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)

Аналіз та дослідження методів виявлення вразливостей мережного обладнання

(Analysis and research on methods for detecting networks equipment vulnerabilities)

(тема)

Виконав:

студент 2 курсу, групи АМСЗІизм-21-1

Назаров Б. А.

(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: проф. каф. ІКІ імені В.В. Поповського Євдокименко М.О.

(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 Назарову Байрамалі Аріф огли
(прізвище, і'мя, по батькові)

1. Тема роботи: Аналіз та дослідження методів виявлення вразливостей мережного обладнання
затверджена наказом по університету від 24.10.2022 р. № 172Стз
2. Термін подання студентом роботи до екзаменаційної комісії: 15.05.2023 р.
3. Вихідні дані до роботи: бази даних вразливостей NVD (National Vulnerability Database) та CVE (Common Vulnerabilities and Exposures), метрики оцінки вразливостей за допомогою CVSS 3.1 (Common Vulnerability Scoring System), мережне обладнання, математичний апарат для розрахунку кількісних оцінок вразливості елементів інфокомунікаційної мережі.
4. Перелік питань, які потрібно опрацювати в роботі:
1) Провести аналіз атак на інфокомунікаційні мережі та аналіз вразливостей мережного обладнання, методів їх виявлення.
2) Провести огляд найпоширених вразливостей мережного обладнання в інфокомунікаційних мережах, огляд баз даних вразливостей NVD (National Vulnerability Database) та CVE (Common Vulnerabilities and Exposures).
3) Дослідити математичні моделі безпечної QoS-маршрутизації для мінімізації впливу вразливостей мережного обладнання. Проаналізувати результати математичного моделювання моделей при виявленні вразливостей мережного обладнання.

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 баз даних вразливостей NVD та CVE; огляд уразливостей мережного обладнання; методи маршрутизації щодо реагування на кібератаки внаслідок використання вразливостей мережного обладнання; стандарт CVSS щодо кількісного розрахунку критичності вразливості мережного обладнання; математичні моделі безпечної маршрутизації; результати моделювання; висновки).

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	професор Євдокименко Марина Олександрівна		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
7	Оформлення кваліфікаційної роботи	01.05.2023 р.	Виконано

Дата видачі завдання 24 жовтня 2022 р.

Студент _____ Назаров Б. А.
(підпис) (прізвище та ініціали)

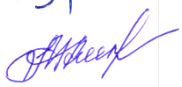
Керівник роботи професор кафедри ІКІ ім. В.В. Поповського

_____ Євдокименко М.О.

(підпис) (посада, прізвище, ініціали)

Робота не містить відомостей, заборонених до відритого опублікування.

Студент  Назаров Б. А.

Керівник роботи  Євдокименко М.О.

РЕФЕРАТ

Пояснювальна записка: 65 с., 12 рис., 17 табл., 37 джерел.

ІНФОКОМУНІКАЦІЙНА МЕРЕЖА, ВРАЗЛИВІСТЬ, МЕРЕЖНА БЕЗПЕКА, МОДЕЛЬ МАРШРУТИЗАЦІЇ.

Об’єкт дослідження – процес забезпечення мережної безпеки у інфокомунікаційних мережах засобами маршрутизації із врахуванням вразливостей мережного обладнання.

Предмет дослідження – методи безпечної маршрутизації у інфокомунікаційних мережах.

Мета роботи – дослідження моделей безпечної QoS-маршрутизації в інфокомунікаційних мережах для мінімізації ризиків під час ймовірного використання вразливостей мережного обладнання.

Методи досліджень – аналітичне моделювання, симуляція, формалізація та порівняння.

В кваліфікаційній роботі вирішено важливу науково-прикладну задачу, пов’язану з оглядом найпоширеніших атак на інфокомунікаційну мережу, аналізом вразливостей мережного обладнання, методів їх виявлення та методів щодо мінімізації впливу вразливостей мережного обладнання за допомогою математичних моделей безпечної QoS-маршрутизації.

Проведений аналіз методів виявлення вразливостей показав необхідність аналізу, виявлення, оцінки критичності та розробки плану усунення знайдених вразливостей, а також мінімізацію ризиків під час їх ймовірного використання.

В результаті досліджень доведено, що за допомогою безпечної маршрутизації та досліджуваного методу, а саме визначаючи пріоритетність безпечних шляхів, розглядаючи системи виявлення/запобігання вторгненням, впроваджуючи політику сегментації мережі, контролю доступу та оцінку критичності вразливостей елементів мережі, можливо суттєво знизити ризики та ймовірні збитки у разі використання вразливостей мережного обладнання із наявними критичними вразливостями.

ABSTRACT

The report contains: 65 p., 12 fig., 17 tables, 37 sources.

INFOCOMMUNICATION NETWORK, VULNERABILITY, NETWORK SECURITY, ROUTING MODEL.

The object of research is the process of ensuring network security in infocommunication networks by means of routing, taking into account the vulnerabilities of network equipment.

The subject of research is secure routing methods in infocommunication networks.

The purpose of the work is to study secure QoS routing models in information communication networks to minimize risks during the probable use of network equipment vulnerabilities.

Research methods are analytical modeling, simulation, formalization, and comparison.

The qualification work solves an important scientific and applied problem related to the review of the most common attacks on the infocommunication network, the analysis of network equipment vulnerabilities, their detection methods and methods for minimizing the impact of network equipment vulnerabilities using mathematical models of secure QoS routing.

The conducted analysis of vulnerability detection methods showed the need to analyze, identify, evaluate the criticality and develop a plan to eliminate the vulnerabilities found, as well as minimize risks during their probable use.

As a result of research, it has been proven that with the help of secure routing and the researched method, namely, by prioritizing secure paths, considering intrusion detection/prevention systems, implementing network segmentation policy, access control and assessing the criticality of network element vulnerabilities, it is possible to significantly reduce risks and potential losses in in case of using vulnerabilities of network equipment with existing critical vulnerabilities.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

РІБ – Ризик інформаційної безпеки

ІКМ – Інфокомунікаційна мережа

ІКТ – Інфокомунікаційні технології

API – Application Programming Interface

APT – Advanced Persistent Threat

ARP – Address Resolution Protocol

CVE – Common Vulnerabilities і Exposures

CVSS – Common Vulnerability Scoring System

DDoS – Distributed Denial of Service

DoS – Denial of Service

EIGRP – Enhanced Interior Gateway Routing Protocol

FRR – Fast ReRoute

H-SPREAD – Hybrid Secure Protocol for Reliable dAta Delivery

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Taskforce

IP – Internet Protocol

IRTF – Internet Research Task Force

IT – Information Technologies

ITU-T – International Telecommunication Union Telecommunication Standardization Sector

MANO – Management and Orchestration, MANO

NIST – National Institute of Standards and Technology

NVD – National Vulnerability Database

ONF – Open Networking Foundation

OPNFV – Open Platform for NFV

OSPF – Open Shortest Path First

QoS – Quality of Service

RADIUS – Remote Authentication Dial-In User Service

SBI – SouthBound Interface

SDN – Software Defined Network

SIEM – Security information and event management
S-FRR – Secure Fast ReRoute
SPREAD – Secure Protocol for Reliable dAta Delivery
SOAR – Security Orchestration, Automation and Response
TE – Traffic Engineering
TLS – Transport Layer Security
VNF – Virtualized Network Functions

ВСТУП

Захист інфокомунікаційних мереж є критично важливим завданням у сучасному цифровому світі. Злочинці, хакери, кібершпигуни та інші зловмисники постійно намагаються зламати інфраструктуру інфокомунікаційних мереж з різноманітними цілями, такими як крадіжка конфіденційної інформації, фінансові шахрайства, руйнування систем і багато іншого. Крім того, кіберзагрози постійно розвиваються у складності та масштабах, боротьба з ними передбачає «поширення» захисту на інфокомунікаційні мережі та системи – сервери, бази даних, сервіси, встановлене програмне забезпечення тощо. Однак заходи кібербезпеки, які застосовуються всередині організації, можуть відрізнятися залежно від розміру компанії, її фінансових можливостей, обладнання, програмного забезпечення та інформації, з якою їй доводиться мати справу під час ділової діяльності тощо.

Для ефективного захисту інфокомунікаційних мереж використовуються комплекс різних підходів та технологій [1-4]. Основними складовими комплексної системи захисту інформації є організаційне забезпечення інформаційної безпеки, а також програмно-апаратні засоби, що виключають несанкціонований доступ до інформації, що захищається. Організаційне забезпечення інформаційної безпеки досягається за рахунок впроваджених політик та правил. Захист за допомогою програмно-апаратних засобів передбачає використання технологій та інструментів безпеки на кожному рівні моделі OSI, починаючи із фізичного захисту периметра ІКМ. Однак, навіть при використанні перевірених засобів безпеки, таких як файєрволи, антівірусні програми, VPN, системи виявлення та протидії атакам, забезпечити захист інфокомунікаційної мережі на 100% не можливо. Це пов’язано з тим, що окрім вищезазначених засобів, необхідно постійно моніторити та спостерігати за ІКМ, виявляти аномальну мережну активність, вразливості та вчасно реагувати на атаки із можливістю швидко відновлювати свою функціональність. Такий моніторинг забезпечують системи управління інформаційною безпекою та подіями безпеки (Security information and event management, SIEM), та системи оркестрації, автоматизації, реагування на інциденти інформаційної безпеки (Security Orchestration, Automation and Response, SOAR). В сукупності дані системи дозволяють збирати дані про події

інформаційної безпеки в ІКМ з різних джерел, обробляти їх та автоматизувати типові сценарії реагування на них.

При цьому одним з головних завдань для підвищення захисту ІКМ є виявлення, аналіз та усунення вразливостей, більшість яких наявні саме в програмному забезпеченні мережного обладнання.

Для виявлення вразливостей в ІКМ, а саме вразливостей мережного обладнання існує декілька методів [3]. Виявлені вразливості та шляхи їх усунення збираються в спеціалізованих базах даних, таких як NVD (National Vulnerability Database) та CVE (Common Vulnerabilities and Exposures) [12, 21], куди вносяться дані про нові вразливості та шляхи їх усунення. Виявлені вразливості дозволяють розрахувати ризики інформаційно безпеки в інфокомунікаційній мережі, та розрахувати сценарії щодо їх мінімізації.

Мінімізувати ризики інформаційної безпеки можливо також за допомогою засобів маршрутизації, а саме протоколів безпечної маршрутизації. Завдяки маршрутним рішенням можна розрахувати та провести аналіз ймовірних сценаріїв використання найпоширених вразливостей мережного обладнання для успішної атаки на інфокомунікаційну мережу.

Таким чином, дана робота присвячена актуальній науково-прикладній задачі, пов’язаній з аналізом вразливостей мережного обладнання інфокомунікаційних мереж, сценаріїв їх використання для проведення атак із подальшою мінімізацією ризиків інформаційної безпеки в ІКМ в цілому за допомогою засобів маршрутизації. Метою роботи є підвищення захисту інфокомунікаційних мереж за допомогою аналізу мережних вразливостей та сценаріїв їх використання зловмисниками шляхом дослідження протоколів безпечної маршрутизації.

В першому розділі було проведено аналіз найпоширеніших атак на компонети інфокомунікаційної мережі та її елементи, аналіз засобів виявлення вразливостей в інфокомунікаційних мережах.

В другому розділі проведено огляд найпоширених вразливостей мережного обладнання в інфокомунікаційних мережах та засобам їх усунення для мінімізації ризиків інформаційної безпеки в інфокомунікаційних мережах, а також базам даних вразливостей NVD та CVE та стандарту з управління ризиками NIST 800-53 щодо кількісного розрахунку рівня вразливості мережного обладнання

Третій розділ присвячено дослідженню та порівняльному аналізу моделей безпечної маршрутизації в ІКМ, що використані в роботі для порівняння впливу на маршрутні рішення показників критичності вразливості мережного обладнання та продуктивності каналів зв’язку. Результатом дослідження є порівняльний аналіз моделей безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей, а також перевірено працездатність, адекватність та ефективність потокових моделі безпечної QoS-маршрутизації за допомогою розрахункових прикладів. Аналітичні результати дослідження довели адекватність та працездатність отримані результати дослідження.

1 ОГЛЯД НАЙПОШИРЕНИХ ТИПІВ АТАК НА ІНФОКОМУНІКАЦІЙНІ МЕРЕЖІ

1.1 Основні компоненти інфокомунікаційних мереж

Сучасні інфокомунікаційні технології (ІКТ) охоплюють широкий спектр інноваційних рішень, які використовуються для передачі, обробки і обміну інформацією. ІКТ використовуються у різних сферах життя, таких як бізнес, освіта, медицина, транспорт, наука, розваги та інші. Вони є основою для розвитку сучасного інформаційного суспільства і мають великий вплив на соціум та взаємодію з оточуючим світом.

ІКТ охоплюють широкий спектр технологій, включаючи телефонію, комп'ютерні мережі, інтернет, бездротовий зв'язок, супутникові зв'язки, цифрове телебачення, радіо, мобільні зв'язки, хмарні обчислення та багато іншого.

Головна мета інфокомунікаційних технологій полягає у забезпеченні ефективного обміну інформацією між користувачами, пристроями та системами. Вони дозволяють передавати, обробляти та зберігати великі обсяги даних, спрощують спілкування, поліпшують доступ до інформації і забезпечують широкі можливості комунікації та обміну даними.

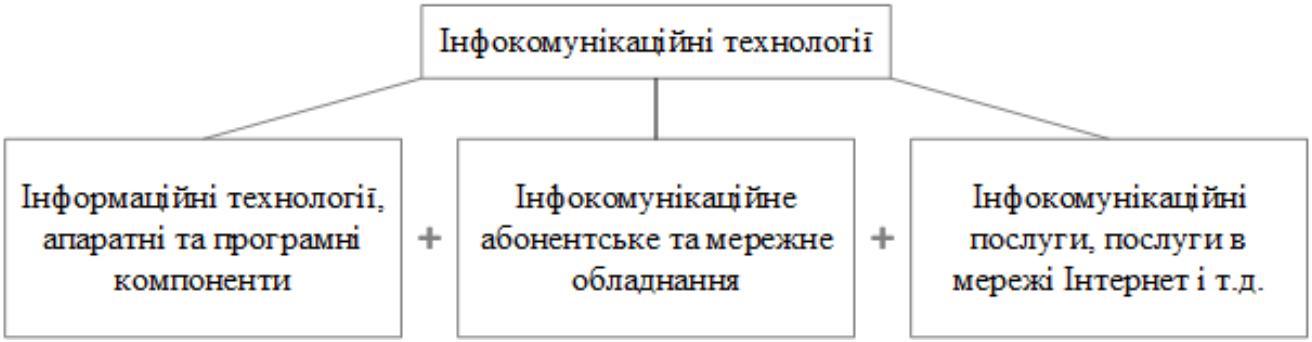


Рисунок 1.1 – Категорії інфокомунікаційних технологій

Найбільш впливові і поширені технології в сучасних інфокомунікаційних системах представлені наступними категоріями [12-16]:

1. Хмарні обчислення: Хмарні обчислення дозволяють доступ до ресурсів обчислювальної потужності, збереження даних та програмного забезпечення через Інтернет. Вони надають гнучкість, масштабованість та швидкий доступ до ресурсів без необхідності локального зберігання і обробки даних.

2. Інтернет речей (IoT): IoT включає в себе підключення фізичних пристроїв, датчиків та обладнання до Інтернету для обміну даними і керування. Ця технологія дозволяє збирати, аналізувати і використовувати великі обсяги даних з різних джерел, що відкриває безліч можливостей для автоматизації і оптимізації процесів.

3. 5G мережі: 5G є п'ятою поколінням мобільних мереж, яке надає значно вищу швидкість передачі даних, зменшення затримок і підвищену пропускну здатність порівняно з попередніми поколіннями. Вона підтримує підключення багатьох пристроїв одночасно і є основою для розвитку смарт-міст і високопродуктивних додатків.

4. Big Data: Великі дані (Big Data) відносяться до обробки і аналізу великого обсягу структурованих і неструктурованих даних, які не можуть бути ефективно оброблені традиційними методами. Ця технологія дозволяє виявляти корисну інформацію, закономірності і тренди з великого масиву даних.

5. Blockchain: Блокчейн є розподіленою базою даних, що забезпечує безпеку, цілісність і недоступність інформації шляхом використання криптографічних методів. Він знаходить застосування у сферах фінансів, логістики, медицини та багатьох інших, забезпечуючи надійну систему запису та перевірки транзакцій.

6. Штучний інтелект (AI) і машинне навчання: Штучний інтелект та машинне навчання використовуються для аналізу даних, розпізнавання образів, автоматизації процесів та прийняття рішень на основі алгоритмів і навчання комп'ютерів. Вони застосовуються в багатьох галузях, включаючи автономні автомобілі, медицину, фінанси та багато інших.

Так, на сьогодняшній день, сучасні інфокомунікаційні мережі побудовані із використанням всіх вищезазначених технологій (рис.1.2).

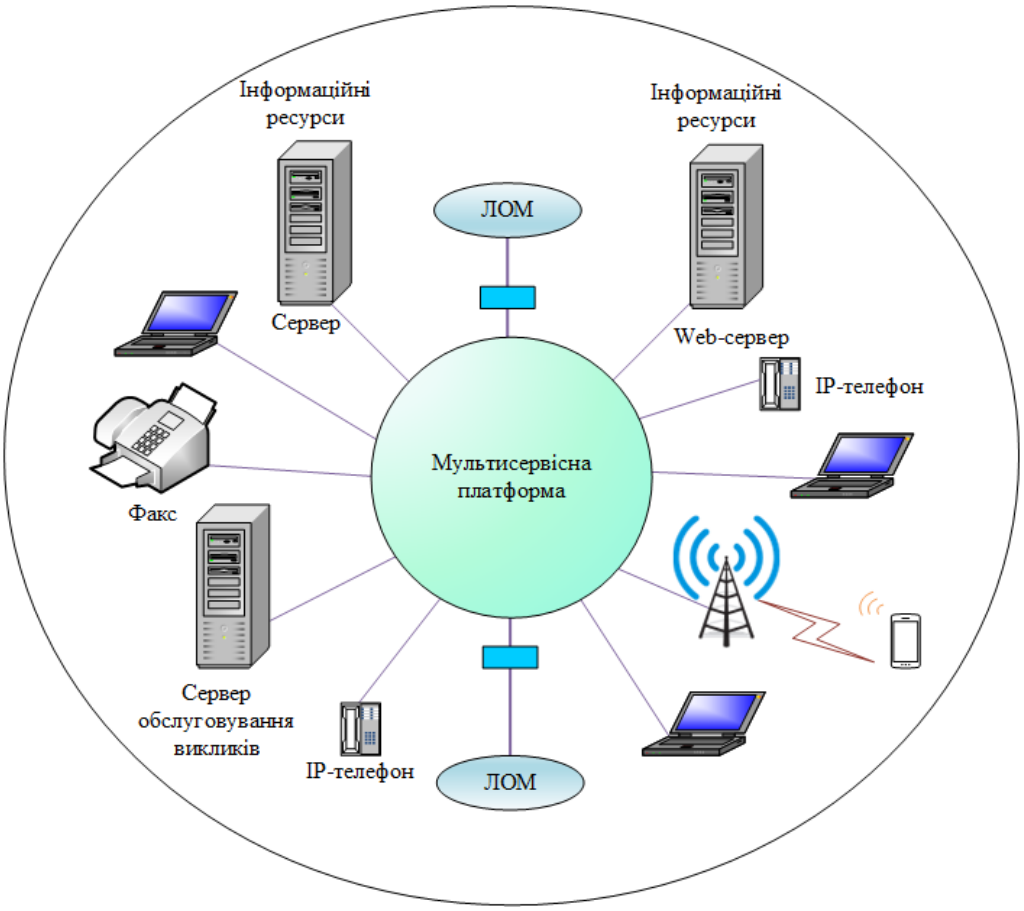


Рисунок 1.2 – Структура інфокомунікаційних мереж

Ядром інфокомунікаційної мережі є мультисервісна платформа (інфраструктура) [4], що забезпечує передачу даних і забезпечує комунікацію між різними пристроями і системами в мережі. Інфокомунікаційна мережа (ІКМ) складається з різних компонентів, які працюють разом для забезпечення передачі даних і комунікаційних послуг. Основні компоненти інфокомунікаційної мережі включають наступні елементи, приведені в таблиці 1.1.

Таблиця 1.1 – Основні компоненти інфокомунікаційних мереж

	Компоненти ІКМ	Опис
1	Вузли	Вузли є кінцевими пунктами мережі, такими як комп'ютери, маршрутизатори, комутатори, сервери, телефони тощо. Вони виконують функції передачі, отримання, обробки і збереження даних.
2	Комунікаційні канали	Канали зв'язку є фізичними шляхами передачі даних в мережі. Вони можуть бути провідними (наприклад, Ethernet-кабелі) або безпровідними (наприклад, Wi-Fi, Bluetooth). Канали забезпечують передачу даних між вузлами.

	Компоненти ІКМ	Опис
3	Протоколи	Інфокомунікаційні мережі використовують протоколи для передачі даних. Протоколи - це набір правил і процедур, які регулюють обмін даними в мережі. Вони визначають формати пакетів даних, методи адресації, контроль помилок, керування потоком і багато іншого. Наприклад, в мережах Інтернет використовуються такі протоколи, як IP (Internet Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol) та інші. Ці протоколи забезпечують стандартизований спосіб передачі, маршрутизації та доставки даних.
5	Мережне обладнання	Це включає комутатори, маршрутизатори, маршрутизатори з віддаленим керуванням (SDN), мережеві пристрої забезпечення безпеки, точки доступу Wi-Fi тощо. Ці пристрої забезпечують передачу даних між різними вузлами мережі.
6	Сервери	Сервери є центральними вузлами, які забезпечують доступ до ресурсів і надають послуги в мережі. Вони можуть бути файловими серверами, веб-серверами, базами даних, електронною поштою тощо
7	Системи управління мережею	Це програмне забезпечення, яке дозволяє керувати та контролювати роботу мережі. Вони включають системи моніторингу, управління пропускною здатністю, керування безпекою мережі, аналіз даних тощо. Ці системи допомагають забезпечити ефективну та надійну роботу мережі. Прикладне програмне забезпечення використовується для виконання конкретних завдань або послуг у мережі. Це можуть бути веб-браузери, електронна пошта, месенджери, соціальні мережі, програми для забезпечення безпеки мережі та інше

Загалом, інфокомунікаційна мережа використовує ці компоненти для забезпечення комунікації, передачі даних та надання послуг користувачам у межах мережі. Кожен з цих компонентів має важливу роль у функціонуванні інфокомунікаційної мережі і взаємодії з іншими компонентами для забезпечення ефективної комунікації і передачі даних.

Однак, кожному з цих компоненів притаманні вразливості, які зловмисники використовують для здійснення кібератак на інфокомунікаційну мережу загалом.

1.2 Основні типи атак на компоненти інфокомунікаційних мереж

Інфокомунікаційні мережі піддаються різноманітним атакам, спрямованим на різні компоненти мережі [12-18]. Основні типи атак на компоненти інфокомунікаційних мереж представлені на рис.1.3.

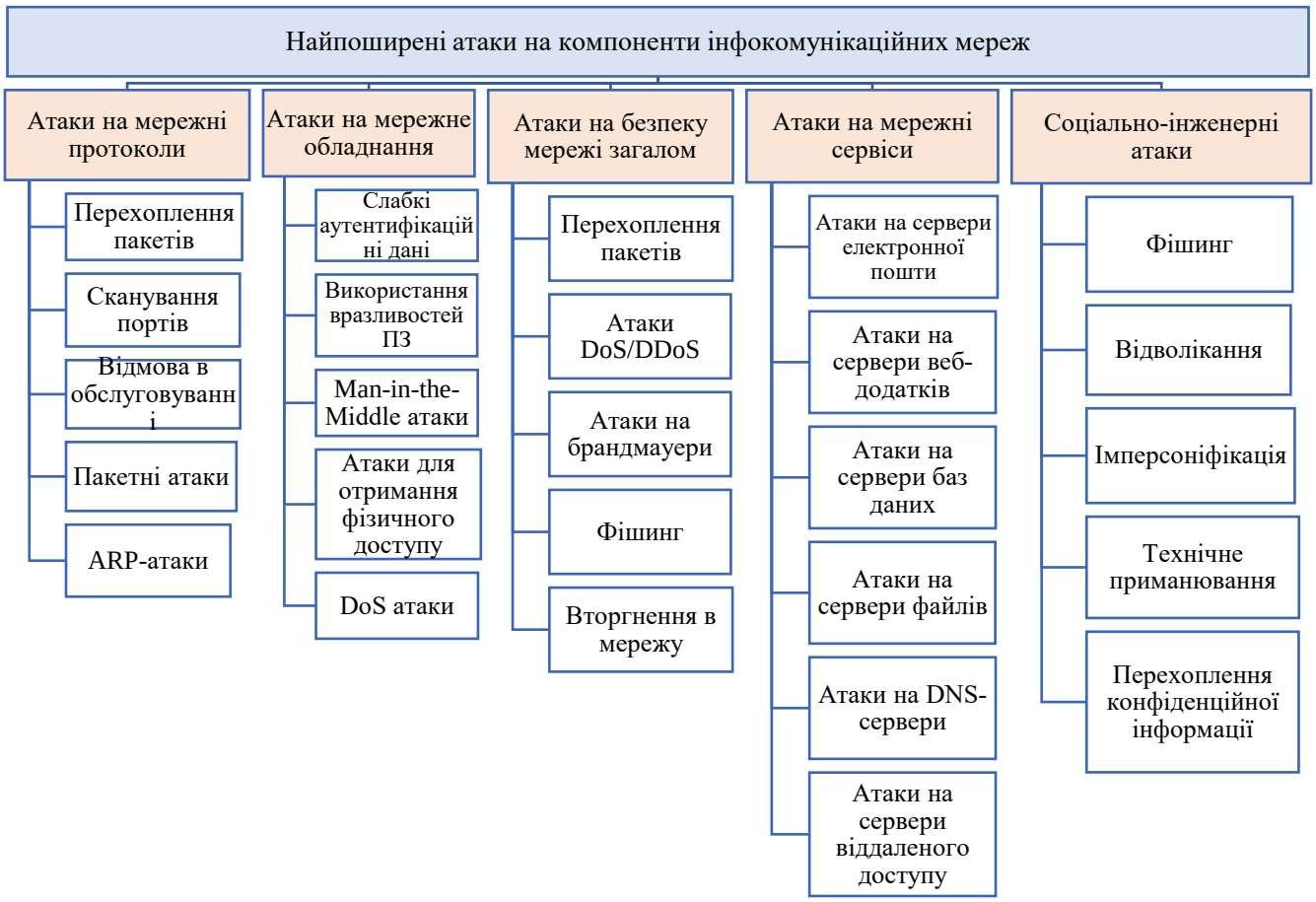


Рисунок 1.3 – Найпоширені атаки на компоненти ІКМ

1) Атаки на мережеві протоколи: Ці атаки спрямовані на вразливості протоколів, використованих у мережі. Наприклад, атаки на протоколи IP, TCP або UDP можуть включати зловживання пакетів, перехоплення трафіку, відмову в обслуговуванні (DoS) або переповнення буфера.

Ось кілька основних типів атак на мережеві протоколи:

- Сканування портів (Port Scanning): Злоумисники використовують сканування портів для виявлення відкритих портів на системі. Це дає їм інформацію про сервіси або програми, які працюють на системі, і може допомогти їм знайти вразливості, які можуть бути використані для подальших атак.
- Перехоплення пакетів (Packet Sniffing): Злоумисники можуть використовувати програми для перехоплення і аналізу мережевого трафіку. Це дозволяє їм отримувати доступ до незашифрованої інформації, яка передається по мережі, такої як паролі, конфіденційна інформація або інші чутливі дані.
- Відмова в обслуговуванні (Denial-of-Service, DoS): Атаки DoS спрямовані на перевантаження ресурсів системи або мережі, щоб вона стала недоступною для законних користувачів. Це може бути досягнуто за допомогою інтенсивної передачі пакетів до системи, спам-атак або використання вразливостей протоколів.
- Пакетні атаки (Packet Manipulation): Це атаки, коли злоумисники змінюють або підробляють пакети, що передаються по мережі. Наприклад, вони можуть змінювати заголовки пакетів, впливаючи на маршрутизацію або вказуючи неправильний джереловказівник. Це може призвести до невірної адресації, перехоплення пакетів або підробки ідентичності.
- ARP-атаки (ARP Spoofing): ARP-атаки спрямовані на зміну таблиці ARP (Address Resolution Protocol) в мережі, щоб зловмисник міг перехоплювати або перенаправляти мережевий трафік. Це може призвести до перехоплення даних або Man-in-the-Middle атак, коли зловмисник отримує доступ до всього мережевого трафіку, який проходить через нього.

2) Атаки на мережеве обладнання: Ці атаки спрямовані на вразливості мережевого обладнання, такі як комутатори, маршрутизатори або мережеві пристрої забезпечення безпеки. Зловмисники можуть спробувати скомпрометувати обладнання, використовуючи вразливості у програмному забезпеченні, виконати атаки типу "Man-in-the-Middle" або використовувати обладнання для розповсюдження шкідливого програмного забезпечення.

Ось кілька типових атак на мережеве обладнання:

- Використання слабких аутентифікаційних даних: Злоумисники можуть намагатися зламати паролі адміністраторів або використовувати за замовчуванням аутентифікаційні дані, які не були змінені після встановлення обладнання. Це дозволяє їм отримати несанкціонований доступ до налаштувань обладнання і його контролю.
- Використання вразливостей програмного забезпечення: Мережеве обладнання, таке як комутатори та маршрутизатори, може мати вразливості у своєму програмному забезпеченні. Злоумисники можуть використовувати ці вразливості для отримання несанкціонованого доступу до обладнання або запуску шкідливого коду.
- Man-in-the-Middle атаки: Злоумисники можуть скомпрометувати мережеве обладнання, щоб перехоплювати та змінювати мережевий трафік. Вони можуть перенаправляти трафік через свої власні сервери або зловживати обладнанням для підробки або впливу на мережевий трафік. Це дозволяє зловмиснику перехопити, змінити або підробити передавані дані та навіть отримати конфіденційну інформацію, таку як паролі чи фінансові дані.
- Атаки для отримання фізичного доступу: Фізичний доступ до мережевого обладнання може дозволити злоумисникам виконати різні види атак. Вони можуть намагатися отримати доступ до портів, встановити шпигунське обладнання або навіть пошкодити апаратне забезпечення обладнання.
- DoS атаки: Злоумисники можуть спробувати перевантажити мережеве обладнання шляхом надсилання великої кількості запитів або пакетів. Це може спричинити відмову в обслуговуванні для легітимного мережевого трафіку і призвести до недоступності мережевого обладнання.

3) Атаки на безпеку мережі: Ці атаки спрямовані на порушення безпеки мережі, такі як злам паролів, перехоплення ідентифікаційних даних, підробка пакетів або зламання шифрування. Це може призвести до несанкціонованого доступу до мережевих ресурсів, витоку конфіденційної інформації або порушення конфіденційності даних.

Таким чином, атаки на безпеку мережі спрямовані на вразливості і слабкі місця в самій мережі. Ось декілька типових атак на безпеку мережі:

- Перехоплення пакетів (Packet Sniffing): Злоумисники можуть використовувати програми для перехоплення мережевого трафіку і отримання

доступу до незашифрованих даних, які передаються по мережі. Це може включати конфіденційну інформацію, таку як паролі, логіни або чутливі дані.

- Атаки DoS/DDoS: Відмова в обслуговуванні (DoS) або розподілена відмова в обслуговуванні (DDoS) атаки спрямовані на перевантаження ресурсів мережі або системи, щоб зробити їх недоступними для легітимних користувачів. Це може бути досягнуто за допомогою інтенсивного надсилання трафіку, засмічення мережевих каналів або використання вразливостей в системі.
- Атаки на брандмауери (Firewall Attacks): Злоумисники можуть спробувати обійти або проникнути через брандмауери, які захищають мережу. Це може включати використання вразливостей брандмауера, отримання несанкціонованого доступу до захищених ресурсів або зміну налаштувань брандмауера.
- Фішинг (Phishing): Фішингові атаки спрямовані на використання соціальної інженерії для отримання конфіденційної інформації, такої як паролі або банківські дані, шляхом введення користувачів в оману. Злоумисники можуть використовувати підроблені електронні листи або веб-сайти, які схожі на офіційні, щоб перехопити особисту інформацію.
- Вторгнення в мережу (Intrusion): Це атаки, коли злоумисники намагаються проникнути в систему або мережу з метою отримання несанкціонованого доступу або виконання шкідливих дій. Це може включати використання вразливостей програмного забезпечення, вторгнення через слабкі місця аутентифікації або використання зловмисних програм.

4) Атаки на мережні сервіси: Багато мереж надають додаткові сервіси, такі як електронна пошта, веб-сервери або бази даних. Ці сервіси також можуть бути піддані атакам, наприклад, включаючи SQL-ін'єкції, хакерські атаки на веб-додатки, DoS атаки на сервери або використання вразливостей у програмному забезпеченні. Таким чином, атаки на мережні сервіси спрямовані на вразливості, що існують у різних мережних сервісах, які надають функціональність та доступ до різних ресурсів в мережі. Ось декілька типових атак на мережні сервіси:

- Атаки на сервери електронної пошти (Email Server Attacks): Злоумисники можуть намагатися зламати сервер електронної пошти, щоб отримати доступ до поштових скриньок, перехоплювати електронні листи або надсилати шкідливі поштові вкладення.

- Атаки на сервери веб-додатків (Web Application Server Attacks): Злоумисники можуть спробувати використати вразливості у веб-додатках, таких як форуми, блоги, електронні магазини тощо, для отримання несанкціонованого доступу до даних користувачів, впровадження шкідливого коду або зміни функціональності додатків.
- Атаки на сервери баз даних (Database Server Attacks): Злоумисники можуть намагатися зламати сервери баз даних, щоб отримати доступ до конфіденційної інформації, видалити або змінити дані або виконати SQL-ін'єкції, що дозволяють виконати шкідливі команди у базі даних.
- Атаки на сервери файлів (File Server Attacks): Злоумисники можуть спробувати зламати сервери файлів, щоб отримати доступ до файлів, які зберігаються на сервері, або виконати шкідливі дії, такі як видалення, модифікація або перенесення файлів.
- Атаки на DNS-сервери (DNS Server Attacks): DNS-сервери відповідають за перетворення доменних імен на IP-адреси. Злоумисники можуть намагатися зламати DNS-сервери, щоб перенаправляти користувачів на фальшиві веб-сайти або перехоплювати їхні дані.
- Атаки на сервери віддаленого доступу (Remote Access Server Attacks): Сервери віддаленого доступу, такі як сервери VPN або сервери термінального доступу, можуть стати об'єктом атак. Злоумисники можуть намагатися зламати сервери віддаленого доступу, щоб отримати несанкціонований доступ до мережі або виконувати шкідливі дії з використанням привілей користувача.

5) Соціально-інженерні атаки: Ці атаки спираються на маніпулювання людьми, щоб отримати доступ до мережі або конфіденційної інформації. Ці атаки використовують психологічні методи і техніки, щоб переконати людей діяти відповідно до бажань зловмисників. Наприклад, фішингові атаки, приховане отримання інформації або соціальна інженерія можуть використовуватися для отримання паролів або інших даних від користувачів.

Ось декілька типових соціально-інженерних атак:

- Фішинг (Phishing): Фішингові атаки включають надсилання підроблених електронних листів або повідомлень, які видаватимуться за легітимні комунікації від організацій, таких як банки, соціальні мережі або інтернет-провайдери. З метою отримання конфіденційних даних, таких як паролі, номери кредитних карток або особиста інформація, злоумисники спонукають людей

перейти на підроблені веб-сайти або відправити свої дані через електронну пошту.

- Відволікання (Diversion): У цьому виді атаки зловмисники спрямовують увагу людей на певні ситуації або події, щоб вони не були уважними до своєї безпеки. Наприклад, зловмисник може створити шумливу відволікучу ситуацію, під час якої вони викрадатимуть конфіденційну інформацію або зламають систему.
- Імперсоніфікація (Impersonation): Це атаки, коли зловмисники видаватимуть себе за інших людей або авторитетних осіб для отримання доступу до конфіденційної інформації або виконання шкідливих дій. Це може включати підроблення імені або ідентифікатора електронної пошти, фальшиве представлення якісь організації або використання соціальних мереж для збору інформації про людей.
- Технічне приманювання (Pretexting): У таких атаках злоумисники створюють фальшиві сценарії або історії, щоб отримати доступ до конфіденційної інформації. Вони можуть представлятися як службовці, технічна підтримка або інші довірені особи, щоб переконати людей розкрити свої паролі, доступ до систем або надати цінну інформацію.
- Перехоплення конфіденційної інформації (Shoulder Surfing): Це атаки, коли зловмисники спостерігають за людьми, коли вони вводять конфіденційну інформацію, таку як паролі або PIN-коди, з метою отримання доступу до систем або ресурсів.

Це лише кілька основних типів атак, які можуть спрямовуватися на компоненти інфокомунікаційних мереж. Забезпечення безпеки мережі включає розробку імплементацію відповідних заходів захисту, таких як використання механізмів аутентифікації, шифрування, брандмауерів, систем виявлення вторгнень, регулярне оновлення програмного забезпечення для усунення вразливостей, а також регулярно аудитувати мережу для виявлення потенційних загроз.

Крім того, для захисту від соціально-інженерних атак важливо проводити навчання співробітників щодо соціопсихологічних впливів зловмисників та використання багаторівневого аутентифікації та інших методів автентифікації для захисту проти витіку конфіденційних даних.

1.3 Основні засоби виявлення вразливостей в інфокомунікаційних мережах

Уразливість у кібербезпеці стосується будь-якої слабкості інформаційної системи, інфокомунікаційної мережі, системних процесів або внутрішнього контролю організації. Загалом вразливості є цілями для кіберзлочинців, завдяки яким змовмисники можуть отримати незаконний доступ до систем і завдати серйозної шкоди конфіденційності даних. Таким чином, уразливості кібербезпеки є надзвичайно важливими для моніторингу для загального стану безпеки, оскільки прогалини в мережі можуть призвести до повномасштабного порушення систем та мереж.

Вразливості не вводяться в систему та мережу, вони там наявні з етапу проектування. Існує небагато випадків кіберзлочинності, які призводять до вразливості. Зазвичай вони є результатом недоліків операційної системи або неправильної конфігурації мережі. А з іншого боку, загрози кібербезпеці впроваджуються в систему, як-от завантаження вірусу або атака соціальної інженерії.

Ризики кібербезпеки напряму пов’язані із вразливостями. Ризики – це ймовірність і вплив використання вразливості. Якщо ці два фактори низькі, то ризик низький. Це прямо пропорційно, і в цьому випадку обернене також вірно; висока ймовірність і вплив вразливостей призводять до високих ризиків. При цьому деякі поширені вразливості не становлять ризику, якщо вразливість не має великої цінності для мережі.

Тож розглянемо методи, які використовуються для виявлення вразливостей. Існує кілька методів виявлення вразливостей в інфокомунікаційних мережах, які включають [23-34]:

1) Активне сканування: Цей метод використовується для сканування мережі з метою виявлення вразливостей. Він передбачає активний запит до вузлів мережі для перевірки доступних портів, сервісів, служб та вразливостей. Такі інструменти, як Nmap, Nessus, OpenVAS, дозволяють здійснити активне сканування мережі.

2) Пасивне сканування: Цей метод полягає у зборі і аналізі даних, що передаються по мережі, без активних дій з боку виявлювача вразливостей. Пасивне сканування може включати моніторинг мережевого трафіку, аналіз

системних журналів, перехоплення пакетів тощо. Цей метод дозволяє виявити аномалії, патерни атак і можливі вразливості, не викликаючи активних дій.

3) Аудит безпеки: Аудит безпеки включає огляд і перевірку безпекових налаштувань, політик безпеки, процедур та систем в мережі. Цей метод допомагає виявити потенційні вразливості, пов'язані з конфігурацією та управлінням системами.

4) Фізична інспекція: Фізична інспекція включає перевірку апаратного забезпечення, кабелів, пристроїв, фізичних з'єднань і простору, в якому розташована мережа. Цей метод допомагає виявити можливі вразливості, пов'язані з фізичним доступом до мережевих ресурсів.

5) Пентестінг (тестування на проникнення): Цей метод включає моделювання атак і спроб переповнення системи для виявлення вразливостей. Пентестінг може включати тестування веб-додатків, використання слабких паролів, перехоплення пакетів, фізичний доступ до системи та інші сценарії атак. Він дозволяє оцінити ефективність заходів безпеки і виявити можливі вразливості, які можуть бути використані зловмисниками.

Ці методи можуть використовуватись окремо або в комбінації для виявлення вразливостей в інфокомунікаційних мережах і покращення їх безпеки.

Таким чином, захист від найпоширеніших атак на інфокомунікаційні мережі має велику важливість на сьогодняшній день. Від захисту ІКМ залежать безперервність роботи мережі, конфіденційність даних і фінансові втрати та порушення довіри користувачів. Крім того, успішно проведені атаки на мережу можуть негативно вплинути на репутацію організації. Компанії, які не забезпечують належний рівень захисту своїх інфокомунікаційних мереж, можуть втратити довіру клієнтів та партнерів. Захист від атак допоможе зберегти репутацію організації і підтримати довіру користувачів. Також слід відзначити, що багато галузей мають вимоги до захисту інформації і дотримання нормативних вимог щодо безпеки. Недотримання цих вимог може мати юридичні наслідки і спричинити штрафи або судові позови. Захист від атак допоможе організації виконувати вимоги безпеки даних та регуляторів.

Важливість захисту від найпоширеніших атак на інфокомунікаційні мережі полягає в забезпеченні неперервності роботи, захисті конфіденційної інформації, запобіганні фінансовим втратам, збереженні репутації та виконанні вимог регуляторів.

Забезпечення безпеки ІКМ та її елементів включає розробку імплементацію відповідних заходів захисту, таких як використання механізмів аутентифікації, шифрування, брандмауерів, систем виявлення вторгнень, систем монуторингу, регулярне оновлення програмного забезпечення для усунення вразливостей, а також регулярно аудитувати мережу для виявлення потенційних загроз.

Для зменшення ризиків щодо успішного проведення різноманітних атак на інфокомунікаційні мережі слід приділяти увагу вчасному виявленню та усуненню вразливостей, як інфокомунікаційної мережі в цілому так і окремих її компонентів. При чому, слід зауважити, що одним з найкритичніших місць ІКМ з точки зору вразливостей є саме мережні компоненти, кожному з яких притаманна певна кількість вразливостей, починаючи з вразливостей їх програмного забезпечення та закінчуючи помилками під час налаштування.

Для подільшого дослідження увагу буде приділено найпоширенішим вразливостям мережних компонентів, вчасне усунення яких дозволить підвищити рівень захисту інфокомунікаційної мережі загалом, а також базам даних мережних вразливостей для виявлення сценаріїв зменшення ризиків їх використання для проведення атак.

2 АНАЛІЗ НАЙПОШИРЕНИХ ВРАЗЛИВОСТЕЙ МЕРЕЖНОГО ОБЛАДНАННЯ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

2.1 Класифікація найпоширених вразливостей мережного обладнання в інфокомунікаційних мережах

Вразливості мережного обладнання можуть бути використані зловмисниками для здійснення атак, таких як вторгнення, перехоплення даних, знищення або перекручування інформації. Саме тому, усунення вразливостей в ІКМ важливо, бо допомагає запобігти таким атакам і забезпечити безпеку мережі та даних. Загалом усунення вразливостей мережного обладнання дозволяє забезпечити захист наступних категорій (рис.2.1).

Рисунок 2.1 – Результати усунення вразливостей мережних елементів

1. Захист конфіденційності. Вразливості мережного обладнання можуть призвести до витоку конфіденційної інформації, такої як паролі, корпоративні дані або особисті дані користувачів. Усунення вразливостей допомагає запобігти незаконному доступу до цієї інформації та зберегти конфіденційність даних.

2. Збереження цілісності даних. Вразливості мережного обладнання можуть призвести до зміни або пошкодження даних, що передаються через мережу. Усунення вразливостей допомагає забезпечити цілісність даних і запобігти їх випадковим або навмисним змінам.

3. Забезпечення неперервності роботи. Вразливості мережного обладнання можуть призвести до перерв у роботі мережі, відмови в обслуговуванні або втрати доступності послуг. Усунення вразливостей допомагає забезпечити неперервну роботу мережі та зменшити час простою.

4. Виконання регуляторних вимог. У багатьох галузях, таких як фінансова, медична або громадська сфера, існують регуляторні вимоги щодо захисту мережного обладнання та даних. Усунення вразливостей допомагає організаціям виконувати ці вимоги і уникнути юридичних наслідків.

Отже, усунення вразливостей мережного обладнання має важливість для забезпечення безпеки, надійності та виконання вимог регуляторів у сфері інформаційної безпеки.

Таким чином, для підвищення захисту ІКМ в цілому, дослідження засобів зменшення ризиків інформаційної безпеки та відповідно кількості успішно проведених атак, розглянемо найпоширеніші категорії вразливостей мережного обладнання, які представлені в таблиці 2.1.

Таблиця 2.1 – Найпоширеніші категорії вразливостей мережного обладнання

	Тип вразливості	Опис
1	Вразливості програмного забезпечення	Мережне обладнання, таке як маршрутизатори, комутатори, файрволи та бездротові точки доступу, може мати вразливості в своєму програмному забезпеченні. Ці вразливості можуть дозволити зловмисникам здійснити атаки на обладнання, перехоплювати дані або навіть отримати несанкціонований доступ до мережі.
2	Застаріле програмне забезпечення	Відсутність оновлень та патчів для мережного обладнання може призвести до вразливостей, оскільки зловмисники можуть використовувати відомі уразливості, для

		здійснення атак
3	Слабкі аутентифікаційні механізми	Використання слабких або простих паролів, недостатня захист аутентифікаційних механізмів, використання зашкварних або зламаних приватних ключів може дозволити зловмисникам отримати несанкціонований доступ до обладнання.
4	Недостатні заходи безпеки	Неправильна конфігурація обладнання або відсутність використання захисних механізмів, таких як брандмауери, системи виявлення вторгнень, можуть залишити обладнання вразливим до атак.
5	Фізичний доступ	Здобуття фізичного доступу до мережного обладнання може дозволити зловмисникам здійснювати різні атаки, встановлювати шпигунське програмне забезпечення, модифікувати настройки або навіть крадіжку обладнання.

Для захисту від цих вразливостей, рекомендується використовувати оновлене програмне забезпечення, слідкувати за випуском патчів і оновлень від виробників обладнання, використовувати сильні аутентифікаційні механізми, встановлювати захисні механізми (брандмауери, системи виявлення вторгнень) та забезпечувати фізичну безпеку обладнання.

2.2 Огляд баз даних класифікації вразливостей мережного обладнання в інфокомунікаційних мережах

Для огляду та аналізу сценаріїв використання типових вразливостей мережного обладнання в інфокомунікаційних мережах використовують декілька баз даних та агрегаційних систем [12-24], класифікація яких представлено на рис.2.2.

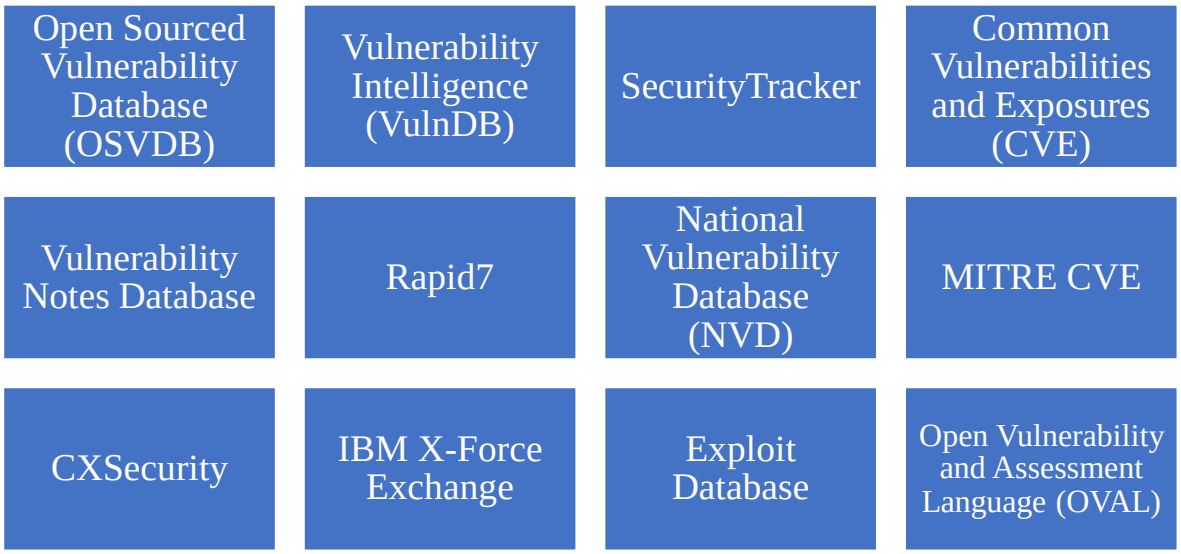


Рисунок 2.2 – Класифікація баз даних уразливостей мережного обладнання

Найпоширеними базами даних вразливостей є National Vulnerability Database (NVD) та Common Vulnerabilities and Exposures (CVE) [12-21]. Розглянемо їх більш детально.

National Vulnerability Database (NVD) [12] є великою базою даних, що містить інформацію про відомі вразливості програмного забезпечення. Вона підтримується Національним інститутом стандартів та технологій (National Institute of Standards and Technology, NIST) у Сполучених Штатах.

NVD збирає, аналізує та надає інформацію про вразливості з різних джерел, включаючи виробників програмного забезпечення, дослідників безпеки, об'єднання інформації про вразливості та інші джерела. Вона використовує стандартизований формат, відомий як Common Vulnerability Enumeration (CVE), для ідентифікації та опису вразливостей.

NVD надає різну інформацію про вразливості, включаючи опис вразливості, її вплив на систему, посилання на додаткові деталі та рекомендації щодо усунення вразливості.

Принцип додавання, аналізу та опису вразливостей за допомогою NVD представлено на рис. 2.3.

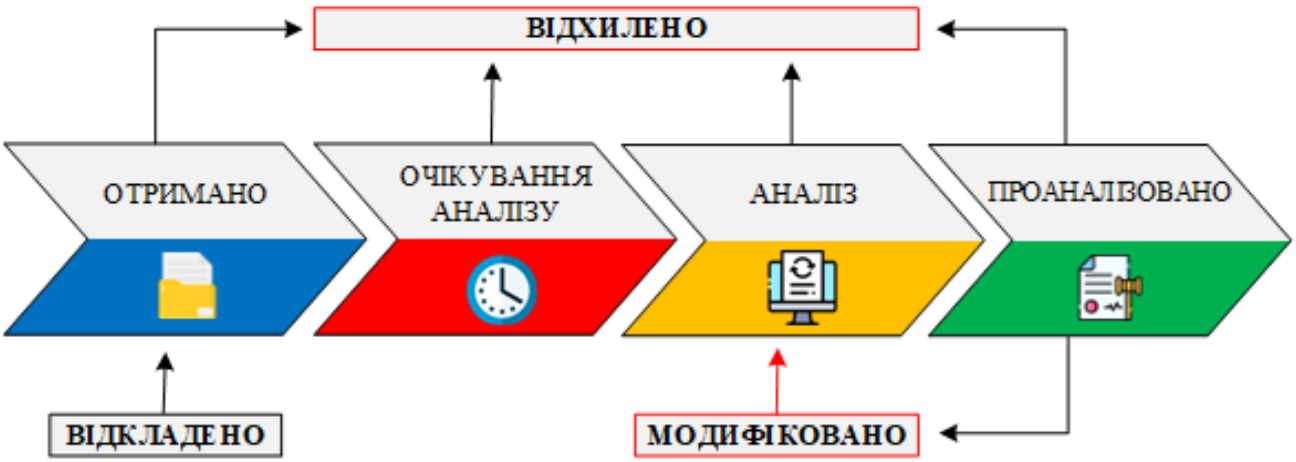


Рисунок 2.3 – Діаграма робочого процесу стану NVD

Common Vulnerabilities and Exposures (CVE) є словником вразливостей, що надає стандартизовані ідентифікатори для вразливостей в програмному забезпеченні [21]. CVE є загальноприйнятим стандартом у галузі безпеки і дозволяє виробникам, дослідникам безпеки та іншим зацікавленим сторонам спільно посилатися на конкретну вразливість.

База даних CVE містить інформацію про вразливості, такі як опис, класифікація, вплив на систему, посилання на детальну інформацію та рекомендації щодо усунення вразливості. Кожна вразливість має унікальний ідентифікатор CVE, що дозволяє однозначно ідентифікувати конкретну вразливість незалежно від мови або системи класифікації.

CVE не надає детального опису самої вразливості або експлоітів, але надає стандартизований ідентифікатор, що дозволяє виробникам, дослідникам та користувачам швидко знайти більш докладну інформацію про вразливість у відповідних джерелах, таких як NVD або веб-сайти виробників.

CVE також використовується для посилання на вразливості в інших базах даних, таких як база даних NVD, що забезпечує зв'язок між стандартизованими ідентифікаторами CVE та конкретними вразливостями.

Використання стандартизованих ідентифікаторів CVE сприяє удосконаленню обміну інформацією про вразливості між різними організаціями та полегшує відслідковування та аналіз вразливостей в програмному забезпеченні та мережному обладнанні.

CVE ID складається з трьох частин (рис.2.4). Префікс однаковий для кожного ідентифікатора, тому кожен ідентифікатор CVE починається з «CVE». Далі йде чотиризначний рік. Тут вказано не рік відкриття, а рік публічного оприлюднення вразливості. У результаті вразливість, виявлена в грудні 2018 року,

але оприлюднена лише в січні 2019 року, буде позначена як 2019. Послідовна нумерація ідентифікатора CVE складається з чотирьох, п’яти або семи цифр [12].

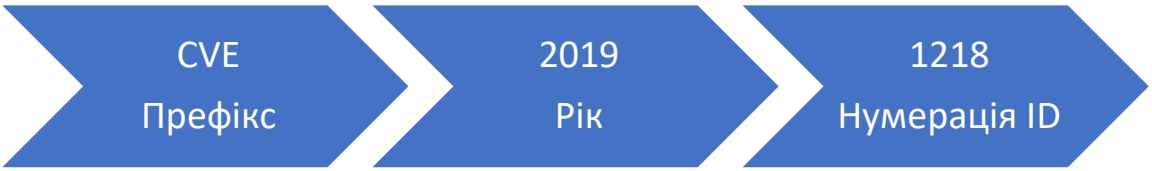


Рисунок 2.4 – Структура ідентифікаторів CVE

Ідентифікатори CVE можуть створюватися лише ліцензованими компаніями, які працюють у рамках програми CVE. Ліцензії видаються корпорацією MITRE. Ці компанії називаються органами нумерації CVE (CNA) і мають право призначати ідентифікатори CVE вразливостям у межах узгодженого обсягу. Під час процесу створення CNA генерують запис CVE з інформацією, відомою на той момент, і передають її до MITRE, що публікує цей запис у каналах CVE.

Рисунок 2.5 – Діаграма робочого процесу додавання вразливостей до CVE

Однією з сильних сторін стандарту CVE є його широке використання та підтримка в сучасних програмних продуктах і сервісах, спрямованих на забезпечення інформаційної безпеки. Це дозволяє організаціям, розробникам програмного забезпечення та дослідникам з безпеки легко ідентифікувати та посилатися на конкретні вразливості.

Деякі сучасні програмні продукти і сервіси, які спрямовані на забезпечення безпеки, використовують базу даних CVE для інтеграції інформації про вразливості. Наприклад, системи виявлення вторгнень, системи управління вразливостями, брандмауери та інші інструменти можуть підтримувати

використання стандартизованих ідентифікаторів CVE для ідентифікації та відстеження вразливостей.

Така підтримка дозволяє забезпечувати більшу прозорість інформації про вразливості, полегшує обмін даними між різними інструментами та системами, а також допомагає забезпечувати швидку реакцію на виявлені вразливості шляхом широкого використання стандартизованого ідентифікатора CVE.

Все вищезазначене робить стандарт CVE цінним інструментом у сфері інформаційної безпеки, сприяючи покращенню виявлення, відстеження та виправлення вразливостей в програмному забезпеченні та мережному обладнанні.

2.3 Метрики оцінки вразливостей за допомогою CVSS в інфокомунікаційних мережах

Для оцінки критичності вразливості використовується CVSS (Common Vulnerability Scoring System) [12]. CVSS – це стандарт для оцінки характеристик і впливу вразливостей, що призначений для надання об'єктивної і однозначної оцінки рівня серйозності вразливостей в програмному забезпеченні.

CVSS використовує числовий рейтингову шкалу від 0 до 10 для визначення критичності вразливості. Кожна вразливість оцінюється за допомогою трьох основних характеристик:

1. Базова оцінка (Base Score), що враховує потенційний вплив вразливості і визначає загальну складність її використання. При визначенні Базової оцінки враховуються такі фактори, як вплив на конфіденційність, цілісність та доступність.

2. Темпоральна оцінка (Temporal Score), що враховує фактори, які можуть змінити рейтинг вразливості в разі з'явлення про неї нових відомостей. Це включає інформацію про доступність вразливості, рівень відомостей, доступних для використання вразливості та рекомендації з її використання.

3. Оцінка навколишнього інфокомунікаційного середовища (Environmental Score), що раховує специфічні умови IT та мережного середовища, в якому застосовується вразливість. Наприклад, вплив вразливості може бути різним в залежності від типу системи, даних, доступу і т.д.

Таким чином, CVSS надає числову оцінку кожній характеристиці, а також загальний числовий рейтинг вразливості. Цей рейтинг допомагає організаціям

приймати рішення про пріоритети усунення вразливостей, встановлення заходів безпеки і реагування на нові загрози. Тож CVSS є важливим інструментом у галузі оцінки ризиків і планування заходів безпеки, оскільки він дозволяє стандартизувати оцінку вразливостей та допомагає фахівцям з безпеки приймати обгрунтовані рішення на основі об'єктивних даних.

2.4 Аналіз метрик критичностей вразливостей CVSS мережного обладнання

Для збору та аналізу метрик критичностей вразливостей CVSS мережного обладнання використовувалися вразливості, що притаманні більшості мережного обладнання згідно бази даних CVE та NVD [12-23]. Перелік Топ-10 вразливостей за 2022-2023 роки включає:

1. ID вразливості: CVE-2023-20035.

Базова оцінка – 7,8.

Рівень критичності – високий.

Опис: Вразливість у CLI програмного забезпечення Cisco IOS XE SD-WAN може дозволити автентифікованому локальному зловмиснику виконувати довільні команди з підвищеними привілеями. Ця вразливість пов’язана з недостатньою перевіркою вхідних даних системним CLI. Зловмисник із правами на виконання команд може використати цю вразливість, спочатку пройшовши автентифікацію на ураженому пристрої за допомогою або локального термінального доступу, або інтерфейсу оболонки керування, а потім надіслав створений вхід до системного CLI. Успішний експлойт може дозволити зловмиснику виконувати команди в базовій операційній системі з привілеями кореневого рівня. Зловмисник з обмеженими правами користувача може використати цю вразливість, щоб отримати повний контроль над системою.

2. ID вразливості: CVE-2023-20065.

Базова оцінка – 7,8.

Рівень критичності – високий.

Опис: Вразливість у підсистемі розміщення додатків Cisco IOx програмного забезпечення Cisco IOS XE може дозволити автентифікованому локальному зловмиснику підвищити привілеї для root-прав на ураженому пристрої. Ця вразливість пов’язана з недостатніми обмеженнями для розміщеної програми. Зловмисник може використати цю вразливість, увійшовши до контейнера

додатків Cisco IOx і вийшовши з нього. Успішний експлойт може дозволити зловмиснику виконувати довільні команди в базовій операційній системі з привілеями root.

3. ID вразливості: CVE-2023-20073.

Базова оцінка – 9,8.

Рівень критичності – високий.

Опис: Вразливість у веб-інтерфейсі керування гігабітними VPN-маршрутизаторами Cisco RV340, RV340W, RV345 та RV345P Dual WAN може дозволити неавтентифікованому віддаленому зловмиснику завантажувати довільні файли на уражений пристрій. Ця вразливість пов’язана з недостатніми механізмами примусової авторизації в контексті завантаження файлів. Зловмисник може використати цю вразливість, надіславши створений HTTP-запит на уражений пристрій. Успішний експлойт може дозволити зловмиснику завантажувати довільні файли на уражений пристрій.

4. ID вразливості: CVE-2022-22211.

Базова оцінка – 7,5.

Рівень критичності – високий.

Опис: Уразливість необмеженого розподілу ресурсів у ресурсах FPC Juniper Networks Junos OS Evolved на серії PTX дозволяє непривілейованому зловмиснику викликати відмову в обслуговуванні (DoS). Постійне опитування SNMP jnxCosQstatTable призводить до того, що в FPC закінчується простір GUID, що спричиняє відмову в обслуговуванні для ресурсів FPC

5. ID вразливості: CVE-2023-23110.

Базова оцінка – 7,5.

Рівень критичності – високий.

Опис: У певних продуктах Netgear було виявлено вразливість модифікації вбудованого програмного забезпечення. Цілісність даних завантаженого образу мікропрограми забезпечується фіксованою контрольною сумою. Таким чином, зловмисник може провести атаку MITM, щоб змінити завантажений користувачем образ прошивки та обійти перевірку контрольної суми. Це впливає на бездротові маршрутизатори WNR612v2 1.0.0.3 і раніші, DGN1000v3 модемний маршрутизатор 1.0.0.22 і раніші, D6100 WiFi DSL модемні маршрутизатори 1.0.0.63 і раніші, бездротові маршрутизатори WNR1000v2 1.1.2.60 і раніші, XAVN2001v2 Wireless-N Extenders 0.4.0. 7 і раніше , бездротові маршрутизатори

WNR2200 1.0.1.102 і раніші, бездротові маршрутизатори WNR2500 1.0.0.34, R8900 Smart WiFi Routers 1.0.3.6 та R9000 Smart WiFi Routers 1.0.3.6.

6. ID вразливості: CVE-2022-27643.

Базова оцінка – 8,8.

Рівень критичності – високий.

Опис: Ця вразливість дозволяє зловмисникам, які знаходяться в мережі, виконувати довільний код на уражених інсталяціях маршрутизаторів NETGEAR R6700v3 1.0.4.120_10.0.91. Для використання цієї вразливості не потрібна автентифікація. Конкретний недолік існує в обробці запитів SOAP. Під час аналізу заголовка SOAPAction процес не перевіряє належним чином довжину наданих користувачем даних перед копіюванням їх у буфер. Зловмисник може використати цю вразливість для виконання коду в контексті root.

7. ID вразливості: CVE-2022-20697.

Базова оцінка – 6,8.

Рівень критичності – середній.

Опис: Уразливість в інтерфейсі веб-служб програмного забезпечення Cisco IOS і програмного забезпечення Cisco IOS XE може дозволити автентифікованому віддаленому зловмиснику викликати стан відмови в обслуговуванні (DoS). Ця вразливість пов’язана з неправильним керуванням ресурсами в коді сервера HTTP. Зловмисник може використати цю вразливість, надіславши велику кількість HTTP-запитів на уражений пристрій. Успішний експлойт може дозволити зловмиснику спричинити перезавантаження пристрою, що призведе до стану DoS.

8. ID вразливості: CVE-2023-28970.

Базова оцінка – 6,5.

Рівень критичності – середній.

Опис: Неправильна перевірка під час обробки пакетів на мережевих інтерфейсах Juniper Networks Junos OS на пристроях JRR200 дозволяє зловмиснику з сусідньої мережі надсилати певний пакет на пристрій, щоб викликати збій ядра, що призводить до відмов в обслуговуванні (DoS). Постійне отримання та обробка цього пакету призведе до тривалої відмови в обслуговуванні (DoS). Цю проблему може спровокувати лише зловмисник у локальному широкомовному домені. Пакети, спрямовані на пристрій, не можуть викликати цей збій.

9. ID вразливості: CVE-2023-20081.

Базова оцінка – 5,9.

Рівень критичності – середній.

Опис: Уразливість у клієнтському модулі IPv6 DHCP (DHCPv6) програмного забезпечення Cisco Adaptive Security Appliance (ASA), програмного забезпечення Cisco Firepower Threat Defense (FTD), програмного забезпечення Cisco IOS і програмного забезпечення Cisco IOS XE може дозволити неавтентифікованому віддаленому зловмиснику викликати відмову стан обслуговування (DoS) на ураженому пристрої. Ця вразливість пов’язана з недостатньою перевіркою повідомлень DHCPv6. Зловмисник може використати цю вразливість, надсилаючи створені повідомлення DHCPv6 на уражений пристрій. Успішний експлойт може дозволити зловмиснику спричинити перезавантаження пристрою, що призведе до стану DoS.

10.ID вразливості: CVE-2023-28961.

Базова оцінка – 5,3.

Рівень критичності – середній.

Опис: Уразливість неправильної обробки неочікуваного типу даних у обробці фільтра брандмауера IPv6 в Juniper Networks Junos OS на пристроях серії ACX перешкоджає належному встановленню фільтра брандмауера з терміном «from next-header ah» у системі пересилання пакетів (PFE). . Немає миттєвих ознак незавершеного фільтру брандмауера, показаного в CLI, який міг би дозволити зловмиснику надіслати дійсні пакети на або через пристрій, які явно призначені для скидання.

Таким чином, проаналізувавши представлені вразливості, можна зробити висновок, що всі найкритичніші вразливості пов’язані із програмним забезпеченням мережних пристроїв. Використання даних вразливостей зловмисником в більшості випадках можуть призвети до відмови в обслуговування як окремого сегменту мережі, так і ІКМ в цілому.

Виявлення даних вразливостей та їх мінімізація можлива на етапах проектування ІКМ під час вибору мережного обладнання, а також на етапах функціонування мережі за допомогою моніторинга патчів та вчасного оновлення програмного забезпечення мережного обладнання.

Загалом для мінімізації вразливостей мережного обладнання можуть використовуватися різні алгоритми і методи. Основні етапи такого алгоритму включають:

1. Збір інформації. Збирання відомостей про мережеві компоненти, включаючи системи, пристрої, програмне забезпечення і сервіси. Це може включати сканування портів, отримання інформації про конфігурацію, версії програмного забезпечення тощо.

2. Аналіз вразливостей. Аналіз отриманої інформації для виявлення вразливостей, які можуть бути присутніми в системах і компонентах мережі. Це може включати порівняння версій програмного забезпечення з базами даних вразливостей, перевірку конфігураційних проблем і т.д.

3. Тестування на експлуатацію. Випробування вразливостей на можливість експлуатації шляхом проведення атак або тестування на проникнення. Це може включати спроби використання вразливостей для отримання несанкціонованого доступу або проведення інших шкідливих дій.

4. Реєстрація та звітність. Документування виявлених вразливостей, їх характеристик, можливого впливу і рекомендацій щодо усунення. Це допомагає організації вжити відповідних заходів безпеки та попередити можливі атаки.

Представлені етапи можуть бути реалізовані як автоматизовані системи, програмні засоби або виконуватися вручну спеціалістами з безпеки мережі. Використання спеціалізованих інструментів, таких як системи виявлення вторгнень (Intrusion Detection Systems) або сканери вразливостей (Vulnerability Scanners), може спростити і поліпшити процес обнаруження уязвимостей, але усунути всі вразливості нажаль неможливо.

Слід зауважити, що використання приведених в першому розділі методів виявлення вразливостей дозволяє проаналізувати, оцінити ризики інформаційної безпеки та розробити план усунення знайдених вразливостей. Але постає проблема в тому, що не всі вразливості можна усунути по причині відсутності оновленого програмного забезпечення, відповідних патчів тощо.

Саме тому, однією з головних задач для підвищення рівня захисту ІКМ є не тільки вчасне виявлення та усунення вразливостей, але й мінімізація ризиків під час їх можливого використання.

Для цього існує декілька підходів, одним з яких є використання маршрутних рішень, які дозволяють зменшувати та балансувати навантаження на

мережне обладнання, яке має неусунуті вразливості з викосим рівнем критичності.

Таким чином, в третьому розділі даної роботи буде розглядатись метод щодо мінімізації ризиків від використання вразливостей в ІКМ в цілому та забезпеченням показників якості обслуговування, що на теперішній час є також головною вимогою до сучасних інфокомунікаційних мереж.

3 ДОСЛІДЖЕННЯ МЕТОДУ ЩОДО МІНІМІЗАЦІЇ ВПЛИВУ ВРАЗЛИВОСТЕЙ МЕРЕЖНОГО ОБЛАДНАННЯ ЗА ДОПОМОГОЮ МОДЕЛЕЙ БЕЗПЕЧНОЇ QOS-МАРШРУТИЗАЦІЇ

3.1 Вплив показників безпеки та якості обслуговування на прийняття маршрутних рішень

Пропускна здатність каналів зв’язку ІКМ і показники мережної безпеки є важливими факторами, які можуть суттєво впливати на рішення щодо маршрутизації. Так, пропускна здатність мережі стосується доступної смуги пропускання та мережних ресурсів. Отже, маршрутні рішення мають враховувати пропускну здатність каналів зв’язку та шляхів (маршрутів) у мережі для забезпечення ефективної передачі даних [25-37].

Відомо, що протоколи маршрутизації (наприклад, OSPF, EIGRP тощо) часто враховують доступну пропускну здатність каналів зв’язку ІКМ під час прийняття рішень щодо формування маршрутів. Вони можуть віддавати перевагу шляхам з більшою пропускною здатністю, щоб забезпечити швидшу передачу даних і уникнути перевантажень.

У разі застосування багатошляхової стратегії маршрутизації в ІКМ, де між відправником та отримувачем формується мультишлях, рішення щодо маршрутизації можуть залежати від пропускної здатності для збалансованого розподілу трафіку за окремими шляхами мультишляху. Отже, враховуючи пропускну здатність різних шляхів, маршрутизатори можуть збалансувати навантаження в мережі та запобігти перевантаженню будь-якого окремого шляху.

Крім того, у сценаріях, коли певні програми або типи трафіку вимагають гарантій якості обслуговування, маршрутні рішення також можуть залежати від пропускної здатності мережі. Шляхи з достатньою пропускною здатністю для задоволення вимог QoS, наприклад, низька затримка або висока пропускна здатність, можуть бути кращими за інших.

Однак зазначимо, що міркування безпеки відіграють вирішальну роль у рішеннях щодо маршрутизації, щоб забезпечити конфіденційність, цілісність і доступність даних, що передаються в ІКМ.

Протоколи маршрутизації можуть визначати пріоритетність безпечних шляхів під час прийняття рішень щодо маршрутизації. Наприклад, якщо доступно декілька шляхів, протокол маршрутизації може віддавати перевагу зашифрованим шляхам або проходити через довірені та безпечні сегменти мережі.

Рішення щодо маршрутизації, орієнтовані на підвищення мережної безпеки, можна приймати на основі систем виявлення та запобігання вторгненням (IDS/IPS). Маршрутизатори можуть таким чином приймати рішення щодо маршрутизації з метою уникнення відомих шкідливих джерел або потенційних векторів атак.

На маршрутні рішення можуть впливати політики безпеки, які забезпечують сегментацію мережі та контроль доступу. Маршрутизатори можуть спрямовувати трафік за певними шляхами, щоб запобігти несанкціонованому доступу до чутливих сегментів мережі. Крім того, важливим напрямком підвищення мережної безпеки є безпечна маршрутизація шляхами, обраними відповідно до критичності вразливостей вузлів (мережних пристроїв) та інцидентних до них каналів зв’язку.

Таким чином, пропускна здатність мережі впливає на рішення щодо маршрутизації, враховуючи доступну пропускну здатність, балансування навантаження та вимоги до якості обслуговування. Зі свого боку безпека впливає на прийняття маршрутних рішень, визначаючи пріоритетність безпечних шляхів, розглядаючи системи виявлення/запобігання вторгненням, впроваджуючи політику сегментації мережі, контролю доступу та оцінку критичності вразливостей елементів мережі. Отже, пропускна здатність і рівень мережної безпеки відіграють важливу роль в оптимізації продуктивності та безпеки в ІКМ.

3.2 Математичні моделі безпечної маршрутизації в інфокомунікаційній мережі

Розглянемо існуючі моделі безпечної маршрутизації в ІКМ [7, 25], що можуть бути використані для порівняння впливу на маршрутні рішення показників критичності вразливості мережного обладнання та продуктивності каналів зв’язку.

У межах дослідження буде використано дві відомі раніше моделі безпечної маршрутизації, запропоновані у роботі [7].

В обох моделях будуть використовуватися такі характеристики:

– $G = (R,\ E)$ – структура мережі представлена графом;

– $R = \left\{ R_i;\ \ i = \overline{1,m} \right\}$ – маршрутизатори як множина вершин;

– $E = \left\{ E_{i,j};\ \ i,j = \overline{1,m},\ \ i \neq j \right\}$ – канали зв'язку як множина дуг;

– $\varphi_{i,j}$ – кожен канал $E_{i,j} \in E$ має відповідну пропускну здатність у пакетах за секунду (пак/с).

Нехай в мережі передається К потоків пакетів між відповідними парами вузлів відправників s_k та отримувачів d_k для окремого k-го потоку, для якого також маємо його середню інтенсивність λ^k (пак/с).

Отже необхідно визначти маршрутні змінні $x_{i,j}^k$, що характеризують долю k-го потоку в каналі зв'язку $E_{i,j} \in E$. Відповідно до багатошляхової стратегії маршрутизації на них накладаються наступні умови [7, 25-37]:

$$0 \le x_{i,j}^k \le 1. \tag{3.1}$$

Використання умови (3.1) підтримує багатошляхову маршрутизацію, проте не забороняє одночасне використання й одношляхової. Множина застосованих шляхів надалі називається мультишляхом.

Крім того, під час розрахунку маршрутних змінних мають виконуватися умови збереження потоку на всіх вузлах мережі [1]:

$$\begin{cases} \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = 1,\ \ k \in K,\ \ R_i = s_k; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = 0\ ,\ \ k \in K,\ \ R_i \neq s_k, d_k; \\ \sum\limits_{j:E_{i,j} \in E} x_{i,j}^k - \sum\limits_{j:E_{j,i} \in E} x_{j,i}^k = -1,\ \ k \in K,\ \ R_i = d_k. \end{cases} \tag{3.2}$$

Задоволення умов (3.2) гарантує відсутність втрат пакетів на кожному маршрутизаторі, а також забезпечує зв'язність маршрутів між відправником та

отримувачем пакетів k-го потоку. Далі з метою запобігання перевантаження каналів потрібно виконати такі умов за кількістю каналів зв’язку в мережі [1]:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \le \varphi_{i,j},\ E_{i,j} \in E. \tag{3.3}$$

Далі визначаємо моделі для дослідження. Обидві моделі представлятимуть собою оптимізаційні моделі безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей. Вони базуватимуться на класичних умовах (3.1) – (3.3), але відрізнятимуться критеріями оптимальності.

Відповідно до результатів, отриманих в роботі [1], оптимальний маршрут має розраховуватися на сонові базових метрик критичності вразливостей і пропускної здатності каналів зв’язку, що містяться в маршруті.

Таким чином, виникає потреба у використанні комбінованої маршрутної метрики $f_{i,j}^{комб} = f_{i,j}^{OSPF} + f_{i,j}^{SEC}$, що відповідає за продуктивність та безпеку розраховуваного мультишляху:

$$f_{i,j}^{OSPF} = \frac{10^8}{\varphi_{i,j}}. \tag{3.4}$$

Відповідно компонент метрики, заснований на параметрі мережної безпеки – базових метриках критичності вразливостей каналів зв’язку обчислюється таким чином:

$$f_{i,j}^{SEC} = \frac{10^8}{R} w_{i,j}, \tag{3.5}$$

де $w_{i,j}$ у даній роботі визначатиметься відповідно до імовірностей використання вразливостей на маршрутизаторах.

Як це показано в [7], R – це співвідношення між ваговими коефіцієнтами метрик продуктивності та мережної безпеки:

$$R = \frac{w^{OSPF}}{w^{SEC}},\ w^{SEC} = \frac{w^{OSPF}}{R} = \frac{10^8}{R}. \quad (3.6)$$

Отже, в моделі 1 для реалізації балансування навантаження під час безпечної QoS-маршрутизації застосовуватиметься квадратичний критерій оптимальності [7]:

$$J_1 = \min_x \sum_{k \in K} \sum_{E_{i,j} \in E} \left(f_{i,j}^{OSPF} + f_{i,j}^{SEC} \right) \cdot x_{i,j}^2. \quad (3.7)$$

Ця модель буде порівнюватися з моделлю 2, яка також базуватиметься на умовах (3.1) – (3.6), але з лінійним критерієм:

$$J_2 = \min_x \sum_{k \in K} \sum_{E_{i,j} \in E} \left(f_{i,j}^{OSPF} + f_{i,j}^{SEC} \right) \cdot x_{i,j}. \quad (3.8)$$

3.3 Дослідження та аналіз потокових моделей безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей

Розглянемо структуру транспортної мережі AzerTelecom, показану на рис. 3.1 [37]. Структура цієї мережі ґрунтується на кількох кільцях, об’єднаних в єдину систему, які централізовано керуються мережним операційним центром, контролюючим весь трафік.

Далі аналізучи особливості топологічної структури мережі AzerTelecom, виберемо для наступних числових досліджень спрощену узагальнену структуру фрагменту мережі для проведення відповідних розрахунків (рис. 3.2).

Рисунок 3.1 – Транспортна мережа AzerTelecom

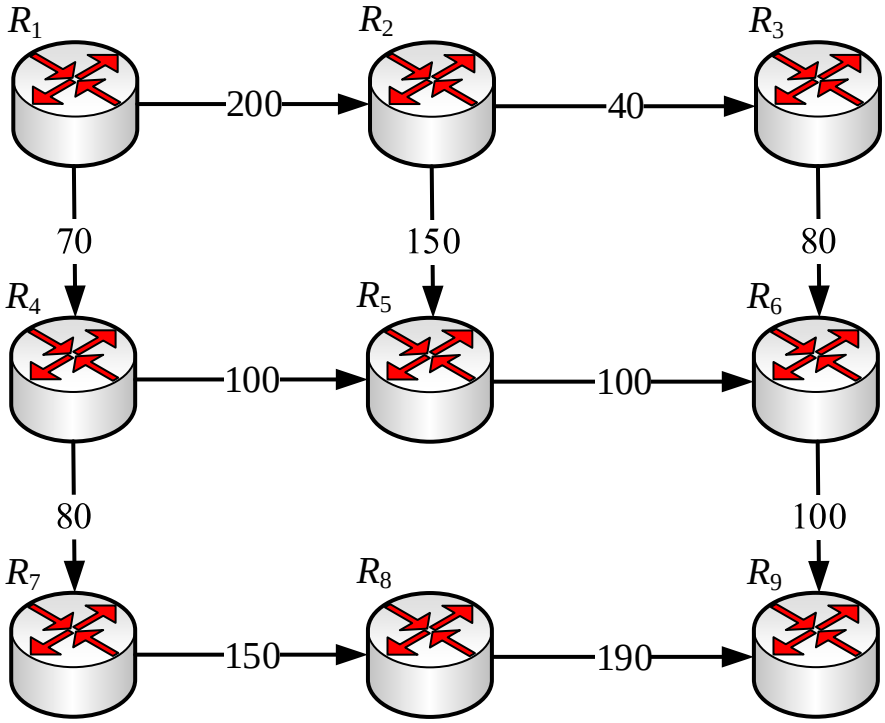


Рисунок 3.2 – Досліджуваний фрагмент ІКМ

Далі буде проведено дослідження та порівняльний аналіз розглянутих моделей, а також перевірено працездатність, адекватність та ефективність потокових моделі безпечної QoS-маршрутизації за допомогою розрахункових прикладів.

Таким чином, обрана структура ІКМ, зображена на рис. 3.2, містить дев’ять вузлів (маршрутизаторів) та одинадцять каналів зв’язку. Під час дослідження генерувався лише один потік потоків, тобто k = 1. Вузлами відправником пакетів є маршрутизатор R_1, а отримувачем – маршрутизатор R_9. У розривах каналів зв’язку (рис. 3.2) показана їхня пропускна здатність (пак/с).

Відповідно до вихідної структури вектор маршрутних змінних $\vec{x}$, що потрібно розрахувати, та вектор комбінованих метрик у межах моделей 1 і 2 мають вигляд:

$$\vec{x} = \begin{bmatrix} x_{1,2} \\ x_{2,3} \\ x_{1,4} \\ x_{2,5} \\ x_{3,6} \\ x_{4,5} \\ x_{5,6} \\ x_{4,7} \\ x_{6,9} \\ x_{7,8} \\ x_{8,9} \end{bmatrix}, \quad \vec{f}^{\,комб} = \begin{bmatrix} f_{1,2}^{комб} \\ f_{2,3}^{комб} \\ f_{1,4}^{комб} \\ f_{2,5}^{комб} \\ f_{3,6}^{комб} \\ f_{4,5}^{комб} \\ f_{5,6}^{комб} \\ f_{4,7}^{комб} \\ f_{6,9}^{комб} \\ f_{7,8}^{комб} \\ f_{8,9}^{комб} \end{bmatrix}.$$

Зі свого боку умови збереження потоку (3.2) для структури ІКМ (рис. 3.2) наступні:

$$\begin{cases} x_{1,2} + x_{1,4} = 1; \\ -x_{1,2} + x_{2,3} + x_{2,5} = 0; \\ -x_{2,3} + x_{3,6} = 0; \\ -x_{1,4} + x_{4,5} + x_{4,7} = 0; \\ -x_{2,5} - x_{4,5} + x_{5,6} = 0; \\ -x_{3,6} - x_{5,6} + x_{6,9} = 0; \\ -x_{4,7} + x_{7,8} = 0; \\ -x_{7,8} + x_{8,9} = 0; \\ -x_{6,9} - x_{8,9} = -1. \end{cases}$$

У досліджуваній структурі ІКМ мультишлях може містити такі окремі шляхи в процесі розв'язання задачі багатошляхової безпечної QoS-маршрутизації:

– Шлях 1: $R_1 \to R_2 \to R_3 \to R_6 \to R_9$;

– Шлях 2: $R_1 \to R_2 \to R_5 \to R_6 \to R_9$;

– Шлях 3: $R_1 \to R_4 \to R_5 \to R_6 \to R_9$;

– Шлях 4: $R_1 \to R_4 \to R_7 \to R_8 \to R_9$.

Розрахунок вагових коефіцієнтів $w_{i,j}$ для кожного каналу зв'язку, що використовуються для обчислення компонента (3.5) комбінованої маршрутної метрики у моделях 1 і 2, засновано на настпуних припущеннях [7]. Показник критичності q-ї вразливості на і-му вузлі досліджуваної мережі BS_i^q, що залежав від базових метрик системи оцінки вразливостей, визначався для різних маршрутизаторів із відповідною ймовірністю використання цієї q-ї вразливості на і-му вузлі мережі P_i^q (табл. 3.1) [31].

Отже, у табл. 3.1 кожному маршрутизатору, використовуватиметься в ІКМ, відповідав опис певної вразливості відповідно до бази даних загальновідомих уразливостей інформаційної безпеки CVE [10].

Треба зазначити, що для дослідження обрано мережне обладнання, якому притаманні найбільш поширені та критичні вразливості, які описані в другому розділі.

Таблиця 3.1 – Характеристики вразливостей мережних пристроїв, обраних для дослідження

Вузол ІКМ	Маршрутизатор	Базова оцінка BS_i^q	Імовірність використання вразливості P_i^q	Опис вразливості відповідно до спеціалізованої бази даних	Рівень критичності вразливості
R_1	Cisco ISR 4461	7,8	0,18	CVE-2023-20035	Високий
R_2	Cisco ASR 9902	7,8	0,18	CVE-2023-20065	Високий
R_3	Cisco 8818	5,9	0,22	CVE-2023-20081	Середній
R_4	Cisco RV345	9,8	0,39	CVE-2023-20073	Критичний
R_5	Juniper JRR200	6,5	0,28	CVE-2023-28970	Середній
R_6	Juniper PTX1000	7,5	0,39	CVE-2022-22211	Високий
R_7	Juniper ACX7509	5,3	0,39	CVE-2023-28961	Середній
R_8	Netgear R9000	7,4	0,22	CVE-2023-23110	Високий
R_9	Netgear XR300	8,8	0,28	CVE-2022-27643	Високий

3.4 Порівняння моделей безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей

Далі проведемо числове дослідження моделей 1 і 2 безпечної QoS-маршрутизації, а саме:

– модель 1, яка представлена умовами та обмеженнями (3.1)-(3.6) і квадратичним критерієм оптимальності (3.7);

– модель 2, яка представлена умовами та обмеженнями (3.1)-(3.6) і лінійним критерієм оптимальності (3.8).

Нехай потік інтенсивністю $\lambda^1 = 150$ пак/с передається між першим і дев’ятим вузлами. Тоді як співвідношення між ваговими коефіцієнтами метрик продуктивності та мережної безпеки (3.6) змінювалось від 1 до 1000. Результати розрахунків наведено в табл. 3.2 та рис. 3.3.

Для розв’язання оптимізаційних задач, обраних для дослідження, використовувались програми, написані мовою Python із застосуванням Python GEKKO Optimization Suite та NumPy.

Таблиця 3.2 – Розподіл потоку $\lambda^1 = 150$ пак/с за умови використання квадратичної моделі 1 безпечної QoS-маршрутизації

R	1	50	100	200	300	400	500	600	1000
Шлях 1	40	32	30	28,8	28,4	28,1	27,9	27,9	27,7
Шлях 2	40	52,8	56,6	59	59,9	60,5	60,7	60,9	61,3
Шлях 3	13,3	5,9	3,4	1,7	1	0,6	0,4	0,2	0
Шлях 4	56,7	59,3	60	60,5	60,7	60,8	61	61	61

Відповідно до отриманих результатів лише за умови R = 1000 вихідний потік розподілявся за трьома, а не за всіма шляхами. Тобто спочатку використовувались усі чотири маршрути, але під час збільшення значення співвідношення R до 1000 третій шлях блокувався для використання у мультишляху для передачі вихідного потоку інтенсивністю $\lambda^1 = 150$ пак/с.

Враховуючи імовірності використання вразливості вузлів, які визначають й рівень вразливості каналів зв’язку, що виходять з нього, знайдемо відповідні ймовірності компрометації шляхів за методикою, вказаною в [10].

Тобто значення імовірності компрометації пакетів k-го потоку вздовж множини шляхів визначатимуться так

$$p_{E2E}^{k} = \sum_{s \in S^k} \frac{\lambda_s^k}{\lambda^k} p_s, \tag{3.9}$$

де S^k – множина шляхів для передачі пакетів k-го потоку між заданою парою маршрутизаторів мережі;

λ_s^k – інтенсивність k-го потоку пакетів в s-му шляху;

p_s – імовірність компрометації s-го шляху, яка обчислюється так

$$p_s = 1 - \prod_{E_{i,j} \in Path_s} (1 - p_{i,j}), \tag{3.10}$$

у якій $Path_s = \{E_{i,j}\}$ – множина каналів зв'язку мережі, які утворюють s-й шлях.

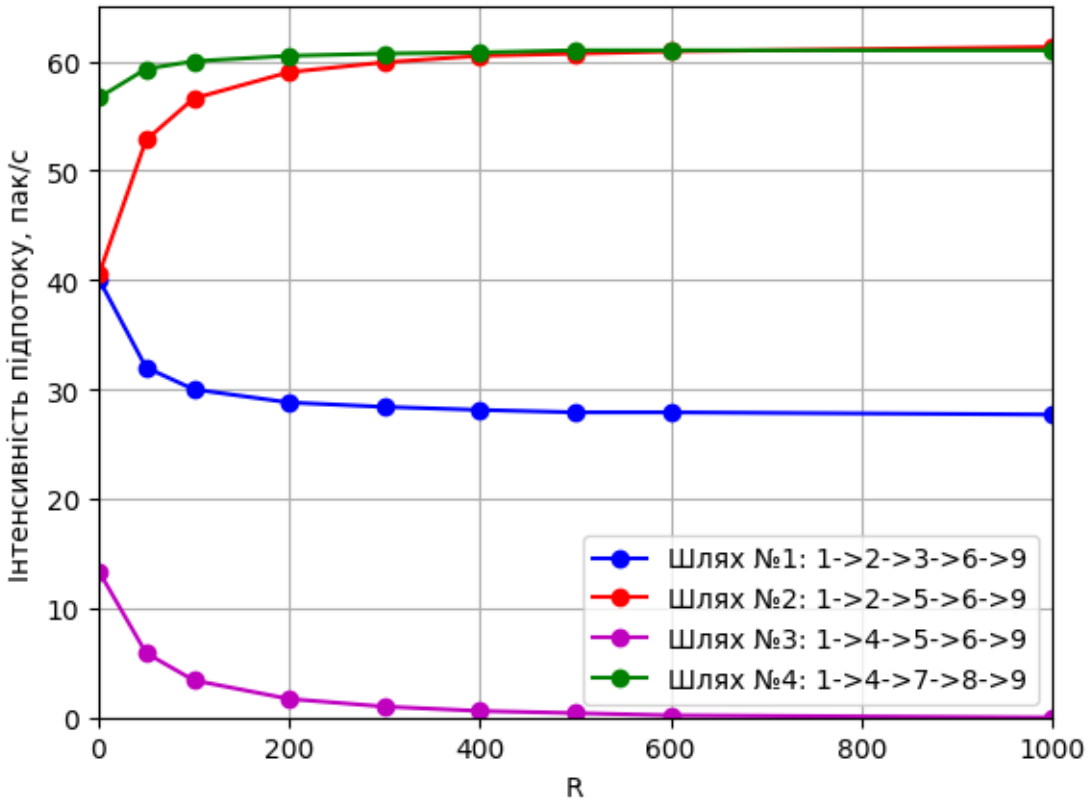


Рисунок 3.3 – Розподіл потоку за шляхами з використанням квадратичної моделі 1 ($\lambda^1 = 150$ пак/с, R = 1÷1000)

Враховуючи відомі імовірності використання вразливостей обраного мережного обладнання (табл. 3.1), отримаємо такі значення імовірностей компрометації каналів зв'язку досліджуваної ІКМ (рис. 3.4), оскільки рівень імовірності використання вразливості вузла визначає й рівень вразливості каналів зв'язку, що виходять з нього. На рис. 3.4 у розривах каналів показано дріб: чисельник – пропускна здатність, а знаменник – імовірність компрометації каналу.

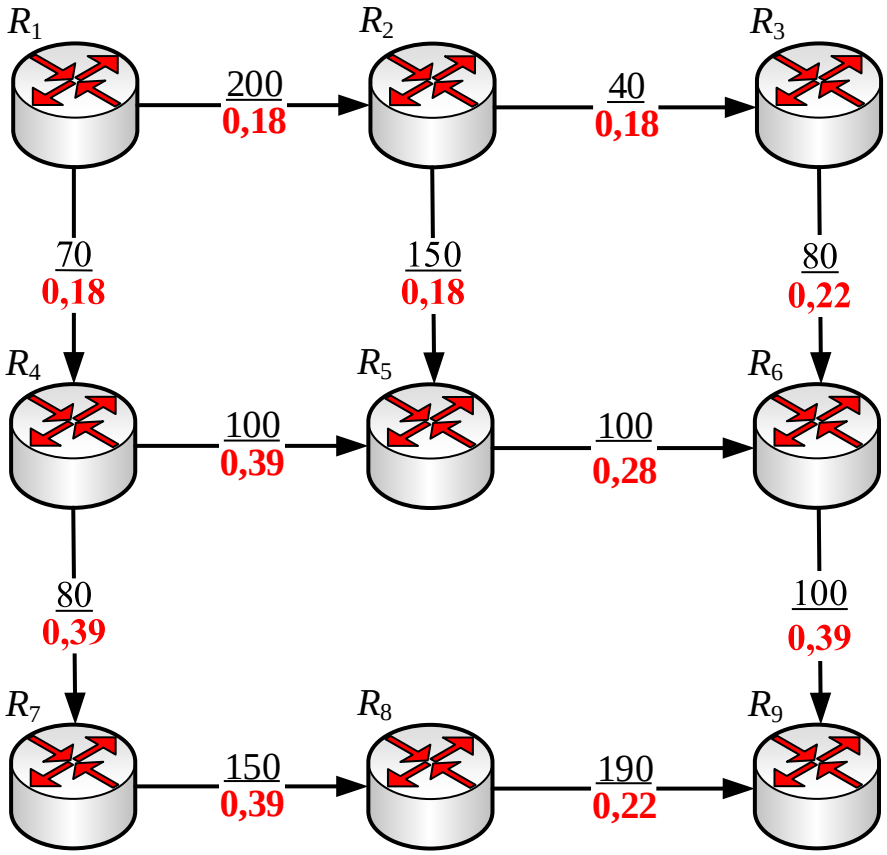


Рисунок 3.4 – Імовірності компрометації каналів зв'язку для фрагмента ІКМ, що досліджується

Отже, згідно з (3.10) отримуємо імовірності компрометації шляхів (табл. 4.3).

Таблиця 3.3 – Імовірності компрометації шляхів

Маршрути, що містяться у мультишляху		Імовірність компрометації шляху
№1	$R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow R_9$	0,680
№2	$R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9$	0,705
№3	$R_1 \rightarrow R_4 \rightarrow R_5 \rightarrow R_6 \rightarrow R_9$	0,780
№4	$R_1 \rightarrow R_4 \rightarrow R_7 \rightarrow R_8 \rightarrow R_9$	0,762

Водночас імовірності компрометації пакетів потоку, що передається, вздовж множини використаних шляхів згідно з (3.9) у разі різних співвідношень R показані в таблиці 3.4.

Таблиця 3.4 – Імовірності компрометації пакетів потоку, що передається, вздовж мультишляху

Модель	p^1_{E2E}		
	R = 1	R = 500	R = 1000
модель 1	0,7265	0,7236	0,7235
модель 2	0,7172	0,7238	0,7238

Отже, збільшення співвідношення R у разі використання моделі 1 призводить до незначного, але зменшення імовірності компрометації пакетів потоку, що передається, вздовж мультишляху. Обернена ситуація спостерігається для моделі 2.

Враховуючи все вищезазначене, найменш завантаженим завжди залишався третій шлях. Це пов’язано зі структурними особливостями досліджуваного фрагмента ІКМ. До того ж він має найгіршу ймовірність компрометації серед усіх шляхів (табл. 3.3). Як зазначалось вище, у разі збільшення значення співвідношення R до 1000 третій шлях блокувався зовсім (рис. 3.3).

Далі проводимо аналогічні розрахунки для лінійної моделі 2, результати яких наведено у таблиці 3.5 та проілюстровано на рис. 3.5.

Таблиця 3.5 – Розподіл потоку $\lambda^1 = 150$ пак/с за умови використання лінійної моделі 2 безпечної QoS-маршрутизації

R	1	2	3	10	100	100
Шлях 1	40	40	0	0	0	0
Шлях 2	60	60	100	100	100	100
Шлях 3	0	0	0	0	0	0
Шлях 4	50	50	50	50	50	50

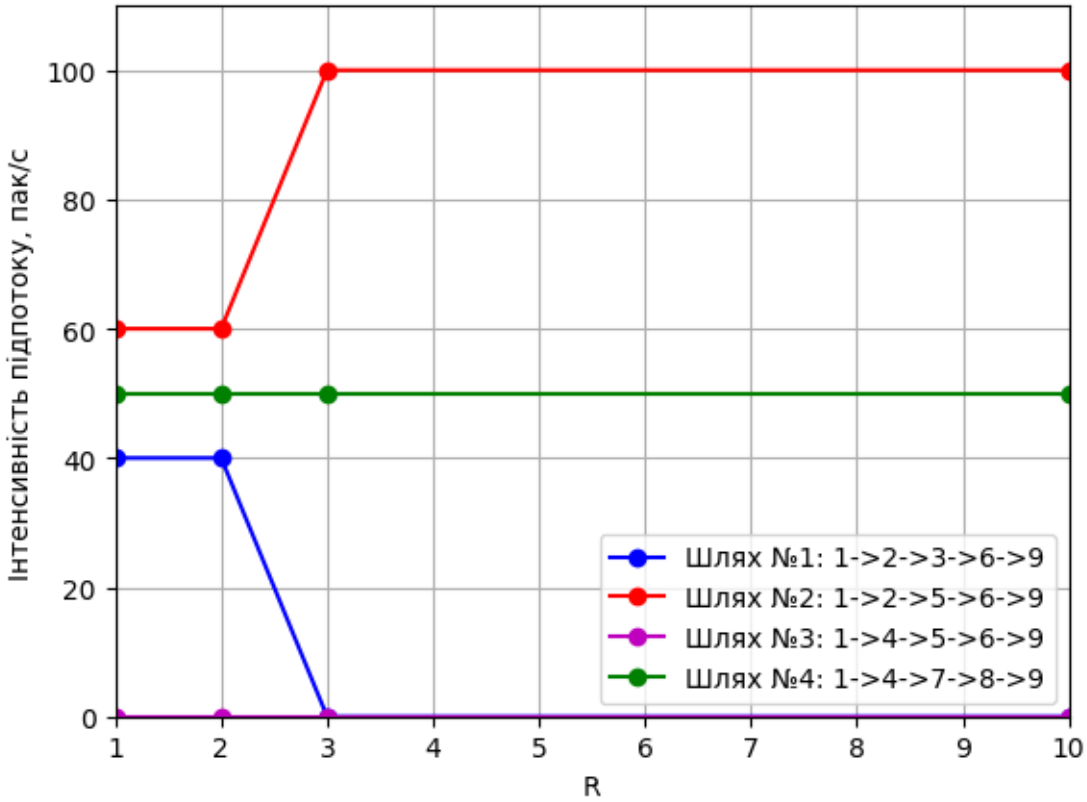


Рисунок 3.5 – Розподіл потоку за шляхами з використанням лінійної моделі 2 ($\lambda^1 = 150$ пак/с, R = 1÷1000)

З рис. 3.5 видно, що чутливість моделі 2 до співвідношення R зовсім низька, і має місце лише при R = 1 і R = 2. За цих значень використовуються три шляхи з усіх можливих, водночас третій шлях не використовується взагалі. Зі зростанням R використовуються лише два шляхи для формування мультишляху: другий та четвертий. Таким чином, балансування навантаження на данній структурі ІКМ не відбувається.

Далі у таблиці 3.6 та на рис. 3.6 показано поведінку квадратичної моделі 1 для випадку, коли інтенсивність потоку $\lambda^1 = 150$ пак/с, а співвідношення між ваговими коефіцієнтами метрик продуктивності та мережної безпеки було R = 100. Чисельні розрахунки показали, що зростання імовірності компрометації каналу $E_{6,9}$ призводить до блокування того ж третього шляху.

Загалом ми бачимо зменшення навантаження на перші три маршрути. Разом з тим четвертий маршрут, за рахунок того, що він стає більш безпечним і має достатню пропускну здатність, завантажується більше.

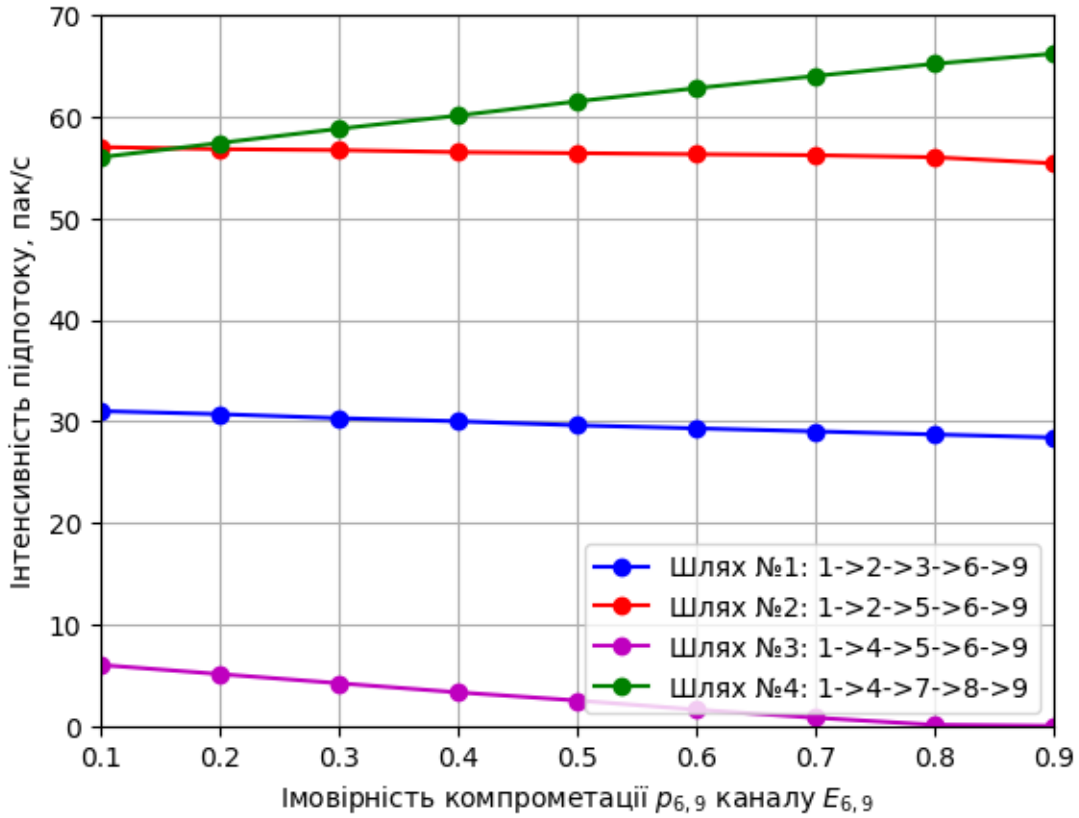


Рисунок 3.6 – Динаміка розподілу потоку при безпечній QoS-маршрутизації за квадратичною моделлю 1 ($\lambda^1 = 150$ пак/с, R = 100, $p_{6,9} = 0{,}1 \div 0{,}9$)

Таблиця 3.6 – Розподіл потоку на підпотоки за квадратичною моделлю 1 ($\lambda^1 = 150$ пак/с, R = 100, $p_{6,9} = 0{,}1 \div 0{,}9$)

$p_{6,9}$	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
Шлях 1	31	30,7	30,3	30	29,6	29,3	29	28,7	28,4
Шлях 2	57	56,8	56,7	56,5	56,4	56,3	56,2	56	55,4
Шлях 3	6	5,1	4,2	3,3	2,5	1,6	0,8	0,1	0
Шлях 4	56	57,4	58,8	60,1	61,5	62,8	64	65,2	66,2

Таким же чином отримуємо результат розподілу розподілу потоку при безпечній QoS-маршрутизації за моделлю 2. Однак, оскільки чутливість моделі низька до співвідношення компонентів комбінованої метрики, задаємо R = 2. У цьому разі третій шлях, як і раніше, блокується, перший шлях передає підпотік з незмінною інтенсивністю, і лише другий та четвертий шляхи балансують між

собою більшу частку навантаження відповідно до імовірності компрометації цих шляхів.

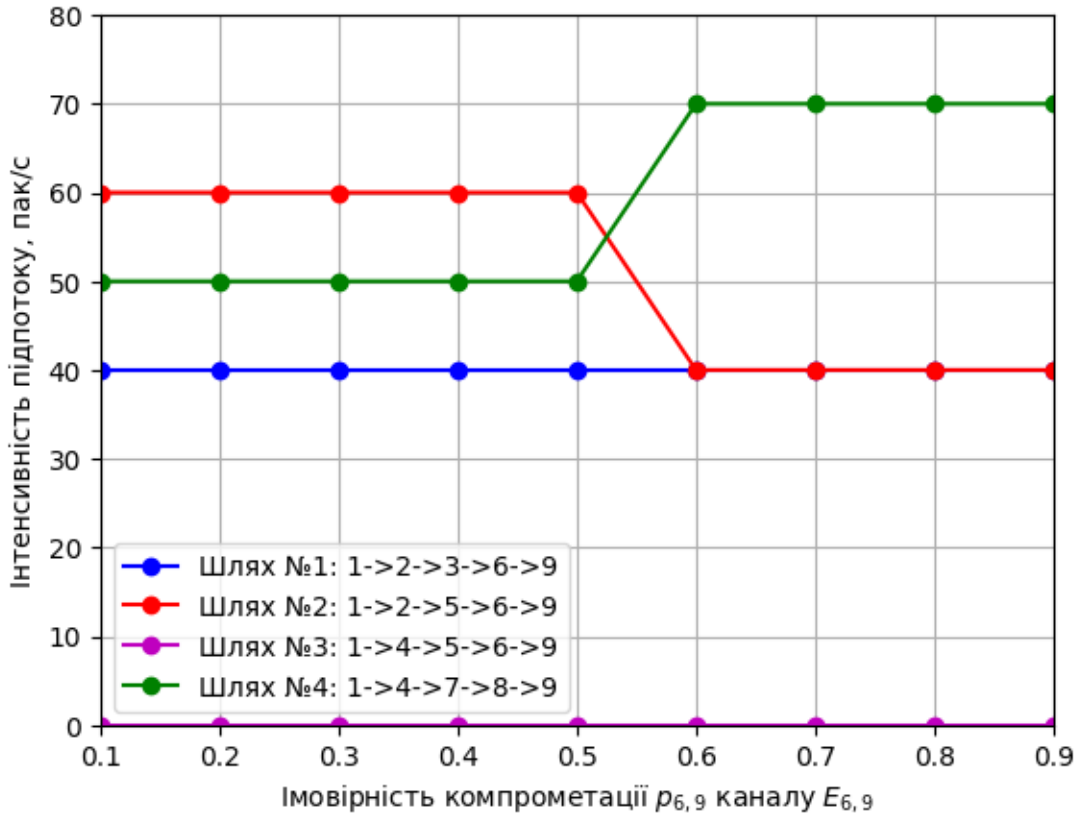


Рисунок 3.7 – Динаміка розподілу потоку при безпечній QoS-маршрутизації за моделлю 2 ($\lambda^1 = 150$ пак/с, R = 2, $p_{6,9} = 0{,}1 \div 0{,}9$)

Таблиця 3.7 – Розподіл потоку на підпотоки за лінійною моделлю 2 ($\lambda^1 = 150$ пак/с, R = 2, $p_{6,9} = 0{,}1 \div 0{,}9$)

$p_{6,9}$	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
Шлях 1	40	40	40	40	40	40	40	40	40
Шлях 2	60	60	60	60	60	40	40	40	40
Шлях 3	0	0	0	0	0	0	0	0	0
Шлях 4	50	50	50	50	50	70	70	70	70

Далі в таблицях 3.8 і 3.9 та рис. 3.8 і 3.9 наведено результати розв’язання задачі маршрутизації з використанням моделей 1 і 2 для порівняльного аналізу.

На цих рисунках у розривах каналів зв'язку вказано (згори донизу) їхні пропускні здатності (пак/с), інтенсивність потоку, що протікає в каналі зв'язку (пак/с), а також імовірності компрометації каналів зв'язку.

Як показано на рис. 3.8, розв'язання задачі безпечної QoS-маршрутизації за квадратичною моделлю 1 у разі передачі потоку пакетів інтенсивністю $\lambda^1 = 150$ пак/с та R = 100 містить усі чотири шляхи у межах досліджуваної структури мережі, що підтверджують розрахункові результати, наведені у таблицях 3.8 і 3.9.

Водночас рис. 3.9 демонструє результат розв'язання задачі безпечної QoS-маршрутизації під час використання лінійної моделі 2. На відміну від моделі 1, під час використання моделі 2 потік пакетів інтенсивністю $\lambda^1 = 150$ пак/с передавався лише двома маршрутами, найкращими з погляду пропускної здатності та імовірності компрометації, що показано на рис. 3.9, а також у таблицях 3.8 і 3.9.

Зазначимо, що обидві моделі використовують комбіновану маршрутну метрику.

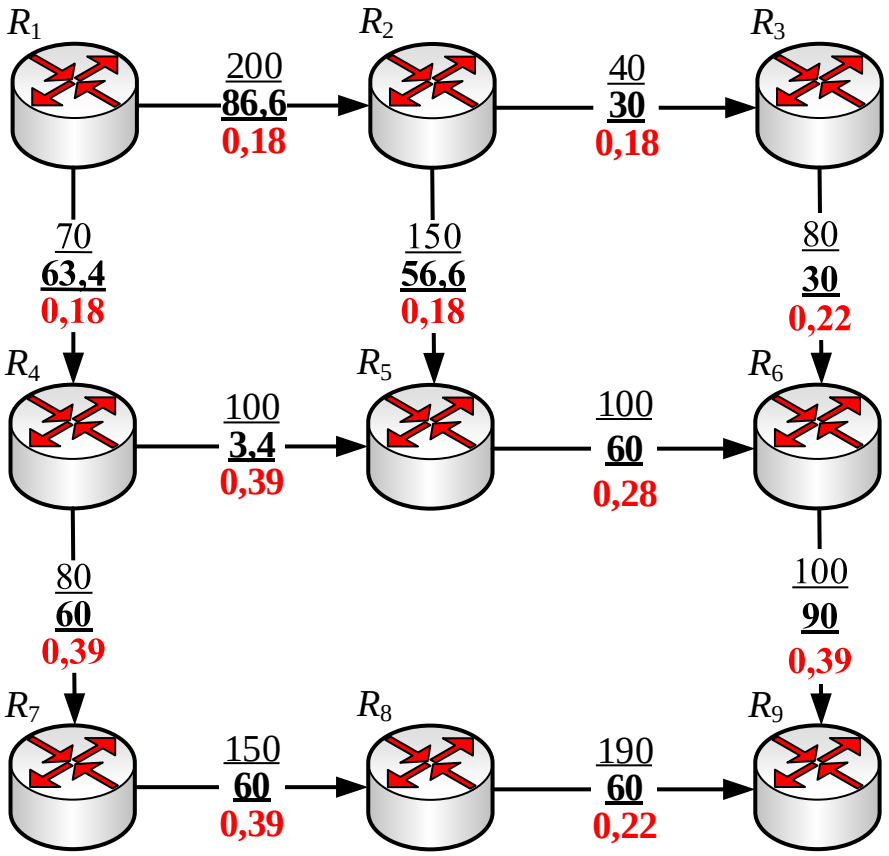


Рисунок 3.8 – Результат розв'язання задачі безпечної QoS-маршрутизації з використанням квадратичної моделі 1

($\lambda^1 = 150$ пак/с, R = 100)

Таблиця 3.8 – Результати порівняльного аналізу моделі 1 і моделі 2 (R = 100) за умови інтенсивності потоку пакетів $\lambda^1 = 150$ пак/с

Канали зв'язку	Пропускна здатність каналу, $\varphi_{i,j}$, пак/с	Модель 1	Модель 2
		Інтенсивність потоку, пак/с	Інтенсивність потоку, пак/с
$E_{1,2}$	200	86,6	100
$E_{2,3}$	40	30	0
$E_{1,4}$	70	63,4	50
$E_{2,5}$	150	56,6	100
$E_{3,6}$	80	30	0
$E_{4,5}$	100	3,4	0
$E_{5,6}$	100	60	100
$E_{4,7}$	80	60	50
$E_{6,9}$	100	90	100
$E_{7,8}$	150	60	50
$E_{8,9}$	190	60	50

Таблиця 3.9 – Результати порівняльного аналізу розподілу потоку в межах мультишляху під час використання моделей 1 і 2 (R = 100) за умови інтенсивності потоку пакетів $\lambda^1 = 150$ пак/с

№ шляху	Імовірність компрометації шляху	Модель 1	Модель 2
		Інтенсивність потоку, пак/с	Інтенсивність потоку, пак/с
1	0,680	30	–
2	0,705	56,6	100
3	0,780	3,4	–
4	0,762	60	50

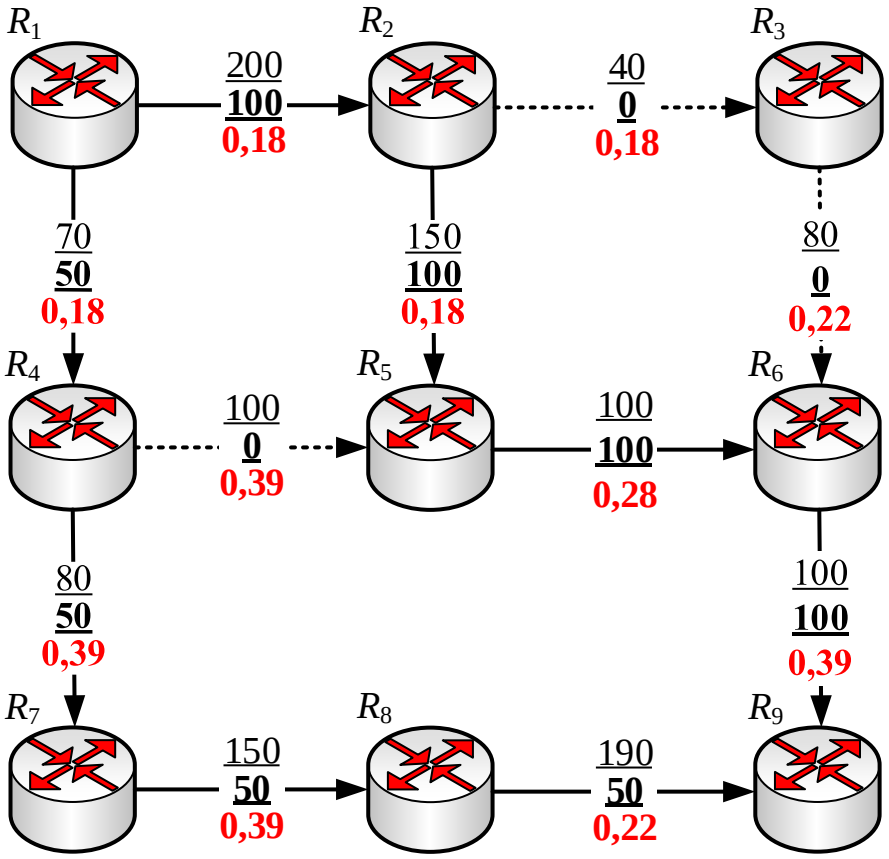


Рисунок 3.9 – Результат розв'язання задачі безпечної QoS-маршрутизації з використанням лінійної моделі 2

($\lambda^1 = 150$ пак/с, R = 100)

Таблиця 3.10 – Порівняння імовірності компрометації пакетів потоку, що передається, вздовж множини використаних шляхів

Model	Paths	p^1_{E2E}
Model 1	№1: $R_1 \to R_2 \to R_3 \to R_6 \to R_9$ №2: $R_1 \to R_2 \to R_5 \to R_6 \to R_9$ №3: $R_1 \to R_4 \to R_5 \to R_6 \to R_9$ №4: $R_1 \to R_4 \to R_7 \to R_8 \to R_9$	0,7244
Model 2	№2: $R_1 \to R_2 \to R_5 \to R_6 \to R_9$ №4: $R_1 \to R_4 \to R_7 \to R_8 \to R_9$	0,7238

Зі свого боку, табл. 3.10 демонструє результати розрахунку імовірностей компрометації пакетів потоку, що передається вздовж множини використаних

шляхів, у разі застосування розглянутих моделей. Таким чином, модель 1 і модель 2 проявляють майже однакові імовірності компрометації пакетів потоку, що передається. Проте модель 2 використовує лише два шляхи у розрахованому мультишляху, не зважаючи на те, що жоден з них не є найбільш безпечним за показником мережної безпеки. Крім того, модель 2 майже не чутлива до співвідношення компонентів комбінованої метрики.

Відповідно до проведеного моделювання та порівняльного аналізу математичних моделей безпечної QoS-маршрутизації можна зробити висновок щодо доцільності подальшого використання саме квадратичної моделі. Оскільки вона дійсно дозволяє ефективно реалізувати розподіл навантаження у межах структури ІКМ, а саме балансування навантаження, обґрунтоване за показниками не тільки пропускної здатності, а також і мережної безпеки каналів зв’язку.

ВИСНОВКИ

В кваліфікаційній роботі вирішено важливу науково-прикладну задачу, пов’язану з оглядом найпоширеніших атак на інфокомунікаційну мережу, аналізом вразливостей мережного обладнання, методів їх виявлення та методом щодо мінімізації впливу вразливостей мережного обладнання за допомогою математичних моделей безпечної qos-маршрутизації.

Слід зазначити, що для зменшення ризиків щодо успішного проведення різноманітних атак на інфокомунікаційні мережі слід приділяти увагу вчасному виявленню та усуненню вразливостей, як інфокомунікаційної мережі в цілому так і окремих її компонентів. При чому, слід зауважити, що одним з найкритичніших місць ІКМ з точки зору вразливостей є саме мережні компоненти, кожному з яких притаманна певна кількість вразливостей, починаючи з вразливостей їх програмного забезпечення та закінчуючи помилками під час їх налаштування.

З цією метою для подільшого дослідження увагу приділено найпоширенішим вразливостям мережних компонентів, вчасне усунення яких дозволить підвищити рівень захисту інфокомунікаційної мережі загалом, а також базам даних мережних вразливостей для виявлення сценаріїв зменшення ризиків їх використання для проведення атак.

Проведений аналіз методів виявлення вразливостей показав необхідність аналізу, виявлення, оцінки критичності та розробки плану усунення знайдених вразливостей. Але постає проблема в тому, що не всі вразливості можна усунути по причині відсутності оновленого програмного забезпечення, відповідних патчів тощо. Саме тому, однією з головних задач для підвищення рівня захисту ІКМ є не тільки вчасне виявлення та усунення вразливостей, але й мінімізація ризиків під час їх ймовірного використання.

В роботі показано, що існує декілька підходів щодо мінімізації ризиків від використання наявних та не усунутих вразливостей, одним з яких є використання маршрутних рішень, які дозволяють зменшувати та балансувати навантаження в мережі між мережним обладнанням з вразливостями з високим рівнем критичності.

Таким чином, в третьому розділі даної роботи буде розглядатись метод щодо мінімізації ризиків від використання вразливостей в ІКМ в цілому та

забезпеченням показників якості обслуговування, що на теперішній час є також головною вимогою до сучасних інфокомунікаційних мереж.

В роботі зазначено, що на маршрутні рішення можуть впливати політики безпеки, які забезпечують сегментацію мережі та контроль доступу. Маршрутизатори можуть спрямовувати трафік за певними шляхами, щоб запобігти несанкціонованому доступу до чутливих сегментів мережі. Крім того, важливим напрямком підвищення мережної безпеки є безпечна маршрутизація шляхами, обраними відповідно до критичності вразливостей вузлів (мережних пристроїв) та інцидентних до них каналів зв’язку.

Для проведення дослідження розглянуті існуючі моделі безпечної маршрутизації в ІКМ, що можуть бути використані для порівняння впливу на маршрутні рішення показників критичності вразливості мережного обладнання та продуктивності каналів зв’язку. Результатом дослідження є порівняльний аналіз моделей безпечної QoS-маршрутизації з урахуванням базових метрик критичності вразливостей, а також перевірено працездатність, адекватність та ефективність потокових моделі безпечної QoS-маршрутизації за допомогою розрахункових прикладів.

Розв’язання оптимізаційної задачі під час дослідження відбувалось застосуванням програми на мові програмування Python IDLE із бібліотеками Python GEKKO Optimization Suite та NumPy.

Таким чином, доведено, що за допомогою безпечної маршрутизації та дослідуваного методу, а саме визначаючи пріоритетність безпечних шляхів, розглядаючи системи виявлення/запобігання вторгненням, впроваджуючи політику сегментації мережі, контролю доступу та оцінку критичності вразливостей елементів мережі, можливо суттєво знизити ризики та ймовірні збитки у разі використання вразливостей мережного обладнання із наявними критичними вразливостями.

Окремі результати роботи доповідались на міжнародних науково-практичних конференціях [8 – 11].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Hu C. Guidelines for Access Control System Evaluation Metrics [Електронний ресурс] / C. Hu, K. Scarfone // NIST Interagency/Internal Report (NISTIR), National Institute of Standards and T3echnology, Gaithersburg, MD. – 2012. – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.IR.7874 (Accessed March 26, 2021).

2. Router Security Strategies Securing IP Network Traffic Planes / Schudel, G., Smith, D. J. // Cisco Press. – 2008. – С. 673.

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

4. ATIS. *ATIS | In a rapidly changing industry, innovation needs a home*. URL: http://www.atis.org/ (дата звернення: 15.12.2022).

5. The Internet Engineering Taskforce (IETF) Home. *IETF*. URL: https://ietf.org (дата звернення: 15.12.2022).

6. The Open Data Centre Alliance (ODCA). URL: https://opendatacenteralliance.org/ (дата звернення: 15.05.2023).

7. Єременко О.С., Плєхова Г.А. Дослідження моделей безпечної маршрутизації на основі базових метрик уразливостей у мережах SDN. Проблеми телекомунікацій. 2022. № 2(31). С. 34-50. URL: https://pt.nure.ua/wp-content/uploads/2022/12/222_yeremenko_secure.pdf

8. 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.

9. 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.

10. Назаров Б. Огляд вразливостей мережного обладнання в інфокомунікаційних мережах / Б. Назаров // Харків, ХНУРЕ, Матеріалі XXVII міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Том 4. – 2023. – С. 100 – 101.

11. Назаров Б. Огляд баз даних вразливостей для оцінки ризиків інформаційної безпеки в інфокомунікаційних мережах / Б. Назаров // Харків,

ХНУРЕ, Матеріалі XXVII міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Том 4. – 2023. – С. 102 – 103.

12. Common Vulnerability Scoring System v3.1: Examples [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.first.org/cvss/examples. (дата звернення: 15.05.2023)

13. Open-source vulnerabilities database shuts down [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.csoonline.com/article/3053549/open-source-vulnerabilities-database-shuts-down.html. (дата звернення: 15.05.2023)

14. Datasources VulnDB [Електронний ресурс] – Режим доступу до ресурсу: https://docs.dependencytrack.org/datasources/vulndb/. (дата звернення: 15.05.2023)

15. All Primary Archived Entries [Електронний ресурс] – Режим доступу до ресурсу: https://securitytracker.com/archives/summary/9000.html. (дата звернення: 15.05.2023)

16. Open Vulnerability and Assessment Language [Електронний ресурс] – Режим доступу до ресурсу: https://oval.mitre.org/inuse/. (дата звернення: 15.05.2023)

17. Баз даних експлойтів для пошуку вразливостей [Електронний ресурс] – Режим доступу до ресурсу: https://null-byte.wonderhowto.com/how-to/top-10-exploit-databases-for-finding-vulnerabilities-0189314/. (дата звернення: 15.05.2023)

18. IBM X-Force Exchange [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/products/xforce-exchange. (дата звернення: 15.05.2023)

19. Exploit Database Free Security List [Електронний ресурс] – Режим доступу до ресурсу: https://cxsecurity.com/exploit/. (дата звернення: 15.05.2023)

20. Secunia Research [Електронний ресурс] – Режим доступу до ресурсу: https://community.flexera.com/t5/Secunia-Advisories/ct-p/advisories. (дата звернення: 15.05.2023)

21. National Vulnerability Database [Електронний ресурс] – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/data-feeds. (дата звернення: 15.05.2023)

22. Frequently Asked Questions [Електронний ресурс] – Режим доступу до ресурсу: https://cve.mitre.org/about/faqs.html#what_is_cve. (дата звернення: 15.05.2023)

23. . Scarfone K., Scarfone K., Mell P. NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS)., National Institute

of Standards and Technology, 2012. URL: http://csrc.nist.gov/publications/drafts/800-94- rev1/draft_sp800-94-rev1.pdf. (дата звернення: 15.05.2023)

24. Yeremenko O., Persikov M., Lemeshko V., Altaki B. Research and development of the secure routing flow-based model with load balancing. *Проблеми телекомунікацій.* 2021. № 2(29). С. 3–14. URL: https://pt.nure.ua/wp-content/uploads/2021/12/212_yeremenko_secure.pdf

25. 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

26. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. IEEE *Transactions on Vehicular Technology*. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: https://doi.org/10.1109/TVT.2006.877707

27. Lou W., Liu W., Fang Y. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. INFOCOM 2004: *Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*. Hong Kong, China, 7–11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: https://doi.org/10.1109/INFCOM.2004.1354662

28. Снегуров А.В., Чакрян В.Х. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности. *Системи управління, навігації та зв'язку*. 2012. № 4(24). С. 105–110.

29. Євдокименко М. О., Шаповалова А. С., Шаповал М. М. Потокова модель маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. *Проблеми телекомунікацій*. 2020. № 1(26). С. 48–62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf

30. Yevdokymenko M., Yeremenko O., Shapovalova A., Shapoval M., Porokhniak V., Rogovaya N. Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. Workshop Proceedings of the MoMLeT+DS 2021: *3rd International Workshop on Modern Machine Learning Technologies and Data Science*, June 5, 2021, Lviv-Shatsk, Ukraine. P. 207–217. URL: http://ceur-ws.org/Vol-2917/paper19.pdf

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

32. CVSS v3.1 Examples. *FIRST – Forum of Incident Response and Security Teams*. URL: https://www.first.org/cvss/examples (дата звернення: 15.05.2023).

33. NIST National Vulnerability Database. *NVD - Home*. URL: https://nvd.nist.gov (дата звернення: 15.05.2023).

34. 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: 15.05.2023).

35. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : монографія / О.В. Лемешко, О.С. Єременко, М.О. Євдокименко та ін. Харків : ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1

36. 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).

37. AzerTelecom | AZERBAIJAN NETWORK. *AzerTelecom*. URL: https://www.azertelecom.az/en/aznetwork/ (дата звернення: 15.05.2023).