МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп’ютерної інженерії

Юзефович Владислав Ігорович

Програмні засоби захисту корпоративних мереж на основі фаєрволів / Software-based corporate network security solutions based on firewalls

спеціальність: 123 – Комп’ютерна інженерія
освітньо-професійна програма – Комп’ютерна інженерія

Кваліфікаційна робота

Виконав: студент групи КІ-41
Юзефович Владислав Ігорович

Науковий керівник
к.т.н. Мельник Г.М.

Кваліфікаційну роботу допущено
до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____О.Л. Дубчак

ТЕРНОПІЛЬ - 2023

АНОТАЦІЯ

Кваліфікаційна робота на тему «Програмні засоби захисту корпоративних мереж на основі фаєрволів» зі спеціальності 123 «Комп'ютерна інженерія» освітнього ступеня «бакалавр» містить 67 сторінок пояснюючої записки, 19 рисунків, 11 таблиці, 3 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою кваліфікаційної роботи є розробка програмного засобу захисту корпоративних мереж за допомогою фаєрволу, що забезпечить високий рівень безпеки від зовнішніх та внутрішніх загроз.

Кваліфікаційна робота присвячена дослідженню та розробці програмних засобів захисту корпоративних мереж, зокрема, використання фаєрволів як ключового елементу в цьому контексті. За результатом проведеної роботи очікується, що розроблені програмні засоби нададуть ефективний захист корпоративних мереж від різноманітних загроз, забезпечуючи надійну фільтрацію трафіку, управління доступом та вчасну виявлення потенційно небезпечних ситуацій. Результати дослідження та розробки можуть бути використані в корпоративних середовищах для підвищення рівня безпеки мереж та захисту конфіденційної інформації. Розроблено програмний засіб для захисту корпоративних мереж.

Особлива увага приділяється питанням налаштування фаєрволів для забезпечення оптимального рівня безпеки, враховуючи специфіку корпоративних мереж. Розглядаються також методи моніторингу та управління мережевою безпекою, включаючи виявлення і реагування на інциденти.

Робота містить висновки щодо доцільності використання програмних фаєрволів у корпоративних мережах, а також перспективи розвитку та вдосконалення даних засобів захисту в умовах швидко змінюваних кіберзагроз.

Ключові слова: ФАЄРВОЛ, КОРПОРАТИВНА МЕРЕЖА, БЕЗПЕКА, ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ, ДОСТУП ДО МЕРЕЖІ, МОНІТОРИНГ ТРАФІКУ.

ANNOTATION

The qualification work on the topic "Software-based corporate network security solutions based on firewalls" from specialty 123 "Computer engineering" of the bachelor's degree contains 67 pages of explanatory note, 19 figures, 11 tables, 3 appendices. The amount of graphic material is 2 sheets of A3 format.

The purpose of the qualification work is to develop a software tool for protecting corporate networks using a firewall, which will ensure a high level of security from external and internal threats.

The modern corporate environment requires effective tools to ensure security and protection from various cyber threats. The qualification work is dedicated to researching and developing software tools for protecting corporate networks, specifically using firewalls as a key element in this context. As a result of the work carried out, it is expected that the developed software tools will provide effective protection for corporate networks from various threats, ensuring reliable traffic filtering, access management, and timely detection of potentially dangerous situations. This qualification work will contribute to the field of information security by developing and improving methods and tools for effectively protecting corporate networks. The research and development results can be used in corporate environments to enhance network security and protect confidential information. A software tool for protecting corporate networks has been developed.

Special attention is paid to the issues of firewall configuration to ensure an optimal level of security, taking into account the specifics of corporate networks. Methods of monitoring and managing network security, including incident detection and response, are also considered.

The work contains conclusions regarding the feasibility of using software firewalls in corporate networks, as well as the prospects for the development and improvement of these protection tools in the context of rapidly changing cyber threats.

Keywords: FIREWALL, CORPORATE NETWORK, SECURITY, PROTECTION SOFTWARE, NETWORK ACCESS, TRAFFIC MONITORING.

ЗМІСТ

ВСТУП

Сучасне бізнес-середовище, насичене технологічними інноваціями та швидким розвитком інформаційних технологій, створює нові можливості для ефективності та конкурентоспроможності підприємств. Зростання обсягів обміну корпоративною інформацією, основане на використанні мережевих технологій, вимагає надійного захисту від потенційних загроз інформаційної безпеки. Одним із ключових елементів системи захисту є використання програмних засобів, здатних контролювати та фільтрувати мережевий трафік - фаєрволів.

Робота присвячена створенню програмних засобів захисту корпоративних мереж на основі фаєрволів. Фаєрвол є важливим інструментом у забезпеченні безпеки мережевих з'єднань, відповідаючи за фільтрацію трафіку та обмеження доступу до ресурсів мережі. Його ефективне використання дозволяє запобігти несанкціонованому доступу, атакам та іншим загрозам, що можуть виникнути в електронному середовищі. Дослідження буде охоплювати різноманітні аспекти, такі як архітектура фаєрволів, їхні можливості, взаємодія з іншими системами безпеки, а також аналіз практичних сценаріїв використання.

Предметом дослідження є програмні засоби захисту корпоративних мереж на основі фаєрволів. Особлива увага приділяється аналізу різних типів фаєрволів, їх функціональних можливостей, а також методів та практик їхнього використання в умовах сучасних кіберзагроз. У роботі розгнянуто наступні аспекти:

– типи фаєрволів, особливості апаратних, програмних та гібридних фаєрволів, їх переваги та недоліки;

– архітектуру та принципи роботи фаєрволів дослідження механізмів фільтрації трафіку, управління доступом та моніторингу;

– оцінку ефективності фаєрволів, розробку критеріїв та методик для оцінювання ефективності захисту, який забезпечують фаєрволи, в умовах реальних загроз.

Практичні аспекти впровадження та налаштування фаєрволів: рекомендації щодо вибору, конфігурації та експлуатації фаєрволів з урахуванням специфіки діяльності організації. Кваліфікаційна робота спрямована на вивчення принципів роботи та ефективності файерволів, а також на розробку рекомендацій щодо оптимального вибору та налаштування програмних засобів для забезпечення безпеки корпоративних мереж.

Метою роботи є розроблення програмного засобу захисту корпоративних мереж на основі фаєрволу. Для досягнення мети потрібно вирішити наступні завдання:

– провести аналіз принципів і технологій безпеки мереж;

– провести аналіз існуючих засобів захисту;

– вибрати платформу для розробки;

– виконати реалізацію програмного забезпечення захисту корпоративних мереж;

– виконати тестування програмної частини системи.

Рішення цих задач дозволить створити ефективну систему захисту корпоративних мереж, що базується на використанні сучасних фаєрволів, та забезпечити високий рівень інформаційної безпеки для організацій.

За результатами роботи опубліковано тези доповіді на IX науково-практичній конференції «Інтелектуальні комп’ютерні системи та мережі» [1]. Копії публікації наведено у додатку Б.

Кваліфікаційна робота складається із вступу, трьох розділів, висновків та списку використаних джерел.

Другий розділ присвячений розробці архітектури програмного засобу, аналізу типів атак, моделей правил фільтрації

1 ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Базові поняття та принципи безпеки мереж

Мережева безпека є ключовим елементом забезпечення надійності, конфіденційності та доступності інформації. У цьому розділі описано основні поняття та принципи мережевої безпеки, серед них:

– Автентифікація та авторизація: ідентифікація осіб або ресурсів у мережі. Встановлення особи, зазвичай за допомогою пароля або інших засобів. Надання прав доступу після успішної автентифікації.

– Шифрування: використання математичних алгоритмів для перетворення інформації в нечитабельну форму.

– Firewall (брандмауер): захист мережі від несанкціонованого доступу шляхом контролю пакетів даних, що проходять через точки мережі.

– Антивірусний захист: використання програмних засобів для виявлення та усунення вірусів, троянських коней та інших загроз мережевій безпеці.

– Оновлення та виправлення: регулярне оновлення та виправлення програмного забезпечення для усунення вразливостей і запобігання атакам.

– Фізична безпека: захист мережевого обладнання та інфраструктури від фізичних загроз, таких як крадіжка, пожежа та повідомлення.

– Моніторинг та аудит: систематичне спостереження за мережею для виявлення аномалій та невизначеностей. Проведення аудитів для оцінки безпеки системи.

– Безпека бездротової мережі: захист від несанкціонованого доступу до бездротових мереж за допомогою механізмів шифрування та аутентифікації. Безпека електронної пошти та веб-сайтів. Захист від фішингу, несанкціонованих атак та інших загроз, які можуть виникнути через електронну пошту та веб-сайти.

– Заборона несанкціонованого використання ресурсів: забезпечення безпеки корпоративних мереж вимагає розуміння та визначення різних типів загроз, які

можуть впливати на їхню надійність та конфіденційність інформації.

Malware програми - одні з найпоширеніших загроз корпоративним мережам. Включають в себе віруси, черв'яки, троянські коні та інші види шкідливого програмного забезпечення. Вони можуть викликати втрати даних, завдати шкоди системам або створити "задні входи" для несанкціонованого доступу.

Віруси - програми, які вбираються у інші файли та можуть розповсюджуватися через використання інфікованих файлів. Хробаки - автономні програми, які спроможні самостійно поширюватися через мережу, використовуючи вразливості в операційних системах. Троянські коні - приховані шкідливі програми, які приховуються під корисними, але викликають шкідливу дію.

Атаки на відмову в обслуговуванні (DoS) та атаки на відмову в обслуговуванні застосунків (DDoS) - ці типи атак спрямовані на перекриття роботи серверів чи мережі, забираючи їхні ресурси або переповнюючи їх трафіком. Це може викликати зниження продуктивності та навіть повний відмов роботи інфраструктури.

Фішинг та соціальний інженерінг є методами атак, які спираються на маніпулювання людьми, а не технічними уразливостями. Атаки цієї природи можуть включати в себе відправлення підроблених електронних листів, які спонукають співробітників виконувати небезпечні дії, такі як надання конфіденційної інформації або відкриття вірусних вкладень. Фішингові атаки включають в себе використання підроблених комунікацій для отримання конфіденційної інформації. Соціальний інженерінг використовує маніпулювання психологією людей для отримання конфіденційної інформації або здійснення несанкціонованих дій.

Несанкціонований доступ - включає в себе намагання отримати доступ до корпоративних ресурсів, використовуючи вкрадені або піддельні облікові записи. Атакувальники можуть використовувати слабкі паролі, перехоплення сесій або використання інших методів для проникнення в систему.

Витік інформації - включає в себе несанкціоноване розголошення конфіденційної інформації. Витік даних може стати результатом атак на захищені ресурси або втрати носіїв інформації.

Не завжди загроза приходить ззовні. Внутрішні загрози включають в себе дії або недбалість власних працівників, які можуть випадково або навмисно викликати проблеми безпеки.

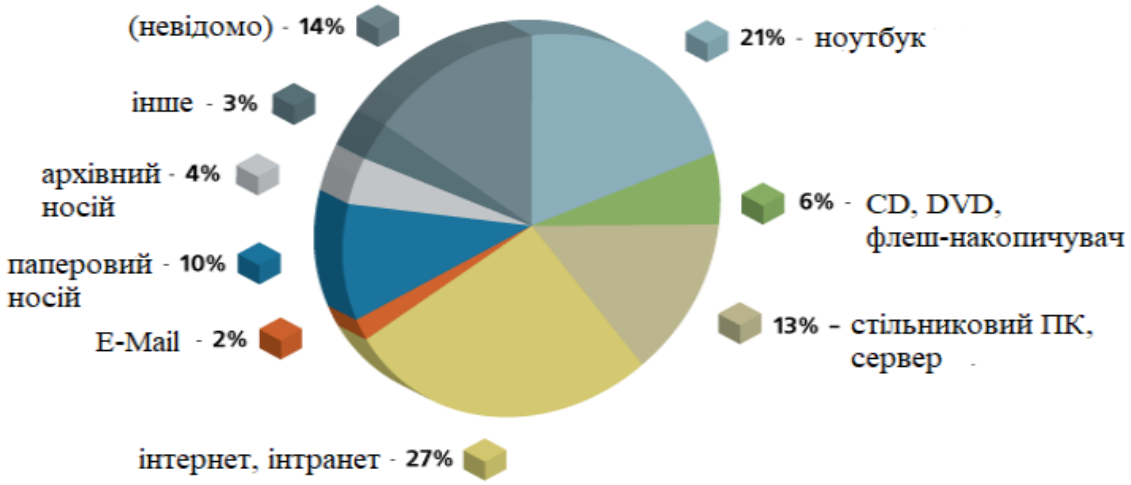

Рисунок 1.1 – Статистика втрати інформації за 2023 рік

Розуміння цих типів загроз є критично важливим для вибору та розгортання відповідних засобів захисту, таких як фаєрволи, які допомагають ефективно протистояти цим потенційно шкідливим сценаріям.

Цей детальний аналіз різних типів загроз визначає різноманітні сценарії, на які система безпеки корпоративних мереж повинна бути готовою реагувати для забезпечення ефективного захисту. Брандмауери є ключовим елементом систем безпеки корпоративних мереж, надаючи захист від різноманітних загроз. Розглянемо роль брандмауерів та їхній внесок у загальний захист мережі:

Фільтрація трафіку: брандмауери використовуються для фільтрації мережевого трафіку, визначаючи, який трафік може пройти через мережевий вузол, а який повинен бути заблокований. Це включає в себе контроль над портами, IP-адресами та протоколами, що допомагає виявляти та блокувати підозрілий чи потенційно шкідливий трафік.

Моніторинг мережевої активності: брандмауери надають можливість моніторити мережеву активність, що дозволяє виявляти незвичайну чи підозрілу поведінку. Вони записують інформацію про трафік, ініційований ззовні та зсередини мережі, що сприяє вчасному виявленню можливих загроз.

Захист від внутрішніх загроз: брандмауери використовуються для запобігання внутрішнім загрозам, таким як несанкціоновані спроби доступу власних співробітників чи розповсюдження шкідливого програмного забезпечення всередині мережі.

Керування доступом: регулюють доступ до різних частин мережі, встановлюючи правила та обмеження для користувачів та пристроїв. Це допомагає забезпечити, що лише авторизовані особи мають доступ до конфіденційних ресурсів.

Виявлення та запобігання атакам: брандмауери виявляють та запобігають різноманітним атакам, включаючи віруси, черв'яки, атаки DoS і DDoS, завдяки вбудованим алгоритмам аналізу трафіку та підписів відомих загроз.

VPN та Захист трафіку: надають можливість встановлення захищених тунелів VPN (віртуальна приватна мережа), що дозволяє шифрувати мережевий трафік і забезпечує безпеку комунікацій між різними вузлами.

Роль брандмауерів у системі захисту корпоративних мереж визначається їхнім багатоаспектним внеском у контроль, моніторинг та захист мережевого середовища. Ефективне використання брандмауерів визначає рівень безпеки та стійкість корпоративних мереж до різноманітних загроз.

1.2 Типи фаєрволів та їх функціонал

Брандмауери можуть бути класифіковані за різними критеріями, такими як методи фільтрації, рівні мережі, архітектурні особливості тощо. Давайте розглянемо основні типи брандмауерів та їх функціонал:

1. Статичні брандмауери: цей тип брандмауерів аналізує інформацію в заголовках мережевих пакетів, таку як IP-адреси та порти, для прийняття рішення щодо пропуску чи блокування трафіку. Статичні брандмауери можуть бути менш гнучкими, оскільки вони не враховують динамічні зміни в мережі.

2. Динамічні брандмауери: використовують розуміння контексту мережі, враховуючи динамічні зміни впродовж часу. Вони можуть приймати рішення на основі актуальних умов та змінюваних властивостей мережі, що робить їх більш гнучкими для реагування на нові загрози.

3. Брандмауери застосунків: ці брандмауери працюють на рівні застосунків і здатні аналізувати та контролювати трафік, враховуючи конкретні застосунки чи сервіси, які використовуються. Вони здатні виявляти шкідливий вміст і керувати доступом до конкретних веб-сервісів чи додатків.

4. Брандмауери на рівні мережі: працюють на рівні мережі і взаємодіє з пакетами даних, визначаючи, які з них можуть проходити через брандмауер. Вони зазвичай використовують правила на основі IP-адрес, портів та протоколів.

5. Брандмауери з глибокою інспекцією пакетів: ці брандмауери виявляють та аналізують вміст пакетів даних, що проходять через мережу. Вони можуть визначати конкретні аплікації та протоколи, навіть якщо вони використовують нестандартні порти.

6. Брандмауери на основі стану з'єднань: Ведуть облік стану активних з'єднань та роблять рішення щодо пермісій на основі контексту з'єднань. Вони спроможні враховувати стан передаваної інформації, забезпечуючи більший контроль над трафіком.

7. Проксі-брандмауери: Працюють як посередники між внутрішньою мережею та зовнішньою мережею, фільтруючи трафік та забезпечуючи анонімність та додатковий рівень безпеки.

Різноманітні типи брандмауерів надають можливість вибору оптимального рішення для конкретного середовища. Важливо враховувати потреби та характеристики мережі для вибору брандмауера, який найкраще відповідає конкретним вимогам щодо безпеки.

1.3 Аналіз переваг та недоліків фаєрволів

На ринку існує багато виробників брандмауерів, які пропонують різні рішення для захисту мережі. Розглянемо деяких з найпопулярніших виробників брандмауерів та їхні ключові характеристики:

Check Point виробляє різноманітні рішення для кібербезпеки, включаючи брандмауери, які використовують технологію виявлення загроз та керування доступом для захисту мережі. Одним з продуктів є CP Firewall — це комплексне програмне рішення, яке забезпечує багаторівневий захист корпоративних мереж. Цей продукт включає широкий спектр функціональних можливостей, спрямованих на забезпечення безпеки. Головне вікно програми зображено на рисунку 1.2. Серед переваг продукту:

– Аналіз та фільтрація мережевого трафіку: використання правил безпеки для контролю вхідного і вихідного трафіку.

– Захист від мережевих атак: інтегровані системи виявлення та запобігання вторгнень (IDS/IPS) для захисту від кіберзагроз.

– VPN (Virtual Private Network): забезпечення захищеного віддаленого доступу до корпоративної мережі.

– Application Control: контроль доступу до додатків та управління їх використанням.

– URL Filtering: блокування доступу до шкідливих та небажаних веб-сайтів.

– Anti-Bot та Anti-Virus: захист від шкідливих програм та ботнетів.

– Data Loss Prevention (DLP): запобігання витоку конфіденційної інформації.

Програма має також свої недоліки:

– Складність налаштування.

– Висока вартість ліцензійної програми.

– Ускладнені оновлення.

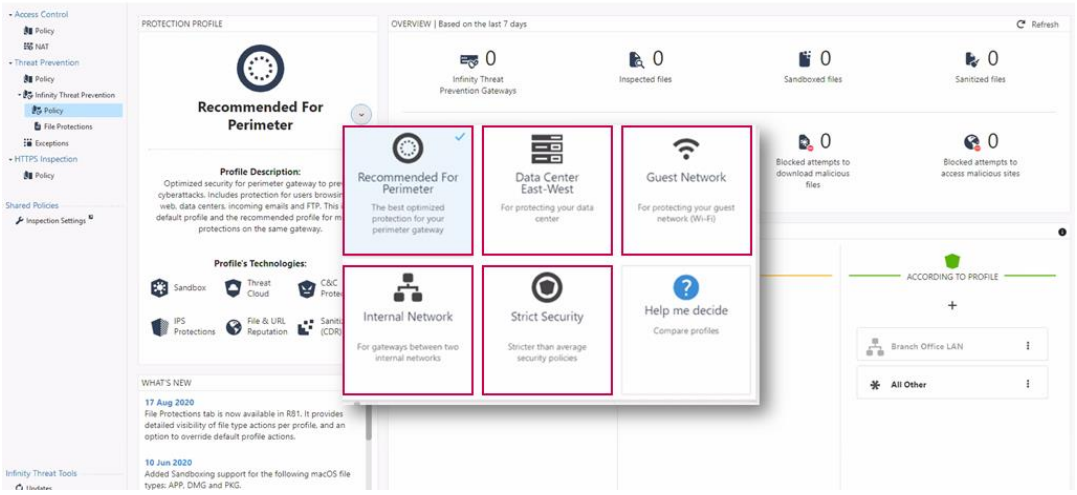

Рисунок 1.2 – Головне вікно програми CP Firewall

Fortinet виробляє широкий спектр мережевих рішень, включаючи брандмауери, мережеві брокери та інші пристрої безпеки. Їхні продукти визначаються високою продуктивністю та інтеграцією захисних функцій. Основним продуктом компанії є FortiGate Next-Generation Firewall — це інтегрована система забезпечення безпеки мережі, яка поєднує в собі багатофункціональний фаєрвол, систему виявлення та запобігання вторгнень (IDS/IPS), VPN, захист від вторгнень, антивірусні та антиспамові функції, а також керування широкосмуговим доступом і контроль додатків. На рисунку 1.3 буде зображено головне вікно програмного забезпечення. До переваг можна віднести:

- Широкий функціонал: FortiGate пропонує широкий спектр інтегрованих безпекових функцій, що дозволяє організаціям ефективно захищати свої мережі від різних кіберзагроз.
- Швидкість та продуктивність: FortiGate пропонує високу швидкість обробки мережевого трафіку навіть під час застосування різноманітних безпечних функцій.
- Централізоване управління: Система керування FortiManager дозволяє централізовано керувати та моніторити мережами з великою кількістю FortiGate пристроїв.
- Інтеграція з FortiGuard Services: FortiGate може інтегруватися з облачною платформою FortiGuard, що забезпечує доступ до оновлень підписів

загроз, інтелектуальних сервісів та інших безпечних сервісів.

Серед недоліків можна виділити тільки те, що старіші моделі FortiGate можуть мати обмежену продуктивність, особливо при використанні всіх доступних безпечних функцій. Інтеграція з іншими рішеннями може бути обмеженою внаслідок залежності від Fortinet екосистеми, що може ускладнити вибір продуктів для різних потреб організації.

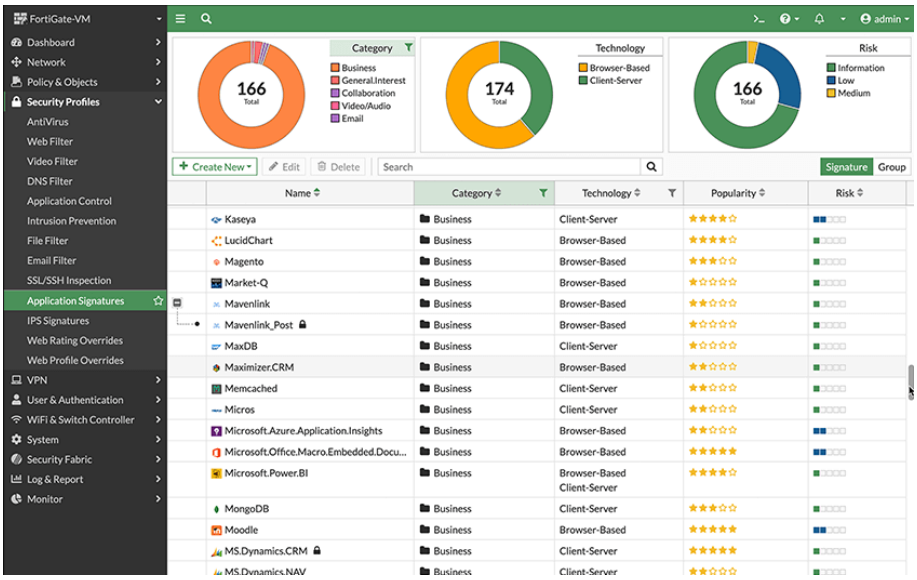

Рисунок 1.3 – Головне вікно програми FortiGate-VM

Juniper Networks спеціалізується на створенні мережевого обладнання та рішень з безпеки. Їхні брандмауери використовують технології інтелектуального фільтрування трафіку для ефективного захисту мережі. Одним із ключових продуктів є SRX Series Firewall. SRX Series Services Gateways є сімейством брандмауерів та мережевих пристроїв, які забезпечують високий рівень захисту мереж і дозволяють розгортати різноманітні безпечні послуги. На рисунку 1.4 буде зображено пристрій SRX Series Firewall. Серед переваг пристрою можна виділити:

– Універсальність функцій: SRX Series Gateways комбінують у собі функції файерволу, VPN, IDS/IPS, а також здатність до обробки шифрованого трафіку.
– Швидкість та продуктивність: Ці пристрої мають високу швидкість

обробки трафіку та можуть легко масштабуватися від малих офісів до великих дата-центрів.

– Захист від загроз: SRX Series Gateways використовують різноманітні методи захисту, такі як аналіз підписів, аналіз поведінки та застосування загальновідомих списків контролю доступу (ACL), для виявлення та блокування загроз.
– Централізоване управління: За допомогою Juniper Networks Junos Space Security Director адміністратори можуть централізовано керувати політиками безпеки та моніторити стан мережі.

До недоліків можна віднести наступні пункти:

– SRX може обмежувати можливості інтеграції з додатками сторонніх виробників порівняно з іншими рішеннями на ринку.
– Іноді можуть виникати проблеми з підтримкою або доступом до оновлень програмного забезпечення.
– Відсутнє програмне забезпечення.

Рисунок 1.4 – Продукт компанії Juniper Networks

Cisco є одним із провідних виробників мережевого обладнання, включаючи брандмауери. Їхні рішення включають в себе інтегровані системи безпеки, які надають міцний захист та можливості аналізу трафіку. Cisco ASA Internet Access є інтегрованим рішенням для забезпечення безпеки мережі, яке поєднує в собі функції файерволу, VPN, IDS/IPS та інші. Рисунок 1.5 відображає додаток Cisco ASDM. Переваги додатку:

– Багатофункціональність: ASA надає різноманітні можливості безпеки, включаючи функції файерволу, VPN, IDS/IPS, а також функції захисту від

вторгнень.

- Швидкість та продуктивність: Продукти ASA пропонують високу швидкість обробки трафіку та можуть ефективно використовуватися як у невеликих офісів, так і в великих дата-центрах.
- Широкі можливості налаштування: ASA надає широкі можливості налаштування політик безпеки, контролю доступу та моніторингу мережевого трафіку.
- Централізоване управління: За допомогою Cisco Firepower Management Center адміністратори можуть керувати політиками безпеки та моніторити стан мережі з централізованого інтерфейсу.

Додаток також має свої недоліки:

- Деякі протоколи та функції можуть бути обмежені або не підтримуватися ASA, що може ускладнити інтеграцію з іншими системами.
- Інтеграція з іншими рішеннями безпеки та моніторингу може вимагати додаткових зусиль або використання додаткового програмного забезпечення.

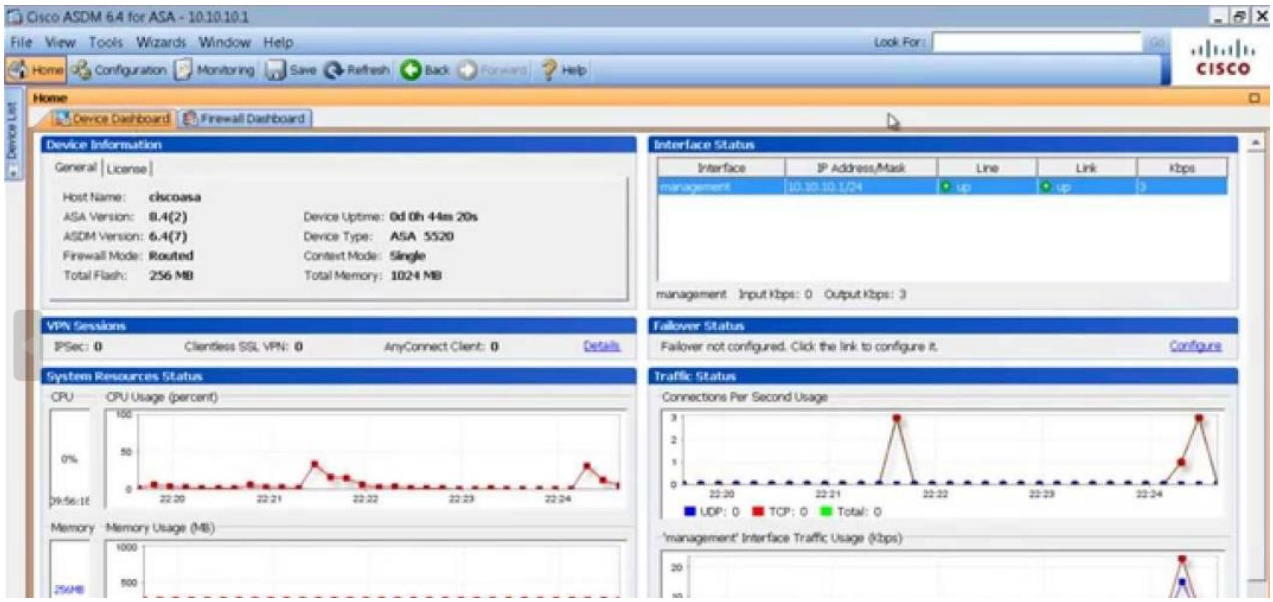

Рисунок 1.5 – Додаток Cisco ASDM

Sophos надає інтегровані рішення для кібербезпеки, включаючи брандмауери, які використовують технології шифрування трафіку та виявлення загроз для захисту мережі. Sophos XG Firewall є інтегрованим рішенням для захисту мережі, яке поєднує в собі багатофункціональний фаєрвол, систему виявлення та запобігання вторгнень (IDS/IPS), VPN та інші функції безпеки. На рисунку 1.6 зображено програму Sophos XG Firewall. Серед переваг програми можна виділити:

– Багатофункціональність: Sophos XG Firewall пропонує широкий спектр функцій безпеки, таких як фільтрація веб-трафіку, захист від вторгнень, контроль за додатками та шифрування VPN.

– Простота у використанні: Інтерфейс користувача Sophos XG Firewall дуже інтуїтивний та простий у використанні, що робить його ідеальним рішенням навіть для менш досвідчених адміністраторів.

– Захист від загроз: Sophos XG Firewall використовує різноманітні методи захисту, включаючи аналіз підписів, аналіз поведінки та застосування загальновідомих списків контролю доступу (ACL), для виявлення та блокування загроз.

До недоліків можна віднести:

– У порівнянні з деякими іншими рішеннями, Sophos XG Firewall може мати обмежені можливості налаштування політик безпеки та контролю доступу.
– Sophos XG Firewall може бути відносно дорогим у впровадженні та підтримці, особливо для малих підприємств.
– Деякі протоколи та функції можуть бути обмежені або не підтримуватися Sophos XG Firewall, що може ускладнити інтеграцію з іншими системами.

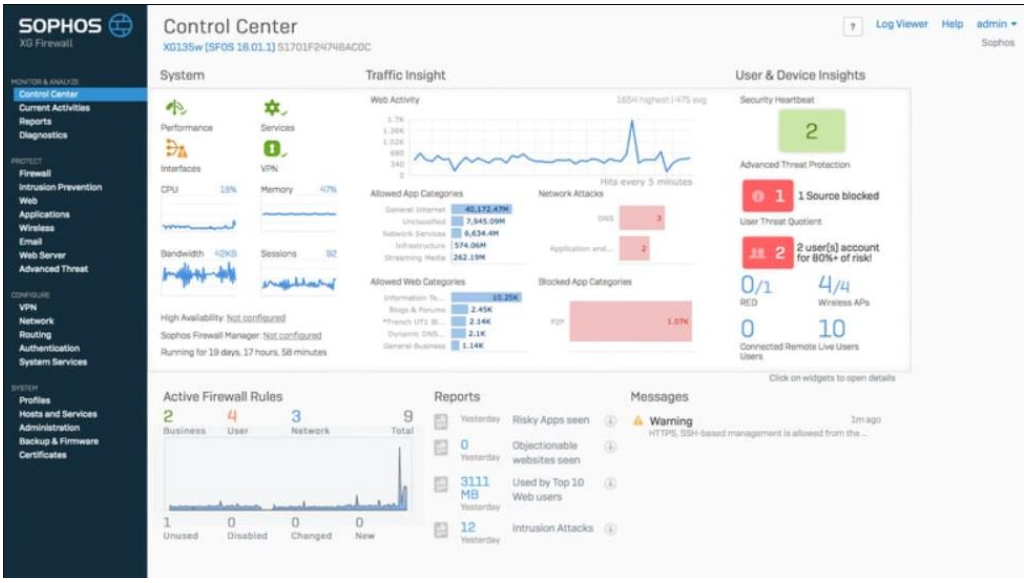

Рисунок 1.6 – Програма Sophos XG Firewall

Важливо враховувати, що переваги та недоліки кожного виробника можуть змінюватися в залежності від конкретної моделі брандмауера та вимог користувача. В таблиці 1.1 буде вказано основні характеристики та порівняння.

Таблиця 1.1 – Таблиця порівняння за основними характеристиками

Характеристика	Cisco ASA	Sophos XG	FortiGateVM	CP Firewall
Багатофункціональність	Так	Так	Так	Так
Простота використання	Середня	Висока	Середня	Низька
Захист від загроз	Так	Так	Так	Так
Складність	Низька	Висока	Середня	Середня
Вартість	Низька	Середня	Середня	Висока
Обмежена підтримка протоколів	Так	Ні	Так	Так
Централізоване управління	Так	Так	Так	Так

На основі наведеної таблиці порівняння чотирьох популярних рішень для захисту мереж (Cisco ASA, Sophos XG Firewall, Juniper Networks SRX Series Services Gateways та Check Point Firewall) можна зробити наступні висновки:

а) Для організацій, що шукають просте у використанні рішення з широкими функціональними можливостями: Sophos XG Firewall може бути найкращим вибором завдяки своїй інтуїтивній конфігурації та середній вартості;

б) Для великих підприємств з досвідченими адміністраторами: Cisco ASA та Check Point Firewall забезпечують високий рівень захисту та гнучкість налаштування, але потребують значних ресурсів для налаштування та підтримки;

в) Для організацій, які потребують високої продуктивності та можливості масштабування: Juniper SRX Series може бути найбільш відповідним рішенням завдяки своїй здатності обробляти великий обсяг трафіку та інтеграції з іншими мережевими рішеннями.

1.4 Постановка задач кваліфікаційної роботи

Завдання кваліфікаційної роботи

1. Огляд літератури:
   - Провести аналіз основних концепцій та принципів безпеки мереж.
   - Визначити загальні вимоги до захисту корпоративних мереж.
2. Види загроз корпоративним мережам:
   - Класифікувати основні види загроз, з якими стикаються корпоративні мережі.
   - Визначити специфіку кожного типу загрози та їх потенційні наслідки.
3. Роль брандмауерів у системі захисту:
   - Проаналізувати функціонал брандмауерів як ключового елемента захисту мережі.
   - Визначити роль брандмауерів у контексті захисту від різноманітних загроз.
4. Типи брандмауерів та їх функціонал:
   - Класифікувати брандмауери за різними критеріями (статичні,

динамічні, на рівні мережі, застосунків тощо).

- Дослідити функціональні можливості кожного типу брандмауера.

5. Популярні виробники брандмауерів:
   - Проаналізувати продукцію відомих виробників брандмауерів.
   - Визначити переваги та недоліки кожного виробника.
6. Аналіз існуючих рішень та архітектура засобів захисту:
   - Вивчити типи атак та їхні характеристики.
   - Розглянути архітектурні особливості програмних засобів захисту.
7. Розпізнавання атак і створення правил:
   - Дослідити методи розпізнавання атак.
   - Розробити правила фільтрації для брандмауера з урахуванням розглянутих типів атак.
8. Проектування і розробка:
   - Вибір платформи для розробки та опис архітектури розроблюваного засобу.
   - Тестування та аналіз ефективності.
9. Техніко-економічне обґрунтування:
   - Моделі ціноутворення при укладанні угод на розробку ІТ продукту.

Літературний аналіз: Для отримання теоретичних знань та поглибленого розуміння проблеми.

Аналіз виробників та їхніх продуктів: Для отримання інформації про функціонал брандмауерів різних виробників.

Аналіз інцидентів та випадків застосування: Для збору даних щодо ефективності захисних заходів в реальних сценаріях.

Ці завдання та методи дослідження спрямовані на досягнення мети роботи та визначення оптимальних стратегій захисту корпоративних мереж на основі фаєрволів.

Метою кваліфікаційної роботи є розроблення програмного засобу захисту корпоративних мереж на основі фаєрволу. Для досягнення мети потрібно вирішити наступні завдання:

– провести аналіз принципів і технологій безпеки мереж;

– провести аналіз існуючих засобів захисту;

– вибрати платформу для розробки;

– виконати реалізацію програмного забезпечення захисту корпоративних мереж;

– виконати тестування програмної частини системи.

2 АРХІТЕКТУРА ПРОГРАМНОГО ЗАСОБУ ЗАХИСТУ

2.1 Типи атак

Модель правила фільтрації є ключовим аспектом в забезпеченні безпеки корпоративних мереж. Вона визначає правила, які використовуються для контролю та обробки трафіку, який проходить через брандмауер.

Активно зростаюча кількість загроз у сфері інформаційної безпеки підкреслює важливість вивчення та розуміння різних типів атак, яким можуть бути піддані корпоративні мережі. Дослідження типів атак дозволяє розробити ефективні заходи захисту для запобігання та виявлення подібних загроз. Цей розділ детально розгляне основні принципи цієї моделі та її роль у забезпеченні ефективного фільтрування та захисту мережі від різних загроз. Нижче буде представлено основні види атак з якими може зіткнутися кожен користувач ПК:

а) мережеві атаки - правила фільтрації представляють собою набір умов, які визначають, як брандмауер повинен обробляти трафік. Ці умови можуть бути базовими, такими як IP-адреса або порти, або враховувати додаткові параметри, такі як протоколи, або стани пакетів. Атаки, які спрямовані на перевантаження ресурсів мережі чи служби, знижуючи їх доступність для законних користувачів. Методи протидії: Створення правил фільтрації дозволяє адміністраторам мережі точно налаштовувати, яким чином брандмауер повинен обробляти різні типи трафіку. Використання фільтрів для виявлення та блокування аномального трафіку, використання CDN для розподілення навантаження;

Як приклад можна навести маштабну атаку на всім відомий monobank. У вікенд 20–21 січня monobank пережив надпотужну DDoS-атаку, про що співзасновник необанку Олег Гороховський систематично звітував у Telegram-каналі. На піку загальне навантаження на сервіс сягало 580 млн запитів. «Це просто космос», – писав Гороховський 21 січня.

Під час DDoS-атак хакери намагалися перенавантажити сервіс, щоб він почав гальмувати або став недоступний для звичайних користувачів. monobank,

який має майже 900 000 активних клієнтів, вдалося уникнути такого сценарію. «Я хочу сказати велике спасибі нашій IT-команді, яка стоїть на варті нашої IT-інфраструктури», – написав Гороховський. Загальна схема як відбувалася атака зображена на рисунку 2.1

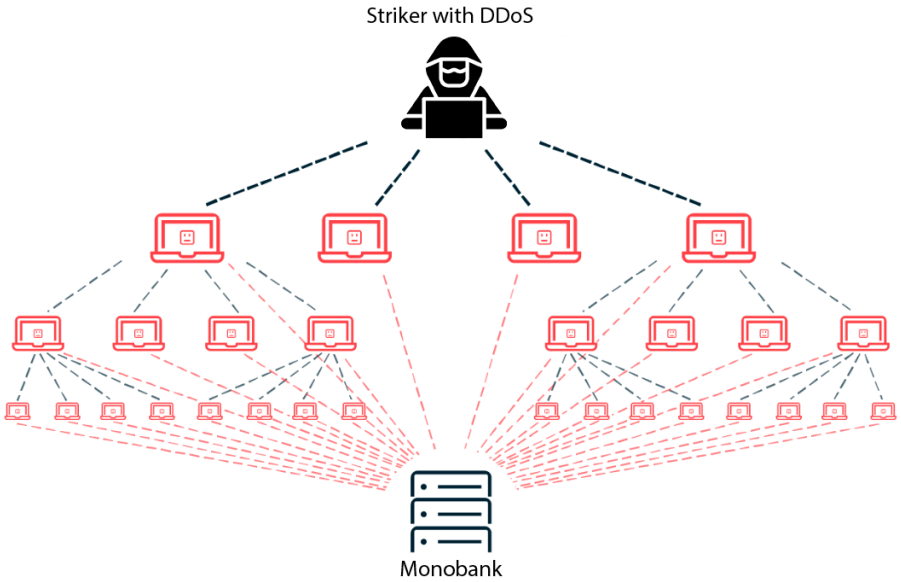

Рисунок 2.1 – Схема DDoS атаки

б) спуфінг атаки - фальшиве представлення або модифікація даних з метою приховати справжню ідентичність атакуючого. Методи протидії: Використання методів перевірки аутентичності та криптографічних технік для уникнення фальсифікації даних;

в) пошкоджувальні атаки - шкідливі програми, які вставляються в систему та розповсюджуються, завдаючи шкоди або крадучи конфіденційні дані. Методи протидії: Регулярне оновлення антивірусного програмного забезпечення, сегментація мережі для запобігання розповсюдженню;

г) вимагаючі програми - атаки, що блокують доступ до файлів чи системи з метою вимагання викупу для їхнього розблокування. Методи протидії: Резервне копіювання даних, використання антивірусного та анти-рансомвірусного програмного забезпечення;

г) захоплення аутентифікації - спроби вивести користувачів з легітімних джерел для викрадення конфіденційних інформацій, таких як ім'я користувача та

пароль. Методи протидії: Навчання персоналу щодо визначення фішингових атак, використання анти-фішингових фільтрів;

д) Брутфорс атаки - Спроби неправомірного доступу, випробування всіх можливих комбінацій для зламування пароля. Методи протидії: Використання складних паролів та блокування аккаунтів після кількох спроб введення неправильного пароля.

Взявши до уваги всі вищеперераховані методи атак, було виділено наймасивніші кібератаки в Україні та їх наслідки які траплялися в період 2023-2024 роки на рисунку 2.2

Рисунок 2.2 – Кібератаки та наслідки в Україні в 2023-20234

Дослідження різних типів атак виявляє широкий спектр загроз, з якими можуть стикатися корпоративні мережі. Розуміння цих атак дозволяє розробляти ефективні стратегії та заходи безпеки для забезпечення стійкості та захисту мережевого середовища.

2.2 Модель правил фільтрації

У цьому підрозділі ми розглянемо принципи та функціонал моделі правила фільтрації та його роль у забезпеченні безпеки корпоративних мереж.

Основні принципи моделі правила фільтрації - правила фільтрації визначають умови, за якими брандмауер приймає рішення щодо проходження чи блокування трафіку. Вони можуть бути встановлені на основі IP-адрес, портів, протоколів, тощо. Застосування: Створення правил фільтрації дозволяє брандмауеру ефективно контролювати та обмежувати доступ до різних ресурсів мережі. Становища правил визначають порядок, в якому брандмауер обробляє правила фільтрації. Перевірка може виконуватися в порядку визначеному вручну або автоматично. Правильне розташування правил дозволяє оптимізувати швидкість обробки трафіку та зменшити навантаження на брандмауер.

Дії правил визначають, що має робити брандмауер з пакетами, які відповідають встановленим умовам. Налаштування дій дозволяє визначити, чи блокувати, чи допускати трафік, а також виконувати інші дії, такі як запис до журналу або сповіщення про певні події.

Модель правил фільтрації може бути реалізована як набір if-then правил, де кожне правило встановлює умову і дію, що повинна бути виконана, якщо умова виконується. Також можуть використовуватися статистичні методи, машинне навчання або комбінації різних підходів.

Наприклад, у фільтрації електронної пошти модель правил може визначати, що листи з певних адрес або з певними ключовими словами будуть автоматично переслані у папку спаму. Це може забезпечити ефективну фільтрацію небажаних повідомлень.

У більш складних сценаріях, таких як фільтрація мережевого трафіку для виявлення зловживань або кібератак, модель правил може базуватися на аналізі великих обсягів даних та використанні складних алгоритмів для виявлення аномалій або підозрілих патернів. Роль моделі правила фільтрації у системі захисту:

- Фільтрація трафіку;
- Захист від атак;
- Моніторинг та журналювання.

Модель правила фільтрації використовується для фільтрації трафіку, що проходить через брандмауер. Це дозволяє обмежувати доступ до ресурсів та послуг відповідно до встановлених правил. Встановлення правил фільтрації допомагає у виявленні та блокуванні потенційно шкідливого трафіку, зменшуючи ризик атак, таких як DoS, атаки на основі портів та інші. Модель правила фільтрації також використовується для моніторингу та журналювання подій. Запис в журнал дозволяє адміністраторам відстежувати та аналізувати трафік для виявлення аномальних подій.

Розуміння її принципів та ефективного використання дозволяє адміністраторам забезпечити стабільну та безпечну роботу мережі, знижуючи ризики та реагуючи на потенційні загрози.

2.3 Розпізнавання атак, створення правил, сповіщення та реакція

Розпізнавання атак та створення ефективних правил фільтрації є важливим етапом в системі захисту корпоративних мереж. У цьому розділі розглянемо різні методи розпізнавання атак та процес створення правил для ефективного виявлення та захисту від потенційних загроз. Нижче буде представлено методи розпізнавання атак:

а) Сигнатурний аналіз використовує базу сигнатур, що представляють собою характеристики відомих атак. Коли мережевий трафік відповідає будь-якій із цих сигнатур, система визначає його як потенційно загрозливий. Дії: створення бази сигнатур із відомих атак. Виявлення сигнатур у трафіку: Аналіз мережевого трафіку на відповідність сигнатурам.

б) Аномалійний аналіз базується на виявленні невластивого чи відхільного поведінки мережі. Система аналізує статистику мережевого трафіку та сповіщає про будь-які незвичайні або аномальні події. Дії: Створення бази зразків нормальної поведінки: Аналіз та визначення зразків, які вважаються

нормальними. Виявлення відхилень: Систематичний моніторинг та виявлення будь-яких аномалій у мережевому трафіку. Визначення потенційно загрозливих ситуацій: Сигналізація адміністратору при виявленні аномальних подій. Серед переваг:

- Здатність виявляти нові атаки або змінені патерни;
- Адаптація до змін у середовищі.

До недоліків можна віднести:

- Велика ймовірність помилкових спрацювань через нормальні аномалії;
- Потреба у складних алгоритмах для визначення нормального стану.

Визначення конкретних атак, які можуть статися в конкретному мережевому середовищі. Це включає в себе аналіз потенційних загроз та уразливостей мережі. Дії: Вивчення інформації про попередні атаки або інциденти. Використання інструментів виявлення вразливостей: Сканування мережі для виявлення слабких місць.

На основі визначених атак створюються правила фільтрації, які дозволяють виявляти та блокувати конкретний трафік, що вказує на атаку. Дії: Встановлення параметрів для виявлення атак. Встановлення правил на брандмауері: Налаштування правил фільтрації на основі визначених критеріїв. Тестування ефективності: Перевірка, чи правила правильно розпізнають та блокують визначені атаки.

Систематичне оновлення та оптимізація правил для врахування нових атак, змін в мережі та покращення ефективності. Дії: Оновлення бази сигнатур для сигнатурного аналізу. Перегляд журналів безпеки: Вивчення інформації про нові атаки або події. Впровадження коректівів: Оновлення та вдосконалення правил відповідно до знайдених недоліків або змін у мережі.

Розпізнавання атак та створення правил фільтрації є невід'ємною частиною ефективної системи захисту корпоративних мереж. Використання сигнатурного та аномалійного аналізу, разом із систематичним створенням та обслуговуванням

правил, дозволяє виявляти та блокувати різноманітні атаки, забезпечуючи стабільну та безпечну роботу мережі.

Система сповіщення та реакції є необхідною складовою для забезпечення безпеки корпоративних мереж. Детальні аспекти виявлення інцидентів, механізмів сповіщення адміністраторів та автоматичної реакції на потенційні загрози. Система виявлення інцидентів використовує різноманітні техніки та інструменти для ретельного аналізу мережевого трафіку та системних журналів з метою виявлення незвичайних або підозрілих активностей. Дії які виконує система сповіщення:

- Моніторинг мережевого трафіку;
- Використання інтрузійних систем виявлення аномалій для пошуку несправжнього чи підозрілого трафіку;
- Аналіз пакетів для виявлення патернів атак або аномалій;
- Моніторинг системних та додаткових журналів подій для виявлення аномальних активностей;
- Використання інструментів аналізу журналів для виявлення атак, змін у конфігураціях та інших аномалій;
- Використання технологій машинного навчання та штучного інтелекту для аналізу аномальних патернів;
- Взаємодія з базами даних загроз та сучасними інструментами виявлення вразливостей.

Сповіщення адміністраторів - система генерує сповіщення для адміністраторів, які включають деталі виявлених інцидентів та необхідні заходи для подальших дій. До основних дій належать:

- Створення сповіщень;
- Систематичне формування сповіщень, що включають тип інциденту, деталі атаки, час виявлення та рекомендації для адміністраторів;
- Використання каналів сповіщення, таких як електронна пошта, SMS, месенджери або спеціальні панелі управління;
- Призначення пріоритетів та рівнів серйозності для кожного сповіщення в

залежності від характеру інциденту;

Визначення правил реакції - адміністратор визначає конкретні правила, які система повинна автоматично виконувати під час виявлення певного типу інцидентів. Основні дії які виконуються:

- Аналіз типів інцидентів;
- Класифікація інцидентів за їхньою серйозністю та потенційним впливом на мережу;
- Визначення найбільш критичних інцидентів, які вимагають автоматичної реакції;
- Визначення конкретних дій, які система повинна виконувати при виявленні певного типу інциденту;
- Налаштування параметрів, таких як порогові значення та таймінг виклику правил.

Виконання автоматичних заходів - система автоматично виконує визначені правила реакції при виявленні інцидентів, забезпечуючи швидку реакцію на потенційні загрози. Ключові дії які виконуються:

- Блокування трафіку;
- Використання брандмауерів для негайного блокування трафіку від підозрілих джерел;
- Автоматичне створення правил фільтрації для припинення потенційно загрозливого трафіку;
- Відключення атакованих систем від мережі для запобігання поширенню інциденту;
- Визначення параметрів ізоляції та часу її дії для мінімізації впливу на роботу інших компонентів мережі;
- Автоматичне включення аудиторських систем для детального вивчення інциденту та збору додаткової інформації;
- Аналіз зібраної інформації для подальших дій та вдосконалення системи виявлення і реакції.

На основі вищепредставленої інформації було створено таблицю 2.1, де кожен аспект представлений з різних точок зору, що дозволить краще зрозуміти різні підходи до кожного етапу процесу розпізнавання атак, створення правил, сповіщення та реакції

Таблиця 2.1 - Аспекти розпізнавання атак

Розпізнавання атак	Сигнатурний аналіз	Використовується база сигнатур відомих атак для виявлення аномалій в мережевому трафіку або системі.
	Аналіз аномалій	Використовується статистичний аналіз та машинне навчання для виявлення несподіваних змін у звичайному зразку поведінки системи або мережі.
Створення правил	Базові правила	Прості if-then правила, які визначають дії для конкретних типів атак або аномалій.
	Експертні правила	Правила, розроблені експертами з використанням їхніх знань про систему або мережу для виявлення та реагування на атаки.
Сповіщення	Електронна пошта	Автоматичні або ручні повідомлення електронною поштою про виявлені атаки або аномалії.
	Повідомлення в системі моніторингу	Використання спеціалізованих систем моніторингу для відображення повідомлень про атаки та аномалії.
Реакція	Автоматичне блокування	Автоматичне блокування атакувального трафіку або вимкнення доступу до компрометованої системи.

Продовження таблиці 2.1

	Запуск аварійного аудиту	Запуск процедур аудиту для виявлення джерела атаки та оцінки її впливу на систему.
	Автоматичне сповіщення служби безпеки	Повідомлення про виявлені атаки або аномалії надсилаються до команди безпеки для подальшого аналізу та реагування.

Система сповіщення та реакції є важливим елементом безпекового заходу для корпоративних мереж. Детальний аналіз і виявлення інцидентів, ефективна система сповіщення та автоматична реакція дозволяють забезпечити високий рівень безпеки, швидко реагуючи на потенційні загрози та забезпечуючи стійкість мережевого середовища.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОЇ СИСТЕМИ ЗАХИСТУ

3.1 Вибір платформи для розробки

Для розробки програмного засобу захисту корпоративних мереж на основі фаєрволів, необхідно уважно вибрати платформу, що найкраще відповідає поставленим завданням та технічним вимогам. Дана ділянка дослідження включає в себе наступні етапи та аспекти:

а) Аналіз потреб користувача: Визначення основних вимог та функціональних можливостей, які має задовольняти програмний засіб. Розгляд специфічних вимог до безпеки, ефективності та масштабованості;

б) Вибір мови програмування: Аналіз можливих мов програмування для розробки, з урахуванням ефективності, швидкодії та підтримки відповідних бібліотек безпеки. Розгляд мов з високою продуктивністю та розширюваністю для забезпечення оптимальної розробки;

в) Вибір розробницького середовища: Оцінка різних розробницьких середовищ, враховуючи зручність використання та підтримку необхідних інструментів для розробки безпечного програмного засобу. Вибір інтегрованих середовищ з можливістю відлагодження, аналізу коду та інших необхідних функцій;

г) Сумісність та інтеграція: Розгляд сумісності обраної платформи з існуючими системами безпеки та корпоративними інфраструктурами. Врахування можливостей інтеграції з іншими рішеннями та стандартами безпеки;

г) Врахування факторів експлуатації: Оцінка можливостей підтримки та обслуговування розробленого засобу на різних операційних системах. Розгляд аспектів моніторингу, логування та підтримки користувачів;

д) Відкритість та спільнота розробників: Аналіз наявності відкритих рішень та спільноти розробників для обраної платформи. Розгляд можливостей отримання підтримки, обміну досвідом та участі в розвитку відкритих рішень;

е) Безпека розробки: Забезпечення використання безпечних практик програмування та вибір інструментів для перевірки коду на вразливості. Врахування можливостей для розробки засобів безпеки, що враховують специфічні вимоги безпеки корпоративних мереж.

Опираючись на вище перераховані пункти моїм вибором стала мова програмування C\C++ на платформі .NET Framework. Основною метою цієї мови програмування рахується можливість легкої компіляції за допомогою простого компілятора, забезпечення прямого доступу до оперативної пам'яті, формування низькорівневого коду з декількома машинними інструкціями для кожного елементу мови та відсутність потреби у великій динамічній підтримці. В результаті це дозволяє писати код, що підходить для більшості системного програмного забезпечення, яке традиційно розробляли на асемблері. Незважаючи на низькорівневі можливості, мова була спроектована з орієнтацією на платформонезалежне програмування. Програми, написані мовою С і відповідні стандартам і платформонезалежні, можуть бути легко скомпільовані на різних апаратних платформах та операційних системах з мінімальними змінами.

Мову С спроектовано для використання в системному програмуванні. Тому вона не потребує додаткового часу на виконання перевірок різних умов, які ніколи не відбудуться у правильно написаній програмі. Крім того, вона забезпечує простий, прямий доступ до адреси будь-якого об'єкта (наприклад, карти пам'яті, пристрою контролю регістрів), і початковий код компілюється у послідовність примітивних машинних операцій.

3.2 Опис архітектури розроблюваного засобу

Архітектура системи спроектована згідно з модульним підходом, що сприяє чіткій організації функціональних блоків системи. До основних компонентів системи належать:

- Модуль керування: Цей модуль відповідає за керування загальним потіком виконання програми. Він ініціалізує роботу інших модулів, встановлює потрібні зв'язки між ними, а також контролює основний цикл виконання програми.
- Модуль обробки даних: Цей модуль відповідає за обробку вхідних даних, їх аналіз і перетворення у внутрішні структури даних, зрозумілі для інших модулів. Він також може забезпечувати функції валідації даних і підготовки їх до подальшої обробки.
- Модуль взаємодії з користувачем: Цей модуль відповідає за взаємодію з користувачем через консольний інтерфейс. Він обробляє введені дані від користувача, передає їх для обробки модулю обробки даних, а також виводить результати роботи системи користувачеві.

Структурні зв'язків належать:

- Модуль керування є центральним елементом системи і координує роботу інших модулів. Він може викликати функції з інших модулів для обробки певних завдань.
- Модуль обробки даних отримує вхідні дані від модуля взаємодії з користувачем або зовнішніх джерел, обробляє їх згідно з логікою системи та передає результати модулю керування або модулю взаємодії з користувачем.
- Модуль взаємодії з користувачем забезпечує інтерфейс для взаємодії з користувачем. Він чекає на введення від користувача, обробляє його і виконує необхідні дії згідно з внутрішньою логікою програми. Використані технології:

Використовуючи програмний засіб Visual Paradigm було створено UML Class Diagram яка зображена на рисунку 3.1, де показано, як можна моделювати мережу з основними компонентами, такими як мережа, пристрої (маршрутизатори, комутатори, комп'ютери) та їх взаємодію. Клас Network має асоціацію з класом Device, що показує, що мережа містить декілька пристроїв.

Класи пристроїв наслідують від Device і реалізують методи connect і disconnect відповідно до їх функціональності.

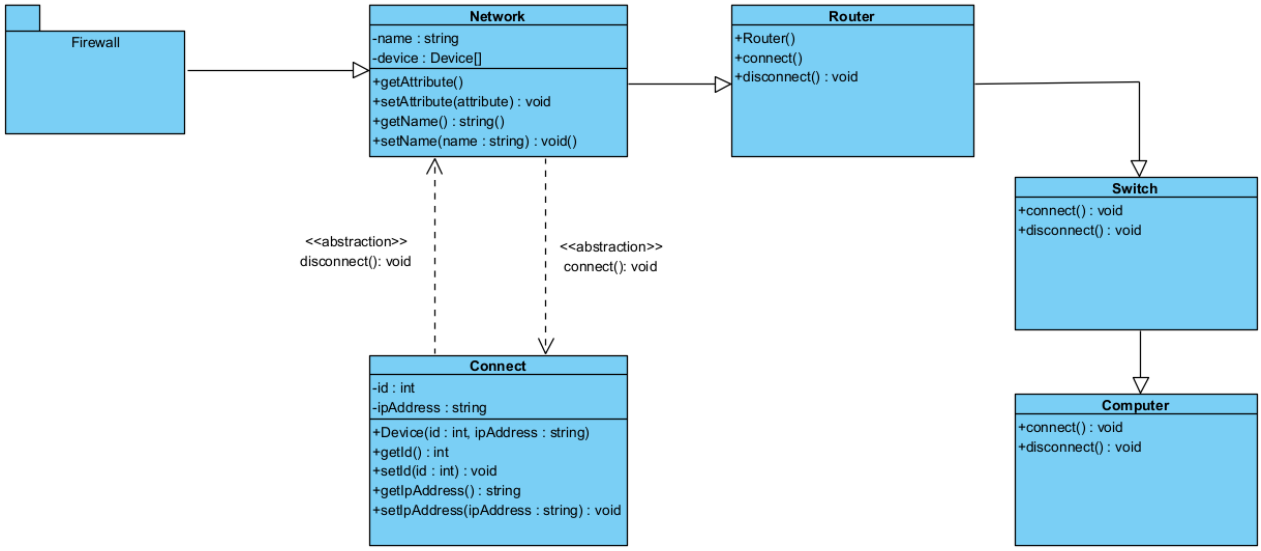

Рисунок 3.1 - UML Class Diagram

У цій діаграмі ми маємо клас Network який представляє мережу зі списком підключених пристроїв таких як router, switch, computer. Нижче описано використані атрибути та методи:

Атрибути:

- name: назва мережі;
- devices: масив пристроїв у мережі.

Методи:

- Network(name: string): конструктор мережі;
- addDevice(device: Device): void: додає пристрій до мережі;
- getDevices(): Device[]: повертає список пристроїв у мережі;
- getName(): string: повертає назву мережі;
- setName(name: string): void: встановлює назву мережі;
- Device: Абстрактний клас, що представляє загальні властивості пристроїв у мережі.

Атрибути:

- id: ідентифікатор пристрою;
- ipAddress: IP-адреса пристрою.

Методи:

- Device(id: int, ipAddress: string): конструктор пристрою;
- getId(): int: повертає ідентифікатор пристрою;
- setId(id: int): void: встановлює ідентифікатор пристрою;
- getIpAddress(): string: повертає IP-адресу пристрою;
- setIpAddress(ipAddress: string): void: встановлює IP-адресу пристрою;
- {abstract} connect(): void: абстрактний метод для підключення пристрою;
- {abstract} disconnect(): void: абстрактний метод для відключення пристрою;
- Router, Switch, Computer: Конкретні класи пристроїв, які наслідують від Device і реалізують методи connect і disconnect згідно зі своєю функціональністю.

а) Структури даних: Використання структур даних для організації і керування інформацією в пам'яті.

б) Покажчики: Використання покажчиків для роботи з пам'яттю, передачі даних між функціями і модулями, а також для оптимізації доступу до даних.

в) Бібліотеки C: Використання стандартних бібліотек мови C для реалізації різноманітних функціональностей, таких як робота з рядками, введення-виведенням даних, робота з файлами тощо.

Використовуючи цей підхід було створено ефективну, легко змінювану та розширювану програму “Firewall App”, яка відповідає вимогам функціональності і продуктивності. Для більш детального розгляду створеної програми було прийнято рішення поділити її на дві частини:

1. Основний інтерфейс програми до якого входять всі функціональні можливості.

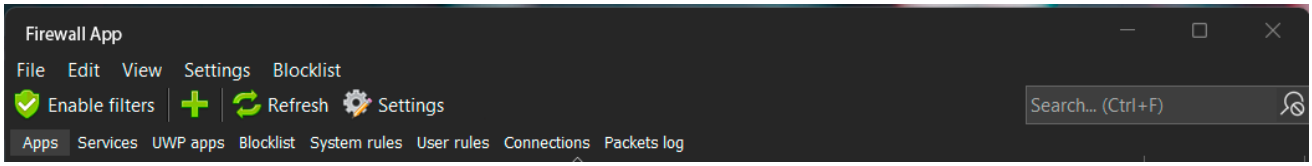

Рисунок 3.2 – Основний інтерфейс програми

2. Частина виводу інформації де відображаються усі дії при взаємодії з програмою.

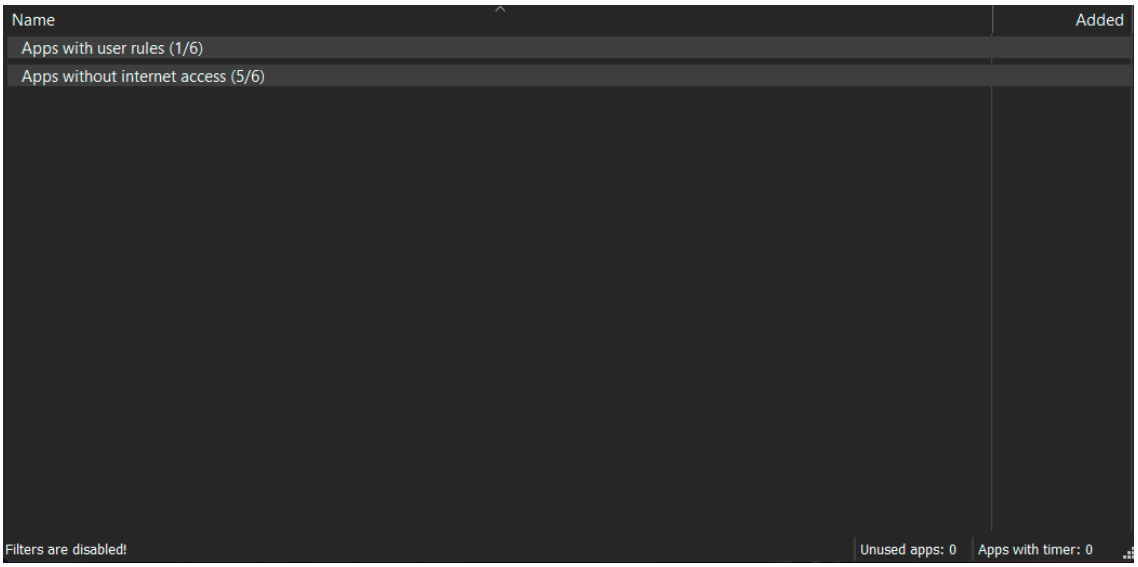

Рисунок 3.3 – Частина виводу інформації

Програма Firewall App, написана мовою програмування C, призначена для захисту комп'ютерних мереж від несанкціонованого доступу та контролю трафіку.

Основні функції Firewall App включають:

а) Перехоплення пакетів: Програма може перехоплювати вхідний і вихідний мережевий трафік, що проходить через мережевий інтерфейс комп'ютера.

б) Аналіз трафіку: Firewall App аналізує кожен мережевий пакет згідно з встановленими правилами безпеки. Це може включати перевірку джерела та призначення пакета, порти, протоколи тощо.

в) Прийняття рішень: На основі аналізу пакетів програма приймає рішення щодо дозволу або блокування певного трафіку. Наприклад, вона може блокувати пакети, що намагаються з'єднатися з певними небезпечними IP-адресами чи портами.

г) Конфігурація правил: Користувач може настроїти правила безпеки для Firewall App через конфігураційні файли або взаємодіючи з інтерфейсом програми. Ці правила визначають, який трафік слід блокувати або допускати.

г) Логування подій: Програма може вести журнал подій, реєструючи дії Firewall App, такі як блокування певного трафіку чи відхилення пакетів відповідно до правил.

д) Захист від атак: Firewall App може відстоюватися від різних мережевих атак, таких як злами, перехоплення даних або зміна пакетів.

Програма Firewall App реалізується за допомогою мережевих бібліотек у мові C, таких як libpcap або WinPcap для перехоплення пакетів, і може використовувати структури даних, такі як файрвол-таблиці, для ефективного аналізу та фільтрації трафіку. Вона є інструментом для забезпечення мережевої безпеки комп'ютерних систем і може бути використана для захисту як окремого комп'ютера, так і цілої корпоративної мережі від потенційних загроз. Основні частини коду написаної програми будуть подані в додатках.

3.3 Визначення і реалізація основних функцій

Основні функції системи:

а) Зчитування вхідних даних - розроблена система забезпечує можливість зчитування вхідних даних з різних джерел, клавіатури або з файлів. Для цього реалізовані відповідні функції зчитування і обробки вхідних потоків даних.

б) Обробка та аналіз вхідних даних - після зчитування вхідних даних система виконує їх обробку та аналіз відповідно до визначених правил і логіки роботи. Ця функціональність реалізується за допомогою відповідних функцій обробки даних, що включають у себе валідацію, перевірку на коректність та підготовку до подальшої обробки.

в) Виконання основної функціональності - програма реалізує основну функціональність згідно з поставленими завданнями. Це може бути обробка даних, генерація вихідних результатів або виконання специфічних операцій згідно з логікою програми.Вивід результатів - після виконання основних операцій система виводить результати своєї роботи. Нижче буде розглянуто основні функції програми такі як: правила блокування адрес, фільтрація, списки додатків та налаштування. На рисунку 3.4 зображено список встановлених додатків які не потребують доступу в інтернет, при наведенні буде відображено всю потрібну інформацію про той чи інший додаток.

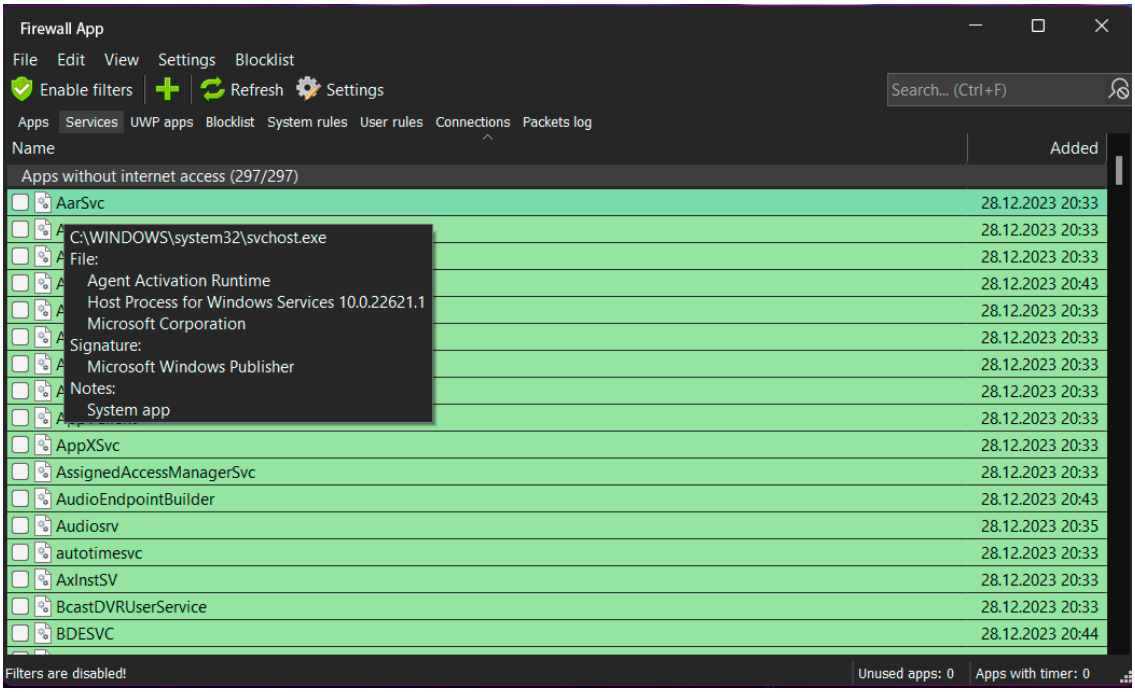

Рисунок 3.4 – Список додатків які не потребують доступ в інтренет

На рисунку 3.5 зображено всі програми які використовуються в даний момент часу, також вказано їх IP адреси та порти на момент використання, за потреби можна додати правило фільтрації до кожної програми.

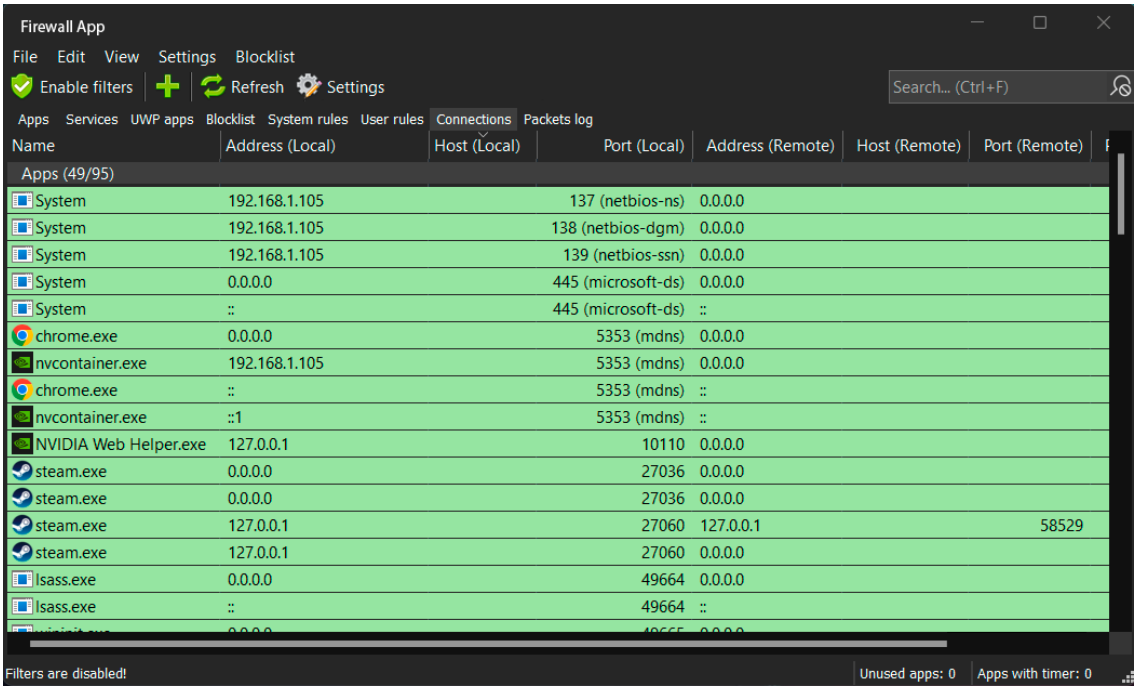

Рисунок 3.5 – Список підключених програм та їх адреси

Рисунок 3.6 відображає стантартні протоколи до яких входять: DNS, DNCP, IGMP, NTP та інші. Кожен з них виконує важливу роль у мережевому середовищі, та їх блокування може мати різні наслідки в залежності від контексту мережі та потреб користувачів.

DNS перетворює доменні імена в IP-адреси і навпаки, дозволяючи користувачам зручно використовувати імена веб-сайтів замість запам'ятовування IP-адрес. DHCP автоматично надає IP-адреси та інші мережеві параметри пристроям у мережі, що дозволяє їм автоматично підключатися до мережі. IGMP використовується для керування багатозадачними мережами, де пакети мультимедійного потоку передаються тільки тим пристроям, які виразили бажання отримати такий потік. NTP забезпечує синхронізацію часу між різними комп'ютерами у мережі, що дозволяє забезпечити точність часового управління.

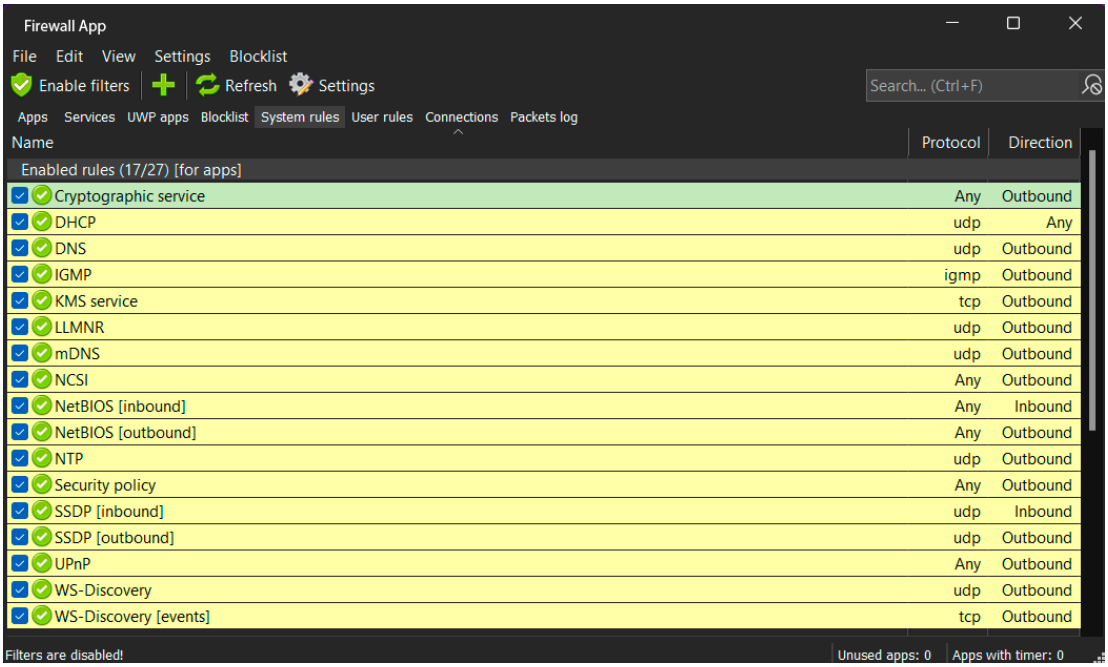

Рисунок 3.6 – Протоколи

Також в програмі за потреби є можливість додавати та редагувати протоколи. Протоколи визначають правила обміну даними, формати пакетів, порядок взаємодії і обробки помилок. Такі правила дозволяють різним системам ефективно і надійно спілкуватися, незалежно від їхніх характеристик чи виробників. Вдало розроблений протокол дозволяє забезпечити ефективну та надійну комунікацію між різними системами у мережевому середовищі.

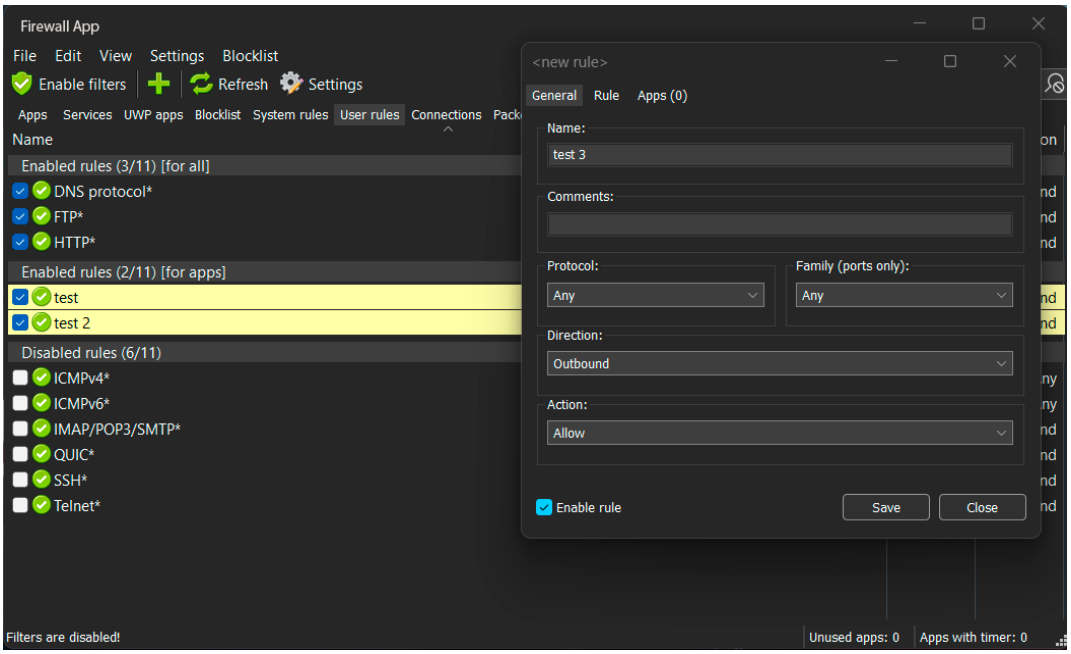

Рисунок 3.7 – Додавання та редагування протоколів

На рисунку 3.8 зображено можливість блокувати та надавати дозвіл для тієї чи іншої адреси. Це дає можливість більш гнучко налаштовувати захист пристрою під потреби користувача.

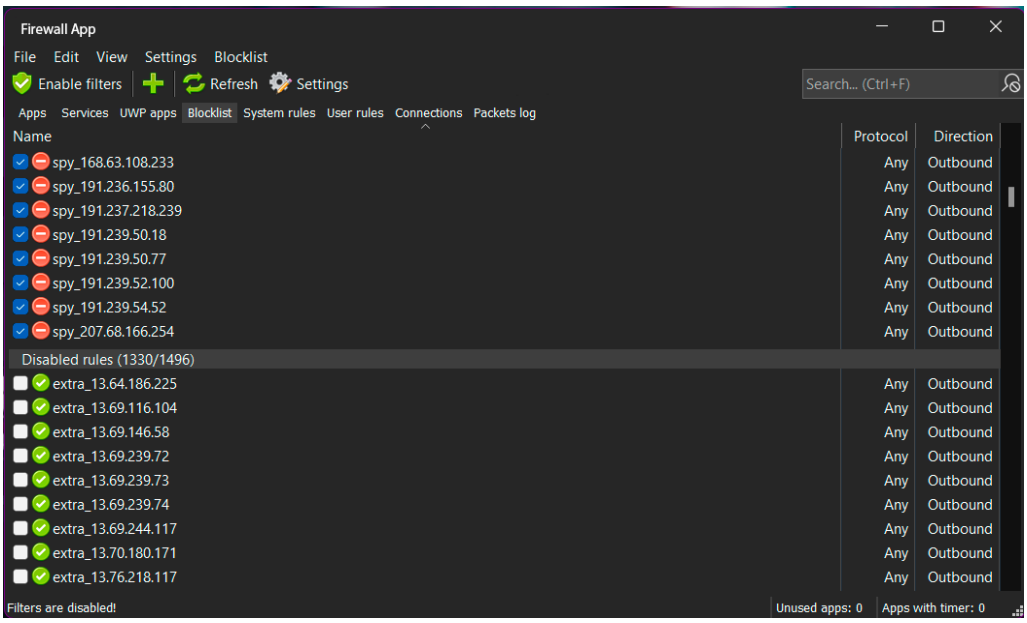

Рисунок 3.8 – Блокування та дозвіл адрес

Також було реалізовано гнучке налаштування самої програми Firewall App. Налаштування дозволяють адміністраторам точно керувати захистом і безпекою трафіку з урахуванням вимог конкретного середовища. До основних налаштувань входять: General, Interface, Highlighting, Rules, Blocklist, Notification, Packet log Exclude.

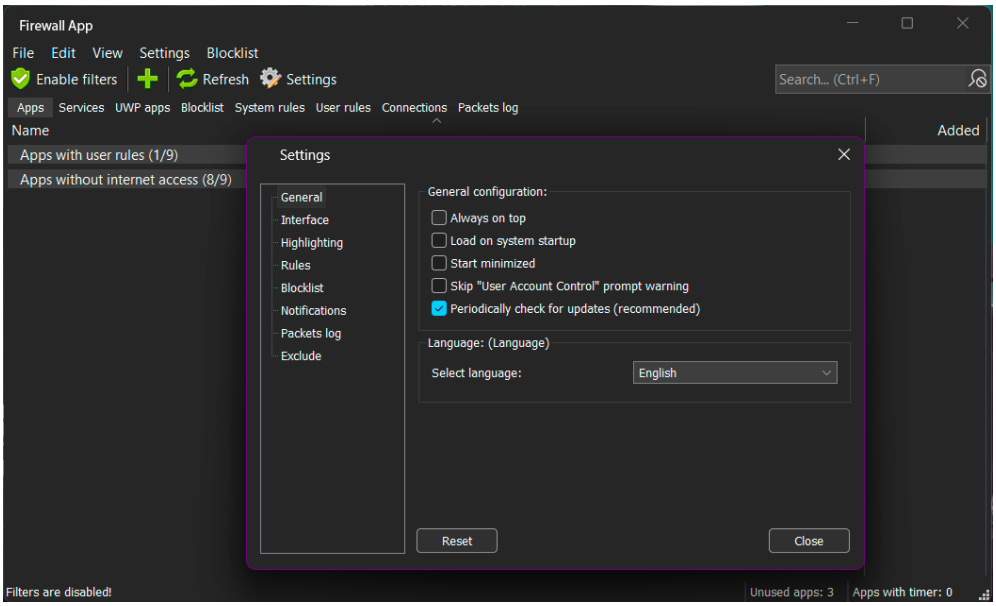

Рисунок 3.9 – Налаштування програми

У цьому розділі було детально розглянуто визначення та реалізацію основних функцій розробленого засобу, програмуваного мовою С. Основні функції системи включають зчитування вхідних даних, їх обробку та аналіз, виконання основної функціональності та вивід результатів.

Реалізація основних функцій була продемонстрована у прикладі коду, де показано послідовність дій зчитування даних, їх обробки та виведення результатів за допомогою функцій мови програмування С.

Виконання цих основних функцій дозволяє системі ефективно взаємодіяти з користувачем або іншими системами, обробляти вхідні дані та надавати корисні результати відповідно до вимог та цілей програмного продукту. Детальна реалізація основних функцій забезпечує стабільну та ефективну роботу системи, що дозволяє досягти поставлених цілей розробки.

3.4 Тестування та аналіз ефективності

Процес тестування та аналізу ефективності розробленого застосунку Firewall App включає ряд кроків та методів, спрямованих на перевірку функціональності, стабільності та продуктивності програми.

Обраний метод тестування: Тестування проводиться вручну за допомогою розроблених тестових сценаріїв. Введення вхідних даних та перевірка правильність реакції програми на ці дані.

Функціональне тестування: Проводиться тестування окремих функціональних частин Firewall App. Перевірка коректності роботи правил фільтрації, обробка пакетів ідентифікації загроз, перевірка правильності збереження налаштувань. Після ввімкнення програми основні задані правила фільтрації застосувалися коректно, з можливістю додавання вторичних. Також було виявлено недоліки такі як:

1. Після ввімкнення неможливо додати нові правила фільтрації

2. Кнопка “Refresh” працює не до кінця коректно

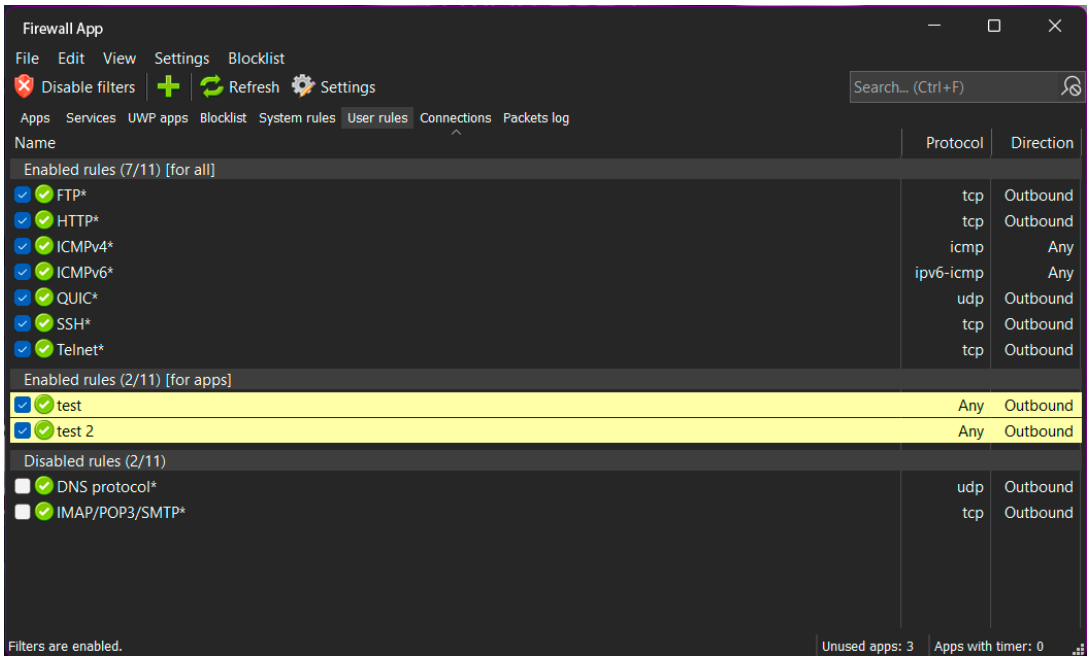

Рисунок 3.10 – Перевірка коректності правил фільтрації

Інтеграційне тестування: Тестування взаємодії між різними компонентами Firewall App. Включає перевірку взаємодії між модулями фільтрації, модулями обробки загроз, системою керування правилами. Під час тестування програми не було виявлено помилок які б відображалися в журналі, під час тестування також не було виявлено помилок які б привели до закриття чи некоректної поведінки програми. Із недоліків цього тестування було виявлено наступне:

– “Packets log” працює але не відображає актуальні мережеві зв’язки;
– Під час активного працювання програми система керування правилами не працює.

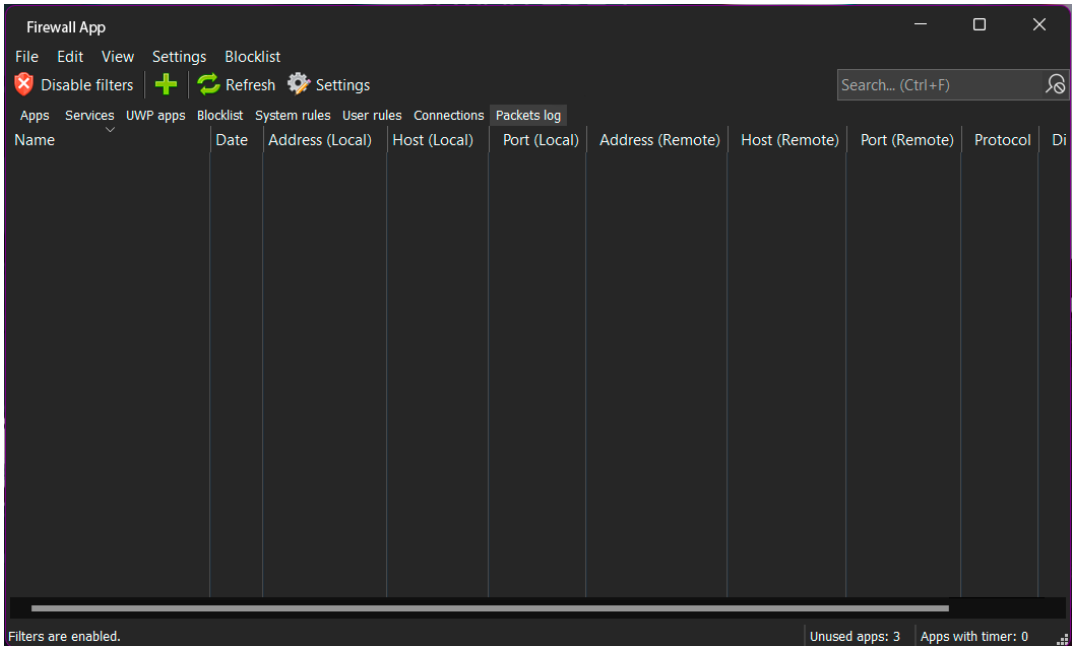

Рисунок 3.11 – Перевірка помилок

Стрес-тестування: Проведення тестування з метою визначення стійкості та продуктивності Firewall App при великому обсязі трафіку або при інтенсивному навантаженні. Під час тестування не було виявлено зниження продуктивності, тестування проводилося на одному пристрої з одним користувачем, можливо під час навантаження будуть певні проблеми.

Проведений аналіз ефективності допоміг виявити потенційні проблеми та можливі вдосконалення, необхідні для оптимального функціонування Firewall App. Щодо в досконалення то можна вивести наступні кроки які покращать програму:

- Виправити всі недоліки перераховані вище;
- Оптимізувати швидкодію та ефективність Firewall App під час обробки мережевого трафіку. Використання більш ефективних алгоритмів фільтрації або оптимізація обробки великих обсягів даних;
- Розширити функціональність і покращити зручність використання інтерфейсу для забезпечення більшої зрозумілості та ергономічності для користувачів;
- Ідентифікувати потенційно можливі розширення функціональності Firewall App, наприклад, додати нові типи правил фільтрації, підтримку додаткових

протоколів, аналіз нових видів загроз.

Ці кроки допоможуть досягти більшої ефективності, функціональності та безпеки програми Firewall App, що сприятиме її успішному впровадженню та використанню у реальних умовах.

Порівняння Firewall App з відомими аналогами, такими як Check Point, Fortinet і Juniper Networks, відбувається за кількома ключовими критеріями, що включають функціональність, продуктивність, безпеку та зручність використання:

- Функціональність: Firewall App надає широкий набір функцій, включаючи фільтрацію трафіку, керування правилами доступу, виявлення загроз. Check Point, Fortinet, Juniper Networks: Відомі своїми розширеними функціональними можливостями, такими як розумна аналітика трафіку, управління доступом на основі ідентифікації користувачів, захист від апаратних та програмних загроз, технології миттєвої відновлення роботи після витоку даних тощо.
- Продуктивність: Firewall App демонструє задовільну продуктивність при обробці мережевого трафіку та використанні ресурсів.Check Point, Fortinet, Juniper Networks: Відомі своєю високою продуктивністю та ефективністю в управлінні великими обсягами трафіку, забезпечуючи низьку затримку та високу пропускну здатність.
- Безпека: Firewall App має ефективні механізми виявлення та реагування на загрози, але може потребувати покращень для конкурентного рівня захисту. Check Point, Fortinet, Juniper Networks: Володіють високим рівнем захищеності, здатністю виявлення та запобігання різноманітним кіберзагрозам, включаючи атаки DDoS, шкідливе ПЗ та витоки даних.
- Зручність використання: Firewall App має зручний інтерфейс користувача, але може потребувати додаткових поліпшень для більшої зрозумілості та зручності налаштування правил. Check Point, Fortinet, Juniper Networks: Відомі своїм інтуїтивно зрозумілим інтерфейсом, детальними звітами та документацією, а також широким спектром інструментів адміністрування.

Висновок: Firewall App є конкурентоспроможним рішенням з широким набором функцій та задовільною продуктивністю. Однак в порівнянні з Check Point, Fortinet і Juniper Networks, він може потребувати додаткових покращень у відношенні до захисту від загроз та зручності використання. Користуючись результатами порівняльного аналізу, можна зробити висновки щодо потреби у подальшому розвитку та вдосконаленні Firewall App для покращення конкурентоспроможності та забезпечення задоволення вимог користувачів.

ВИСНОВКИ

1. Проведено аналіз принципів та технологій безпеки мереж. Основна увага приділялася визначенню базових концепцій мережевої безпеки, таких як контроль доступу, фільтрація трафіку, виявлення та реагування на інциденти. Вивчено різні методи захисту від кібератак, включаючи використання фаєрволів, систем виявлення вторгнень (IDS) та систем запобігання вторгненням (IPS).

2. Проведений аналіз існуючих засобів захисту показав, що фаєрволи є одними з найважливіших компонентів у забезпеченні безпеки корпоративних мереж. Виявлено, що сучасні програмні фаєрволи мають високу гнучкість і можуть ефективно інтегруватися в існуючі мережеві інфраструктури, забезпечуючи при цьому високий рівень захисту від широкого спектру загроз.

3. На основі аналізу вимог до системи захисту корпоративних мереж було обрано платформу .NET Framework для розробки програмного забезпечення. Враховувалися критерії, такі як сумісність з існуючими мережевими інфраструктурами, масштабованість, продуктивність та можливість інтеграції з іншими засобами безпеки.

4. Розроблено програмне забезпечення для захисту корпоративних мереж. Реалізовано функціонал фаєрвола, який включає фільтрацію трафіку, контроль доступу та моніторинг мережевої активності. Особлива увага приділялася оптимізації продуктивності та забезпеченню простоти налаштування для кінцевих користувачів. При розробці було використано модулі фільтрації трафіку та моніторингу мережевої активності. Використання цих модулів надало можливість створити комплексний захист мережі.

5. Тестування включало функціональне, навантажувальне та безпекове тестування. Результати показали, що система ефективно виявляє та блокує підозрілий трафік, забезпечує надійний захист від DDoS атак, тим самим забезпечуючи високу надійність та продуктивність у реальних умовах експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юзефович В.І. Програмні засоби захисту корпоративних мереж на основі фаєрволів. IX Науково-практична конференція молодих вчених і студентів «Інтелектуальні комп'ютерні системи та мережі». 21 травня 2024 р. Тернопіль. Україна. с.46.
2. Комп'ютерні мережі (5-е видання) / Таненбаум, А. С. та Везерол, Д. Дж., 2011, – 65с.
3. Комп'ютерна безпека (5-е видання) / Пфлігер, Ч. П., та Пфлігер, С. Л., 2012, – 14-55 с.
4. Том 1: Протоколи (2-е видання) / Стівенс, В. Р., Феннер, Б., та Рудофф, А. М., 2004. – 14 с.
5. Довідник з інтернет-протоколів / Козьєрок, Ч., 2005, – 67-69 с.
6. Check Point Software Technologies, посібник покупця міжмережевих екранів наступного покоління: веб-сайт. URL: https://www.checkpoint.com/next-generation-firewall-buyers-guide/ (дата звернення: 13.04.2024)
7. Fortinet Inc, порівняння міжмережевих екранів наступного покоління: веб-сайт. URL: https://www.fortinet.com/products/next-generation-firewall/comparison.html (дата звернення: 13.04.2024)
8. Juniper Networks, огляд міжмережевого екрану: веб-сайт. URL: https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-security-overview.html (дата звернення: 14.04.2024)
9. Cisco. Understanding Firewall Fundamentals: веб-сайт. URL: https://www.cisco.com/c/en/us/products/security/what-is-a-firewall.html (дата звернення: 14.04.2024)
10. Sophos. Sophos XG Firewall: Next-Gen Protection: веб-сайт. URL: https://www.sophos.com/en-us/products/next-gen-firewall.aspx (дата звернення: 14.04.2024)
11. FireEye. Advanced Threat Report: веб-сайт. URL:

https://www.fireeye.com/current-threats/annual-threat-report.html (дата звернення: 19.04.2024)

12. Snort Documentation: веб-сайт. URL: https://www.snort.org/documents (дата звернення: 19.04.2024-24.04.2024)

13. Економіка і управління в інноваційній діяльності. Навчальний посібник. Центр учбової літератури / Іванова О. О., 2019. 52-78с.

14. Техніко-економічне обґрунтування інвестиційних проектів. Центр учбової літератури / Даниленко, С. А., 2018. - 24-31с.

15. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 «Комп'ютерна інженерія» / І.Р. Паздрій – Тернопіль: ТАНГ, 2014. – 37 с.

16. Основи мережевої безпеки: додатки та стандарти (6-е вид.) / Сталлінгс В., 2016 – 134-136с.

17. Посібник для підготовки сертифікованих фахівців з інформаційної безпеки (8-е вид.) / Стюарт Д., 2018 – 44с.

18. Політики, процедури та стандарти інформаційної безпеки: керівництво для ефективного управління інформаційною безпекою (2-е вид.) / Пельтьє, Т. Р., 2016 – 92-122с.

19. Комп'ютерні мережі: підхід зверху вниз (7-е вид.) / Курос, Дж. Ф., & Росс, К. В., 2017 – 55с.

20. Внутрішня безпека мережевих периметрів (3-е вид.) / Норткатт, С., Зелцер, Л., Вінтерс, С., Фредрик, К., & Ранум, М., 2015 – 45-51с.

21. Керівництво по системах виявлення та запобігання вторгнень (IDPS) / Скарфон, К., & Хоффман, П., 2009 - 145с.

22. Практика моніторингу мережевої безпеки: розуміння виявлення інцидентів та реагування на них / Бейтліх Р., 2013 – 244-251с.

23. Біблія мережевої безпеки (3-е вид.) / Коул, Е., & Норткатт, С., 2019 – 15-22с.

24. Хаки мережевої безпеки: поради та інструменти для захисту вашої

приватності / Гаспар, Т., 2020 – 33-37с.

25. Повне керівництво з мережевої безпеки / Грем, Р., & Говард, С., 2011 – 61с.

26. Архітектура мережевої безпеки: принципи та практика (2-е вид.) / Ендрюс, Д., 2017 – 259-272с.

27. Основи мережевої безпеки (5-е вид.) / Кім Д., 2019 – 178с.

28. Практичний підхід до захисту мереж (4-е вид.) / Фішер, Е., Ерліх, Г., & Німет, Дж., 2018 – 167-170с.

29. Основи інформаційної безпеки (3-е вид.) / Фішер, А., & Іванов, О., 2016 – 41-50с.

30. Berezsky O., Berezska K., Batko Yu., Melnyk G. Vision-based medical expert system. 6th International Scientific and Technical Conference “Computer Sciences and Information Technologies”(CSIT'2011, Lviv, Ukraine, 16-19 November), 2011. P. 49-50.

31. Мережеві фаєрволи та VPN: будівництво безпечних мереж (4-е вид.) / Ніколс, Р., 2020 – 18-42с.

32. Методичні вказівки до випускних кваліфікаційних робіт освітнього рівня “Бакалавр” спеціальності “Комп’ютерна інженерія”/ О.М. Березький, Г.М. Мельник, Л.О. Дубчак, Ю.М. Батько, О.Й. Піцун / Під ред. О.М. Березького. Тернопіль: ЗУНУ, 2024. 52 с.

33. Методичні вказівки до виконання практичних робіт з дисципліни «Техніко-економічне обґрунтування розробки комп’ютерних систем”/ Н.Я. Савка, І.Р. Паздрій / Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2019. 40 с.

34. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» / І.В. Гураль, Л.О. Дубчак / Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2019. 33 с.