показують, що при раціональній організації робочих місць продуктивність праці зростає на 15-25% [21, с.64].

Основні ергономічні вимоги до проектування робочого місця:

- гігієнічні вимоги визначають умови життєдіяльності і працездатності людини. В процесі взаємодії з технікою і середовищем, показниками є рівень освітлення, температура, вологість, шум, вібрація, токсичність, загазованість тощо;
- антропометричні вимоги визначають відповідність конструкцій техніки антропометричним характеристикам людини (зріст, розміри тіла та

окремих рухових ланок). Показниками є раціональна робоча поза, оптимальні зони доступу, раціональні трудові рухи.

Ергономічні вимоги до організації робочого місця оператора ПК включають наступні аспекти:

Параметри робочого місця: Площа кабінету, в якому буде проходити робота повинна бути не менш 6 м², а об'єм не менш 20 м³. Розміщення робочих місць у підвальних приміщеннях, на цокольних поверхах заборонено.

Для внутрішньої обробки приміщення повинні використовуватися дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі - 0,7-0,8; для стін - 0,5-0,6; для підлоги - 0,3-0,5. Забороняється застосовувати для оздоблення інтер'єру приміщень матеріали, що виділяють у повітря шкідливі хімічні речовини.

У приміщеннях з візуальними дисплейними терміналами (ВДТ) слід щоденно робити вологе прибирання. При них мають бути обладнані побутові приміщення для відпочинку під час роботи, кімната психологічного розвантаження [16, розд. 2].

Робочі місця з ВДТ слід так розташовувати відносно світових прорізів, щоб природнє світло падало переважно зліва, забезпечивши відстань 1,2 м між бічними поверхнями ВДТ та 2,5 м від тильної поверхні одного ВДТ до екрана іншого.

Конструкція робочого столу повинна забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання. Конструкція крісла повинна забезпечувати підтримку раціональної робочої пози під час роботи з ВДТ і ПЕОМ, дозволяти змінювати позу з метою зниження статичного напруження м'язів шийно-плечової області і спини [18].

Під час роботи сидячи нижня частина корпуса розслаблена, а основне статичне навантаження припадає на м'язи шиї, спини, таза, стегон. Неправильна сидяча поза може викликати застій крові в ногах, а якщо виконується великий обсяг роботи для пальців рук — запалення суглобів.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного

розташування ергономічним вимогам, як відображено на рисунку 4.2 [21, с.138], де 1 - кут екрана; 2 - кут огляду (зору); 3 - відстань огляду; 4 - висота середини екрана; 5 - висота клавіатури; 6 - висота столу; 7 - відстань колін від столу; 8 - підставка для ніг; 9 - підставка для документів; 10 - положення рук; 11 - кут ліктів; 12 - спинка крісла; 13 - підлокітник; 14 - опора для попереку; 15 - кут колін; 16 - кут спинки крісла; 17 - висота сидіння.

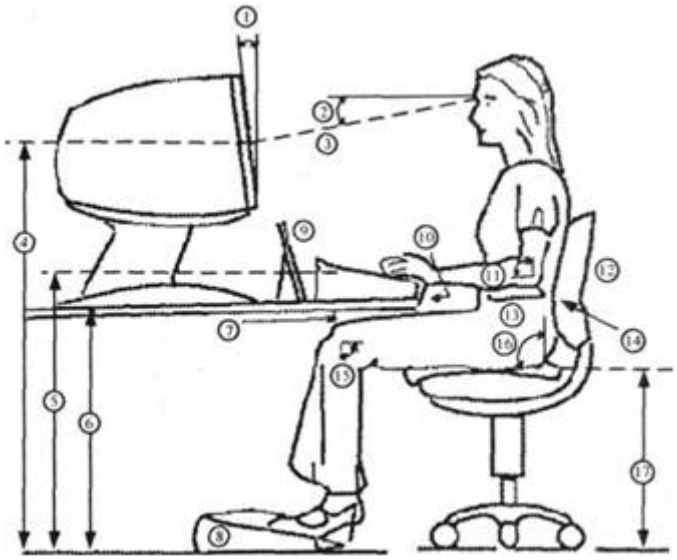


Рисунок 4.2 - Робоче місце і робоча поза користувача комп’ютера:

Висота робочої поверхні столу має регулюватися в межах 680-800 мм, він повинен мати простір для ніг висотою не менше 600 мм, шириною – не менше 500 мм, не менше 450 мм в глибину на рівні колін і на рівні простягнутої ноги - не менше 650 мм.

Відстань від очей користувача до екрану дисплея має становити 600-700 мм. Розташування екрана має забезпечувати зручність зорового спостереження у вертикальній площині під кутом 30 градусів.

Освітленість також впливає на стан здоров’я і працездатність людини. Приміщення повинні мати природне та штучне освітлення відповідно до СНиП II-4-79. Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500 лк, а освітленість екрана має не перевищувати 300 лк [16, розд. 4].

Блок-схема організації робіт на ПК розміщена в Додатку 1. Ці та інші викладені в нормативних документах вимоги допомагають забезпечити комфортні умови праці при роботі з комп’ютером.

У наш час використання ергономічних принципів і рекомендацій є особливо потрібним для створення нових і модернізації існуючих видів обладнання. Використання досягнень ергономіки дозволяє суттєво змінити зміст праці людини, полегшити і підвищити її продуктивність. Увага до ергономічних досліджень постійно збільшується, оскільки з кожним роком зростає "вартість" помилки людини під час управління складними технічними системами.

ВИСНОВКИ

В результаті написання кваліфікаційної роботи було проведено дослідження особливостей налаштування міжмережевих екранів та застосовано на практиці отримані знання. Питання розглянуте у взаємозв'язку з проблемою вироблення політик безпеки та формування цілісної системи інформаційної безпеки.

У роботі було розглянуто функції міжмережевих екранів на різних рівнях моделі OSI, описане їх призначення та принцип роботи. Наведені способи класифікації міжмережевих екранів, їх види і компоненти.

Проведений аналіз переваг і недоліків різних видів міжмережевих екранів, розглянуто основні схеми їх організації та особливості їх налаштування. Виконане налаштування міжмережевого екрану на обладнанні Cisco. Сформульовані рекомендації з ефективного застосування міжмережевих екранів.

Актуальність опрацьованої тематики пов'язана з гостротою питання забезпечення кібербезпеки. Вона може застосовуватися для оптимізації налаштування міжмережевої взаємодії в організації та підвищення ефективності використання міжмережевих екранів.

Також дана кваліфікаційна робота може бути використана в навчальних цілях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Davies G., Networking Fundamentals, Packt Publishing, 2019.
2. Gilman, Evan and Barth, Doug. Zero trust networks. O'Reilly Media, Incorporated, 2017.
3. Jena S.R., Cisco Packet Tracer Implementation: Building and Configuring Networks, 1st ed., 2023.
4. Kaufman, C., Perlman, R., and Speciner, M.: Network Security, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2002.
5. Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., & Karelina, O. Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model.
6. Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021, March). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. In Journal of Physics: Conference Series (Vol. 1840, No. 1, p. 012026). IOP Publishing.
7. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034Tanenbaum A., Wetherall D. Computer Networks, 6th Edition. – 2021.
8. Tanenbaum A., Wetherall D. Computer Networks, 6th Edition. – 2021.
9. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.
10. Безпека життєдіяльності: Навчальний посібник/ Ю. Скобло, В. Цапко, Д. Мазоренко, Л. Тіщенко,; Ред. В. Г. Цапко. - 4-те вид., перероб. і доп.. - К.: Знання, 2006. - 397 с.
11. Безпека невиробничої діяльності: Навчальний посібник для студентів усіх спеціальностей денної, заочної та дистанційної форм навчання / В. А.

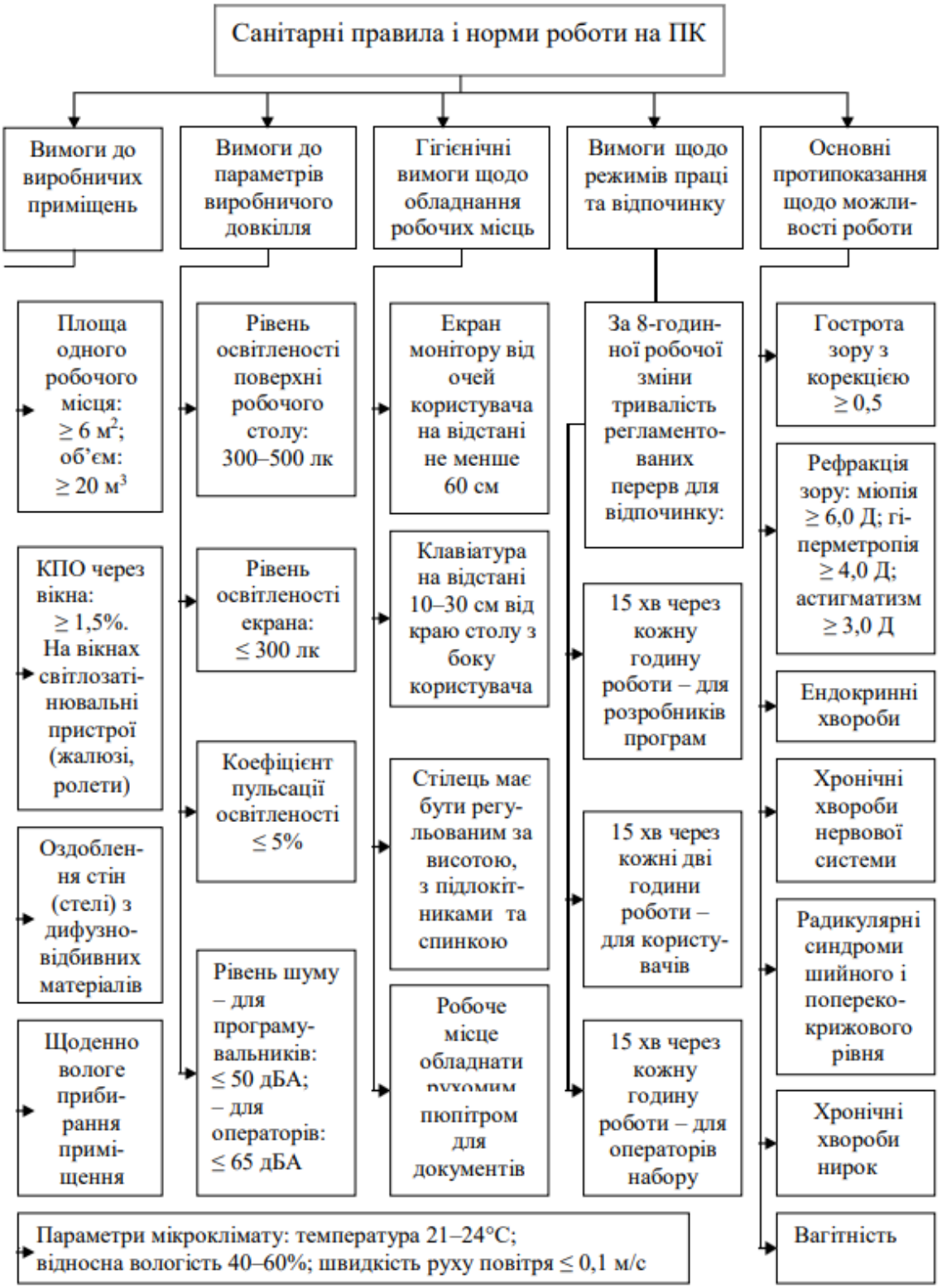
Смирнов, С. А. Дикань, Р. І. Пахомов - Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2011. - 306 с.

12. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.
13. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
14. Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями, затверджені Наказом Міністерства соціальної політики України № 207 14.02.2018р.
15. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
16. ГОСТ 22269-76. Система «людина - машина». Робоче місце оператора. Взаємне розміщення елементів робочого місця. Загальні ергономічні вимоги.
17. ДСанПІН 3.3.2-007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно обчислювальних машин, затверджені Постановою Головного державного санітарного лікаря України № 7 10.12.1998р.
18. ДСТУ 7234:2011. Дизайн і ергономіка. Обладнання виробниче. Загальні вимоги дизайну та ергономіки, затверджені наказом Держспоживстандарту України від 02.02.2011 р. № 37.
19. ДСТУ 8604:2015 Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги, затверджені наказом ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» 21.12.2015 № 204
20. Дуднікова І. Безпека життєдіяльності: Навч. посібник/ І. Дуднікова,; Європейський ун-т. - 2-е вид., доп. - К.: Вид-во Європейського ун-ту, 2006. - 267 с.

21. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
22. Лапін В. М. Безпека життєдіяльності людини. Навч. посіб. — 6-те вид., перероб. і доп. — К.:Знання, 2007, — 332 с.
23. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.
24. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.
25. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.

ДОДАТКИ.

Додаток А Блок-схема організації робіт на ПК


Санітарні правила і норми роботи на ПК
Вимоги до виробничих приміщень
Вимоги до параметрів виробничого довкілля
Гігієнічні вимоги щодо обладнання робочих місць
Вимоги щодо режимів праці та відпочинку
Основні протипоказання щодо можливості роботи
Площа одного робочого місця: ≥ 6 м²; об'єм: ≥ 20 м³
КПО через вікна: ≥ 1,5%. На вікнах світлозатінювальні пристрої (жалюзі, ролети)
Оздоблення стін (стелі) з дифузно-відбивних матеріалів
Щоденно вологе прибирання приміщення
Рівень освітленості поверхні робочого столу: 300–500 лк
Рівень освітленості екрана: ≤ 300 лк
Коефіцієнт пульсації освітленості ≤ 5%
Рівень шуму – для програмувальників: ≤ 50 дБА; – для операторів: ≤ 65 дБА
Екран монітору від очей користувача на відстані не менше 60 см
Клавіатура на відстані 10–30 см від краю столу з боку користувача
Стілець має бути регульованим за висотою, з підлокітниками та спинкою
Робоче місце обладнати пюпітром для документів
За 8-годинної робочої зміни тривалість регламентованих перерв для відпочинку:
15 хв через кожну годину роботи – для розробників програм
15 хв через кожні дві години роботи – для користувачів
15 хв через кожну годину роботи – для операторів набору
Гострота зору з корекцією ≥ 0,5
Рефракція зору: міопія ≥ 6,0 Д; гіперметропія ≥ 4,0 Д; астигматизм ≥ 3,0 Д
Ендокринні хвороби
Хронічні хвороби нервової системи
Радикулярні синдроми шийного і поперекового рівня
Хронічні хвороби нирок
Вагітність
Параметри мікроклімату: температура 21–24°С; відносна вологість 40–60%; швидкість руху повітря ≤ 0,1 м/с