Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

(повна назва)

Кафедра Інфокомунікаційної інженерії імені В.В. Поповського

(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження ефективності засобів проактивного захисту приграничних маршрутизаторів IP-мережі

(тема)

Виконав:

студент 2 курсу, групи АМСЗІизм-21-1

Алієв Д.Х.

(прізвище, ініціали)

Спеціальність: 125 Кібербезпека

(код і повна назва спеціальності)

Тип програми: освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Освітня програма: Адміністративний менеджмент у сфері захисту інформації

(повна назва освітньої програми)

Керівник: зав. каф. ІКІ імені В.В. Поповського Лемешко О.В.

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Лемешко О.В.

(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ

Зав. кафедри___ _____
(підпис)

«____»_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Алієву Джейхуну Хідаят огли
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження ефективності засобів проактивного захисту пригранічних маршрутизаторів IP-мережі
затверджена наказом по університету від 24.10.2022 р. № 173Стз
2. Термін подання студентом роботи до екзаменаційної комісії: 15.05.2023 р.
3. Вихідні дані до роботи: методи математичного програмування; моделі та методи безпечної маршрутизації без і з балансуванням навантаження; засоби моделювання процесів безпечної маршрутизації (середовище Python IDLE); вихідні дані для проведення моделювання (структура досліджуваної мережі, пропускна здатність каналів зв'язку, базові метрики критичності вразливостей обраного мережного обладнання).
4. Перелік питань, які потрібно опрацювати в роботі:
1) Аналіз стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання.
2) Огляд функціональних можливостей протоколів сімейства FHRP.
3) Аналіз ймовірних атак на протоколи сімейства FHRP та методів боротьби з ними.
4) Огляд методів протидії атакам на пригранічні маршрутизаторів IP-мережі.
5) Вибір та дослідження методів та засобів проактивного захисту пригранічних маршрутизаторів IP-мережі

6) Розробка рекомендацій щодо практичного використання досліджених рішень
5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації (титульний слайд; опис проблеми, об'єкт, предмет і мета дослідження; аналіз стандарту CVSS; класифікація протоколів маршрутизації; порівняння протоколів сімейства FHRP; опис та результати дослідження методу проактивного захисту приграничних маршрутизаторів мережі; висновки).

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	завідувач кафедри Лемешко Олександр Віталійович		01.05.2023

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	24.10.2022 р.	Виконано
2	Збір матеріалів для дослідження	14.11.2022 р.	Виконано
3	Розробка 1 розділу	28.11.2022 р.	Виконано
4	Розробка 2 розділу	23.12.2022 р.	Виконано
5	Розробка 3 розділу	17.01.2023 р.	Виконано
6	Розробка 4 розділу	05.13.2023 р.	Виконано
7	Оформлення кваліфікаційної роботи	01.05.2023 р.	Виконано

Дата видачі завдання 24 жовтня 2022 р.

Студент _____ Алієв А.Х.
(підпис) (прізвище та ініціали)

Керівник роботи завідувач кафедри ІКІ ім. В.В. Поповського

_____ Лемешко О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 62 с., 28 рис., 5 табл., 39 джерела.

ІНФОКОМУНІКАЦІЙНА МЕРЕЖА, МЕРЕЖНА БЕЗПЕКА, АТАКА, ВРАЗЛИВІСТЬ, ЗАХИСТ, МЕТОД, ДОСЛІДЖЕННЯ.

Об’єкт дослідження – процес забезпечення проактивного захисту пригранічних маршрутизаторів IP-мережі.

Предмет дослідження – методи забезпечення проактивного захисту пригранічних маршрутизаторів IP-мережі.

Мета роботи – підвищення рівня проактивного захисту пригранічних маршрутизаторів IP-мережі.

Методи досліджень – аналітичне моделювання, симуляція, оптимізація.

В роботі проводиться аналіз рівня безпеки маршрутизаторів мережі, методів їх кіберзахисту від мережних атак та вторгнень. Основна увага приділяється аналізу та дослідженню методів проактивного захисту пригранічних маршрутизаторів у IP-мережі, заснованих на забезпеченні балансування навантаження у відповідності до рівня безпеки цих маршрутизаторів. Рівень безпеки оцінювався відповідно до методики, запропонованої стандартами CVSS з врахуванням переліку ймовірних вразливостей, їх важливості та ймовірності реалізації.

Запропонована система рекомендацій щодо впровадження у IP-мережах обраних для дослідження методів забезпечення проактивного захисту пригранічних маршрутизаторів на підставі автоматизації налаштування протоколу відмовостійкої маршрутизації GLBP.

ABSTRACT

The report contains: 62 p., 28 fig., 5 tables, 39 sources.

INFORMATION COMMUNICATION NETWORK, NETWORK SECURITY, ATTACK, VULNERABILITY, PROTECTION, METHOD, RESEARCH.

The object of research is the process of providing proactive protection of border routers of the IP network.

The subject of research is methods of providing proactive protection of border routers of the IP network.

The work aims to increasing the level of proactive protection of border routers of the IP network.

Research methods are analytical modeling, simulation, optimization.

The paper analyzes the level of security of network routers, methods of their cyber protection against network attacks and intrusions. The main attention is paid to the analysis and research of the methods of proactive protection of border routers in the IP network, based on ensuring load balancing in accordance with the security level of these routers. The level of security was evaluated according to the methodology proposed by the CVSS standards, taking into account the list of possible vulnerabilities, their importance and probability of implementation.

The proposed system of recommendations for the implementation of the methods selected for research in IP networks to provide proactive protection of border routers based on the automation of configuration of the GLBP fault-tolerant routing protocol.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

БШМ – багатошляхова маршрутизація

ІКМ – телекомунікаційна мережа

ОС – операційна система

ОШМ – одношляхова маршрутизація

ПЗ – програмне забезпечення

CVSS – Common Vulnerability Scoring System

DDoS – Distributed Denial of Service

DoS – Denial of Service

EIGRP – Enhanced Interior Gateway Routing Protocol

FRR – Fast ReRoute

IP – Internet Protocol

ITU-T – International Telecommunication Union Telecommunication Standardization Sector

NGN – Next Generation Network

OSI – Open Systems Interconnection

OSPF – Open Shortest Path First

QoS – Quality of Service

SDN – Software Defined Network

TE – Traffic Engineering

ВСТУП

Основною вимогою, яка висувається до сучасних систем захисту інформації, є забезпечення кібербезпеки на всіх етапах життєвого циклу інформації: від її створення, зберігання, обробки, прийому та передачі – до відображення, архівування та знищення. Ключове місце у загальній архітектурі захисту інформації належить саме етапам її передачі, прийому та проміжної обробки на комунікаційних пристроях інфокомунікаційних мереж (ІКМ) [1 – 3].

ІКМ – це територіально розподілені гетерогенні системи. Це, у свою чергу, значно ускладнює процес контролю та координації процесі захисту інформації. Використання обладнання різних компаній-виробників мережного обладнання, які підтримують різні стеки протоколів, також вносить певні складності у забезпечення комплексного захисту інформації в ІКМ. Таким чином, все більше уваги фахівцями у галузі захисту інформації приділяється питанням мережної безпеки [4 – 9]. Тобто інформація має захищатись як на рівні термінального обладнання, персональних, локальних та глобальних мереж, так і на рівні сервісів та площини управління мережею. Це, як правило, забезпечується модифікацією програмного забезпечення комунікаційних пристроїв та мережних екранів (фаєрволів) на рівні їх операційних систем.

Проте і самі комутатори, маршрутизатори та фаєрволи самі можуть ставати об’єктами, проти яких здійснюються мережні атаки. При цьому метою таких вторгнень може бути не тільки заволодіння конфіденційною інформацією, яка передається в ІКМ, але й порушення працездатності самої мережі, яка відповідає за надійну і своєчасну передачу різноманітних даних – мультимедіа (відео, аудіо), файлів тощо. Тобто однією з цілей мережних атак може бути зрив надання ІКМ інфокомунікаційних сервісів та/або зниження рівня якості обслуговування (Quality of Service).

Для забезпечення високого рівня мережної безпеки на практиці використовується досить широкий спектр методів, схем та засобів, які умовно можна розділити на дві великі групи: проактивні та реактивні рішення [1, 8 – 10]. Проактивні рішення, як правило, направлені на створення таких умов, щоб максимально ускладнити роботу зловмиснику з точки зору організації мережних атак. Це досягається постійним оновленням апаратного та програмного

забезпечення комунікаційного обладнання для ліквідації або мінімізації наслідків від використання наявних вразливостей. Реактивні рішення реалізуються після встановлення факту використання вразливості у процесі мережної атаки. Їхньою метою є, як правило, мінімізація наслідків від дії такої атаки. Ці рішення потрібно реалізувати у комплексі, на системним принципах взаємодоповнення та цілісності.

У даній роботі основна увага приділяється задачам дослідження ефективності засобів проактивного захисту пригранічних маршрутизаторів IP-мережі на рівні математичних методів та технологічних протоколів. Проведено аналіз відомих методів проактивного захисту пригранічних маршрутизаторів, встановлено їх переваги, недоліки та область застосування [1, 8 – 14]. Для дослідження обрано оптимізаційний метод проактивного захисту пригранічних маршрутизаторів IP-мережі, заснований на використанні декількох пригранічних маршрутизаторів, які виконують функцію шлюзу за замовчуванням. Балансування навантаження реалізується на принципах врахування рівня мережної безпеки маршрутизаторів, який оцінюється на підставі використання стандартів CVSS (Common Vulnerability Scoring System) [15 – 18].

За результатами дослідження запропоновано систему рекомендацій щодо практичного використання результатів дослідження в існуючих IP-мережах та програмно-конфігурованих мережах.

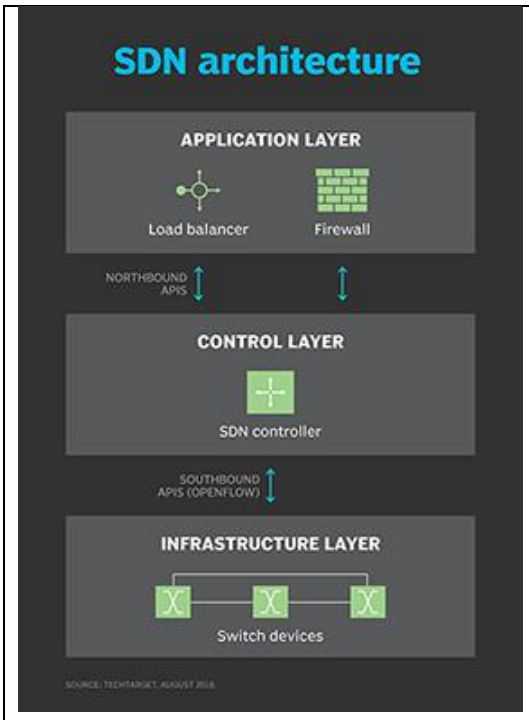
1 ЗНАЧЕННЯ МЕРЕЖНОЇ БЕЗПЕКИ ДЛЯ СУЧАСНИХ ІНФОКОМУНІКАЦІЙ

1.1 Вимоги, які висуваються до сучасних інфокомунікаційних систем та мереж

Сучасний світ нерозривно пов'язаний з розвитком інформаційних та комунікаційних технологій. При цьому матеріалізація цих технологій відбувається в межах інфокомунікаційних систем та мереж, що дозволяють отримати повний, безперервний та безперешкодний доступ до сучасних сервісів та інформаційних ресурсів кожній людині [1-3, 5]. Інфокомунікаційні мережі вже давно пройшли етап інтеграції сервісів та будуються як складні мультисервісні платформи відповідно до стандартів мереж зв'язку наступного покоління (Next Generation Network, NGN).

Найбільш новітнім технологічним рішенням останніх років, яке стосується ІКМ, є створення та розвиток технологій програмно-конфігурованих мереж (Software-Defined Networking, SDN) [4]. Основною рисою таких мереж э відділення у мережному обладнанні площини управління від площини пересилання даних та підсилення функцій централізації управління мережею (рис. 1.1). Інтелектуальним центром SDN стає SDN-контролер, на який покладаються ключові функції щодо збору інформації про стан мережі, її обробки у реальному часі та управління мережею з виконанням операцій щодо надання та підтримки тих чи інших сервісів. Для підвищення надійності орієнтованих на централізацію функцій управління в архітектурі SDN може налаштовуватись множина SDN-контролерів, частина з яких можуть працювати у режимах «холодного» та/або навантаженого резерву.

В межах SDN можливо створити єдину надійну розподілену систему управління для централізованого обслуговування всіх процесів, що запущені в ІКМ. Ініціатори створення та розробники SDN планують впровадження насамперед у центрах обробки та зберігання даних, у хмарних середовищах, а також у територіально-розподілених, локальних мережах, мережах мобільного зв’язку тощо.



Архітектура SDN	
Рівень застосунків	
Рівень управління	
Рівень інфраструктури	

Рисунок 1.1 – Загальна архітектура SDN

Основні принципи програмно-конфігурованих мереж полягають у наступному:

- відділення рівня передачі від рівня управління;
- єдиний, уніфікований, незалежний від постачальника інтерфейс між рівнем управління та рівнем передачі даних;
- переважно централізоване управління мережею, яке здійснюється за допомогою контролера з мережевою операційною системою (ОС);
- віртуалізація фізичних ресурсів мережі.

Головна вимога, яка висувається до ІКМ, – це виконання нею своєї основної функції: надання користувачам мережі сучасних інфокомунікаційних функцій із забезпеченням високого рівня якості обслуговування [5]. До подібних сервісів, як правило, відносять (рис. 1.2):

- організація відеоконференцій;
- голосовий зв’язок;
- передача рухомих та нерухомих зображень;
- інтернет телебачення;
- передача файлів;

- передача коротких повідомлень тощо.

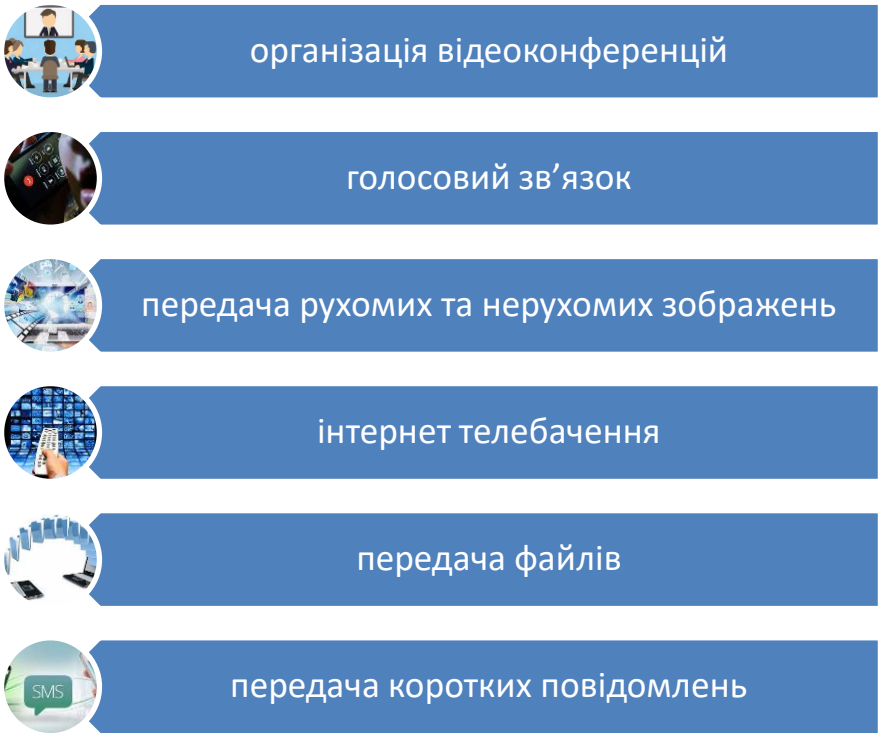


Рисунок 1.2 – Перелік основних інфокомунікаційних сервісів

Проте систему вимог, які так чи інакше висуваються до сучасних ІКМ [5, 8], можна спробувати представити таким переліком (рис. 1.3):

- забезпечення мультисервісності;
- підтримка мультимедійності сервісів;
- підтримка мультипротокольності та гетерогенності;
- забезпечення високої надійності, відмовостійкості та доступності;
- орієнтованість на відриті стандарти;
- забезпечення апаратної та програмної сумісності;
- підтримка автоматизованих та масшабованих рішень.

Рисунок 1.3 – Перелік основних вимог, які висуваються до ІКМ

Однак з підвищенням рівня автоматизації управління мережею, коли більшість функцій щодо передачі інформації, розподілу мережних ресурсів та надання сервісів перекладається на комунікаційні протоколи, загострюється проблема забезпечення мережної безпеки. Під мережною безпекою (Network security) надалі буде розумітись одна з частин інформаційної безпеки, яка зосереджена на захисті інфокомунікаційних мереж від кіберзагроз. Взагалі мережна безпека має такі основні цілі:

- запобігання та протидія несанкціонованому доступу до мережних ресурсів;

- запобігання, виявлення та припинення випадкового або навмисного втручання в роботу мережі, поточних кібератак і порушень безпеки мережі, спроб руйнування її компонентів – пристроїв, програм, протоколів та сервісів;

- гарантування авторизованим користувачам безпечного доступу до необхідних мережних ресурсів та сервісів, коли вони їм потрібні.

При налаштуванні плав та політик мережної безпеки, технологій та протоколів її забезпечення важливою задачею стає визначення методики оцінювання рівня мережної безпеки комунікаційного та мережного обладнання, яке використовується ІКМ для виконання своїх функцій.

1.2 Аналіз стандарту CVSS щодо визначення рівня вразливості мережного обладнання

Як показав проведений аналіз [15 – 18] дуже розповсюдженою практикою при оцінювання рівня мережної безпеки є використання систем оцінки вразливостей (Common Vulnerability Scoring System, CVSS), описаної в межах стандартів Національного інституту стандартів та технологій (National Institute of Standards and Technology, NIST). CVSS – це відкритий галузевий стандарт для оцінки важливості вразливостей безпеки інформаційних систем, заснований на аналізі виявлених загроз безпеці тих чи інших пристроїв та їх програмному забезпеченню.

Двома поширеними способами використання CVSS є обчислення (оцінка) важливості вразливостей, виявлених у інформаційних системах, і визначення пріоритетності заходів з усунення виявлених вразливостей. Національна база даних про вразливості (NVD), яка постійно поповнюється, надає оцінки CVSS для багатьох відомих вразливостей. NVD підтримує стандарти CVSS v2.0 і v3.X. NVD надає «базові оцінки» CVSS, які представляють характерні ознаки тієї чи іншої вразливості. Зараз CVSS працює у своїй третій основній версії (v3), яка була розроблена для усунення деяких недоліків її попередниці, v2. Зокрема, версія 3 враховує на привілеї, необхідні для використання вразливості, а також можливість для шкідливого програмного забезпечення (ПЗ) поширюватися між системами після використання вразливості.

CVSS належить і управляється FIRST.Org, Inc. (FIRST), яка є некомерційною організацією зі штаб-квартирою в США, місія якої полягає в тому, щоб допомагати групам реагування на інциденти інформаційної безпеки по всьому світу. Офіційна документація CVSS розміщена на ресурсі https://www.first.org/cvss/. У загальному випадку CVSS складається з трьох груп показників: базові (Base), часові (Temporal) і середовища (Environmental) (рис. 1.4).

Рисунок 1.4 – Групи показників CVSS

Як показано на рис. 1.4 базові фактори представляють характеристики самої вразливості, вони дають оцінку в діапазоні від 0 до 10. Ці характеристики не змінюються у часі не залежать від можливості використання в реальному світі або від компенсаційних факторів, які підприємство запровадило для заборони використання. Загальнодоступні рейтинги, наприклад ті, що перераховані в національній базі даних вразливостей NIST (NVD), стосуються виключно базових балів CVSS [15 – 18].

Оцінки Base CVSS має обмежене використання, оскільки не враховує реальні експлойти, доступність виправлень або інші засоби контролю, які запроваджує організація. Базові показники CVSS складаються з трьох елементів підрахунку – можливості використання, масштабу та впливу. У свою чергу показники можливості використання складаються з характеристик уразливого компонента, при цьому можливість використання складається з чотирьох додаткових підкомпонентів: вектор атаки, складність атаки, необхідні привілеї, взаємодія користувача.

Вектор атаки залежить від рівня доступу, необхідного для використання вразливості. Ця оцінка буде вищою для експлойтів, які можна виконати віддалено (тобто за межами мережі компанії), ніж для експлойтів, які вимагають фізичної присутності (тобто необхідно мати доступ до фізичного порту на пристрої або доступ до локальної мережі всередині приватних даних центр). Складність атаки змінюється залежно від факторів поза контролем зловмисника, необхідних для використання вразливості. Саме ця оцінка буде вищою для експлойтів, які вимагають додаткової роботи з боку зловмисника, як-от викрадення спільного секретного ключа або атаки «людина посередині», ніж для атаки, яка не потребує таких додаткових зусиль. Необхідні привілеї залежать від

привілеїв, необхідних зловмиснику для здійснення експлойту. Уразливість, для використання якої потрібні адміністративні привілеї, матиме вищу оцінку, ніж уразливість, яка не потребує автентифікації або підвищених привілеїв з боку зловмисника. Взаємодія користувача залежить від того, чи повинен зловмисник залучити добровільного чи випадкового учасника, щоб виконати своє завдання. Оцінка буде вищою, якщо зловмисник зможе працювати автономно, без участі користувача.

Масштаб стосується того, чи може вразливість в одному компоненті поширюватися на інші компоненти. Оцінка масштабу вища, якщо можливе поширення. Приклади масштабу включають можливість доступу та використання базової операційної системи після використання вразливості ПЗ або доступ зловмисника до серверної бази даних після успішного використання вразливості на веб-сервері.

Вплив зосереджується на фактичному результаті, якого може досягти атакуючий в результаті використання даної вразливості. Показники впливу складаються з трьох підметрик – конфіденційності, цілісності та доступності. Конфіденційність залежить від обсягу даних, до яких зловмисник отримує доступ. Він буде вищим, якщо зловмисник матиме доступ до всіх даних у враженій системі, і нижчим, якщо дані недоступні. Цілісність як показник змінюється залежно від здатності зловмисника змінювати дані в зараженій системі. У випадку можливості повних та суттєвих непрямих змін даних, цей бал буде високим. Оцінка доступності змінюється залежно від втрати доступності використовуваної інформаційної системи. Оцінка буде високою, якщо в результаті атаки система стає недоступною або непридатною для використання навіть авторизованими користувачами.

Назва часових показників CVSS пов’язана з вразливістю, яка змінюється з часом. Ці показники вимірюють поточну можливість використання вразливості, а також доступність засобів управління виправленням. Підкомпоненти часових показників включають ефективність коду експлойту, рівень виправлення та достовірність звіту. Всім зрозуміло, що доки не існує методу використання вразливості, вона є відносно безпечною. Як і у випадку з більшістю прикладів програмного забезпечення, код, що доступний для здійснення експлойтів, може з часом розвиватися, вдосконалюватись, ставати стабільнішим і доступнішим. Коли це станеться, оцінка цього підкомпонента збільшиться. Рівень виправлення

впливає на те, що коли вразливість виявляється вперше, можливо, не буде доступного виправлення. Але з часом стають доступними тимчасові виправлення та, зрештою, офіційні оновлення, що призводить до зниження оцінки вразливості в міру вдосконалення виправлення. Достовірність вимірює рівень перевірки, який демонструє, що вразливість є реальною та її можна використовувати.

Показники середовища CVSS дозволяють організації (компанії) змінювати базовий CVSS на основі вимог безпеки та модифікацій базових показників. Вимоги безпеки характеризують критичність відповідного активу. Критично важливі дані або ресурси отримують вищу оцінку, ніж менш важливі активи. Наприклад, уразливість, виявлена в базі даних усіх клієнтів, отримає вищу оцінку, ніж уразливість, виявлена на робочій станції рядового непривілейованого користувача. З іншого боку, організація може змінити значення базових показників CVSS на основі заходів протидії, які вона застосувала. Наприклад, відключення серверу або зовнішніх мережних з'єднань заборонить зловмисникові використовувати вразливість, яка раніше була доступна віддалено. Результатом є те, що базова метрика вектору атаки в цьому випадку зменшується.

Іноді корисно, зіставити оцінки CVSS (0÷10) з якісними оцінками. FIRST порівнює бали CVSS із цими якісними оцінками наступним чином [15 – 18]:

Таблиця 1.1 – Порівняння балів CVSS із якісними оцінками

Оцінка CVSS	Якісна оцінка уразливості
0,0	Відсутня
0,1 – 3,9	Низька
4,0 – 6,9	Середня
7,0 – 8,9	Висока
9,0 – 10,0	Критична

1.3 Огляд технологічних засобів забезпечення мережної безпеки

Як правило засоби забезпечення мережної безпеки працюють на двох рівнях: на периметрі мережі та всередині самої мережі. На периметрі засоби безпеки намагаються зупинити кібератаки від проникнення в мережу. У випадку проникнення кіберзагрози до мережі відповідні засоби мають контролювати стан мережної безпеки всередині ІКМ. Щоб побудувати системи мережевої безпеки, поєднують можливості такі дієві інструменти, як брандмауери, засоби контролю доступу до мережі, системи виявлення та запобігання вторгненням, віртуальні приватні мережі, різноманітні засоби управління трафіком тощо [6, 12, 19].

Брандмауер запобігає надходженню або виходу підозрілого трафіку з мережі, одночасно пропускаючи легітимний трафік. Брандмауери можна розгорнути на границі мережі або ж використовувати всередині, розділивши велику мережу на окремі підмережі. Тому коли буде скомпрометована певна частина мережі, інша частина мережі все ж буде залишатись у безпеці. Як правило брандмауери використовують фільтрацію пакетів для перевірки трафіку. Вдосконалені варіанти брандмауерів наступного покоління доповнюються засобами запобігання вторгненням, які функціонують за допомогою методів штучного інтелекту і машинного навчання.

Рішення з контролю доступу до мережі діють як поліцейські, автентифікуючи та авторизуючи користувачів, щоб чітко визначити, якому трафіку дозволено входити в мережу та що він може роботи у подальшому у мережі всередині. Рішення з контролю доступу до мережі часто використовують політики управління доступом на основі ролей, у яких права та привілеї користувачів залежать від їхніх посадових функцій. Окрім автентифікації користувачів, деякі рішення з цієї області можуть виконувати оцінку ризиків на рівні користувачів. Це потрібно для того, щоб незахищені або скомпрометовані пристрої не мали доступу до мережі. Наприклад, якщо користувач намагається увійти в мережу з кінцевого пристрою із застарілим антишкідливим (антивірусним) програмним забезпеченням або неправильними конфігураціями, то засоби контролю автоматично заборонять доступ.

Системи виявлення та запобігання вторгненням (IDPS) можна розгорнути безпосередньо за брандмауером для сканування та аналізу вхідного трафіка на наявність загроз безпеці. Ці інструменти безпеки розвинулися на основі систем

виявлення вторгнень (IDS). IDS лише позначали підозрілу активність для подальшої перевірки. А вже IDPS мають додаткову можливість автоматично реагувати на можливі порушення, наприклад, блокуючи трафік або, навіть, скидаючи з'єднання. IDPS особливо ефективні у виявленні та блокуванні атак грубої сили та атак на відмову в обслуговуванні (DoS) або розподілених атак на відмову в обслуговуванні (DDoS).

Віртуальні приватні мережі (VPN) захищають особистість користувача на підставі шифрування його даних, маскування його IP-адреси та місцезнаходження у цілому. З використанням VPN користувач підключається не безпосередньо до мережі, а до захищеного сервера, який підключається до мережі від його імені. Одним з призначень VPN є те, що вони можуть допомогти віддаленим працівникам безпечно отримувати доступ до корпоративних мереж, навіть через відносно незахищені публічні з'єднання типу Wi-Fi. VPN шифрують трафік користувача, захищаючи його від зловмисників.

Поруч з VPN деякі компанії нерідко використовують доступ до мережі з нульовою довірою (ZTNA). Замість використання проксі-сервера ZTNA використовує політики контролю доступу з нульовою довірою для безпечного підключення віддалених користувачів. Таким чином, якщо віддалені користувачі входять у мережу через ZTNA, то вони отримують доступ лише до певних інформаційних ресурсів, які їм дозволено використовувати, а до всієї мережі їм доступ закритий. Користувача потрібно повторно перевіряти щоразу, коли вони отримують доступ до нового ресурсу.

Крім зазначених рішень на практиці досить часто для підвищення рівня мережної безпеки залучаються і інші засоби управління та фільтрації трафіка. Це особливо стосується протоколів маршрутизації, які можуть досить гнучко налаштовуватись адміністративно та за допомогою відповідних керуючих політик під вимоги мережної безпеки. При цьому засоби маршрутизації (як статичні маршрути, так і динамічні) можуть використовуватись як на проактивній основі, так і як реактивні рішення.

Проактивний характер маршрутних рішень, як правило, стосується того, що маршрут базується на попередньому зборі та аналізі інформації про стан безпеки окремих елементів (сегментів) маршрутів: маршрутизаторів та каналів зв'язку. Подібна інформація може базуватись, наприклад, на оцінках CVSS [15 – 18], або ж на накопиченій статистиці щодо інтенсивності кібервторгнень у

реальному масштабі часу. Це дозволить визначити маршрути передачі пакетів, які є найбільш безпечними з точки зору обраної метрики. На жаль існуючі протоколи IP-маршрутизації напряму не підтримують у своїх метриках компоненти мережної безпеки [20 – 24]. Але це можна зробити опосередковано, адміністративно змінивши значення метрики інтерфейсу маршрутизатора, як, наприклад, показано на рис. 1.5 для протоколу OSPF (Open Shortest Path First). Для більш безпечних пристроїв та інтерфейсів (каналів) значення метрики (cost) має бути мінімальним, а для небезпечних – максимальним. У загальному випадку значення адміністративної метрики може змінюватись від 1 до 65535, що дозволяє охопити досить широкий діапазон рівнів мережної безпеки комунікаційних пристроїв.

```
R1(config)#inter fa0/0
R1(config-if)#ip ospf cost ?
  <1-65535>  Cost
```

Рисунок 1.5 – Приклад адміністративного налаштування метрики інтерфейсу fa0/0 маршрутизатора R1 для протоколу OSPF

На відміну від протоколу OSPF вплинути на метрику маршруту, який будується протоколом RIP (Routing Information Protocol), неможливо. У пропрієтарному протоколі EIGRP (Enhanced Interior Gateway Routing Protocol) використовується досить складна композитна метрика, яка, перш за все, орієнтована на підтримку показників якості обслуговування, серед яких (рис. 1.6) пропускна здатність каналу/маршруту (BW) та середня затримка пакетів (DLY).

```
R1#show inter f0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is c001.4d94.0001 (bia c001.4d94.0001)
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Рисунок 1.6 – Приклад перевірки параметрів інтерфейсу f0/1 маршрутизатора R1, які впливають на метрику маршруту, що визначається протоколом EIGRP

Проте, як і у випадку з OSPF, номінальні значення BW та DLY можуть бути

адміністративно змінені відповідно до встановленого (або розрахованого) рівня мережної безпеки.

Недоліком описаних рішень є те, що налаштування на практиці, як правило, реалізуються адміністратором вручну, що негативно впливає на час реакції проативної маршрутизації як засобу забезпечення мережної безпеки. Підвищити швидкість реакції протоколу маршрутизації на зміни у стані мережі можна досягти засобами мережної автоматизації, коли на певному керуючому сервері (контролері мережі) буде налаштований програмний код для автоматичного збору, аналізу цієї інформації та віддаленого налаштування метрик інтерфейсів маршрутизаторів мережі за допомогою, наприклад, протоколу SSH (Secure Shell).

До проктивних властивостей протоколів маршрутизації можна віднести той факт, що більшість з них підтримує реалізацію багатошляхової маршрутизації (БШМ), коли відбувається балансування навантаження за множиною маршрутів. Тим самим значно ускладняється задача зловмисника, який має скомпрометувати всі шляхи за якими передається конфіденційний трафік, який його цікавить. Це особливо складно, якщо використані шляхи не перетинаються між собою. Протоколи RIP, OSPF, IS-IS підтримують балансування навантаження за шляхами, які мають однакову метрику. А протокол EIGRP здійснює балансування за маршрутами як з однаковою метрикою (у автоматичному режимі), так і за маршрутами з різними метриками (після деяких додаткових адміністративних налаштувань). Про це свідчить наявність у маршрутній таблиці як оптимального, так і не оптимального маршрутів (рис. 1.7).

```
R1#show ip route eigrp
D    192.168.4.0/24 [90/284160] via 192.168.2.2, 00:00:20, FastEthernet0/1
D    192.168.5.0/24 [90/5401600] via 192.168.3.2, 00:00:30, FastEthernet1/0
                    [90/309760] via 192.168.2.2, 00:00:30, FastEthernet0/1
D    192.168.6.0/24 [90/5427200] via 192.168.3.2, 00:00:30, FastEthernet1/0
                    [90/309760] via 192.168.2.2, 00:00:30, FastEthernet0/1
```

Рисунок 1.7 – Приклад маршрутної таблиці на маршрутизаторі R1, де присутні маршрути до мережі 192.168.6.0, які побудовані протоколом EIGRP та мають різні метрики

Особливістю балансування навантаження за допомогою протоколу EIGRP (рис. 1.8) є те, що за маршрутом, який мав меншу метрику (309760), буде передаватись більше пакетів (120). А за маршрутом, який мав більшу метрику (5427200), передається менше пакетів (7). У випадку налаштування метрик відповідно до показників мережної безпеки більш інтенсивно буде завантажуватись більш безпечний маршрут.

```
R1#show ip route 192.168.6.0
Routing entry for 192.168.6.0/24
  Known via "eigrp 1", distance 90, metric 309760, type internal
  Redistributing via eigrp 1
  Last update from 192.168.3.2 on FastEthernet1/0, 00:03:59 ago
  Routing Descriptor Blocks:
    192.168.3.2, from 192.168.3.2, 00:03:59 ago, via FastEthernet1/0
      Route metric is 5427200, traffic share count is 7
      Total delay is 12000 microseconds, minimum bandwidth is 500 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
  * 192.168.2.2, from 192.168.2.2, 00:03:59 ago, via FastEthernet0/1
      Route metric is 309760, traffic share count is 120
      Total delay is 2100 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

Рисунок 1.8 – Перевірка порядку балансування навантаження протоколом EIGRP за шляхами, які мали різну метрику

Важливим функціоналом протоколу EIGRP є підтримка відмовостійкості мережі, у т.ч. при наявності відмов, пов’язаних з наслідками мережних атак типу DoS чи DDoS, у результаті яких той чи інший елемент мережі не зможе функціонувати відповідно до свої номінальних можливостей або навіть взагалі буде блокованим. Тому протокол одночасно з основним маршрутом розраховує і резервний, який може відображатись не у маршрутній таблиці, а у таблиці топології (рис. 1.9). При відмові основного маршруту перемикання на резервний маршрут займе орієнтовно 40 мс [24 – 26]. Подібний варіант роботи характеризує реактивну складову протоколу EIGRP щодо забезпечення стійкості до ймовірних відмов в обслуговуванні з боку мережного обладнання.

Резервний маршрут, як правило, має метрику більшу, а ніж основний. Відмовостійку маршрутизацію також можна налаштувати і засобами статичної маршрутизації за допомогою т.з. плаваючих маршрутів (floating static route) на

підставі зміни не метрик, а адміністративних відстаней. Проте статичні маршрути за визначенням не забезпечують адаптацію до зміни стану мережі.

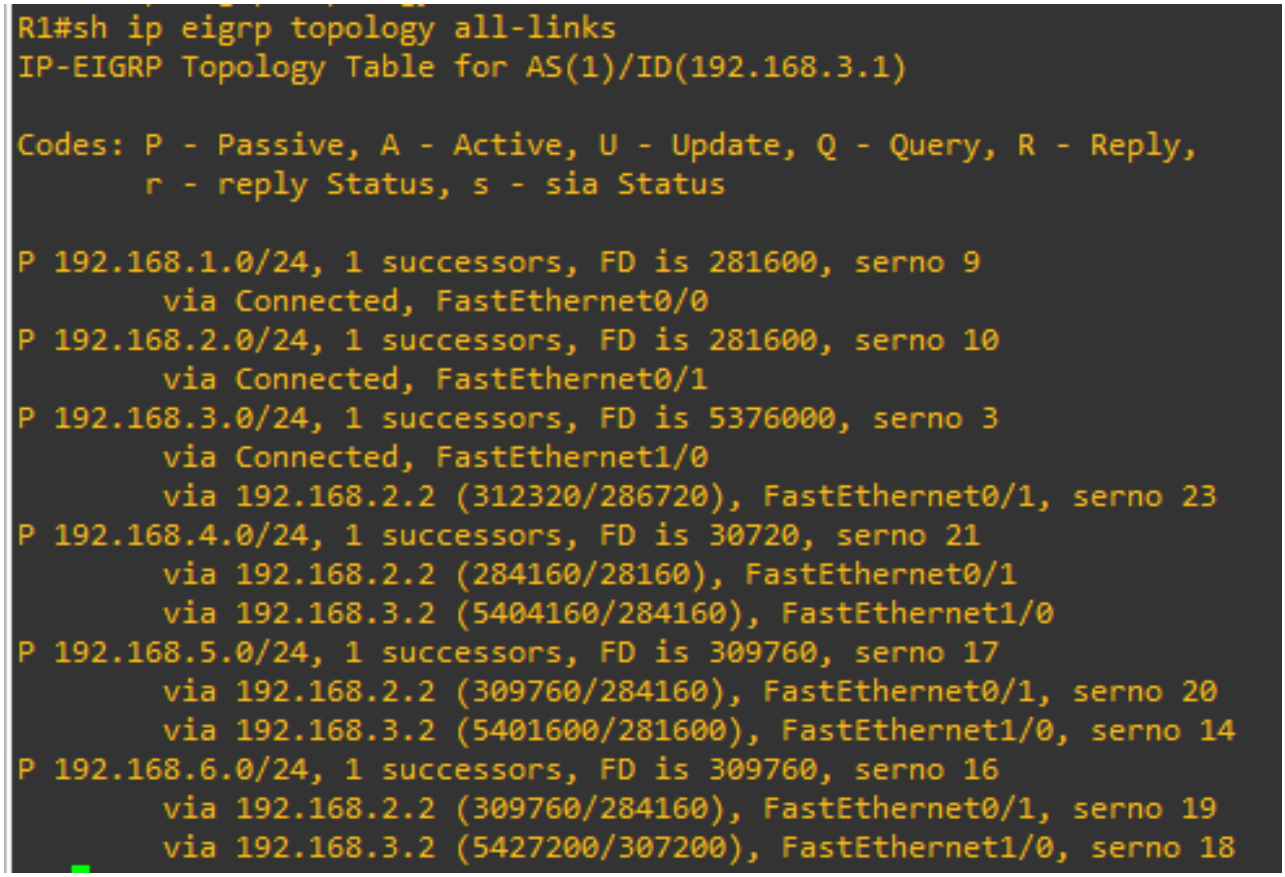


Рисунок 1.9 – Перевірка у таблиці топології наявності основних та резервних маршрутів до віддалених мереж

Подібними властивостями щодо балансування навантаження, віддаленого налаштування та можливості врахування параметрів безпеки також володіють протоколи маршрутизації із захистом шлюзу за замовчуванням (First Hop Redundancy Protocol, FHRP). Саме вони і будуть об’єктом розгляду даної роботи з точки зору їх модифікації під задачі мережної безпеки на алгоритмічному та програмному рівнях.

1.4 Висновки до першого розділу

1. Встановлено, що однією з основних вимог, які висуваються до сучасних інфокомунікаційних мереж, є забезпечення високого рівня мережної безпеки. При цьому бажано, щоб забезпечення мережної безпеки негативно не впливало

на рівень якості обслуговування та відмовостійкості, або ж такий вплив був мінімальним.

2. Для забезпечення мережної безпеки на практиці комплексно використовується цілий спектр технічних та організаційних заходів. При цьому технічні заходи базуються як на апаратних, так і на програмних рішеннях, до яких, перш за все, варто віднести використання брандмауерів, засобів контролю доступу до мережі, систем виявлення та запобігання вторгненням, віртуальних приватних мереж, протоколів управління трафіком тощо.

3. Серед дієвих засобів як проактивного, так і реактивного забезпечення мережної безпеки в ІКМ виділяють протоколи IP-маршрутизації. Саме протоколи OSPF та EIGRP при коректному налаштуванні можуть забезпечувати використання маршрутів, які є найбільш безпечними; балансувати навантаження за множиною шляхів з врахуванням параметрів безпеки елементів шляхів; використовувати як основні, так і резервні маршрути у випадку компрометації певного сегменту ІКМ.

4. Об’єктом подальшого дослідження обрано протоколи відмовістійкої маршрутизації сімейства FHRP, які забезпечують захист шлюзу за замовчуванням у випадку його компрометації або перевантаження за результатами мережної атаки на приграничні маршрутизатори, які і виконують роль шлюзу за замовчуванням для підключених до них локальних мереж (мереж доступу). Дослідження буде присвячено задачам маршрутизації та балансування навантаження з врахуванням параметрів безпеки комунікаційного обладнання.

2 ОГЛЯД ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ ПРОТОКОЛІВ СІМЕЙСТВА FHRP

2.1 Порівняльний аналіз протоколів сімейства FHRP

У випадку відмови приграничного маршрутизатора ІКМ, інтерфейси якого виступають як шлюз за замовчуванням для багатьох підключених до нього локальних мереж, ці локальні мережі фактично будуть блокованими. Термінальні пристрої таких мереж не зможуть обмінюватись інформацією з серверами та комп'ютерами інших віддалених мереж. З метою підвищення рівня стійкості до відмов, викликаних у т.ч. кібервторгненнями, в ІКМ для захисту приграничних маршрутизаторів (шлюзу за замовчуванням) використовуються протоколи відмовостійкої маршрутизації сімейства FHRP. В загальному випадку (рис. 2.1) у мережах IP до сімейства протоколів FHRP входять такі рішення [26, 27]:

- VRRP (Virtual Router Redundancy Protocol);
- HSRP (Hot Standby Router Protocol),
- GLBP (Gateway Load Balancing Protocol);
- CARP (Common Address Redundancy Protocol).

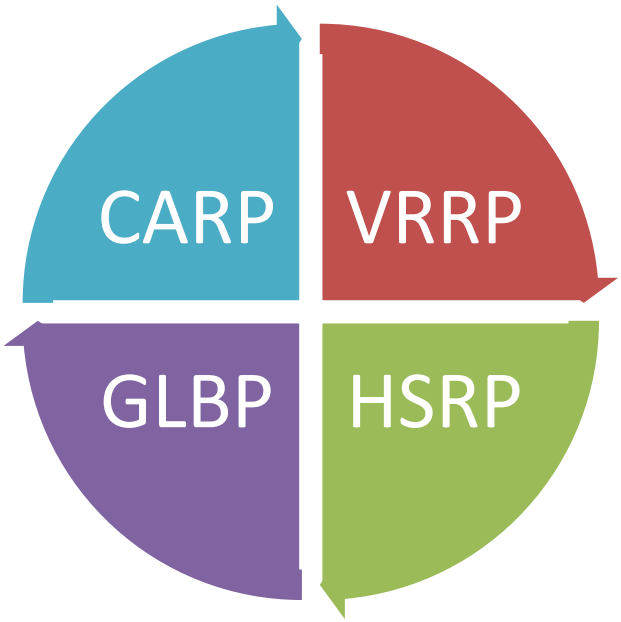


Рисунок 2.1 – Протоколи сімейства FHRP

Основна ідея роботи перерахованих протоколів полягає у тому, що комутатор однієї локальної мережі комутується одночасно до декількох (двох та більше) пригранічних маршрутизаторів (рис. 2.2).

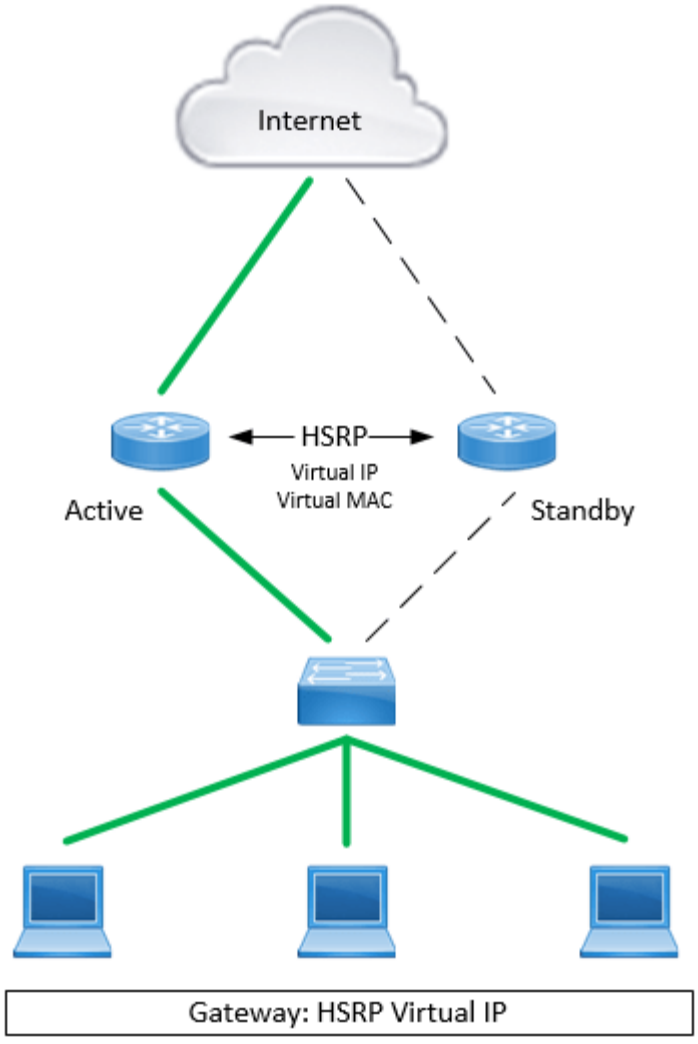


Рисунок 2.2 – Принцип комутації елементів мережі у випадку використання протоколів FHRP

При цьому інтерфейси цих пригранічних маршрутизаторів конфігуруються протоколами сімейства FHRP для створення віртуального шлюзу за замовчуванням, IP-адреса якого і вказується у налаштуваннях кінцевих пристроїв (хостів) локальних мереж. До задач протоколу з множини FHRP відносяться:

- визначення основного (активного) маршрутизатора, через який будуть передаватись пакети у нормальному режимі функціонування, тобто за відсутності відмов;

- визначення одного або множини резервних маршрутизаторів, які будуть виконувати роль основного, коли цей маршрутизатор відмовить;

- визначення порядку балансування навантаження між інтерфейсами, які входять до налаштованого віртуального шлюзу за замовчуванням, якщо протокол підтримує такий режим роботи.

Досить детальна інформація щодо опису та порівняльного аналізу протоколів сімейства FHRP (табл. 2.2) наведені у роботах [8, 26, 27].

Протокол VRRP є міжнародним стандартом та детально описаний в RFC 5798. Він забезпечує вирішення проблеми шляхом об'єднання двох або більше фізичних пристроїв у логічне групування, яке називається віртуальним маршрутизатором (VR). Тоді фізичні пристрої працюють разом, створюючи єдиний логічний шлюз для хостів у локальній мережі.

Віртуальний маршрутизатор налаштований як шлюз хоста та складається з кількох фізичних маршрутизаторів. Хости можуть бачити лише віртуальний маршрутизатор, тому кількість фізичних маршрутизаторів, які складають віртуальний маршрутизатор, є прозорою. Якщо фізичні маршрутизатори у віртуальному маршрутизаторі виходять з ладу, то трафік до та з хостів все одно буде перенаправлятися, якщо існує принаймні один функціонуючий фізичний маршрутизатор, хостам не потрібно змінювати конфігурацію.

Перевагою VRRP перед HSRP та GLBP є те, що протокол VRRP підтримується практично на всіх пристроях різних вендорів, так як є відкритим стандартом. Крім того VRRP може використовувати як віртуальну IP адресу, яка налаштована на інтерфейсі одного з маршрутизаторів, що входять до віртуального маршрутизатора. До недоліків VRRP варто віднести те, що він безпосередньо не підтримує режим навантаженого (гарячого) резерву, коли навантаження локальної мережі балансується, тобто одночасно передається як через основний (Master) маршрутизатор, так і через резервний (Backup). Однак це може бути налаштовано за допомогою створення додаткових VRRP-груп (віртуальних маршрутизаторів) на тих же інтерфейсах приграничних маршрутизаторів.

Таблиця 2.1 – Порівняння протоколів сімейства FHRP [8]

Характеристика	HSRP	VRRP	GLBP	CARP
Застосування	Cisco Proprietary	IEEE Standard	Cisco Proprietary	Not a standard (BSD based OS)
Стандарт	RFC 2281	RFC 5798	Ні	Ні
Рівень моделі OSI	Мережний	Мережний	Канальний	Мережний
Балансування навантаження	Не підтримується	Підтримується	Підтримується	Підтримується
IPv6	Підтримується	Підтримується	Підтримується	Підтримується
Переваги	– легка конфігурація; – низьке навантаження мережі службовим трафіком.	– спрощене управління мережею; – висока адаптованість; – низьке навантаження мережі службовим трафіком; – балансування навантаження; – мінімізація обчислювальних витрат.	– ефективне використання мережних ресурсів; – висока доступність; – автоматичне балансування навантаження; – низькі витрати на адміністрування; – ефективне проектування рівня доступу.	– відкрита альтернатива HSRP і VRRP; – резервування для брандмауерів та маршрутизаторів; – балансування навантаження.
Недоліки	– неефективний для передачі трафіку реального часу; – слабкий рівень безпеки; – пропрієтарний протокол Cisco.	– слабкий рівень безпеки (не містить жодного типу автентифікації).	– пропрієтарний протокол Cisco; – висока складність управління мережею.	– несумісність з чинними стандартами; – слабкий рівень безпеки.

VRRP підтримує аутентифікацію, для захищеності можна використовувати алгоритм MD5. За замовчуванням керуючі таймери мінімальні, що дозволяє досить швидко реагувати на відмови: Hello timer 1 секунда, hold time

3 секунди. Кількість налаштованих VRRP-груп може складати до 255.

Протокол HSRP відноситься до корпоративних стандартів, він є пропрієтарним протоколом, який запропонований компанією Cisco. Як і протокол VRRP він не підтримує балансування за множиною пригранічних маршрутизаторів. Протокол HSRP на основі аналізу пріоритетів інтерфейсів обирає один активний (Active) маршрутизатор та один резервний (Standby), інші маршрутизатори є кандидатами на ролі активного та резервного маршрутизаторів. Кількість віртуальних маршрутизаторів (Standby-груп) – до 16. За замовчуванням керуючі таймери дещо більші, а ніж у протоколу VRRP: Hello timer 3 секунди, hold time 10 секунди, які можуть бути змінені у більшу або меншу сторони (рис. 2.3).

```
FastEthernet0/0 - Group 1 (version 2)
  State is Active
    13 state changes, last state change 01:35:21
    Track object 1 state Up
  Virtual IP address is 192.168.1.11
  Active virtual MAC address is 0016.3e01.0001
    Local virtual MAC address is 0016.3e01.0001 (bia)
  Hello time 5 sec, hold time 15 sec
    Next hello sent in 0.368 secs
```

Рисунок 2.3 – Приклад перевірки керуючих таймерів у протоколі HSRP

Протокол GLBP як і протокол HSRP є пропрієтарним Cisco протоколом. На відміну від HSRP та VRRP він дозволяє балансувати навантаження між маршрутизаторами, які приймають участь у резервуванні. Базовими режимами (рис. 2.4) балансування навантаження для протоколу GLBP є Round Robin та Weighted (зважене). У режимі Round Robin підтримується рівномірне балансування навантаження, яке надходить від терміналів (хостів): до кожного пригранічного маршрутизатора GLBP-групи підключається для передачі пакетів приблизно однакова кількість комп’ютерів. Зважений режим балансування полягає у тому, що для кожного інтерфейсу, який входить до віртуального шлюзу за замовчуванням, адміністративно налаштовується вага. Саме співвідношення цих вагових коефіцієнтів і визначає порядок балансування.

```
R1(config-if)#glbp 1 load-balancing ?
  host-dependent  Load balance equally, source MAC determines forwarder choice
  round-robin     Load balance equally using each forwarder in turn
  weighted        Load balance in proportion to forwarder weighting
```

Рисунок 2.4 – Режими балансування навантаження у протоколі GLBP

GLBP підтримує до 1024 віртуальних маршрутизаторів (GLBP-груп) на кожному фізичному інтерфейсі, а також до 4-х маршрутизаторів у кожній групі. Протокол GLPB підтримує аутентифікацію MD5. За замовчуванням керуючі таймери співпадають з параметрами протоколу HSRP: Hello timer 3 секунди, hold time 10 секунди.

Крім того, що протоколи сімейства FHRP є засобом забезпечення проактивного та реактивного захисту ІКМ, ці протоколи самі є об’єктом кібератак, бо контроль над приграничним маршрутизатором дозволяє контролювати весь трафік, який передається у глобальну мережу від локальної мережі компанії (підприємства) або надходить із глобальної мережі.

2.2 Аналіз ймовірних атак на протоколи сімейства FHRP та методів боротьби з ними

Маршрутизатори – це пристрої мережного рівня моделі OSI, тому на них можуть поширюватись практично всі типи атак цього рівня, метою яких є порушення процесу управління трафіком в ІКМ: створення перенавантажених ділянок у мережі, блокування роботи маршрутизаторів, перенаправлення трафіка на нелегітимні пристрої з метою компрометації конфіденційної інформації тощо [28]. До найпоширеніших атак на маршрутизатор зазвичай відносять:

- атака на відмову в обслуговуванні (DoS), розподілена атака на відмову в обслуговуванні (DDoS);
- атаки на неправильну обробку пакетів (Packet Mistreating Attacks, PMA);
- отруєння таблиці маршрутизації (Routing Table Poisoning, RTP);
- атаки викрадення маршруту (Route Hijacking);
- атака «Людина посередині» (Man in the middle, MitM).

При організації атаки типу DoS або DDoS зловмисник (зловмисники) використовують серію запитів, щоб завантажити маршрутизатори мережі запитами, які, як правило, надсилаються за допомогою протоколу ICMP (Internet

Control Message Protocol). Подібні пакети можуть надсилатись з високою або змінюваною інтенсивністю протягом короткого проміжку навіть з кількох різних хостів (при DDoS). Будь-який маршрутизатор має обмежені можливості щодо своєї продуктивності, тому при збільшенні навантаження він не зможе впоратися з величезним обсягом запитів, що призводить до його перевантаження та неспроможності виконувати «штатні» функції, які пов'язані з управлінням трафіком: фільтрацією, буферизацією, профілюванням, маршрутизацією тощо. Тому у результаті спочатку деякий мережний сегмент, а потім і вся мережа може припинити обслуговувати пакет .

При організації атаки Hit and Run DDoS зловмисники виконують DDOS-атаку протягом 15–45 хвилин, а потім повторюють її через 1 або 2 доби. Це призводить до використання організацією більших ресурсів для протидії атакам, та обробки вхідного трафіку.

Метою атаки на неправильну обробку пакетів є впровадження зловмисного коду. Подібно до DoS-атаки, атака PMA впроваджує пакети зі зловмисним кодом, щоб ускладнити та порушити ефективну роботу маршрутизатора та мережі взагалі. Шкідливі пакети спочатку блокують процес маршрутизації на одному або групі маршрутизаторів, а потім, циркулюючи безконтрольно у мережі, можуть створювати петлі, перевантажуючи інші сегменти мережі.

При атаках на таблицю маршрутизації через її отруєння (RTP) зловмисник спотворює зміст маршрутної таблиці. Без належного захисту та шифрування таблиця маршрутизації може стати надзвичайно вразливою. Мета атаки полягає, як правило, у перенаправленні трафіка на нелегітимні пристрої для отримання доступу та наступної компрометації інформації, яка передається мережею. Побідні маніпуляції характерні і для атак щодо викрадення маршруту, коли зловмисник нав'язує через скомпрометований маршрутизатор неправдиві маршрути іншим маршрутизаторам. При цьому ці маршрути можуть мати більш привабливі атрибути – мінімальні адміністративні відстані та/або метрики. Ефективність реалізації подібних атак багато у чому залежить від наявних вразливостей апаратного та програмного забезпечення маршрутизаторів та від ефективності використання цих вразливостей з боку зловмисника.

Атака «Людина посередині» (MitM) є досить розповсюдженою, найстарішою і найнебезпечніших мережною атакою. При MitM злочинець стає певним посередником між відправником пакетів та одержувачем. У разі

реалізації подібної атаки зловмисники перехоплюють і змінюють мережний трафік, знову ж, маніпулюючи маршрутною інформацією, можуть перенаправляти трафік на шкідливі мережні пристрої.

Для боротьби з розглянутими типами атак запропоновано до використання множину методів, які варто використовувати у комплексі на взаємодоповнюючій основі, бо жоден з них не гарантує стовідсотковий позитивний результат. До найбільш поширених та ефективних методів боротьби та протидії атакам варто віднести [12, 14, 28]:

- впровадження контролю доступу із застосуванням політики паролів;
- використання послуги AAA(authentication, authorization, accounting – автентифікація, авторизація, облік);
- використання NTP (Network Time Protocol);
- шифрування трафіка;
- періодичне оновлення програмного забезпечення мережних пристроїв;
- вимкнення служб, які не використовуються;
- вимкнення портів на мережних пристроях, які не використовуються;
- впровадження та постійне оновлення правил фільтрації пакетів (ACL), особливо що стосується керуючого трафіка, підробка якого може вплинути на втрату контролю над мережним пристроєм (маршрутизатором);
- у випадку використання маршрутизаторів з обмеженою продуктивністю варто у структуру мережі додати брандмауери, IDS/IPS;
- блокування поширення важливого керуючого трафіка (трафіка маршрутизації) до локальних мереж, використання т.з. «пасивних» інтерфейсів;
- запровадження постійного контролю за станом мережних пристроїв, маршрутних таблиць з метою своєчасного реагування на суттєві непрогнозовані зміни в їх структурі та кількості записів.

Організація мережних атак на протоколи сімейства FHRP та маршрутизатори, які їх реалізують, має певні особливості. Так, наприклад, домени мереж, які підтримують FHRP, уразливі до Hijack-атак. Особливо це актуально, коли пристрої, які виступають як Active (для HSRP), Master (для VRRP) та AVG (для GLBP), не мають максимального значення пріоритету щодо своєї конфігурації. Тому пристрій зловмисника в межах атаки спуфінгу може видати себе за легітимний пристрій FHRP для отримання доступу до мережі. Він знаходиться у локальній мережі організації і може провести ін'єкцію

HSRP/VRRP/GLBP-пакету з максимальними значеннями пріоритетів (255), зможе виконувати роль основного маршрутизатора (Active або Master) або координатора (AVG) та повністю контролювати цей домен, перехоплюючи трафік та перенаправляючи його на нелегітимні пристрої. З цією метою зловмисник проводить розвідку стану мережі, аналізуючи віртуальні IP-адреси та MAC-адреси, значення пріоритетів інтерфейсів, шляхи обходу автентифікації. Далі проводиться етап заміни віртуальних MAC та IP адрес, здійснюється генерація та відправлення шкідливої FHRP-ін'єкції. Фактично пристрій зловмисника, який візьме на себе роль основного маршрутизатора, стане «людиною посередині».

Використання сегментації мережі на VLAN дозволить обмежити можливості зловмисника щодо намірів контролювати маршрутизатори. Таким самим чином можна і обмежити ймовірний контроль трафіка зловмисника тільки тим VLAN, у якій він сам і знаходиться. Крім того, використання балансування навантаження між множиною пригранічних маршрутизаторів, інтерфейси яких створюють віртуальний шлюз за замовчуванням, дозволить мінімізувати об’єми скомпрометованої інформації, яка передається через маршрутизатор, який все ж буде контролюватись зловмисником. Таким чином актуальним представляється завдання, пов’язане із забезпеченням ефективного балансування навантаження між пригранічними маршрутизаторами з врахуванням рівня їх безпеки на основі інформації стандартів CVSS.

2.3 Висновки до другого розділу

1. У розділі проведено порівняльний аналіз протоколів сімейства FHRP, до якого входять, перш за все, протоколи VRRP, HSRP та GLBP. Ці протоколи призначені для підвищення доступності шлюзу за замовчуванням шляхом резервування функцій пригранічних маршрутизаторів. Дані протоколи можуть забезпечувати як проактивний, так і реактивний захист шлюзу за замовчуванням, ускладнюючи роботу зловмисника щодо контролю над трафіком, який передається від локальної мережі до глобальної. З цієї сторони найбільш ефективним виявився протокол GLBP, який підтримує декілька режимів балансування навантаження між пригранічними маршрутизаторами без налаштування додаткових GLBP-груп, як це практикується протоколами VRRP

та HSRP.

2. Проведено огляд основних типів мережних атак, реалізація яких може призвести до порушення рівня мережної безпеки та компрометації мережного обладнання, а також інформації, яка передається у мережі. Ці методи є класичними для атак мережного рівня, так як їх об’єктом є маршрутизатор – пристрій мережного рівня OSI. Проте їх реалізація у доменах FHRP має певні особливості. Спуфінг та атака «людина посередині» на основі маніпуляції пріоритетами інтерфейсів пригранічних маршрутизаторів, які створюють віртуальний шлюз за замовчуванням, можуть призвести до втрати контролю над деякими мережними пристроями та заволодінням зловмисником того обсягу інформації, що ними передається. Крім того, скомпрометовані пристрої можуть самі стати певною базою для організації інших видів атак.

3. Пропонується до використання комплексу організаційних та технічних заходів, направлених на ускладнення роботи зловмисника щодо компрометації мережі, які стосуються використання політик паролів, контролю доступу, своєчасного оновлення програмного забезпечення мережних пристроїв, використання IDS/IPS, постійному контролю за станом мережі, пристроїв, маршрутних таблиць тощо. Пропонується для забезпечення проактивного захисту мережі здійснювати ефективне балансування навантаження між пригранічними маршрутизаторами з врахуванням рівня їх безпеки на основі інформації стандартів CVSS.

3 ВИБІР ТА ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПРОАКТИВНОГО ЗАХИСТУ ПРИГРАНИЧНИХ МАРШРУТИЗАТОРІВ IP-МЕРЕЖІ

3.1 Огляд методів та засобів проактивного захисту пригранічних маршрутизаторів IP-мережі

У роботі [29] запропоновано підвищити доступність віддаленого доступу до захищеної корпоративної мережі концентратора подвійного DMVPN (Dynamic Multipoint VPN). DMVPN — це технологія, яка може бути пов’язана з різними концепціями протоколів, такими як шифрування IPsec, протокол розв’язання наступного стрибка, загальна інкапсуляція маршрутизації (GRE), і вона забезпечує динамічний і статичний тунель IPsec. У даній роботі реалізована технологія DMVPN для побудови захищеної корпоративної мережі для організації та використання протоколу маршрутизації HSRP для покращення доступності при збоях у мережі. Моделювання було виконано у GNS3, а пакети перехоплювались за допомогою Wireshark. Під час тестування було виявлено, що технологія DMVPN з протоколами HSRP повністю відповідає вимогам доступності. Вона забезпечує швидший режим передачі пакетів, а також високу доступність мережних функцій, створюючи таким чином більш безпечну та надійну мережеву інфраструктуру.

У роботі [30] представлено Round Robin Load Balancing and Redundancy Protocol (R ^{2} LBRP) для мережних маршрутизаторів. R ^{2} LBRP. R ^{2} LBRP використовує ту саму концепцію віртуального маршрутизатора, що й VRRP, але керує фізичними маршрутизаторами інакше: замість того, щоб мати лише один активний маршрутизатор, R ^{2} LBRP використовує всі маршрутизатори та використовує їх для пересилання пакетів. R ^{2} LBRP підтримує майже миттєве виявлення збоїв, розширені механізми відновлення після збоїв і може збільшити пропускну здатність віртуального маршрутизатора та забезпечити точніший контроль над балансуванням навантаження.

Стаття [31] спрямована розробку програмного пакету, здатного автоматично створювати комунікаційні клієнти за допомогою захоплення пакетів (pcap) і дисекторів TShark. Методології, розроблені в рамках цієї роботи, поширюватимуться на інші складні протоколи, такі як протокол балансування

навантаження шлюзу (GLBP), протокол агрегування портів (PAgP) і відкритий найкоротший шлях (OSPF). Використовуючи запропоновану методологію, вдалося автоматично створити програмне забезпечення, яке спілкується з іншими хостами за допомогою автоматично створеної клієнтської програми протоколу керуючих повідомлень Інтернету.

У статті [32] представлено аналіз продуктивності концепції високої доступності на основі сегрегації трафіку за допомогою Multi-Protocol Label Switching (MPLS) Traffic Engineering (TE). Так як забезпечення високої доступності для балансування навантаження та резервування в існуючій магістральній мережі постачальника послуг все ще є складним завданням, то авторами представлене рішення на основі протоколу резервування віртуального маршрутизатора (VRRP) налаштовано для підтримки високої доступності. Концепція рознесення трафіку використовується, коли маршрутизація на основі політики обробляє сегрегацію трафіку для використання трафіку в основному та резервному каналах.

У статтях [33, 34] встановлено, що важливим рішенням щодо проактивного забезпечення відмовостійкості мереж є підтримка балансування навантаження як на рівні мережі, так і на рівні доступу засобами FHRP. Тому у роботі описано та здійснено порівняльний аналіз чотирьох математичних рішень задачі проактивної відмовостійкої маршрутизації, які підтримують вимоги концепції Traffic Engineering. Два з рішень враховують рівень надійності приграничних маршрутизаторів. У процесі дослідження встановлено, що врахування рівня надійності приграничних маршрутизаторів при організації балансування навантаження між ними призводило до незначного підвищення порогу завантаженості каналів зв’язку мережі. У роботі продемонстровано, що впровадження аналізованих рішень щодо балансування навантаження може бути забезпечено за допомогою протоколу GLBP.

Рішення, яке представлене у роботі [33] пропонується вдосконалити та адаптувати під задачі мережної безпеки, коли при балансуванні навантаження враховувався б рівень кібербезпеки приграничних маршрутизаторів.

3.2 Опис обраних методів проактивного захисту пригранічних маршрутизаторів IP-мережі

Методу проактивного захисту пригранічних маршрутизаторів IP-мережі базується на математичній моделі, яка детально описана у роботах [8, 33, 34]. Структура мережі описується у вигляді орієнтованого графу $G = (M, L)$ (табл. 3.1), K – це множина потоків, які протікають у мережі. До кожного k-го потоку пакетів ($k \in K$) співставлені дві мережі доступу – джерело (V_s^k) та отримувач (V_d^k). Параметр λ^k характеризує середню швидкість пакетів k-го потоку на вході в ІКМ (1/с).

Таблиця 3.1 – Використані позначення

Позначення	Опис
$G = (M, L)$	Граф мережі
$M = R \cup V$	Множина вершин графа G ($R \cap V = \varnothing$)
$R = \left\{ R_i, i = \overline{1,m} \right\}$	Підмножина вершин, які описують маршрутизатори
$V = \left\{ V_j, j = \overline{1,v} \right\}$	Підмножина вершин, що моделюють мережі доступу
$R^+ \subset R$	Підмножина вершин, що описують пригранічні маршрутизатори ІКМ
$R^- \subset R$	Підмножина вершин, що моделюють транзитні маршрутизатори ІКМ
$R_j^+ \subset R^+$	Підмножина вершин графа , що моделює ті пригранічні маршрутизатори, які утворюють віртуальний маршрутизатор для мережі доступу V_j
$L = E \cup W$	Множина дуг графа G ($E \cap W = \varnothing$)
$E = \left\{ E_{i,j}, i, j = \overline{1,m}, i \neq j \right\}$	Множина дуг, які моделюють канали зв'язку ІКМ, які з'єднують маршрутизатори
$W^+ = \left\{ W_{i,j}^+, i = \overline{1,v}, j = \overline{1,m^+} \right\}$	Множина дуг, які описують лінії доступу, що з'єднують мережі доступу та пригранічні маршрутизатори
$W^- = \left\{ W_{i,j}^-, i = \overline{1,m^+}, j = \overline{1,v} \right\}$	Множина дуг, які описують лінії доступу, що з'єднують пригранічні маршрутизатори ІКМ та мережі доступу

Продовження таблиці 3.1	
$\varphi_{i,j}$	Пропускна здатність каналу зв'язку, який моделюється дугою $E_{i,j} \in E$
K	Множина потоків пакетів, що циркулюють в ІКМ
K_i^+	Множина потоків, що надходять до ІКМ від мережі доступу V_i
K_i^-	Множина потоків, що виходять з ІКМ до мережі доступу V_i
V_s^k	Мережа доступу, яка є джерелом k-го потоку пакетів
V_d^k	Мережа доступу, яка є отримувачем пакетів k-го потоку
λ^k	Середня інтенсивність пакетів k-го потоку
$x_{i,j}^k$	Маршрутна змінна, яка характеризує частку k-го потоку в каналі зв'язку, представленого дугою $E_{i,j}$
$y_{i,j}^k$	Змінна доступу, яка визначає частку k-го потоку, який протікає в лінії доступу, представленій дугою $W_{i,j}^+$
$z_{j,i}^k$	Змінна доступу, яка характеризує частку k-го потоку, що протікає в лінії доступу, представленій дугою $W_{j,i}^-$
α	Верхній поріг завантаженості каналів зв'язку ІКМ

Якщо у мережі буде використана одношляхова маршрутизація потоків в ІКМ, то на маршрутні змінні $x_{i,j}^k$ накладаються обмеження виду:

$$x_{i,j}^k \in \{0;1\}, \tag{3.1}$$

а у випадку реалізації багатошляхової маршрутизації:

$$0 \le x_{i,j}^k \le 1. \tag{3.2}$$

При умові що мережа доступу взаємодіє лише з одним з приграничних маршрутизаторів ІКМ, як при VRRP чи HSRP, на змінні доступу накладаються наступні обмеження:

$$y_{i,j}^{k} \in \{0;1\} \quad \text{та} \quad z_{j,i}^{k} \in \{0;1\}. \tag{3.3}$$

Якщо балансування навантаження підтримується на рівні доступу, як це реалізовано в протоколі GLBP [33, 34], то на ці ж змінні накладаються умови,:

$$0 \le y_{i,j}^{k} \le 1 \text{ та } \quad 0 \le z_{i,j}^{k} \le 1. \tag{3.4}$$

Щоб забезпечити відсутність втрат пакетів на рівні доступу на змінні (3.4) накладаються наступні умови-обмеження:

$$\sum_{R_j \in R_p^+} y_{p,j}^{k} = 1,\ V_p = V_s^k; \tag{3.5}$$

$$\sum_{R_j \in R_h^+} z_{j,h}^{k} = 1, \quad V_h = V_d^k. \tag{3.6}$$

Для забезпечення збереження потоку на рівні мережі взагалі, на всі змінні накладаються наступні умови [33, 34]:

$$\begin{cases} \sum\limits_{j:E_{i,j} \in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^{k} = 0; \quad k \in K\ , R_i \in R^{-}; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^{k} = y_{p,i}^{k}; \quad k \in K\ , R_i \in R^{+}, V_p = V_s^k; \\ \sum\limits_{j:E_{j,i} \in E} x_{j,i}^{k} = z_{i,h}^{k}; \quad k \in K\ , R_i \in R^{+}, V_h = V_d^k. \end{cases} \tag{3.7}$$

Для забезпечення балансування навантаження в ІКМ на принципах ТЕ, в модель було введено умови запобігання перевантаження наступного виду [12]:

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \alpha \varphi_{i,j}, \tag{3.8}$$

де α – верхній поріг завантаженості каналів зв'язку ІКМ (табл. 3.1), який також є керуючою змінною, на яку накладається обмеження виду:

$$0 \le \alpha \le 1. \tag{3.9}$$

Тоді задача балансування навантаження в ІКМ формулюється як оптимізаційна, я кій критерієм оптимальності буде виступати умова:

$$\min_{x,y,z,\alpha} \alpha, \tag{3.10}$$

а обмеженнями – умови (3.1)-(3.9).

У загальному випадку ця задача відносить до оптимізаційних задач змішаного цілочисельного лінійного програмування, тому що α приймає дійсні значення, а маршрутні змінні та змінні управління доступом можуть бути як цілими, так і дійсними. Нехай рішення, яке відповідає моделі (3.1)-(3.10), має назву MethodTE (Method «Traffic Engineering»).

У даній роботі по аналогіями з рішеннями, які представлені у [33 - 35] пропонується замінити критерій оптимальності на таку умову

$$\min_{x,y,z,\alpha} \left(\sum_{k \in K} \sum_{V_p \in V} \sum_{R_i \in R_p^+} A_i y_{p,i}^k + \sum_{k \in K} \sum_{V_p \in V} \sum_{R_j \in R_p^-} A_j z_{j,p}^k + c_\alpha \alpha \right), \tag{3.11}$$

де A_i – інтегральний показник мережної безпеки приграничного маршрутизатора R_i. Як приклад, показником кібербезпеки маршрутизатора може виступати ймовірність його компрометації P_i або бали CVSS – $CVSS_i$ (табл. 1.1), які пов'язані, наприклад, з найбільш значущою вразливістю маршрутизатора R_i.

Значення вагового коефіцієнта c_α має перевищувати на порядок значення інтегральні показники мережної безпеки маршрутизаторів приграничного маршрутизатора, щоб забезпечити першочерговість розв'язання задачі балансування навантаження та якості обслуговування в ІКМ. Надалі серед цих рішень буде обиратись рішення, яке відповідає за мережну безпеку.

Використання такого критерію дозволить обирати найбільш безпечний маршрутизатор як основний шлюз за замовчуванням по аналогії із визначенням пристроїв Active та Master у протоколах HSRP та VRRP. Резервним шлюзом за замовчуванням буде виступати пристрій, який має друге за величиною показник безпеки A_i. Нехай рішення, засноване на моделі (3.1)-(3.9), (3.11), має назву MethodNB (Method «no balancing»).

За необхідності забезпечення балансування навантаження між приграничними маршрутизаторами, які створюють віртуальний шлюз за замовчуванням, варто використати такі вирази [33 – 35]:

$$\sum_{k\in K_p^+} \lambda^k y_{p,j}^k = m_{p,j}^+ \sum_{k\in K_p^+} \lambda^k, \tag{3.12}$$

де $m_{p,j}^+$ – метрики балансування, які характеризують частку сумарного трафіку, що надходить в ІКМ від мережі доступу V_p через маршрутизатор R_j. При цьому має бути виконуватись рівність

$$\sum_{R_j\in R_p^+} m_{p,j}^+ = 1. \tag{3.13}$$

Тому для балансування навантаження з урахуванням рівня безпеки приграничних маршрутизаторів, за аналогією з роботами [33 – 35], метрики балансування будуть визначатись за такою формулою:

$$m_{p,j}^+ = \frac{1/A_j}{\sum\limits_{R_i\in R_p^+} 1/A_i},\ R_j \in R_p^+ \tag{3.14}$$

за умови, що $A_i \neq 0$, що відповідає особливостям практики, коли абсолютно безпечних пристроїв не існує.

Відповідно до (3.12)-(3.14) та критерію (3.10) при балансуванні навантаження між інтерфейсами віртуального маршрутизатора більше пакетів буде відправлятись на більш безпечний мережний пристрій. Аналогічні до (3.12)-(3.14) вирази вводяться і для метрик балансування на виході ІКМ. Тоді рішення, яке засноване на моделі (3.1)-(3.10), (3.12)-(3.14), буде мати назву MethodWB (Method «with balancing»).

3.3 Дослідження обраних методів проактивного захисту приграничних маршрутизаторів IP-мережі

Описані у попередньому підрозділі методи були досліджені у середовищі MatLab, коли сформульовані оптимізаційні задачі розв’язувались за допомогою програми «intlinprog» з пакету Optimization Toolbox.

Фрагменти коду в середовищі Matlab показані на рис. 3.1-3.3.

Як приклад, дослідження проводились на мережній структурі, яка показана на рис. 3.4 [33]. Джерелом одного потоку пакетів виступала мережа доступу V_1, а отримувачем пакетів була мережа доступу V_2. У таблиці 3.2 наведені пропускні здатності каналів зв’язку ІКМ.

```
% r - інтенсивність потоку, який надходить до мережі
j=1;
i = 0;
Lmax=500;
for r=10:10:Lmax
    i = i + 1;
    lyambda(i) = r;
% c - вектор пропускних здатностей каналів зв'язку
c=[250; 420; 150; 270; 250; 350; 220; 150; 110; 390; 280; 330];


v = [0.05; 0.15; 0.0001; 0.0001]; % імовірність компрометації
% f - вектор метрик каналів зв'язку

% формалізація у векторно-матричній формі обмежень у формі рівнянь
% Aeq*x=beq
            %  12 14 23 25 36 45 47 56 58 69 78 89
Aeq = [-1  0    1  1  0  0  0  0  0  0  0  0  0  0    0  0    0
        0  0   -1  0  1  1  0  0  0  0  0  0  0  0    0  0    0
        0  0    0  0 -1  0  1  0  0  0  0  0  0  0    0  0    0
        0 -1    0 -1  0  0  0  1  1  0  0  0  0  0    0  0    0
        0  0    0  0  0 -1  0 -1  0  1  1  0  0  0    0  0    0
        0  0    0  0  0  0 -1  0  0 -1  0  1  0  0    1  0    0
        0  0    0  0  0  0  0  0 -1  0  0  0  1  0    0  0    0
        0  0    0  0  0  0  0  0  0  0 -1  0 -1  1    0  0    0
        0  0    0  0  0  0  0  0  0  0  0 -1  0 -1    0  1    0

        1  1    0  0  0  0  0  0  0  0  0  0  0  0    0  0   0
        0  0    0  0  0  0  0  0  0  0  0  0  0  0    1  1   0];
beq = [0; 0; 0; 0; 0; 0; 0; 0; 0; 1; 1];
```

Рисунок 3.1 – Фрагмент коду в середовищі Matlab, який відповідає за вихідні дані

```
lb=zeros(17,1);
ub=ones(17,1);
intcon = []; % з балансированням  в транспортній мережі та на шлюзах

    if ii==1 % MethodTE
    f= [0; 0; 0; 0; 0;  0; 0;  0; 0; 0; 0; 0; 0; 0; 0; 0; 1];
    [x, fval] = intlinprog (f,intcon,A,b,Aeq,beq,lb,ub)
     % Розрахунок інтенсивностей потоку в каналах зв'язку
     %y=r*x(3:14);
     alpha(ii,i) = x(17);
    end
    if ii==2 % MethodNB
        f= [v(1); v(2); 0; 0; 0;  0; 0;  0; 0; 0; 0; 0; 0; 0; v(3); v(4); 1];
        [x, fval] = intlinprog (f,intcon,A,b,Aeq,beq,lb,ub)
     % Розрахунок інтенсивностей потоку в каналах зв'язку
        %y=r*x(3:14);
        alpha(ii,i) = x(17);
    end
    if ii==3 % MethodWB
        lb(1,1)=(1/v(1))/(1/v(1)+1/v(2));
        ub(1,1)=(1/v(1))/(1/v(1)+1/v(2));

        lb(2,1)=(1/v(2))/(1/v(1)+1/v(2));
        ub(2,1)=(1/v(2))/(1/v(1)+1/v(2));
        f= [0; 0; 0; 0; 0;  0; 0;  0; 0; 0; 0; 0; 0; 0; 0; 0; 1];
        [x, fval] = intlinprog (f,intcon,A,b,Aeq,beq,lb,ub)
     % Розрахунок інтенсивностей потоку в каналах зв'язку
        %y=r*x(3:14);
        alpha(ii,i) = x(17);
    end
end
```

Рисунок 3.2 –Фрагмент коду в середовищі Matlab, який відповідає за реалізацію методів відмовостійкої маршрутизації

```
alpha_1 = alpha(1,:);
alpha_2 = alpha(2,:);
alpha_3 = alpha(3,:);
%Графік:

figure (1)
plot (10:10:Lmax, alpha_1, 'b-o', 10:10:Lmax, alpha_2, 'k-s', 10:10:Lmax, alpha_3, 'r-*')
grid on;
title('');
xlabel('інтенсивність потоку, який надходить до мережі');
ylabel('верхній поріг завантаженності каналів звязку');
legend('MethodTE', 'MethodNB', 'MethodWB');
```

Рисунок 3.3 – Фрагмент коду в середовищі Matlab, який відповідає за побудову графіків

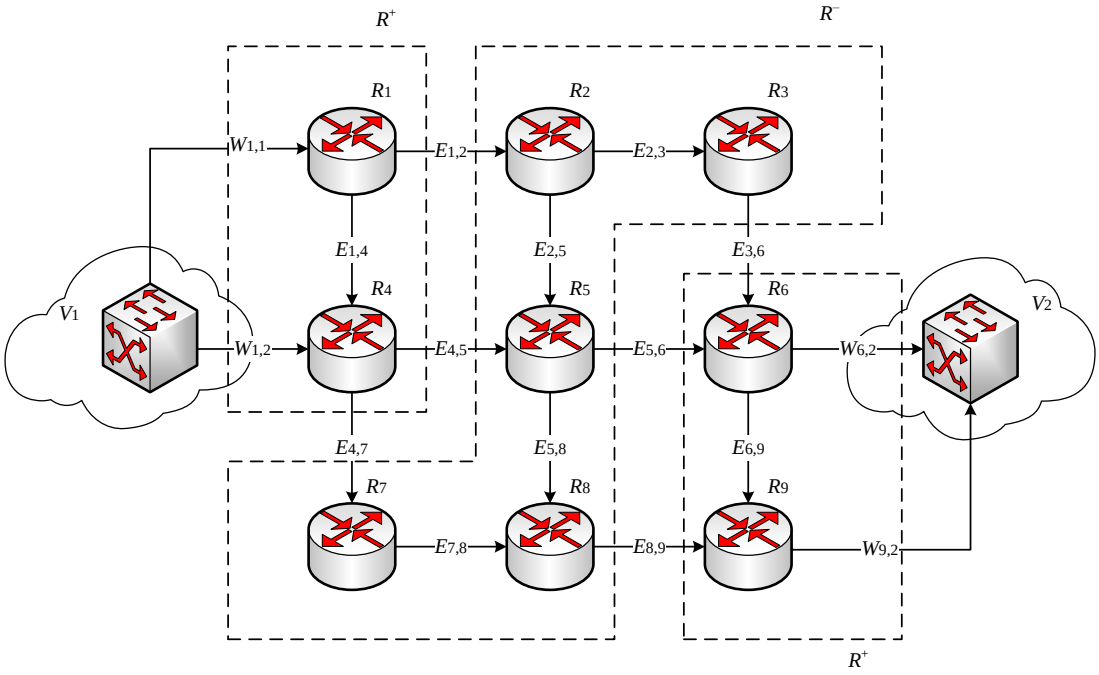


Рисунок 3.4 – Приклад топології мережі, яка підлягала дослідженню

Таблиця 3.2 – Пропускні здатності каналів зв’язку мережі

Канал зв’язку	$E_{1,2}$	$E_{1,4}$	$E_{2,3}$	$E_{2,5}$	$E_{3,6}$	$E_{4,5}$
Пропускна здатність, 1/с	250	420	150	270	250	350
Канал зв’язку	$E_{4,7}$	$E_{5,6}$	$E_{5,8}$	$E_{6,9}$	$E_{7,8}$	$E_{8,9}$
Пропускна здатність, 1/с	220	150	110	390	280	330

Досліджувався випадок, коли використовувались як інтегральні показники мережної безпеки приграничних маршрутизаторів їх ймовірності компрометації (табл. 3.3).

Таблиця 3.3 – Імовірності компрометації приграничних маршрутизаторів

Маршрутизатор	R_1	R_4
A_i	0,05	0,15

Інтенсивність потоку пакетів змінювалась від 10 до 500 пакетів на секунду (1/с). Тоді на рис. 3.5 показані залежності верхнього порогу завантаженості каналів зв’язку мережі від інтенсивності потоку, які отримані для різних методів.

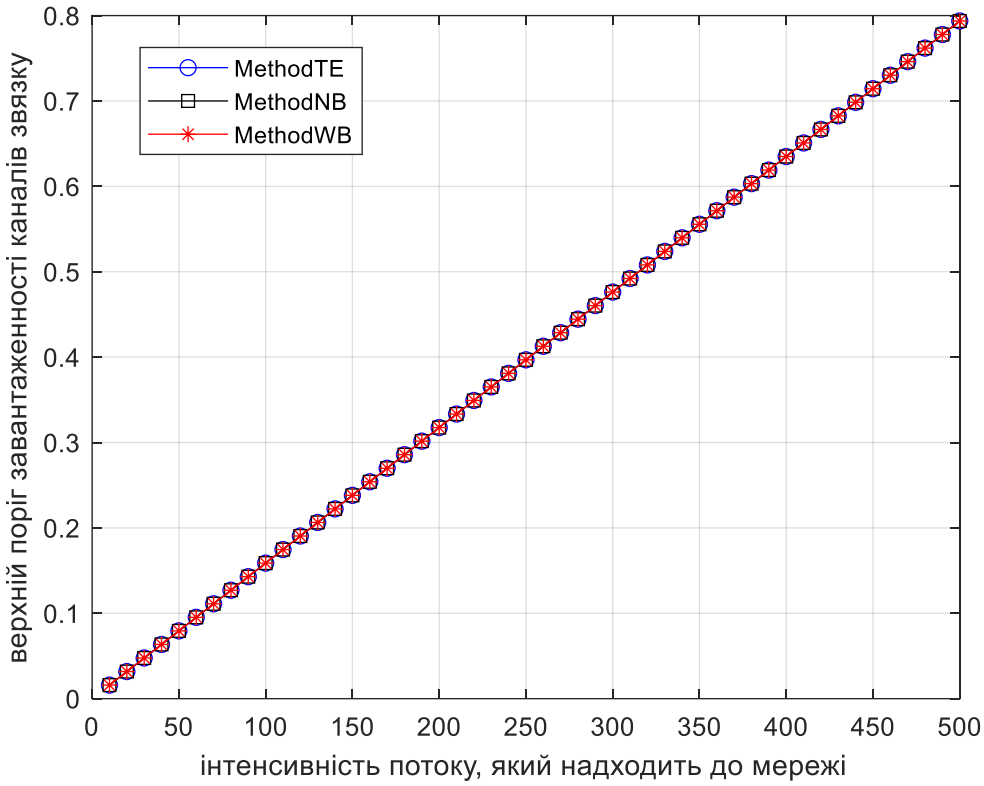


Рисунок 3.5 – Залежності верхнього порогу завантаженості каналів зв’язку мережі від інтенсивності потоку, які отримані для різних методів

З рис. 3.5 можемо зробити висновок, що проаналізовані методи забезпечують однаковий рівень завантаженості мережі, тобто однаковий рівень якості обслуговування. На рис. 3.6 – 3.8 наведено результати розрахунків, а на рис. 3.7 – 3.9 порядок маршрутизації та балансування навантаження між маршрутизаторами, які суттєво відрізнявся один від одного.

```
LP:                Optimal objective value is 0.793651.


Optimal solution found.

No integer variables specified. Intlinprog solved the linear problem.


y =

  119.0476
  380.9524
  119.0476
         0
  119.0476
         0
  119.0476
  206.3492
  174.6032
  119.0476
   87.3016
         0
  174.6032
  261.9048
  238.0952
  261.9048
```

Рисунок 3.6 – Результати розрахунків за методом MethodTE (при $\lambda = 500$ 1/с)

```
LP:                Optimal objective value is 0.843751.


Optimal solution found.

No integer variables specified. Intlinprog solved the linear problem.


y =

  500.0000
         0
  198.4127
  301.5873
  119.0476
   79.3651
  119.0476
  126.9841
  174.6032
  119.0476
   87.3016
         0
  174.6032
  261.9048
  238.0952
  261.9048
```

Рисунок 3.7 – Результати розрахунків за методом MethodNB (при $\lambda = 500$ 1/с)

```
LP:                Optimal objective value is 0.793651.


Optimal solution found.

No integer variables specified. Intlinprog solved the linear problem.


y =

  375.0000
  125.0000
  198.4127
  176.5873
  119.0476
   79.3651
  119.0476
  126.9841
  174.6032
  119.0476
   87.3016
         0
  174.6032
  261.9048
  238.0952
  261.9048
```

Рисунок 3.8 – Результати розрахунків за методом MethodWB (при $\lambda = 500$ 1/с)

На рис. 3.9 – 3.11 у розривах каналів зв'язку вказано дробом їх характеристики: чисельник – інтенсивність потоку, а знаменник – пропускна здатність.

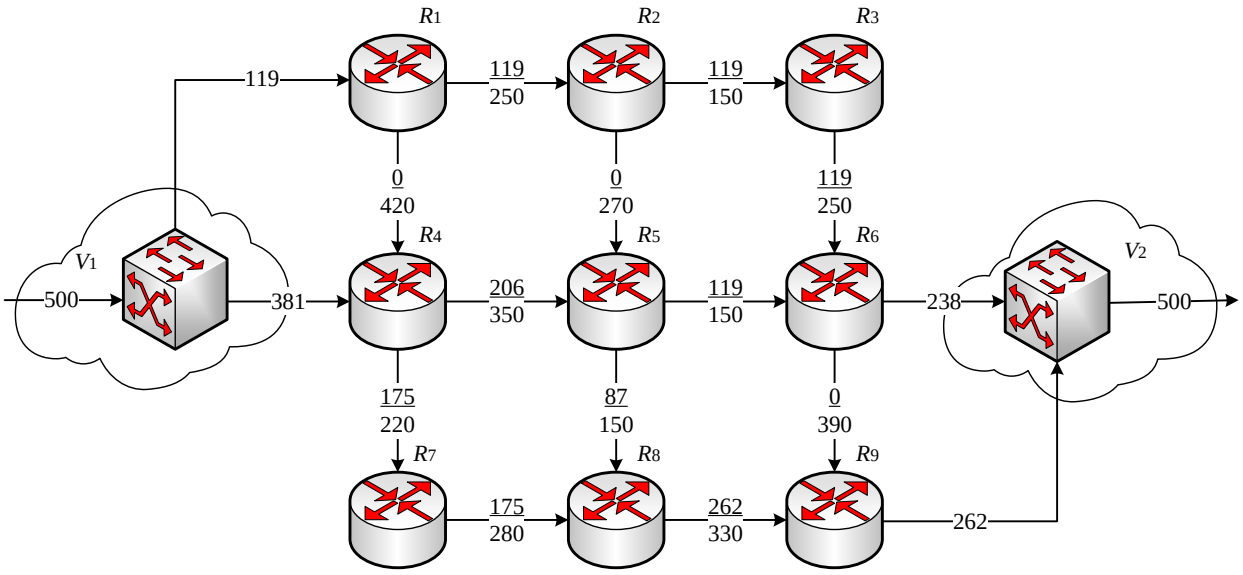


Рисунок 3.9 – Порядок балансування навантаження в ІКМ за методом MethodTE (при $\lambda = 500$ 1/с)

За методом MethodTE навантаження балансується без врахування рівня безпеки приграничних маршрутизаторів, тому, наприклад, через четвертий маршрутизатор, який є втричі небезпечнішим, а ніж перший (табл. 3.3), пакети передавались більш інтенсивно (рис. 3.9).

За методом MethodNB навантаження балансується всередині мережі, на границі мережі балансування відсутнє (рис. 3.10). При цьому весь трафік з першої локальної мережі надходить через перший маршрутизатор, який є більш безпечним, а ніж інший (четвертий) маршрутизатор, що також входить до віртуального шлюзу за замовчуванням для цієї мережі доступу. Таке рішення відповідає фізиці роботи протоколів VRRP та HSRP, адаптованих під вимоги мережної безпеки.

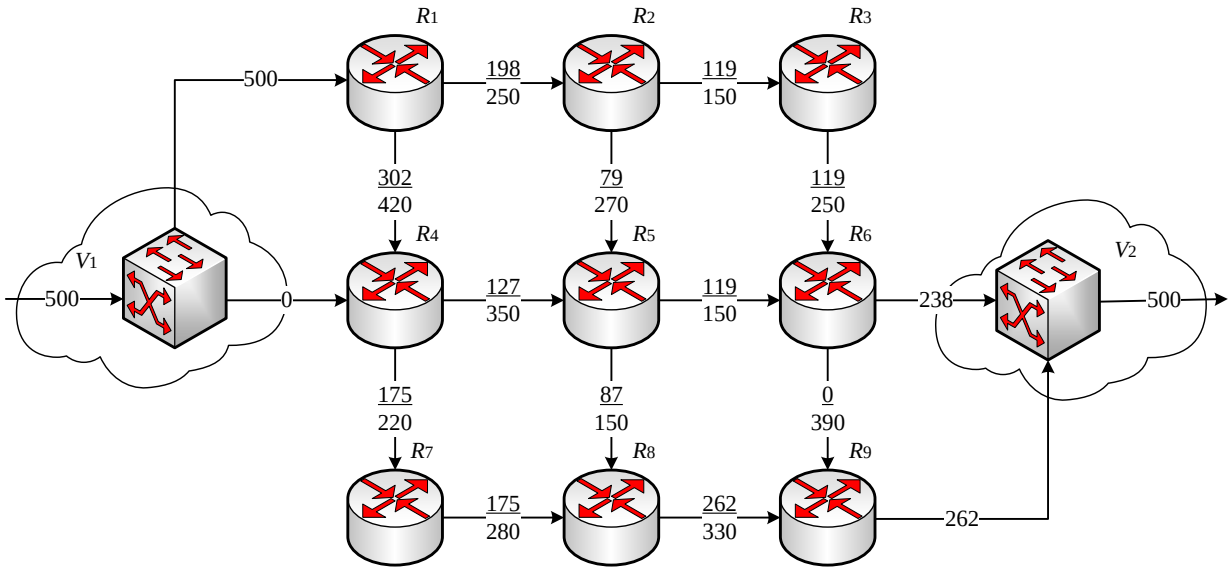


Рисунок 3.10 – Порядок балансування навантаження в ІКМ за методом MethodNB (при $\lambda = 500$ 1/с)

Згідно до методу MethodWB навантаження балансується як всередині мережі, так і на границі мережі (рис. 3.11). При цьому весь трафік з першої мережі доступу надходить як через перший маршрутизатор, так і через четвертий маршрутизатор. При цьому порядок балансування (ступінь використання) приграничного маршрутизатора зовнішнім трафіком напряму залежав від рівня його мережної безпеки (3.14). Четвертий маршрутизатор, наприклад (табл. 3.3), мав ймовірність компрометації втричі вищу, а ніж перший маршрутизатор. Тому через перший маршрутизатор передавався трафік з утричі

вищою швидкістю.

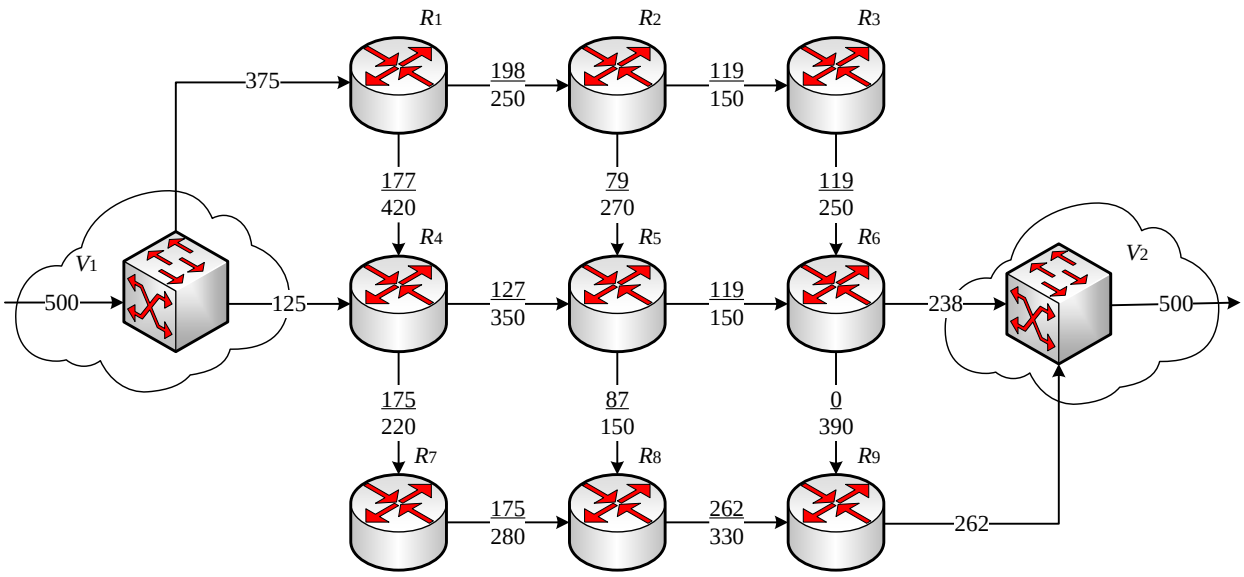


Рисунок 3.11 – Порядок балансування навантаження в ІКМ за методом MethodWB (при $\lambda = 500$ 1/с)

Таким чином, метод MethodWB відповідає принципам роботи протоколу GLBP у режимі зваженого балансування, адаптованого під вимоги мережної безпеки. При цьому вагові параметри інтерфейсів пригранічних маршрутизаторів, які входять до віртуального шлюзу за замовчуванням, мають формуватись відповідно до встановлено рівня безпеки цих маршрутизаторів.

3.4 Розробка рекомендацій щодо практичного використання досліджених рішень

Для реалізації результатів дослідження на практиці варто проаналізувати можливості існуючих протоколів відмовостійкої маршрутизації щодо вдосконалення їх програмного чи алгоритмічного забезпечення. Як зазначалось у першому розділі для вибору основного шлюзу за замовчуванням (Active/Master) у протоколах HSRP та VRRP аналізується налаштовані пріоритети та IP-адреси фізичних інтерфейсів. Тому доречно, щоб, наприклад, пріоритет інтерфейсу налаштовувався відповідно до значень інтегрального показника мережної безпеки.

Значення пріоритетів інтерфейсів (Pr) у протоколах HSRP та VRRP

змінюються у діапазоні від 0 до 255. Тому пропонується використовувати таку функціональну залежність для визначення пріоритету на основі ймовірності компрометації (P_C) маршрутизатора взагалі:

$$\Pr = 255(1 - P_C). \qquad (3.15)$$

Тоді згідно з (3.15) маршрутизатору, який має мінімальне значення ймовірності компрометації, буде налаштовуватись найвищий пріоритет.

На рис. 3.12 наведена мережа, яка налаштовувалась за допомогою протоколу HSRP у симуляторі Packet Tracer. На рис. 3.13 наведено приклад налаштування пріоритету 217 на інтерфейсі приграничного маршрутизатора Router4 (R_4), який має ймовірність компрометації 0,15 (табл. 3.3).

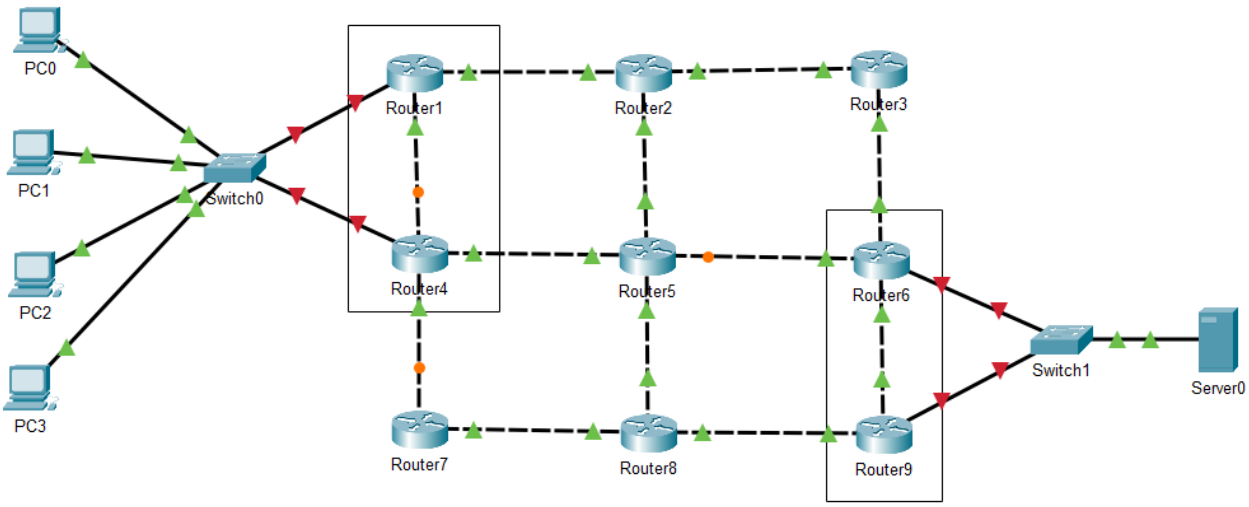


Рисунок 3.12 – Приклад досліджуваної мережі у симуляторі Packet Tracer

```
Router(config-if)#standby 1 priority 217
```

Рисунок 3.13 – Приклад налаштування пріоритету інтерфейсу приграничного маршрутизатора Router4

Перший маршрутизатор (табл. 3.3) у такому випадку (4.1) матиме пріоритет 242.

Подібна ситуації характерна і для випадку, коли інтегральним показником виступають бали CVSS, які варіюються у діапазоні від 0 до 10 (табл. 1.1). Таким

чином, пропонується використовувати таку функціональну залежність для визначення пріоритету на основі ймовірності компрометації (P_c) маршрутизатора взагалі:

$$\Pr = 255(10 - CVSS). \qquad (3.16)$$

Тоді згідно з (3.16) маршрутизатору, який є небезпечним та має максимальне значення балів CVSS, буде налаштовуватись найнижчий пріоритет.

Інша ситуація спостерігається у випадку балансування навантаження за методом MethodWB, який можна реалізувати шляхом налаштування зваженого режиму балансування за протоколом GLBP. У протоколі GLBP пріоритет інтерфейсу впливає на вибір AVG – координатора роботи протоколу, всі ж інші маршрутизатори стають AVF. Кожен маршрутизатор GLBP-групи приймає участь у балансуванні навантаження відповідно до налаштованих вагових параметрів. На рис. 3.14 показано приклад налаштування ваги на інтерфейсах маршрутизаторів R_1 та R_4 у симуляторі GNS3.

```
R1(config-if)#glbp 1 load-balancing weighted
R1(config-if)#glbp 1 we
R1(config-if)#glbp 1 weighting 3
```

а) для R_1

```
R4(config-if)#glbp 1 load-balancing weighted
R4(config-if)#glbp 1 we
R4(config-if)#glbp 1 weighting 1
```

б) для R_4

Рисунок 3.14 – Приклад налаштування ваги на інтерфейсах маршрутизаторів R_1 та R_4 у симуляторі GNS3

З метою автоматизації налаштування мережі, а саме параметрів балансування навантаження за протоколом GLBP, можна використати середовище Python. У мережі можна налаштувати спеціальний керуючий сервер, який реалізує Python-код з метою збору та обробки інформації про стан мережі, розрахунку маршрутів та порядку балансування навантаження, адаптуючи Matlab-код (рис. 3.1 – 3.3) та здійснюючи автоматизоване відділене налаштування маршрутизаторів за допомогою протоколу SSH. Приклад Python-

коду для віддаленого налаштування за протоколом SSH процесу зваженого балансування на першому маршрутизаторі відповідно до GLBP показано на рис. 3.15.

```
File  Edit  Format  Run  Options  Window  Help
import paramiko

# SSH connection details
hostname = '192.168.1.1'
port = 22
username = 'admin'
password = 'password'

# GLBP configuration details
interface = 'FastEthernet0/0'
glbp_group = '1'
glbp_weighted_load_balancing = '3'

# Connect to the device
ssh_client = paramiko.SSHClient()
ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
ssh_client.connect(hostname, port, username, password)

# Open an interactive shell
shell = ssh_client.invoke_shell()

# Send commands to configure GLBP weighted load balancing
shell.send('configure terminal\n')
shell.send(f'interface {interface}\n')
shell.send('glbp {0} load-balancing weighted\n'.format(glbp_group))
shell.send(f'glbp {glbp_group} weighting {glbp_weighted_load_balancing}\n')
shell.send('end\n')

# Wait for the command to complete
while not shell.recv_ready():
    pass

# Read the output
output = shell.recv(65535).decode('utf-8')
print(output)

# Close the SSH connection
ssh_client.close()
```

Рисунок 3.15 – Приклад Python-коду для віддаленого налаштування за протоколом SSH процесу зваженого балансування на першому маршрутизаторі відповідно до GLBP

Аналогічним чином може здійснюватися і налаштування інших маршрутизаторів мережі, які використовують протокол GLBP.

3.5 Висновки до третього розділу

1. Проведено огляд методів та засобів проактивного захисту пригранічних маршрутизаторів IP-мережі. Обґрунтовано до використання оптимізаційну потокову модель відмовостійкої маршрутизації (3.1)-(3.10), яка детально описана у роботах [31, 32]. Шляхом доповнення (3.11)-(3.14) обраної моделі виділено для подальшого дослідження три методи проактивного захисту пригранічних маршрутизаторів IP-мережі. Перший метод відповідав моделі (3.1)-(3.10) та носив назву MethodTE (Method «Traffic Engineering»). Другий метод заснований на моделі (3.1)-(3.9), (3.11) та мав назву MethodNB (Method «no balancing»). Третій метод використав модель (3.1)-(3.10), (3.12)-(3.14) та називався MethodWB (Method «with balancing»).

2. Обрані методи було реалізовані у середовищі Matlab (рис. 3.1 – 3.3). Їх дослідження базувалось на використанні мережі, топологія якої представлена на рис. 3.4. У процесі дослідження встановлено, що проаналізовані методи забезпечують однаковий рівень завантаженості мережі, тобто однаковий рівень якості обслуговування (рис. 3.5), а от порядки маршрутизації та балансування навантаження між маршрутизаторами суттєво відрізнялись один від одного (рис 3.9 – 3.11). Базовий метод MethodTE при балансуванні навантаження ніяким чином не враховував показники мережної безпеки комунікаційного обладнання. Метод MethodNB не підтримував балансування на границі мережі, обираючи як шлюз за замовчуванням маршрутизатор з найкращим інтегральним показником мережної безпеки, наприклад, ймовірність компрометації пристрою або бали CVSS. Метод MethodWB підтримував балансування навантаження на границі мережі. При цьому до більш безпечного пригранічного маршрутизатора пакети надходили більш інстенсивно, а ніж на менш безпечний.

3. Розроблено рекомендації щодо практичного впровадження проаналізованих методів проактивного захисту пригранічних маршрутизаторів в IP-мережах. Пропозиції стосувались налаштувань протоколів VRRP та HSRP під метод MethodNB, а також протоколу GLBP під методі MethodWB. Розподіл ролей щодо основного (Master/Active) чи резервного (Backup/Standby) пропонується здійснювати шляхом налаштування пріоритету інтерфейсів маршрутизаторів (рис. 3.13) відповідно до значення інтегрального показника мережної безпеки маршрутизатора. Порядок балансування навантаження у

протоколі GLBP також пропонується здійснювати шляхом налаштування вагових параметрів для режиму зваженого балансування або у ручну (рис. 3.14), або з використанням засобі мережної автоматизації (рис. 3.15).

ВИСНОВКИ

1. Робота присвячена задачам забезпечення мережної безпеки в інфокомунікаціях. Для цього проведено аналіз комплексу заходів, які реалізуються в ІКМ з метою забезпечення мережної безпеки. Встановлено, що одним з ефективних засобів як проактивного, так і реактивного забезпечення мережної безпеки в ІКМ є протоколи IP-маршрутизації. Ці протоколи постійно вдосконалюються у напрямку підвищення рівня безпеки як ІКМ, так і самих протоколів, як об’єктів атак. Тому об’єктом дослідження обрано протоколи відмовістійкої маршрутизації сімейства FHRP, які забезпечують захист шлюзу за замовчуванням у випадку його компрометації або перевантаження за результатами мережної атаки на приграничні маршрутизатори.

2. У роботі проведено порівняльний аналіз протоколів сімейства FHRP, а саме протоколів VRRP, HSRP та GLBP, які призначені для підвищення доступності шлюзу за замовчуванням шляхом резервування функцій приграничних маршрутизаторів. Саме ці протоколи забезпечують як проактивний, так і реактивний захист шлюзу за замовчуванням, ускладнюючи роботу зловмисника щодо контролю над трафіком, який передається від мережі доступу до глобальної мережі. З’ясовано переваги. Недоліки та область застосування даних протоколів. Проведено огляд основних типів мережних атак, реалізація яких може призвести до порушення рівня мережної безпеки та компрометації мережного обладнання, залучених протоколами сімейства FHRP. З метою протидії мережним атакам пропонується у процесі забезпечення проактивного захисту мережі здійснювати ефективне балансування навантаження між приграничними маршрутизаторами з врахуванням рівня їх безпеки на основі, наприклад, інформації стандартів CVSS.

3. На основі проведеного огляду методів та проактивного захисту приграничних маршрутизаторів IP-мережі обґрунтовано до використання оптимізаційну потокову модель відмовостійкої маршрутизації (3.1)-(3.10). Шляхом її вдосконалення (3.11)-(3.14) виділено для подальшого дослідження три методи проактивного захисту приграничних маршрутизаторів IP-мережі. MethodTE (Method «Traffic Engineering»), MethodNB (Method «no balancing») та MethodWB (Method «with balancing»). Ці методи було реалізовані у середовищі Matlab (рис. 3.1 – 3.3).

4. У процесі дослідження встановлено, що проаналізовані методи забезпечують однаковий рівень завантаженості мережі, тобто однаковий рівень якості обслуговування (рис. 3.5). Порядок маршрутизації та балансування навантаження між маршрутизаторами у цих методах суттєво відрізнялись один від одного (рис 3.9 – 3.11). Базовий метод MethodTE при балансуванні навантаження не враховував показники мережної безпеки комунікаційного обладнання, метод MethodNB не підтримував балансування на границі мережі, обираючи як шлюз за замовчуванням маршрутизатор з найкращим інтегральним показником мережної безпеки. Метод MethodWB підтримував балансування навантаження на границі мережі. При цьому до більш безпечного приграничного маршрутизатора пакети надходили більш інстенсивно, а ніж на менш безпечний.

5. Розроблено рекомендації щодо практичного використання та реалізації проаналізованих методів проактивного захисту приграничних маршрутизаторів в IP-мережах. Пропозиції стосувались особливостей налаштувань протоколів VRRP та HSRP згідно з методом MethodNB, а також протоколу GLBP (метод MethodWB). Пропонується вибір основного (Master/Active) та резервного (Backup/Standby) маршрутизаторів здійснювати шляхом налаштування пріоритету інтерфейсів маршрутизаторів (рис. 3.13) відповідно до значення інтегрального показника мережної безпеки маршрутизатора. Порядок балансування навантаження у протоколі GLBP також пропонується здійснювати шляхом налаштування вагових параметрів для режиму зваженого балансування або у ручну (рис. 3.14), або з використанням засобі мережної автоматизації (рис. 3.15).

6. Результати магістерської роботи опубліковані у працях [36 – 39].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. 181 p.

2. Поповський В.В. Основи теорії телекомунікаційних систем: підручник. Харків: ХНУРЕ, 2018. 368с.

3. Kurose J.F., Ross K. Computer Networking. 8th Edition. Pearson, 2020. 775 p.

4. Blokdyk G. Software-Defined Networking SDN production, 1st edition. 5STARCooks, 2019. 238 p.

5. Лемешко О.В., Лошаков В.А., Поповський В.В. та ін. Багатоканальний електрозв'язок та телекомунікаційні технології: підручник у 2-х частин. Ч.1 / О.В. Лемешко, В.А. Лошаков, В.В. Поповський та ін .; за заг. ред. проф. Поповського В.В. – Х .: ТОВ "Компанія СМІТ", 2010. – 470 с.

6. Chapman C. Network Performance and Security (Testing and Analyzing Using Open Source and Low-Cost Tools), 1st edition, Syngress, 2016. 380 p.

7. Edgar T., Manz D. Research Methods for Cyber Security, 1st edition. Syngress, 2017. 428 p.

8. Лемешко О.В., Єременко О.С., Невзорова О.С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ, 2020. 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1.

9. Лемешко О.В., Єременко О.С., Євдокименко М.О., Шаповалова А.С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : монографія. М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1.

10. Hoang D.B., Farahmandian S. Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies. In: Zhu, S., Scott-Hayward, S., Jacquin, L., Hill, R. (eds) Guide to Security in SDN and NFV. *Computer Communications and Networks*. Springer, Cham, 2017, P. 3–32. DOI: https://doi.org/10.1007/978-3-319-64653-4_1

11. Yevdokymenko M.O., Shapovalova A.S., Nevzorova O.S. Proactive Approach for Security of the PAAS Model of Cloud System Based on Vulnerability

Assessment. *International Journal of Science and Engineering Investigations*. Vol. 8(91). 2019. P. 167–173. URL: http://www.ijsei.com/papers/ijsei-89119-22.pdf.

12. Linkov I., Kott A. Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, Springer, Cham, 2019. P. 1–25.

13. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. *China Communications*. 2019. № 16(7). P. 13–31. DOI: https://doi.org/10.23919/JCC.2019.07.002.

14. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional, 2018. 800 p.

15. CVSS v3.0 User Guide. *FIRST – Forum of Incident Response and Security Teams*. URL: https://www.first.org/cvss/v3.0/user-guide (дата звернення: 15.12.2022).

16. CVSS v3.1 Examples. *FIRST – Forum of Incident Response and Security Teams*. URL: https://www.first.org/cvss/examples (дата звернення: 15.12.2022).

17. NIST National Vulnerability Database. *NVD - Home*. URL: https://nvd.nist.gov (дата звернення: 15.12.2022).

18. CVSS v3.1 Specification Document. *FIRST – Forum of Incident Response and Security Teams*. URL: https://www.first.org/cvss/v3.1/specification-document (дата звернення: 15.12.2022).

19. ISO/IEC 15408-1:2009. Information technology, Security techniques Evaluation criteria for IT security, Part 1: Introduction and general model. URL: https://www.iso.org/standard/50341.html.

20. Medhi D., Ramasamy K. Network Routing (Algorithms, Protocols, and Architectures), 2nd edition, Elsevier Inc, 2018. 1018 p.

21. Misra S., Goswami S. Network Routing: Fundamentals, Applications, and Emerging Technologies 1st Edition. Wiley, 2017. 536 p.

22. Cisco Networking Academy (Ed.). Routing Protocols Companion Guide. Pearson Education. 2014. 792 p.

23. Vegesna S. IP Quality of Service (Cisco networking fundamentals). Cisco press. 2001. 232 p.

24. Osborne E.D., Simha A. Traffic engineering with MPLS. Cisco Press, 2002. 608 p.

25. Cholda P., Tapolcai J., Cinkler T., Wajda K., Jajszczyk A. Quality of resilience as a network reliability characterization tool. IEEE network. 2009. Vol. 23, No. 2. P. 11–19. DOI: 10.1109/MNET.2009.4804331.

26. Hussain I. Fault-Tolerant IP and MPLS Networks (Networking Technology). Indianapolis: Cisco Press, 2005. 336 p.

27. First Hop Redundancy Protocol comparison (HSRP, VRRP, GLBP) with the diagram (2013). Cisco Networking Center. URL: http:// cisconetworkingcenter.blogspot.com/2013/01/first-hop-redundancy-protocol.html.

28. Hamza M. Common Attacks On Routing Protocols And How To Mitigate Them. *Medium*. URL: https://hamzamhirsi.medium.com/common-attacks-on-routing-protocols-and-how-to-mitigate-them-11ec0cad08d7 (дата звернення: 20.05.2023).

29. Alam T.*et al*. Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol, *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, Chittagong, Bangladesh, 2018, pp. 367-371, doi: 10.1109/ICISET.2018.8745601.

30. Abdallah S., Najjar E., Kayssi A. A Round Robin Load Balancing and Redundancy Protocol for Network Routers. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, 2012, pp. 1741-1747, doi: 10.1109/TrustCom.2012.54.

31. Acosta, J. C., Estrada Jr, P. A preliminary architecture for building communication software from traffic captures. In *Disruptive Technologies in Sensors and Sensor Systems*, 2017, Vol. 10206, pp. 189-200.

32. Ab Rahman, R., Alias, F. A., Kassim, M., Yusof, M. I., Hashim, H. Implementation of high availability concept based on traffic segregation over MPLS-TE. ARPN Journal of Engineering and Applied Sciences, 2015, 10(3), 1295-301.

33. Лемешко О.В., Круглова А.О., Журавльова А.С., Лемешко В.О. Вдосконалена модель балансування навантаження в інфокомунікаційній мережі // Проблеми телекомунікацій. 2020. 2(27). С. 56-67. URL: https://pt.nure.ua/wp-content/uploads/2021/11/202_lemeshko_balancing.pdf.

34. Лемешко О.В., Круглова А.О., Крепко А.В. Порівняльний аналіз проактивних рішень з відмовостійкої маршрутизації в інфокомунікаційній мережі. Проблеми телекомунікацій. 2022. № 2(31). С. 3-22. URL: https://pt.nure.ua/wp-content/uploads/2022/12/222_lemeshko_routing.pdf.

35. Lemeshko O., Yeremenko O., Yevdokymenko M., Porokhniak V., Harkusha S., Harkusha O. System of Routing Solutions Based on Security Aware Traffic Engineering Models. Next Generation Cybersecurity Systems and Applications - NGSEC’2022. 14 – 15 July 2022, pp.1-5.

36. Abdiyeva-Aliyeva G., Aliyev J., Nazarov B. Tthe use of artificial intelligence based techniques for detection and prevention of cyber attacks. VI International Scientific Conference Of Young Researchers. BAKU, 2021. P.773-775.

37. Abdiyeva-Aliyeva G., Aliyev J., Sadigov U. Application of classification algorithms of Machine learning in cybersecurity, Procedia Computer Science, Volume 215, 2022, Pages 909-919, https://doi.org/10.1016/j.procs.2022.12.093.

38. Aliyev J. Analizing protocols for layer three network and ways to combat them. Second International conference on "Information security: problems and prospects", November 25, 2022, Baku, Azerbaijan. P. 20-24.

39. Алиев Д., Назаров Б., Ибрагимли И. Обеспечение информационной безопасности на основе SIEM систем. Second International conference on "Information security: problems and prospects", November 25, 2022, Baku, Azerbaijan. P. 17-20.