Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему

Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ. 180246.22.01.25 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 Підпис Чемерис О.Ю.

Керівник: ст. викладач, к.т.н, доц. Підпис Муляр І.В.

Нормоконтролер старший викладач Підпис Мостовий С.В.

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц Підпис Кльоц Ю.П.

11 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма КІБЕРБЕЗПЕКА

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Чемерису Олександру Юрійовичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

Керівник роботи Муляр Ігор Володимирович,
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи) Статистика DDoS – атак, архітектура мережі

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Проаналізувати чинники, що впливають на забезпечення ефективного функціонування мережі, розглянути критерії та існуючі методи їх оцінки. Перевірити можливість використання математичного апарату теорії надійності як інструменту для проведення досліджень. Розробити модель надійності вузла, яка враховує вплив атак і технічних відмов обладнання. Розробити метод експериментального дослідження впливу атак на коефіцієнт готовності. Провести застосування розроблених методів до реальної мережі та дослідити їх ефективність для різних топологій.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	16.10.2023	
6	Робота над розділом 4 – апробація запропонованих рішень	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ О.Ю. Чемерис
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ І.В. Муляр
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні.

Автор роботи: Чемерис Олександр Юрійович

Керівник роботи: к.т.н., доц. Муляр Ігор Володимирович

Загальний обсяг роботи: 86 сторінок, 27 рисунків, 7 таблиць, 2 додатки, 60 посилань.

Ключові слова: надійність, захист інформації, вузли мережі.

Метою даної роботи є підвищення ефективності функціонування корпоративних мереж шляхом удосконалення методики врахування впливу кібератак на стан окремих мережевих вузлів. Запропоновано модифікований підхід до оцінювання стану вузлів зв'язку з урахуванням імовірностей реалізації загроз та їх впливу на безперервну доступність інформаційних ресурсів.

Удосконалена методика разом з рекомендаціями щодо побудови резервних топологій дозволить комплексно аналізувати функціонування мережі та розробляти обґрунтовані заходи для протидії загрозам і підтримки стабільної роботи на заданому рівні показників.

11. 12. 2023

ANNOTATION

Theme of qualification work: A method for assessing the security of network nodes under the influence of denial of service attacks

Author of the work: Chemerys Oleksandr Yuriiovych

Mentor: Ph.D. Muliar Ihor Volodymyrovych

Total volume of work: 86 pages, 27 figures, 7 tables, 2 appendices, 60 links.

Keywords: reliability, information protection, network nodes

The purpose of this work is to improve the efficiency of corporate networks by enhancing the methodology for taking into account the impact of cyberattacks on the state of individual network nodes. An improved approach is proposed for assessing the state of communication nodes, taking into account the probabilities of threats being implemented and their impact on the continuous availability of information resources.

The improved methodology, together with recommendations on designing redundant topologies, will allow for a comprehensive analysis of network operations and the development of reasonable measures to counter threats and maintain stable functioning at a specified level of metrics.

In summary, the goal is upgrading existing assessment methods through incorporating probabilities of cyber threats realization when evaluating network node states. That will assist making decisions on ensuring required reliability and continuity of corporate network services. The mathematical apparatus of probability theory and reliability metrics are leveraged to achieve these improvements.

11. 12. 2023

ЗМІСТ

ВСТУП

Активний прогрес мережевих технологій породжує нові форми атак на комп'ютерні мережі. Множинні методи вторгнень та їх варіації викликають потребу вдосконалення існуючих технологій та засобів захисту корпоративних комп'ютерних мереж.

Використання передових інформаційних технологій є обов'язковою складовою для розв'язання сучасних завдань управління різними системами та об'єктами. Корпоративні комп'ютерні мережі виступають універсальним інструментом, що сприяє ефективності та успішності функціонування різноманітних систем.

З розвитком комп'ютерних мереж зростає число користувачів та передаваної інформації. Однак збільшення інтенсивності мережевого трафіку може вплинути на якість мережевих послуг. Таким чином, виникає завдання вдосконалення інструментів для моніторингу та аналізу мережевого трафіку.

Проблема аналізу трафіку вивчається тривалий час, і для розв'язання цих завдань проводяться численні дослідження. Особливо це актуально через швидкі зміни в мережевому середовищі [1]. Останні методи та алгоритми можуть втрачати свою ефективність або навіть стати непридатними. Зокрема, збільшення обсягу трафіку та пропускної здатності каналу створює потребу в алгоритмах, які зменшують обчислювальну складність.

Ці недоліки походять від того, що існуючі системи виявлення та протидії кібератакам не застосовують динамічно мінливі (регульовані) правила роботи та не ураховують потенційної шкоди. Багато провідних науковців, як в Україні, так і за кордоном, вказують на актуальність вирішення цієї важливої науково-технічної проблеми [2]. Недоліки зазначені через те, що існуючі системи не враховують динамічні зміни в регулюючих правилах та не враховують можливості завданої шкоди. Багато експертів, як в Україні, так і в інших країнах, вказують на необхідність вирішення цієї важливої науково-технічної задачі, зокрема В. М. Астапені, В. Л. Бурячка, С.В. Лєнков, В. М. Богуша, О. Г. Корченко,

Г. Т. Марков, Л.Е. Назаров, С. В. Толюпи, В. О. Хорошко, Дж. Во-зенкрафт, У. Питерсон, Р. Блейхут, Р. Галлагер та інші.

Розвиток інформаційних технологій приводить до формування нового відкритого інформаційного суспільства, яке визначається встановленням взаємодії між людьми у всіх аспектах їхньої діяльності. Цей процес призводить до з'яви віртуальних офісів, які дозволяють працівникам здійснювати координацію своїх дій віддалено, розвитку електронної комерції та створення нових інформаційних засобів.

Комп'ютерна мережа є об'єднанням взаємопов'язаних комп'ютерів через канали передавання даних, яке забезпечує користувачів можливістю обміну інформацією та спільного використання апаратних, програмних та інформаційних ресурсів [3].

Використання персонального комп'ютера без доступу до мережі інформаційних ресурсів втрачає свою доцільність, оскільки його функціональність значно обмежується. Ці ресурси можуть бути сконцентровані локально (у межах офісу чи підприємства) або в глобальних мережах, таких як Інтернет

Основна мета цього дослідження полягає в об'єднанні характеристик надійності та інформаційної безпеки в єдину математичну модель. Для моделювання характеристик надійності та захисту інформації можуть бути використані ланцюги Маркова та експоненціальний розподіл можливих подій. В якості показника, що непрямо відображає властивості системи, рекомендується використовувати коефіцієнт готовності.

З урахуванням зазначеного, розробка методу оцінки ефективності функціонування вузла зв'язку корпоративної мережі умовах впливу атак на відмову в обслуговуванні представляє собою актуальне науково-технічне завдання.

Мета дослідження полягає в удосконаленні методу врахування впливу загроз на функціонування вузла зв'язку мережі.

Для досягнення цієї мети в роботі вирішено наступні завдання:

1. Проведено аналіз факторів, які впливають на ефективне функціонування вузлів мережі.

2. Досліджено доцільність використання математичного апарату теорії надійності для аналізу доступності вузла в умовах впливу атак на відмову в обслуговуванні

3. Розроблено математичну модель надійності вузла мережі в умовах впливу атак на відмову в обслуговуванні устаткування.

4. Досліджено вплив загроз доступності інформації в мережі на її коефіцієнт готовності.

5. Вдосконалено метод оцінювання ефективності роботи окремого вузла в умовах реалізації загроз порушення доступності інформаційних ресурсів.

6. Розроблено алгоритм підвищення ефективності комунікаційних вузлів в умовах хакерських атак.

7. Оцінено ефективність комунікаційних вузлів існуючих мереж, та досліджено їх придатність для корпоративних мереж, з використанням різних фізичних топологій.

Об’єктом дослідження є процес забезпечення ефективного функціонування корпоративних мереж.

Предметом дослідження є характеристики вузла зв'язку мережі.

Наукова новизна результатів магістерського дослідження:

1. Вдосконалена модель надійності комунікаційного вузла, яка вирізняється тим, що враховує вплив загроз пов’язаних з відмовою в обслуговувані.

2. Удосконалено метод дослідження мережі, заснований на моделюванні стану працездатності комунікаційних вузлів в умовах впливу атак на відмову в обслуговувані, який враховує кількісну оцінку ступеня впливу загроз безпеці доступності інформації.

Методи дослідження включали в себе використання різноманітних підходів для вирішення поставлених завдань. Зокрема, використані були методи теорії системного аналізу для глибокого вивчення взаємозв'язків та властивостей

системи. Теорія графів використовувалася для моделювання та аналізу структури мережі. Також використані методи теорії ймовірностей та математичної статистики для об'єктивного врахування ймовірних подій та аналізу статистичних даних. Методи системного аналізу допомагали у визначенні взаємозалежностей між різними елементами системи.

Крім того, використано математичне та імітаційне моделювання для створення абстрактних моделей, які дозволяли аналізувати та передбачати поведінку системи в різних умовах. Апробація результатів підтверджується шляхом реальних експериментів, що сприяло перевірці та підтвердженню ефективності запропонованих рішень.

Практичне значення роботи виявилося в успішній реалізації розроблених у магістерському дослідженні моделей, алгоритмів та методів. Це дозволило ефективно прогнозувати стан комунікаційних вузлів мережі в умовах впливу непрацездатності обладнання та загроз інформаційної безпеки.

Застосування розроблених методів дозволило проводити оцінку ефективності функціонування комунікаційних вузлів мережі у вигляді кількісного показника. Це значно підвищило якість оцінювання, що, в свою чергу, сприяло збільшенню точності та надійності прогнозів щодо впливу непрацездатності обладнання та загроз інформаційної безпеки на функціонування комунікаційних вузлів.

Публікації. Ркзультати мігістерського дослідження доповідалися та обговорювалися на XIX Міжнародній науково-практичній конференції «Військова освіта та наука: сьогодення та майбутнє» у Військовому інституті Київського національного університету імені Тараса Шевченка.

За матеріалами магістерської дослідження опублікована 1 теза.

1 АНАЛІЗ ФУНКЦІОНУВАННЯ ВУЗЛІВ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Властивості корпоративних мереж

Корпоративні комп’ютерні мережі призначені для ефективного функціонування певного підприємства, яке є їх власником, та обслуговування лише його співробітників [3]. На відміну від мереж операторів зв'язку, корпоративні мережі не надають свої послуги іншим організаціям або користувачам загалом.

Корпоративна мережа, яка інтегрує локальні мережі філій або відділень корпорації, є технічною базою для вирішення завдань планування, організації та реалізації виробничо-господарської діяльності підприємства. Вона забезпечує функціонування автоматизованої системи управління та системи інформаційного обслуговування корпорації.

Для оптимального доступу до інформації, що знаходиться на інформаційних серверах національних або корпоративних мереж, їх технологічні компоненти, зокрема телекомунікації, базуються на єдиній технологічній платформі [4]. В цей спосіб користувачі національних мереж та мереж компаній автоматично отримують доступ до глобальної мережі Інтернет.

Мультисервісна корпоративна мережа може включати різноманітні сервіси та системи, такі як загальна база даних для всіх відділень, електронний документообіг, організацію нарад, аудіо- та відеоконференції з віддаленими підрозділами, а також забезпечувати високоякісний телефонний зв'язок на рівні місцевого, міжміського та міжнародного зв'язку [5]. Це сприяє швидкій реакції на зміни в організації та дозволяє раціонально управляти процесами у режимі реального часу. Для організації конференцій та забезпечення високоякісного телефонного зв'язку у корпоративних мережах використовується IP-телефонія, що зменшує залежність організації від операторів мобільного зв'язку і сприяє

значним економіям. Крім того, корпоративна мережа гарантує передачу конфіденційної інформації фінансового чи виробничого характеру з упевненістю в тому, що тільки співробітники підприємства мають до неї доступ.

Мультисервісні корпоративні мережі замінюють спеціалізовані мережі, із розвитком корпоративних мереж та пов'язаних з ними сервісів, вимоги до мультисервісних корпоративних мереж продовжують зростати.

Проблема взаємодії в багатьох інфокомунікаційних систем полягає у великій кількості параметрів, необхідних для опису поведінки системи (системний розмір) [6]. Прийняття вірного рішення в таких мережах виявляється досить складним завданням, особливо враховуючи, що інформація про стан мережі може бути досить суперечливою. Надто, зростаючий розмір сучасних технологій є неухильною тенденцією, що зафіксована в історії розвитку цифрової системи.

Такий зростаючий розмір стає об'єктивною тенденцією, яку можна спостерігати на протязі усього історичного розвитку цифрової системи. Ця проблема зв'язку виникає не лише через велику кількість параметрів для опису системи, але й через те, що інформація про стан мережі часто може бути суперечливою [7]. Це робить важким завдання прийняття належних рішень у

Корпоративна мережа зазвичай є розподіленою територіально, об'єднуючи офіси, фабрики та інші підрозділи, розташовані на значних відстанях один від одного. Іноді підмережі корпоративної мережі розташовані в різних містах чи навіть країнах. Підходи до створення такої мережі відрізняються від тих, які застосовуються для локальних мереж. Основна різниця полягає в тому, що територіально розподілені мережі використовують повільні орендовані лінії зв'язку. У порівнянні зі створенням локальної мережі, де основні витрати пов'язані з придбанням обладнання та прокладкою кабелю, в територіально розподілених мережах вартість оренди каналів стає ключовою, особливо зі збільшенням якості та швидкості передачі даних. Ця обмеженість важлива, і при створенні корпоративної мережі слід розглядати заходи для мінімізації обсягу передаваних даних [8].

Першим завданням у створенні корпоративної мережі є об'єднання підрозділів підприємства. У випадку, коли для вузлів в одному місті можна легко орендувати виділені лінії, включаючи високошвидкісні, для віддалених вузлів вартість оренди каналів стає великою, а якість та надійність можуть страждати. Застосування вже існуючих глобальних мереж стає очевидною альтернативою. У цьому випадку достатньо забезпечити канали від підрозділів до найближчих вузлів глобальної мережі, а глобальна мережа вже візьме на себе обмін інформацією між вузлами. Навіть при створенні невеликої мережі в одному місті слід передбачати можливість розширення та використовувати технології, сумісні з існуючими глобальними мережами [9].

Використання Інтернету як основи для корпоративної мережі вносить додаткові аспекти [10]. Розглядаючи структуру мережі Інтернет, виявляється, що інформація проходить через незалежні та переважно некомерційні вузли, пов'язані різноманітними каналами передачі даних. Це призводить до нагальної проблеми щодо безпеки, оскільки непередбачувані шляхи інформації ускладнюють захист від несанкціонованого доступу та перехоплення. Хоча існують засоби шифрування передаваних даних, які частково вирішують цю проблему, існують інші аспекти безпеки, такі як обмеження доступу до ресурсів приватної мережі. Оскільки Інтернет є відкритою системою, де кожен бачить кожного, будь-хто може спробувати отримати доступ до корпоративної мережі і отримати дані. Хоча існують засоби, такі як брандмауер, вони не надають повного захисту [11]. Також важливо забезпечити безпеку інформації, що передається в межах корпоративної мережі, щоб доступ мали лише співробітники, яким призначено його бачити. Це досягається шляхом розділу корпоративної мережі на віртуальні локальні мережі та застосування політик безпеки.

Не існує двох ідентичних мереж, кожна з них має свій унікальний характер. Тому важливо визначити основні елементи мережі та створити досить просту, але відповідну модель корпоративної мережі, яка здійснює всі основні функції та включає повний набір елементів.

У наш час зросла кількість кіберзлочинців, які мають за мету збір інформації, обробленої відповідним програмним забезпеченням в комп'ютерних корпоративних мережах. Основу будь-якої мережі складає програмне забезпечення на системному рівні, яке може містити різні операційні системи, програмні оболонки, текстові процесори, прикладні програми, редактори та вбудовані програмні пакети, а також системи керування базами даних.

Інформація може вводитися з автоматизованих робочих місць через різні канали зв'язку, може бути введена як за допомогою клавіатури, так і зовнішніми носіями. Крім цього, мережа часом використовує інформаційні ресурси інших підприємств, а також ресурси глобальних розглянути модель корпоративної мережі (рис.1.1.) [12, 13].

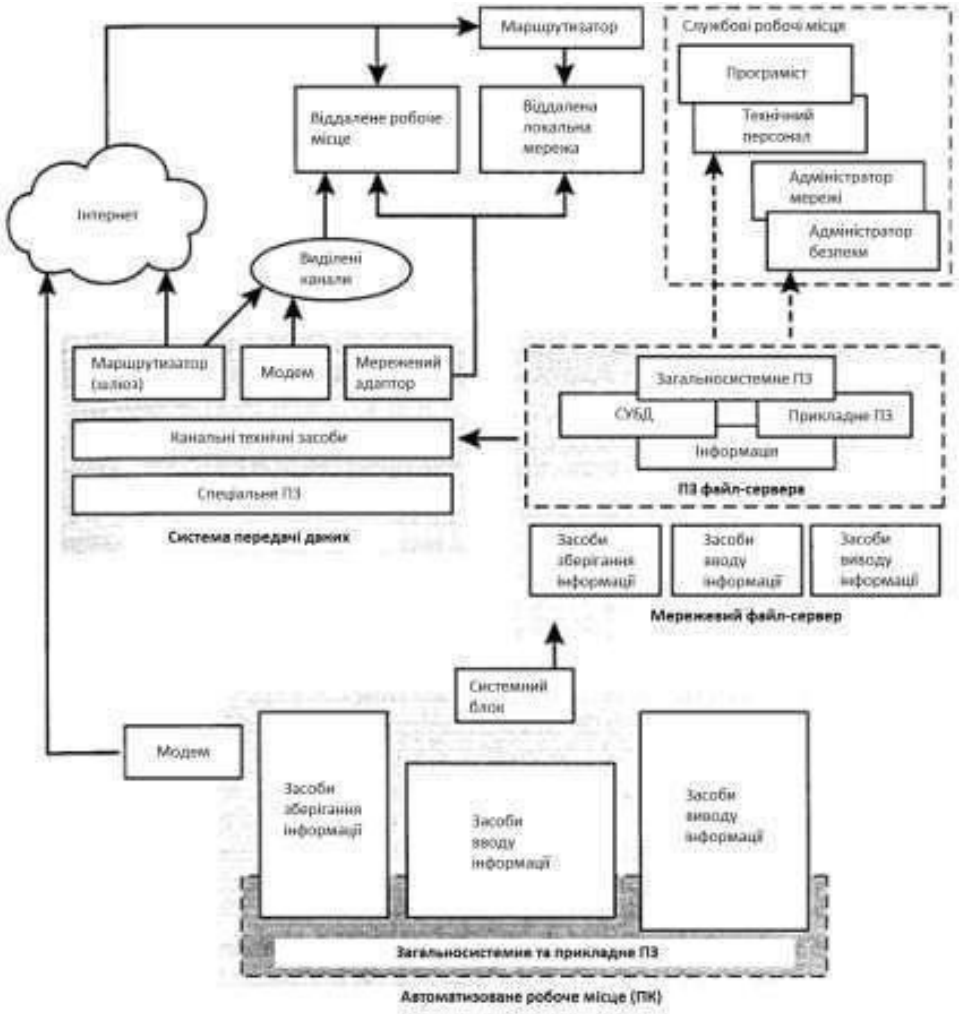


Рисунок 1.1 - Модель корпоративної мережі

Корпоративні структури можуть варіюватися за масштабом: від невеликих з одним або кількома працівниками до філій цілих містечок. Отже, інтеграція корпоративних структур можлива лише за допомогою зовнішнього телекомунікаційного зв'язку, що не є частиною підприємства.

Загальна структура ієрархічного дизайну мережі підприємства описує три ключові рівні, а саме [14]:

- ядра;
- розподілу;
- доступу.

Рівень ядра, бувши вершиною ієрархії, виступає як центральний елемент мережі. Відповідаючи за ефективну та надійну передачу великого обсягу трафіку, рівень ядра призначений для максимально швидкої передачі даних. Основне завдання полягає у забезпеченні швидкості трафіку на максимальному рівні. Трафік, що проходить через ядро, доступний для більшості користувачів. Тим не менш, слід зауважити, що дані користувачів обробляються на рівні розподілу, а ядро отримує запити від рівня розподілу лише при необхідності. Відмова на рівні ядра може вплинути на всіх користувачів. Таким чином, забезпечення відмовостійкості на цьому рівні є крайньо важливим.

При проходженні через ядро великі обсяги трафіку вимагають визначення швидкості та мінімізації затримок. Розуміючи функції ядра, можна розглянути деякі особливості його конфігурації. На рівні ядра необхідно уникати [15]:

- реалізації елементів, що можуть сповільнювати обробку трафіку, таких як списки доступу, VLAN і фільтрація пакетів;
- рідтримки доступу для робочих груп.

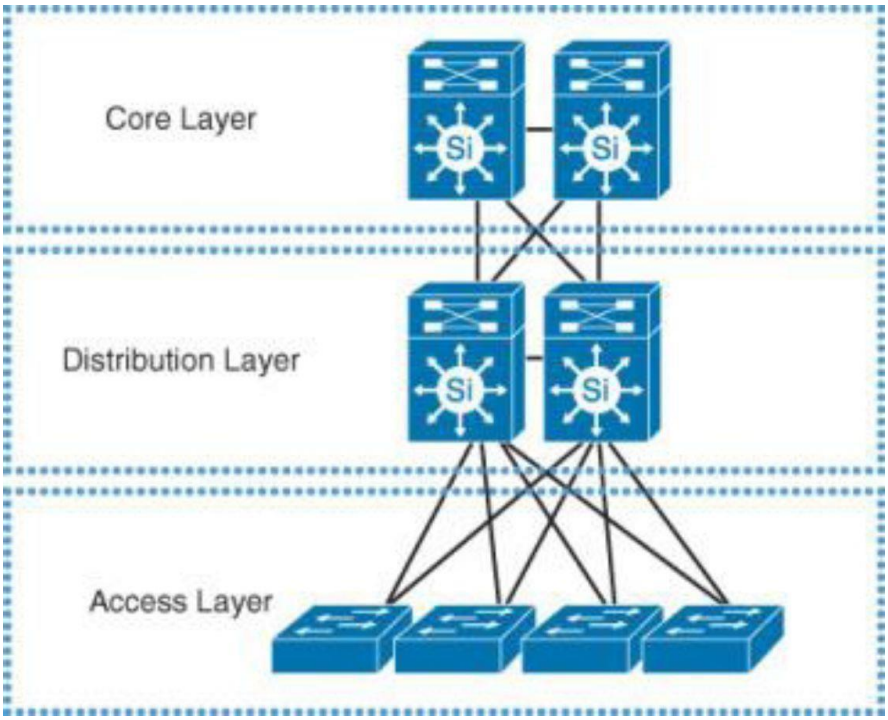


Рисунок 1.2 - Трьохрівнева модель мережі

Рівень розподілу, часто визначений як рівень робочих груп, відповідає за координацію взаємодії між рівнем доступу та рівнем ядра в мережі. Основні завдання рівня розподілу включають маршрутизацію, фільтрацію і забезпечення доступу до глобальної мережі. Крім того, він визначає, як пакети можуть отримати доступ до ядра, якщо така потреба виникає. Рівень розподілу повинен визначити оптимальний маршрут для обробки запитів користувачів, наприклад, маршрут, який використовується для передачі пакета із запитом файлу на сервер. Після вибору найкращого маршруту рівень розподілу відправляє запит на рівень ядра.

Важливо уникати виконання функцій на рівні розподілу, які повинні б бути характерними виключно одному з двох інших рівнів [16].

Рівень доступу відповідає за контроль доступу користувачів та робочих груп до мережевого середовища. Його іноді називають рівнем настільних систем. Локально виділяються мережеві ресурси, необхідні більшості користувачів. Звернення до віддалених служб здійснюються на рівні розподілу.

1.2 Аналіз загроз, що впливають на функціонування вузлів мережі

Архітектура сучасних загроз інформаційним системам потребує комплексного підходу до створення систем захисту. Зростання актуальності та складності захисту кінцевих пристроїв визначається тим, що вони стають частішим об'єктом атак зловмисників.

Атака може розпочинатися з різних шляхів доставки, таких як електронна пошта, Інтернет або застосунки з підозрілим вмістом, USB-пристрої тощо. Процес зараження передбачає спробу поширення шкідливого програмного забезпечення та ініціювання командного центру для отримання інструкцій щодо подальших дій, таких як передача конфіденційної інформації на зовнішні ре сурси або шифрування даних.

Для виявлення та захисту від ланцюга загроз використовуються різноманітні технології та методи - якщо одна технологія недостатньо ефективна, вступає в дію інша. На етапі доставки використовуються системи, такі як аналіз репутації файлів, захист браузера, фільтрація URL-адрес, локальний брандмауер, управління пристроями та контроль програм. Блокування вразливостей для експлойтів в операційних системах та програмах допомагає уникнути зараження та поширення у мережі [17].

Інформація про динаміку розвитку виробничих процесів надходить з різних джерел через канали різної якості, що призводить до частого затримання, і, як наслідок, оперативне управління та планування стають відсутніми у фактичному контексті управлінських об'єктів. Більшість диспетчерських служб підприємств працюють на межі своїх можливостей, ручним чином реалізуючи багато управлінських процедур, здійснюючи значний обсяг рутинних операцій та постійно розподіляючи свою увагу на телефонні дзвінки.

Технології машинного навчання досліджують шкідливе програмне забезпечення до та після його запуску. Детектори використання експлойтів в оперативній пам'яті захищають від атак на застарілі операційні системи. Технології виявлення програм, що вимагають великих витрат ресурсів, працюють

окремо та блокують шифрування файлів користувача. На завершальному етапі використовується аналіз за допомогою командних центрів для відстеження мережевої активності.

Для забезпечення безпеки комп'ютерних мереж важливо спочатку провести систематичний аналіз потенційних загроз для мережі.

Загрози можуть приймати різні форми, але серед найбільш поширених є такі [18]:

– випадкові, які виникають в результаті неналежного дотримання правил та політики, або через випадкові обставини;

– несанкціоновані зміни, непередбачені ризики, пов'язані з оновленнями, змінами в операційних системах, програмах, конфігураціях, сумісності та обладнанні, які можуть виникати в системах промислової автоматизації та управління або відповідних промислових процесах.

Фактор загрози - це термін, який використовується для опису суб'єкта, який може становити загрозу для системи. Сюди входять як зловмисники, так і порушники, такі як:

– довірена особа, працівник, постачальник, який має конфіденційну інформацію і може становити загрозу навіть без зловмисних намірів;

– особи або групи, які не мають офіційного доступу до системи.

Для вивчення загальних тенденцій в забезпеченні безпеки мережі, буде проведено аналіз корпоративної мережі з узагальненими характеристиками.

Більшість мережевих атак включають маніпуляції з використанням IP, такі як заміна IP-адреси хоста, встановлення неправильного маршруту, перехоплення інтервалу IP-адрес зловмисника та отримання інформації про логічну структуру мережі, таку як IP-адреси хостів та імена доменів, час ідентифікації IP, тощо.

Для запобігання таким атакам можна використовувати наступні стратегії:

– встановлення прив'язок портів IP-MAC для уникнення підміни IP-адрес та недозволених підключень до мережі, де основні методи реалізації цієї стратегії розглядалися на рівні каналу і описані в попередній статті циклу [19].

– використання технології перекладу мережевих адрес (Network Address Translation - NAT [20]) для приховування діапазону IP-адрес організації та логічної структури мережі від зовнішніх зловмисників.

– створення списків контролю доступу [21] для обмеження доступу до, протоколів, вузлів та служб рівня додатків.

1.3 Аналіз захищеності функціонування мережі

Зазвичай для оцінки рівня захисту необхідно розпочати з визначення поточного стану інформаційної безпеки. На сьогодні існує два основних підходи до оцінювання стану інформаційної безпеки, а саме "дослідження знизу вгору" та "дослідження зверху вниз".

У першому випадку адміністратори починають перевірку системи безпеки, проводячи власні тести на всі відомі типи атак. Таким чином, вони виконують роль зловмисників, що намагаються проникнути в захист інформаційних ресурсів. Однак зразу стає очевидним, що навіть найкращі адміністратори не можуть знати всі можливі методи атаки та використовуване хакерами програмне та апаратне забезпечення.

Підхід "зверху внизбазується на детальному аналізі всіх на сьогодні відомих схем зберігання та обробки даних. Спочатку ідентифікуються інформаційні ресурси та потоки захисту, після чого аналізується сучасний стан систем захисту інформації з метою визначення впроваджених методів захисту інформаційних ресурсів, а також їх стану та рівня. Потім всі потоки захисту та інформаційні ресурси класифікуються за рівнями відповідно до вимог до конфіденційності, доступності та цілісності.

Останнім етапом є "оцінка ризику", яка включає визначення розміру можливих збитків для організації внаслідок порушень захисту кожного конкретного інформаційного ресурсу. Приблизний ризик визначається як результат "можливого збитку від атаки" помножити на "імовірність такої атаки". Оцінка ризику включає аналіз ризиків та оцінку збитків.

Потім складається список переважних загроз та переліку вразливих місць для кожного інформаційного ресурсу, а потім обрахування ймовірності можливих загроз або атак. Згідно зі стандартом [22], загрози інформаційної безпеки можуть трактуватися двояко, наприклад: як умова використання вразливості ресурсу (в даному випадку вразливості і загрози ідентифікуються окремо); як загальна потенційна подія, яка може призвести до несанкціонованої спроби доступу до інформаційного ресурсу (коли можливість усвідомлення вразливості є загрозою).

Фактично, рівень захисту визначається як відношення ризиків у захищеній системі до ризиків у системі без захисту. Цей підхід дозволяє більш детально описати інформаційні ресурси, враховуючи їх вразливості та визначаючи цінність самого ресурсу. Також він дозволяє класифікувати ризики та інформаційні ресурси згідно з їхньою критичністю для організації.

Фактичний рівень захисту визначається як відношення ризиків у захищеній системі до ризиків у системі, яка не має налагодженого захисту. Цей підхід дозволяє провести детальний аналіз інформаційних ресурсів, враховуючи їхні вразливості та вартість, а також визначити пріоритети у відношенні ризиків та інформаційних ресурсів залежно від їхнього впливу на організацію [23].

Для здійснення оцінки безпеки запропоновано наступні кроки. На етапі аналізу загроз та оцінки ймовірності проводиться створення списку потенційних загроз. Оцінюється ймовірність виникнення цих загроз та ймовірність їхнього уникнення системою захисту. Також враховується вартість інформаційних ресурсів. Далі проводиться введення обмежень. При цьому встановлюються обмеження відносно витрат на створення системи захисту інформації та зниження продуктивності комп’ютерної інформаційної системи.

При побудові математичної оцінки рівня захисту застосовуються загальні математичні формули для визначення рівня захисту комп’ютерної інформаційної системи за запропонованими засобами. Далі проходить вибір оптимального варіанту,при цьому вибирається оптимальний варіант з розглянутих і оцінених, який найкраще відповідає визначеним критеріям і встановленим рамкам.

Характеристики, які визначаються індивідуально для кожної організації та не підпадають під державне регулювання, наразі не широко використовуються для оцінки ефективності з використанням інформаційно-орієнтованого підходу [24]. Однак цей підхід є перспективним для вивчення та використання великими підприємствами. На рисунку 1.3 представлена блок-схема процесу формування оцінки захищеності комп'ютерної системи.

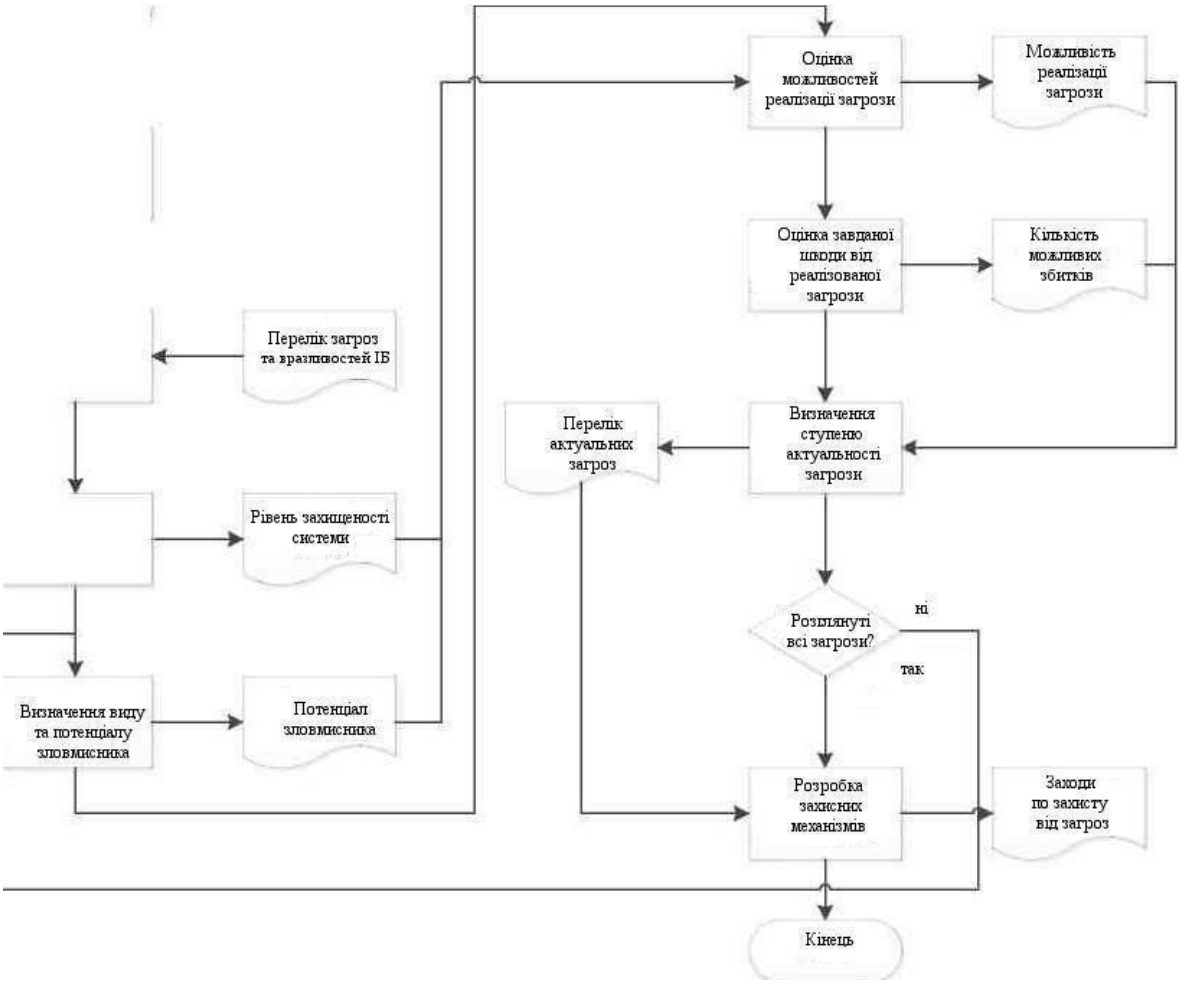


Рисунок 1.3 – Блок схема оцінки захищеності

Оскільки робота відповідно до даного алгоритму включає процес, що описаний циклом Демінга-Шухарта, на завершення впровадження захисних механізмів проводяться повторні та періодичні оцінки [25]. Недоліки цього процесу включають значну складність систематичної та регулярної переоцінки впливу загроз. Це обумовлено тим, що характер впливу загроз на інформаційно-

комунікаційні системи змінюється досить динамічно, і для ефективної оцінки потрібно враховувати всі зміни, як у переліках загроз, так і в поточній ситуації в сфері. На момент написання статті не відомо жодного програмного забезпечення, що автоматизує процес оцінки за даним методом.

Завдання оцінки ефективності інформаційно-комунікаційних систем може розглядатися як одне з ключових завдань у сучасній теорії дослідження операцій. З такого підходу можна визначити завдання оцінки ефективності такої системи як потрібно: за заданих вихідних умов потрібно визначити систему, яка є кращою за визначеним критерієм порівняно з еталонною системою [26, 13].

Результати оцінки та її практична цінність значною мірою залежать від вибору критерію та системи показників якості. Загальний підхід до розробки показників для складних систем включає формулювання численних локальних показників, які відображають сукупність властивостей системи, що впливають на виконання її завдань. Глобальний показник, який характеризує спільне, основне завдання інформаційно-комунікаційної системи, реалізується через включення оригінальних локальних.

Основними внутрішніми характеристиками інформаційно-комунікаційних систем є типи та рівень надання інформаційних послуг для користувачів. Графічне зображення взаємозв'язків між характеристиками системи та відповідними критеріями ефективності можна знайти на рис.1.4

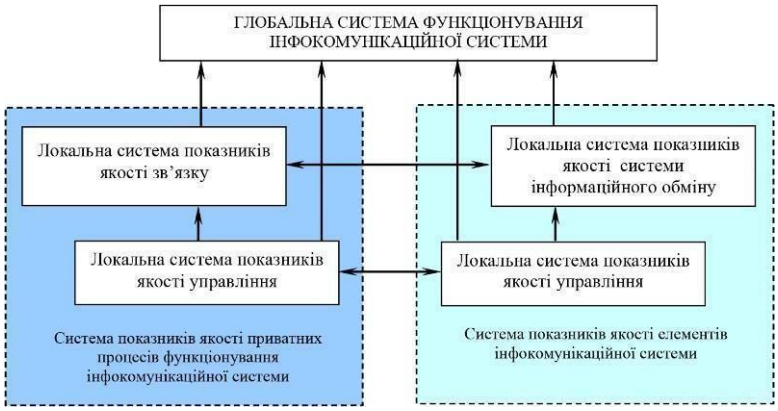


Рисунок 1.4 – Критерії якості в мережі

Детальне визначення загальної мети створення охоронної системи об'єкта замовника представлено через набір чинників або критеріїв, які конкретизують цю мету. Цей набір чинників є основою для формулювання вимог до системи та вибору оптимальних альтернатив.

Під час оцінки інформаційної системи важливо визначити її ресурси та чітко відокремити ці ресурси від зовнішніх елементів, які взаємодіють з системою. Ресурсами можуть бути враховані комп’ютери, програмне та апаратне забезпечення, а також дані. Зовнішні елементи, такі як мережі зв'язку, представляють собою додаткові фактори в цьому аналізі.

Визначення взаємозв’язків між ресурсами стає основою для створення загальної моделі інформаційної безпеки організації, що відображає її структуру та взаємодію компонентів системи.

Принципи створення збалансованої системи інформаційної безпеки для організації включають визначення та впровадження системи розподілу інформації на визначені рівні доступу [27];

- системний аналіз та передбачення можливих загроз та перешкод для інформаційних ресурсів;
- розробка та впровадження умов, спрямованих на підвищення безпеки інформаційних ресурсів;
- розробка ефективних механізмів та умов для оперативного реагування на загрози та проведення відновлювальних робіт у короткі терміни;
- створення механізму та засобів для максимально можливої компенсації та локалізації загрози;
- розробка ефективних засобів для компенсації та локалізації загроз, що виникають внаслідок незаконних дій фізичних та юридичних осіб.
- розробка та впровадження механізмів для оптимального вибору контрзаходів;
- систематична оцінка ефективності заходів з метою їхнього вдосконалення та оптимізації.

На підставі побудованої моделі ви маєте можливість обґрунтовано вибрати систему контрзаходів, спрямовану на зниження ризиків до прийнятних рівнів. Невід'ємною складовою цієї системи повинна бути регулярна перевірка її ефективності, а також перевірка відповідності існуючого режиму захисту інформації політиці безпеки та сертифікації інформаційної системи (технології) відповідно вимогам визначеного стандарту безпеки.

У межах магістерської роботи розглядаються загрози інформаційної безпеки, спрямовані на обмеження доступності інформації в комунікаційних мережах [28, 31]. Зазначені загрози відповідають наступним критеріям:

- загроза інформаційної безпеки спрямована на порушення доступу до інформації;
- загроза орієнтована на вузли зв'язку, їх складові та телекомунікаційне обладнання, що розташоване на вузлах зв'язку;
- загроза інформаційної безпеки проявляється в рамках інфраструктури, яка використовується в конфіденційних комунікаційних мережах.

Зазначені критерії дозволяють об'єктивно визначити і проаналізувати загрози, що потенційно можуть вплинути на доступність інформації в розглядуваній конфіденційній комунікаційній мережі.

Обладнання вузла приймає інформацію від передавача, виконує конвертацію форматів переданої інформації, обробляє мережевий трафік, приймає рішення про напрямок подальшої передачі, і лише після цього передає дані одержувачу. У зв'язку з цим виникають затримки у передачі інформації на вузлі зв'язку. Характеристики цих затримок залежать від швидкодії обладнання, обсягу трафіку, який проходить через нього, а також видів операцій, що виконуються з інформацією. Процес обробки мережевого трафіку на вузлі зв'язку ілюстровано на рис. 1.5.

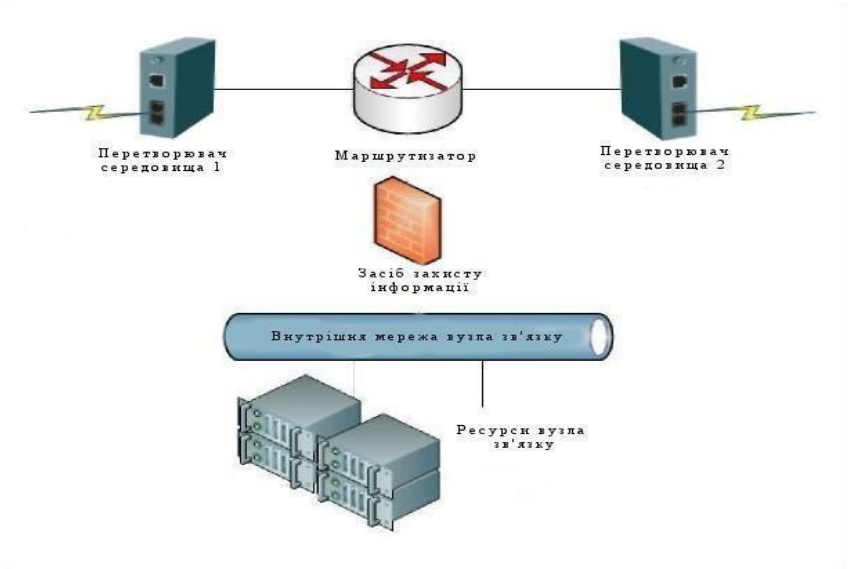


Рисунок 1.5 – Обробка трафіку на вузлі зв'язку

В залежності від свого місця розташування, вузол зв'язку може бути класифікований як транзитний або кінцевий. Транзитний вузол виступає посередником у мережі, керуючи передачею даних між іншими вузлами. Цей тип вузла зазвичай відповідає за направлення трафіку і визначення оптимальних маршрутів для ефективного переміщення інформації через мережу [32].

Великі виробники мережевого устаткування надають спеціалізовані рішення для вирішення завдань повного захисту корпоративних мереж. Один із прикладів таких рішень - технологія NAC від компанії Cisco [33]. Ця технологія дозволяє не лише проводити перевірку пристроїв та користувачів на етапі їхнього підключення до корпоративної мережі, але й блокувати доступ комп'ютерів, які не відповідають політиці безпеки, включаючи заражені вірусами та шкідливими програмами, системи, які не мають оновлених антивірусних баз, або які не отримали необхідні оновлення операційної системи.

NAC використовує мережеву інфраструктуру для контролю за виконанням політики безпеки на всіх пристроях, які намагаються отримати доступ до ресурсів мережі. Завдяки NAC підприємства можуть [34]:

– зменшити можливі втрати від загроз безпеки та регулювати права доступу користувачів до мережі;

– надавати мережевий доступ лише тим користувачам, які відповідають встановленим вимогам та використовують безпечні кінцеві пристрої (комп'ютери, сервери, КПК);

– обмежувати доступ до мережі для пристроїв, які не відповідають встановленим вимогам.

Пристрій контролю доступу в мережу (технологія NAC Appliance), що базується на продуктах лінійки Cisco Clean Access, забезпечує швидке розгортання з сервісами автономної експертизи на кінцевих вузлах, управління політиками та коректівні дії (рис 1.6).

Рисунок 1.6 - Cisco NAC Appliance

Архітектура контролю доступу в мережу (технологія NAC Framework), реалізована через Cisco Network Admission Control Program, поєднує інтелектуальну мережеву інфраструктуру з рішеннями від 75 і більше провідних світових розробників антивірусного програмного забезпечення і програмного забезпечення для забезпечення безпеки та управління.

Контроль відповідності політиці безпеки реалізовується максимально близько до джерела можливих порушень - на порту комутатора, точці доступу Wi-Fi або маршрутизатора, які підтримують технологію NAC.

1.4 Постановка задачі

Оцінка ефективності функціонування комунікаційних вузлів у цифровому вигляді становить значний внесок у підвищення об'єктивності та точності прогнозів стосовно впливу непрацездатності обладнання та загроз інформаційної безпеки. В результаті цього підвищується якість управління корпоративними мережами, забезпечуючи їх високий рівень надійності та стійкості.

У першому розділі розглянуті основні теоретичні аспекти, пов'язані з проєктуванням корпоративних мереж, організацією їх систем захисту та оцінкою ефективності функціонування. Для чіткої постановки завдань було проведено характеристику комунікаційних вузлів мережі та визначено властивості інформації, на які може впливати загроза ІБ. Сформулюємо основні завдання роботи:

1. Провести аналіз факторів, які впливають на ефективне функціонування вузлів мережі.
2. Дослідити доцільність використання математичного апарату теорії надійності для аналізу доступності вузла в умовах впливу атак на відмову в обслуговуванні
3. Розробити математичну модель надійності вузла мережі в умовах впливу атак на відмову в обслуговуванні устаткування.
4. Дослідити вплив загроз доступності інформації в мережі на її коефіцієнт готовності.
5. Удосконалити метод врахування загроз доступності інформації на коефіцієнт готовності вузлів мережі.
6. Розробити алгоритм підвищення ефективності комунікаційних вузлів в умовах хакерських атак.
7. Оцінити ефективність комунікаційних вузлів існуючих мереж, та досліджено їх придатність для корпоративних мереж, з використанням різних фізичних топологій.

2 МОДЕЛЬ НАДІЙНОСТІ ВУЗЛА КОРПОРАТИВНОЇ МЕРЕЖІ, З ВРАХУВАННЯМ ЗАГРОЗ

2.1 Математична модель стану вузлів

Отже, для визначення безпеки корпоративних мереж потрібно побудувати математичну модель, що дозволить аналізувати стан окремих вузлів та прогнозувати стан усієї мережі в цілому [35-37] .

Для побудови такої моделі необхідно:

1. Визначити набір можливих станів вузлів мережі та причини переходів між цими станами. Стани можуть відображати, наприклад, працездатність вузла, наявність загроз, режими роботи тощо.

2. Обрати ключовий показник, що характеризує безпеку мережі в цілому, наприклад доступність інформації.

3. Зібрати експериментальні дані про поточні стани окремих вузлів мережі. Це можна зробити за допомогою моніторингу мережевого трафіку, журналів подій, сканування вразливостей тощо.

4. Побудувати модель мережі у вигляді зваженого графа, де вузли відповідають пристроям, а ребра - з'єднанням між ними.

5. Розрахувати загальний показник безпеки мережі на основі станів окремих вузлів та топології мережі. Можна застосувати методи теорії ймовірностей, теорії графів, математичного моделювання.

6. Валідувати модель на реальних даних і за потреби допрацювати її.

7. Використовувати побудовану модель для моніторингу безпеки мережі та прогнозування її стану.

Для побудови моделі станів вузлів корпоративної мережі та аналізу їх впливу на мережу в цілому, необхідно спочатку визначити можливі стани, в яких може перебувати кожен окремий вузол, а також причини переходів між цими станами [38, 39]. Потім треба обрати ключовий показник стану всієї мережі, що залежить від станів окремих вузлів, та зібрати експериментальні дані про поточні

стани вузлів за допомогою моніторингу. Наступним кроком є побудова графа мережі, де вершини - окремі вузли, а ребра - зв'язки між ними. На основі цього графа та даних про стани вузлів розраховується значення обраного показника для всієї мережі.

Отримана модель використовується для аналізу впливу станів окремих вузлів на загальний стан корпоративної мережі, і при необхідності уточнюється шляхом додавання нових станів чи показників. Такий підхід дозволяє адекватно оцінити стійкість та надійність мережі в цілому. Такий підхід дозволить побудувати адекватну модель для аналізу стійкості та надійності корпоративної мережі.

Надійність - це властивість об'єкта виконувати задані функції, зберігаючи свої експлуатаційні показники в заданих межах протягом певного часу [40].

Надійність є комплексною властивістю, яка включає:

– безвідмовність - здатність об'єкта не допускати відмови протягом деякого часу;

– довговічність - здатність зберігати працездатність до настання граничного стану при встановленій системі технічного обслуговування;

– ремонтопридатність - пристосованість об'єкта до підтримання й відновлення стану, у якому він здатний виконувати потрібні функції;

– збережуваність - здатність об'єкта зберігати значення показників безвідмовності, довговічності і ремонтопридатності протягом і після зберігання та транспортування.

Оцінка надійності відбувається за допомогою ймовірнісних та статистичних методів на основі даних про наробіток об'єктів на відмову, інтенсивність відмов, час відновлення [41]. Надійність є важливою характеристикою якості технічних систем.

При аналізі надійності мережі необхідно розглянути її структуру та складові елементи. Спочатку потрібно визначити топологію мережі - з'ясувати, як з'єднані між собою її пристрої та лінії зв'язку. Далі слід зробити інвентаризацію

обладнання - маршрутизаторів, комутаторів, серверів, робочих станцій. Потрібно зібрати дані про їхні параметри надійності - середній час напрацювання на відмову, середній час відновлення після збою тощо.

На основі цих даних будується структурно-логічна схема надійності мережі з урахуванням резервування та взаємних зв'язків між компонентами. За допомогою методів теорії ймовірностей та надійності розраховуються кількісні показники - ймовірність безвідмовної роботи, коефіцієнт готовності, середній час простою.

Результати аналізу дозволяють виявити слабкі місця в архітектурі мережі, спрогнозувати ризики відмов і збоїв. На їх основі розробляються рекомендації щодо підвищення надійності - дублювання критичних ділянок, введення резервних шляхів передачі даних, використання надійнішого обладнання. Таким чином забезпечується безперервна та стабільна робота мережі.

Визначення надійності вузла мережі включає в себе аналіз його архітектурита складових компонентів [42].

По-перше, визначаються основні елементи вузла. Для кожного з них на підставі технічної документації чи статистичних даних встановлюються показники надійності - ймовірність безвідмовної роботи, середній час напрацювання на відмову, інтенсивність відмов.

Далі будується структурна схема надійності вузла з урахуванням резервування окремих компонентів та логічних зв'язків між ними. На основі цієї схеми за допомогою аналітичних методів обчислюється ймовірність безвідмовної роботи всього вузла.

Також аналізуються можливі режими відмови вузла та їх наслідки. Визначаються критичні елементи, відмова яких призводить до зупинки вузла.

За результатами аналізу розробляються рекомендації щодо підвищення надійності вузла - введення резервування, використання надійніших компонентів, оптимізації системи охолодження та живлення тощо.

Атака на відмову в обслуговуванні (DoS) або розподілена атака на відмову в обслуговуванні (DDoS) представляє собою спробу недоступності комп'ютерної

системи протягом певного часу для користувачів, для яких ця система була призначена [28]. Одним з найбільш розповсюджених методів здійснення атаки є насичення атакованого комп'ютера або мережевого обладнання значною кількістю зовнішніх запитань, часто є безглуздими або некоректно сформульованими. Метою такої атаки є перешкоджання здатності атакованого обладнання реагувати на запити користувачів або реагувати настільки повільно, що воно фактично стає недоступним.

Ці атаки націлені на завдання шкоди, забираючи доступ до ресурсів та послуг, які мають важливе значення для коректного функціонування системи. У багатьох випадках, атаки типу DoS та DDoS використовуються для перевантаження мережі чи сервера шляхом надмірного обсягу запитів, що призводить до втрати доступності для законних користувачів [43].

Досягнення ефективної захисту від таких атак включає в себе використання спеціальних технічних рішень, таких як вогнегасники атак, і механізмів виявлення та блокування несправедливого трафіку. Крім того, важливо вдосконалювати та регулярно перевіряти політику безпеки, забезпечуючи відповідність сертифікації інформаційної системи вимогам конкретних стандартів безпеки. Систематична перевірка ефективності застосованих контрзаходів та оперативна реакція на нові виклики є також важливими складовими впровадженої системи безпеки.

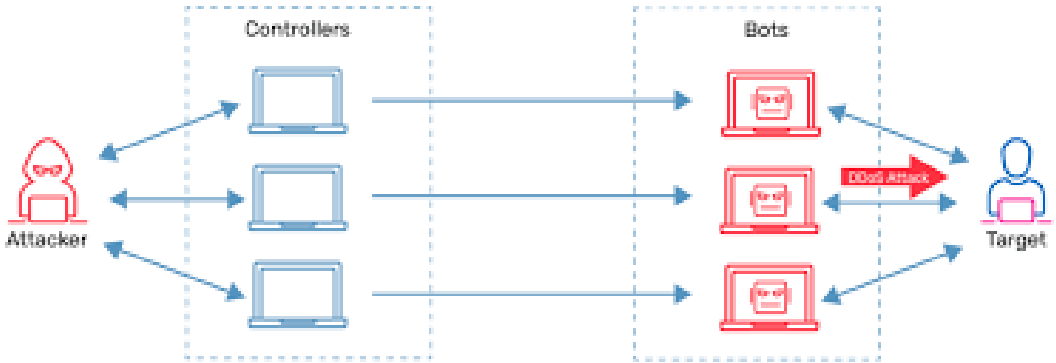


Рисунок 2.1 – DDoS атака

Взагалі відмова в обслуговувані може виникнути внаслідок кількох факторів:

- змушення атакованого устаткування припинити функціонування програмного забезпечення або витратити велику кількість наявних ресурсів, що перешкоджає йому у продовженні нормальної роботи;
- захоплення комунікаційних каналів між користувачами і атакованим устаткуванням, що призводить до втрати якості зв'язку і недоступності системи для законних користувачів.

Ця загроза виникає внаслідок спроби відмовити дискредитованій системі у доступі для законних користувачів шляхом спричинення лавини мережевих підключень до системи. Зауважимо, що успіх цієї загрози залежить від обсягу та частоти мережевих запитів, які порушник може згенерувати. Чим більше ця кількість, тим більша ймовірність успішної реалізації атаки на систему дискредитації [44].

Також, існує загроза впливу на технологічний виробничий процес через тимчасові затримки, які викликаються заходами захисту. Це пов'язано з тим, що кожен пристрій вузла зв'язку, через який проходить інформаційний потік, вносить затримку, що негативно впливає на характеристики сегмента мережі.

Додатково, існує загроза переведення системи в стан DoS або порушення нормального режиму через тимчасові затримки в системах реального часу. Це може бути викликано необхідністю обробки інформації, захищеної заходами безпеки, що призводить до перешкод у виявленні та нейтралізації загроз інформаційній безпеці.

DDoS-атаки можна класифікувати за обсягом трафіку на атаки з низькою та високою інтенсивністю. При атаках з низькою інтенсивністю зловмисник генерує трафік, схожий на законний, але який вичерпує певні ресурси, наприклад процесорну потужність. Натомість потужні DDoS-атаки відзначаються величезними обсягами трафіку, що є найпоширенішим їх типом.

Водночас великі обсяги трафіку можуть бути наслідком і раптового сплеску легальних запитів - того, що називають "натовпом користувачів". Це

явище часто хибно сприймається як DDoS-атака. Проте "натовп користувачів" можна відрізнити за швидким зростанням, а потім спадом кількості унікальних IP-адрес, тоді як при атаці їх кількість залишається високою. Прикладом "натовпу користувачів" є проблеми сайту https://vstup.edbo.gov.ua/ під час початку вступної компанії для абітурієнтівою

DDoS-атаки можна класифікувати залежно від того, чи надсилається шкідливий трафік безпосередньо до жертви або через проміжні системи.

При прямих атаках зловмисники використовують велику кількість заражених пристроїв для генерування навантаження, яке направляється на ресурс жертви.

В непрямих атаках цільова система не атакується напряму. Натомість створюється перевантаження на інших сервісах чи ланках мережі, від функціонування яких залежить робота ресурсу жертви. Прикладом є атаки на мережеве обладнання, які порушують зв'язність мережі і доступність сайтів. Такі непрямі DDoS-атаки складніше виявити та пом'якшити.

DDoS-атаки можна класифікувати за різними характеристиками трафіку, зокрема за динамікою зміни його інтенсивності.

Існують такі типи DDoS-атак залежно від швидкості трафіку [44]:

– з постійною швидкістю, де обсяг трафіку залишається приблизно однаковим протягом усієї атаки;

– зі зростаючою швидкістю коли інтенсивність трафіку плавно збільшується з часом;

– пульсуюча, де періоди сплесків високої активності чергуються з періодами затишшя;

– "підгрупами" - кілька хвиль атаки з різною інтенсивністю трафіку.

Окрім цього, DDoS можна класифікувати за такими ознаками: механізм атаки, повторюваність, об'єм трафіку, наявність посередників. Аналіз динаміки та характеристик дозволяє краще розпізнавати і відбивати атаки.

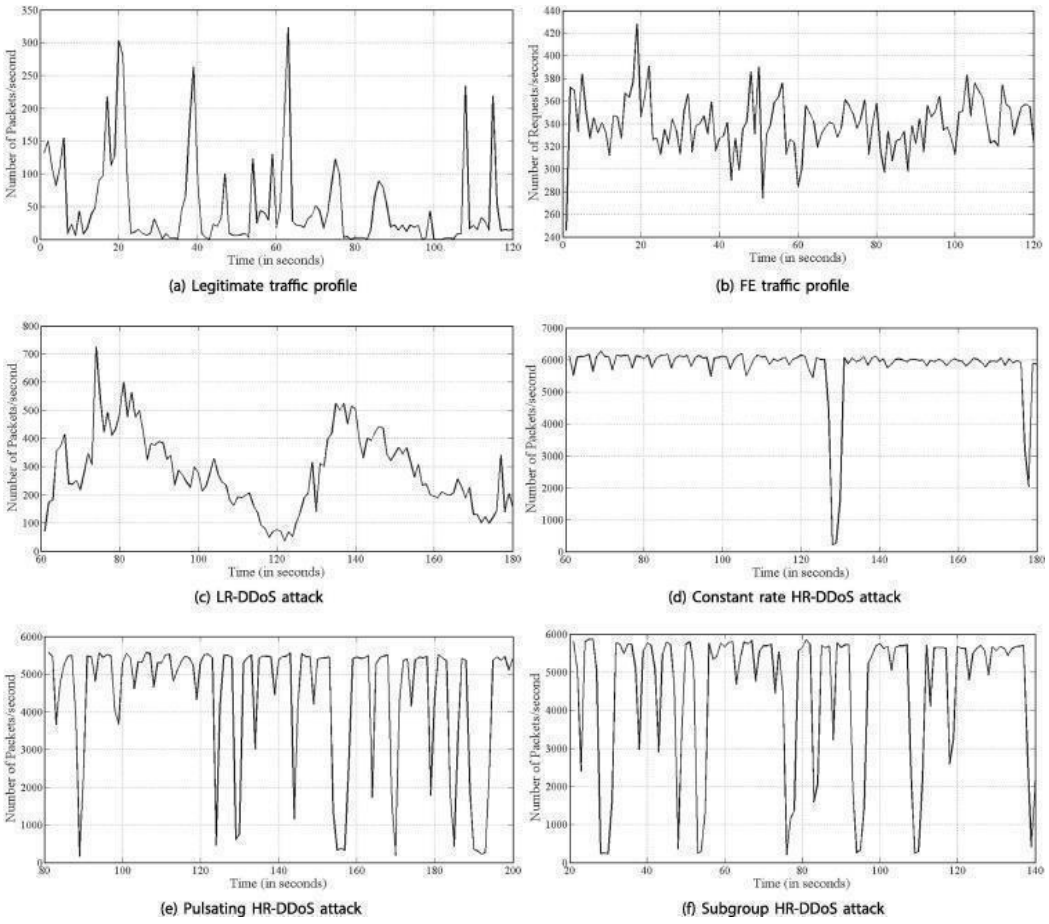


Рисунок 2.2 – Типи DDOS атака на основі динаміки

Визначення надійності вузла мережі в умовах DDoS атак має певні особливості. При аналізі архітектури вузла важливо приділити увагу компонентам, що забезпечують захист від DDoS, таким як firewall чи системи виявлення вторгнень. Необхідно дослідити їх стійкість до перевантажень і атак типу "відмова в обслуговуванні". Крім того, потрібно проаналізувати можливі сценарії DDoS атак на даний вузол - їх інтенсивність та наслідки.

В структурну схему надійності вузла вводиться додатковий фактор - ймовірність конкретної DDoS атаки. На основі цього розраховується ймовірність відмови вузла з урахуванням ефективності засобів захисту. За результатами аналізу пропонуються заходи для підвищення стійкості вузла до DDoS, такі як резервування каналів, використання хмарних сервісів захисту чи аналіз трафіку.

Такий підхід дозволяє оцінити живучість вузла під час цілеспрямованих атак і розробити рекомендації для підвищення його надійності.

Коефіцієнт готовності є одним з основних показників, що використовується для оцінки надійності систем.

Коефіцієнт готовності показує, яку частину загального часу система знаходиться в працездатному стані. Він розраховується як відношення середнього часу безвідмовної роботи системи до суми середніх часів безвідмовної роботи і відновлення після відмови.

При оцінці надійності складних систем типу комп'ютерних мереж коефіцієнт готовності розраховується окремо для кожного компонента. Потім за допомогою аналітичних методів визначається загальний коефіцієнт готовності всієї системи з урахуванням її структури.

Перевагою коефіцієнта готовності є те, що він враховує як надійність окремих елементів, так і швидкість їх відновлення. Це дозволяє оцінити реальну безперервність роботи системи загалом.

Коефіцієнт готовності широко застосовується при проектуванні систем для визначення необхідного рівня резервування компонентів. В процесі експлуатації він дає кількісну оцінку поточного стану системи з точки зору її надійності [45].

Коефіцієнт готовності послідовно з'єднаних вузлів розраховується по формулі (2.1)

$$Кг_{посл} = Кг_1 \cdot Кг_2 \cdot ... \cdot Кг_n. \quad (2.1)$$

де, $Кг_i$ – коефіцієнт готовності послідовних елементів.

Коефіцієнт готовності для паралельно з'єднаних вузлів вираховується (2.2) [45]:

$$Кг_{парал} = 1 - (1 - Кг) \cdot (1 - Кг_2) \cdot ... \cdot (1 - Кг_n) \quad (2.2)$$

де, $Кг_i$ – коефіцієнт готовності паралельних елементів.

Отже, спираючись на формули розрахунку ймовірності безвідмовної роботи та коефіцієнта готовності для послідовно та паралельно з'єднаних елементів, можна оцінити надійність складної мережі. Для цього її подумки розбивають на сукупність лінійних ланцюжків між пристроями, що генерують і споживають трафік.

Збираючи статистику про роботу пристроїв корпоративної мережі, можна визначити кількість їх відмов і час відновлення. Це дозволяє побудувати граф переходів між працездатним та неробочим станами, де параметри λ і μ характеризують відповідно інтенсивності виходу з ладу і відновлення роботи. На основі таких даних обчислюються показники надійності окремих пристроїв і мережі в цілому (рис 2.3).

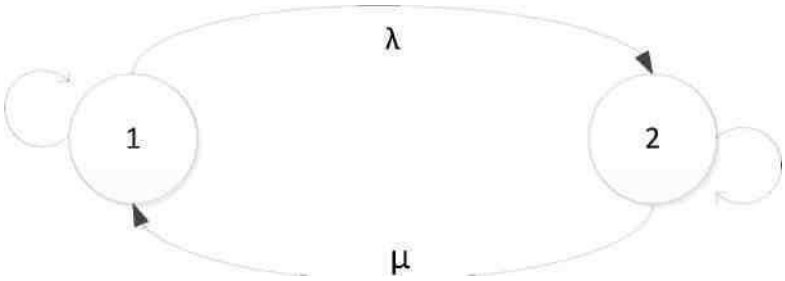


Рисунок 2.3 – Відображення вузла мережі у вигляді графу стану

Інтенсивність відмов обладнання корпоративної мережі можна розрахувати на основі статистики про кількість неробочих пристроїв за певний проміжок часу. Зокрема, інтенсивність відмов дорівнює відношенню кількості зіпсованих вузлів до добутку середньої кількості працюючих пристроїв на тривалість періоду спостереження:

$$\lambda(t) = \frac{n(t)}{N\text{ср} \cdot \Delta t}, \tag{2.3}$$

де, $n(t)$ – кількість пристроїв, в неробочому стані на певному інтервалі часу Δt,

Δt – довільний інтервал часу.

Nср – середня кількість пристроїв, в працездатному станію

Також для розрахунку можна скористатися ймовірністю того, що випадково обраний вузол виявиться неробочим. Цю ймовірність обчислюють через співвідношення середнього часу перебування пристрою у несправному стані до загальної тривалості періоду моніторингу.

Тоді інтенсивність потоку відмов розрахуємо за формулою (2.4):

$$\lambda(t) = \frac{N_0 \cdot a(t)}{N\text{ср}(t)}, \tag{2.4}$$

де N_0 –працездатні вузли;

(t) – середня імовірність пристрою в неробочому стані.

Середня імовірність виявлення вузла в непрацездатному стані обраховується по (2.5):

$$a(\Delta t) = \frac{n(\Delta t) \cdot t_в}{N_0 \cdot \Delta t}, \tag{2.5}$$

де, $n(t)$ – кількість пристроїв, в неробочому стані на певному інтервалі часу Δt;

N_0 –працездатні вузли;

$t_в$- середній час перебування вузла в неробочому стані;

Δt – довільний інтервал часу.

Враховуючи випадковий характер відмов обладнання корпоративної мережі, достовірно передбачити конкретну кількість працездатних вузлів на заданий момент часу неможливо.

Однак, спираючись на статистику попередніх спостережень, можна оцінити ймовірність того, що певна частка пристроїв функціонуватиме справно. Це дозволяє з достатньою точністю спрогнозувати середню частку робочих вузлів у майбутньому.

Крім того, аналіз факторів, які впливають на надійність окремих компонентів мережі - умов експлуатації, якості обладнання, регламентів технічного обслуговування тощо, - дає змогу вдосконалити модель та підвищити точність оцінок кількості працездатних вузлів.

Отже, незважаючи на випадковий характер відмов, їх імовірнісні моделі дозволяють прогнозувати надійність корпоративної мережі з прийнятною точністю (2.6).

$$N(\Delta t) = N0 \times (1 - \frac{n(\Delta t) \times t_в}{\Delta t}), \quad (2.6)$$

де $n(\Delta t)$ – кількість пристроїв, в неробочому стані на певному інтервалі часу;

$t_в$- середній час перебування вузла в неробочому стані;

Δt – довільний інтервал часу.

N_0 - кількість працездатних вузлів,

N_0 –працездатні вузли;

Отже, за наявності статистичних даних можна розрахувати середню кількість пристроїв корпоративної мережі, які перебуватимуть у працездатному стані протягом деякого майбутнього проміжку часу.

Це досягається шляхом аналізу інформації про попередню роботу окремих вузлів - частоту та тривалість їх відмов і відновлень. Комбінуючи ці дані загальною кількістю пристроїв в мережі, можна оцінити середню частку справних компонентів на заданий момент.

Крім того, додатковий аналіз факторів надійності, таких як умови експлуатації чи обслуговування обладнання, дозволяє вдосконалити прогнозну

модель. В результаті збільшується точність оцінювання кількості працездатних пристроїв мережі в майбутньому.

Таким чином, середню кількість пристроїв, що знаходяться в робочому стані буде визначено по (2.7):

$$Nср = \frac{N0+N(\Delta t)}{2}, \quad (2.7)$$

де t - середній час перебування вузла в неробочому стані який відповідає середньому час відновлення вузла.

Середній час відновлення працездатності вузлів корпоративної мережі можна визначити експериментально на основі статистичних даних.

Зокрема, шляхом спостереження за окремими елементами мережі фіксуються моменти виходу їх з ладу та поновлення роботи. Різниця цих значень і є часом відновлення конкретного пристрою після конкретної відмови.

Збираючи такі дані стосовно багатьох вузлів і відмов протягом тривалого періоду, обчислюється середнє значення часу відновлення для цього типу обладнання.

Додаткова інформація про особливості ремонту пристроїв конкретної мережі також може враховуватися для уточнення розрахункових моделей.

Таким чином середній час відновлення працездатності вузлів корпоративної мережі, $t_в^-$ визначається за формулою (2.8):

$$\bar{t} = \frac{1}{i}\int_i^1 f(i), \quad (2.8)$$

де $f(i)$ - функція розподілу часу, необхідного на відновлення;

i - кількість відновлених вузлів в інтервалі часу.

Для розробки моделі надійності вузла корпоративної мережі з урахуванням загроз потрібно врахувати наступні рекомендації:

– визначити основні елементи вузла мережі та їх параметри надійності, ймовірності відмов, час відновлення тощо;

– виділити критичні елементи, відмова яких призводить до відмови всього вузла;

– побудувати структурну схему надійності вузла з урахуванням резервування та взаємозв'язків між елементами;

– визначити можливі загрози - DoS атаки, вторгнення в мережу, пошкодження програмного забезпечення тощо;

– оцінити вплив загроз на параметри надійності окремих елементів та системи в цілому;

– побудувати модель надійності вузла із застосуванням марківських процесів, блок-схем або інших методів;

– врахувати в моделі можливі стани вузла, ймовірності переходів між ними та вплив загроз;

– перевірити адекватність моделі за допомогою імовірнісного моделювання чи порівняння з реальними даними;

– використати модель для аналізу надійності вузла та вибору оптимальних заходів щодо підвищення його стійкості до загроз.

Така модель дозволить комплексно оцінити надійність вузла корпоративної мережі з урахуванням ймовірних кібератак та інших загроз його функціонуванню.

Імовірність безвідмовної роботи вузла в момент часу t визначається за формулою (2.9):

$$P(t) = e^{-\lambda \times t}, \tag{2.9}$$

де t - момент часу, в який обраховується імовірність відмови;

λ – інтенсивність можливого потоку відмов.

Миттєвий коефіцієнт готовності пристрою корпоративної мережі має простий фізичний зміст - він являє собою ймовірність того, що цей пристрій в

заданий момент часу працюватиме справно, тобто не буде перебувати у стані відмови.

Іншими словами, на основі значення даного коефіцієнта можна оцінити, яка частка з певної сукупності однотипних пристроїв мережі функціонуватиме відповідно до своїх технічних характеристик в даний момент.

Такі ймовірнісні оцінки дають корисну інформацію для аналізу поточного рівня надійності мережі та розробки заходів щодо її підвищення з урахуванням ймовірностей відмов окремих компонентів (2.10):

$$\text{Кг}(t) = e^{-\lambda \times t}, \tag{2.10}$$

Відповідно середній коефіцієнт готовності на інтервалі з t_1 до t_2 обрахуємо за формулою (2.11):

$$\text{Кг} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} e^{-\lambda \times t} \, dt, \tag{2.11}$$

Оскільки достовірних даних про частоту та тривалість кіберзагроз недостатньо, однозначно стверджувати про певний закон розподілу цих загроз не можна. Тому використання експоненціального розподілу для оцінки впливу загроз на доступність інформації вимагає додаткових обґрунтувань.

Зокрема, необхідно здійснити аналіз наявних даних про конкретні кібератаки на різні мережі, виявити закономірності та особливості їх повторюваності й тривалості. На підставі емпіричного аналізу можна зробити аргументовані припущення щодо типу розподілу цих характеристик.

В подальшому доцільно розробити методику врахування впливу загроз на надійність вузлів, що ґрунтуватиметься на обґрунтованій ймовірнісній моделі кібератак. Це дозволить точніше оцінювати коефіцієнт готовності та аналізувати ризики порушення безперервної роботи мережі

2.2 Дослідження впливу резервування ліній зв'язку на коефіцієнт готовності

Резервування ліній зв'язку є ефективним способом підвищення надійності та безперервності роботи корпоративних мереж. Використання каналів резервування дозволяє забезпечити функціонування МЕРЕЖІ в разі відмов як основних каналів зв'язку, так і проміжних пристроїв, через які ці канали проходять.

При цьому слід розрізняти резервування каналів зв'язку та резервування мережевого обладнання. У першому випадку активується дублюючий фізичний канал для передачі даних. Наприклад, основне оптоволокно виходить з ладу, трафік перенаправляється на резервне.

У другому випадку задіюється резервний маршрутизатор, комутатор чи інший мережевий пристрій для забезпечення зв'язності мережі. Резервне обладнання має ту саму топологічну роль, але включається при виході з ладу основного.

Комбінація цих підходів дає максимальну надійність функціонування корпоративної мережі при виникненні відмов різного характеру.

Розглянемо вплив топології мережі на її надійність на прикладі деяких базових структур. Інші топології можуть бути досліджені за аналогічною методикою.

При цьому зосередимося саме на аналізі вузлів зв'язку, оскільки саме на активне мережеве обладнання можуть бути спрямовані кібератаки, що становлять загрози безпеці інформації. Пасивні компоненти, такі як кабельні лінії, не мають власних вразливостей, від яких залежить їхня працездатність.

Отже, дослідження впливу топології на надійність корпоративної мережі зводиться до аналізу стійкості різних варіантів структурно-логічних схем з'єднання окремих активних вузлів при реалізації кіберзагроз.

Згідно (2.1) і (2.2) коефіцієнт готовності мережі, з топологією «кільце» (рис. 2.4) для маршруту між вузлами 1 і 3 можна подати як (2.12).

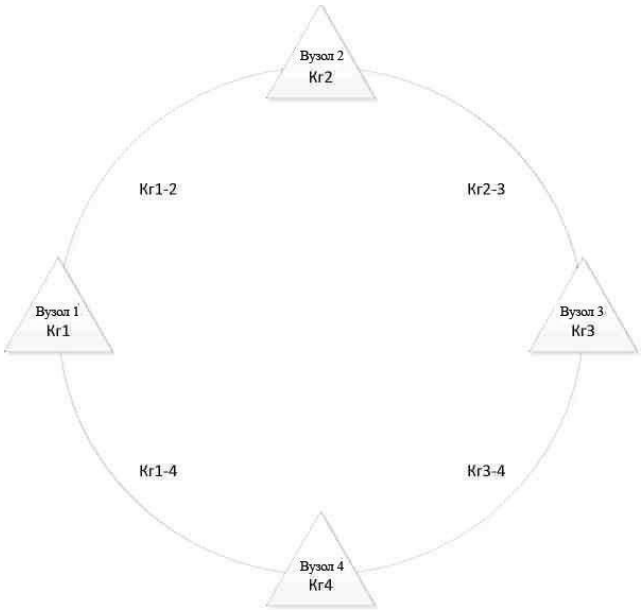


Рисунок 2.4 - Топологія «кільце»

$$\text{Кг}_{1-3}^{\text{Кільце}} = Fa_{\text{у}}^{2} \times (1 - (1 - Fa_{\text{р}}^{2} \times Fa_{\text{у}})^{2}), \quad (2.12)$$

Згідно (2.1) і (2.2) коефіцієнт готовності мережі, з топологією «кільце з горизонтальним резервуванням» (рис. 2.5) для маршруту між вузлами 1 і 3 можна подати як (2.13).

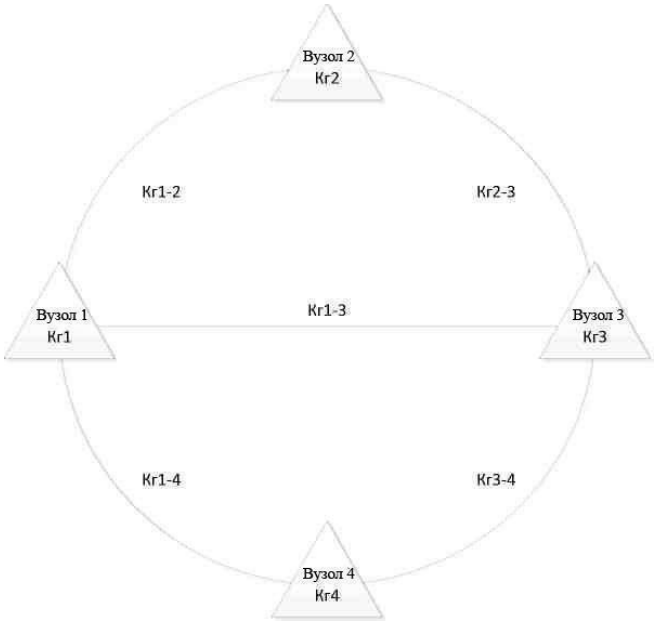


Рисунок 2.5 – Топологія «кільце з горизонтальним резервуванням»

$$\text{Кг}^{\text{К.ГР.}}_{1-3} = Fa^2_{y} \times (1 - (Fa^2_{\text{р}} \times Fa_{\text{у}})^2 \times (1 - Fa_{\text{р}})), \quad (2.13)$$

Згідно (2.1) і (2.2) коефіцієнт готовності мережі, з топологією «лінійна з додатковим резервним ребром та резервуванням ліній зв'язку» (рис. 2.6) для маршруту між вузлами 1 і 3 можна подати як (2.14).

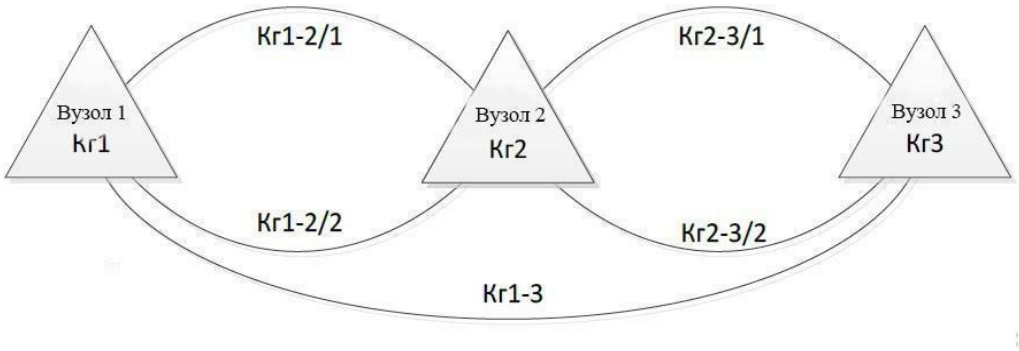


Рисунок 2.6 – Топологія «лінійна з додатковим резервним ребром та резервуванням ліній зв'язку»

$$\text{Кг}^{\text{2К.РР}}_{1-3} = \text{Кг}^2_{\text{у}} \times (1 - (1 - \text{Кг}_{\text{р}}) \times (1 - \text{Кг}_{\text{у}} \times (1 - (1 - \text{Кг}_{\text{р}})^2)^2)), \quad (2.14)$$

Отже, загальний коефіцієнт готовності для корпоративної мережі певної топології можна представити у вигляді функції від коефіцієнтів готовності окремих вузлів та ліній зв’язку між ними.

Вид цієї функції залежатиме від конкретного типу топології мережі - кільцевої, зіркової, ієрархічної тощо. Для різних структур існують свої формули розрахунку Кг через показники елементів, як от формули для послідовного та паралельного з’єднання.

Отже, провівши аналіз надійності окремих вузлів і каналів конкретної мережі, можна на основі її топології та відповідних залежностей розрахувати загальний коефіцієнт готовності мережі в цілому. Це дає кількісну оцінку безперервності надання нею сервісів.

Отже коефіцієнт формалізованої топології представимо як функцію від коефіцієнту готовності вузла мережі та її ребра (2.15)

$$Кг_{КМ} = f(Кг_р; Кг_в). \quad (2.15)$$

2.3 Оптимізація мережевих топологій

Оптимізація мережевих топологій є важливим етапом для підвищення ефективності функціонування мережі. Топологія мережі визначає спосіб, якими вузли і пристрої пов'язані один з одним у мережі. Нижче наведено кілька стратегій оптимізації мережевих топологій:

- визначення балансу між продуктивністю мережі та її надійністю;
- розгляд вимог до мережі, таких як пропускна здатність, завадостійкість та вартість розгортання;
- врахування типу даних та обсягу трафіку для вибору оптимальної топології (зірка, кільце, шина, дерево, сітка, гібридна топологія);
- місцезнаходження вузлів та обладнання з урахуванням фізичних особливостей приміщень;
- мінімізація довжини кабелів для зниження витрат та енергоспоживання;
- використання захисту від атак;
- захист важливих вузлів із важливою інформацією.

Для виконання аналітичних розрахунків та побудови графіка врахуємо змінний коефіцієнт готовності вузла зв'язку, який змінюється в межах від 0,99 до 0,9999 з кроком 0,00099, згідно з таблицею 2.1. Коефіцієнт готовності ребра мережі буде зафіксований на значенні 0,999 для стабілізації. Отримані результати розрахунків будемо вносити в таблицю для подальшого аналізу.

Таблиця 2.1 - Розрахунок коефіцієнту готовності формалізованих топологій з врахуванням коефіцієнту готовності вузла

$Кг_{в}$	Лінійна	Кільце	З резервуванням
0,99	0,968359	0,979959	0,98019
0,99098	0,971267	0,981943	0,982252
0,99186	0,974182	0,983926	0,984016
0,99293	0,977101	0,985809	0,985882
0,99386	0,980026	0,987893	0,987951
0,99582	0,985895	0,99186	0,991892
0,99673	0,988838	0,993744	0,993766
0,99791	0,991783	0,995828	0,995742
0,99881	0,994742	0,997912	0,99772
0,9999	0,997702	0,999796	0,9998

Побудуємо графік залежності (рис. 2.7).

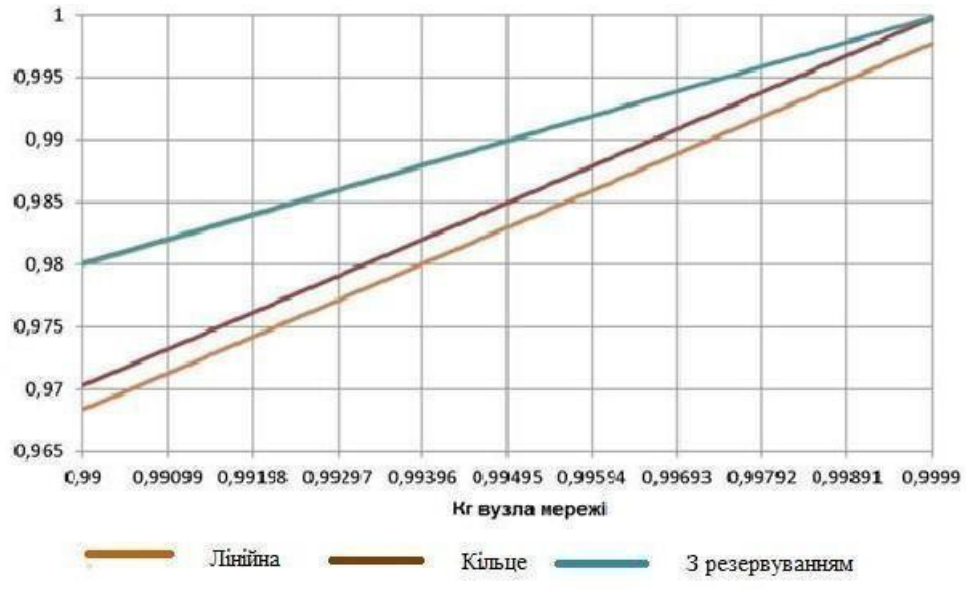


Рисунок 2.7 – Залежність коефіцієнту готовності формалізованих топологій від коєфіцієнту готовності вузла

Таблиця 2.2 - Розрахунок коефіцієнту готовності формалізованих топологій з врахуванням коефіцієнту готовності ребра

Кг $_p$	Лінійна	Кільце	З резервуванням
0,99	0,977162	0,997466	0,997989
0,99098	0,979118	0,997544	0,997990
0,99186	0,981175	0,997814	0,997992
0,99293	0,983034	0,997877	0,997994
0,99386	0,984896	0,997732	0,997995
0,99582	0,986859	0,997878	0,997996
0,99673	0,988923	0,997919	0,997997
0,99791	0,990791	0,99796	0,997998
0,99881	0,99286	0,997975	0,998000
0,9999	0,996804	0,998	0,998002

Побудуємо графік залежності (рис. 2.8).

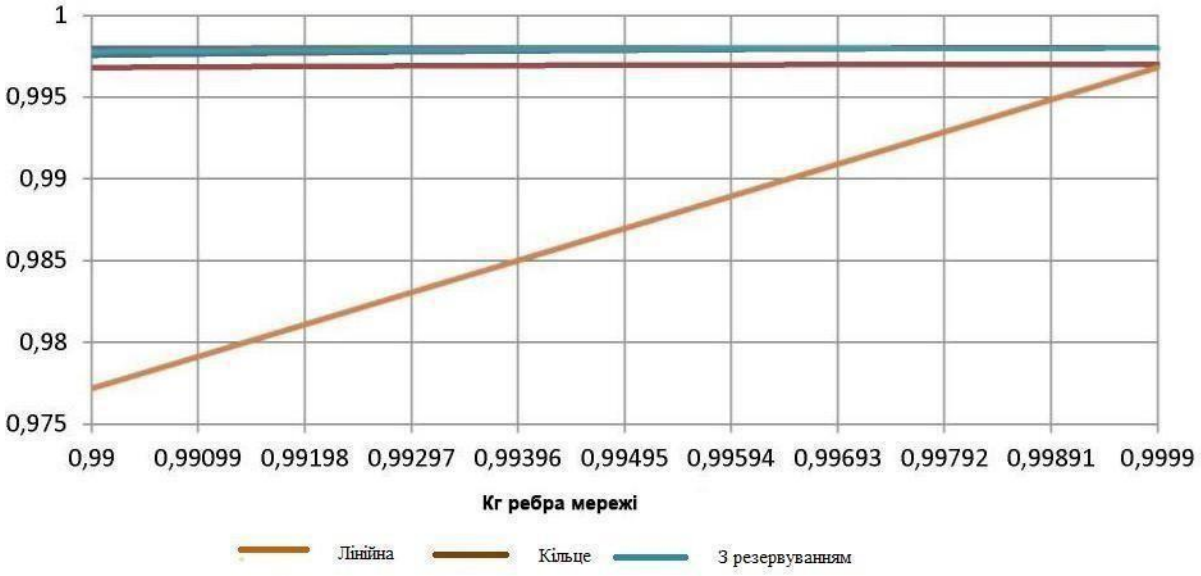


Рисунок 2.8 - Розрахунок коефіцієнту готовності формалізованих топологій з врахуванням коефіцієнту готовності ребра

Проаналізувавши ці графіки ми бачимо, що найбільша залежність коефіцієнта готовності ребра є у лінійної топології. Топології з резервуванням відображають майже лінійний характер залежності від коефіцієнта готовності ребра.

Проведене дослідження підтверджує той факт, що на коефіцієнт готовності формалізованої мережі найбільший вплив має коефіцієнт готовності вузла на відмінну від коефіцієнта готовності ребра.

Отже, це підкреслює актуальність магістерського дослідження. За результатами виявлено, що для забезпечення високих показників надійності корпоративної мережі ключовою є завдання з удосконалення надійності функціонування вузлів. Ця важлива висновок вказує на важливість дослідження та розробки стратегій для підвищення стійкості та ефективності інфраструктури мережі.

2.4 Висновки

У даному розділі проведено ретельний аналіз можливостей використання апарату теорії надійності для детального аналізу структурної надійності складних комп'ютерних систем. В якості ключового показника ефективності функціонування мережі та їхніх елементів обрано коефіцієнт готовності, який виступає нормованим показником надійності.

Була розроблена математична модель, яка детально визначає ймовірність перебування досліджуваного елемента в працездатному або непрацездатному стані, ураховуючи відмови технічних пристроїв. Основним елементом аналізу стала розрахункова формула для коефіцієнту готовності, яка функціонує як залежність від кількості відмов та періодів перебування вузла мережі в працездатному та непрацездатному стані.

Цей підхід дозволяє більш глибоко розуміти та оцінювати структурну надійність технічних комп'ютерних систем і визначити оптимальні стратегії для їхнього покращення.

Проведене дослідження підтверджує той факт, що на коефіцієнт готовності формалізованої мережі найбільший вплив має коефіцієнт готовності вузла на відмінну від коефіцієнта готовності ребра. Оскільки вплив DDoS атак також в основному спрямований на вузол зв'язку, питання розробки методу для оцінки та підвищення безпеки вузлів мережі є актуальним.

3 ДОСЛІДЖЕННЯ ВПЛИВУ АТАК НА ВІДМОВУ В ОБСЛУГОВУВАННІ НА ХАРАКТЕРИСТИКИ МЕРЕЖІ

3.1 Вплив DDoS-атак на коефіцієнт готовності вузла мережі

27 січня 2023 року компанія Qrator Labs, що спеціалізується на забезпеченні доступності інтернет-ресурсів та нейтралізації DDoS-атак, представила статистику DDoS-атак та BGP-інцидентів у 2022 році [49]. За інформацією компанії, 2022 став не просто рекордним, а безпрецедентним за кількістю DDoS-атак та їх інтенсивності. Мінімальні показники останніх місяців минулого року були на порядок вищими від значень на початку року.

Реальне зростання числа атак спостерігається в державному секторі, страхуванні, букмекерських конторах, банках, онлайн сервісах (рис.3.1).

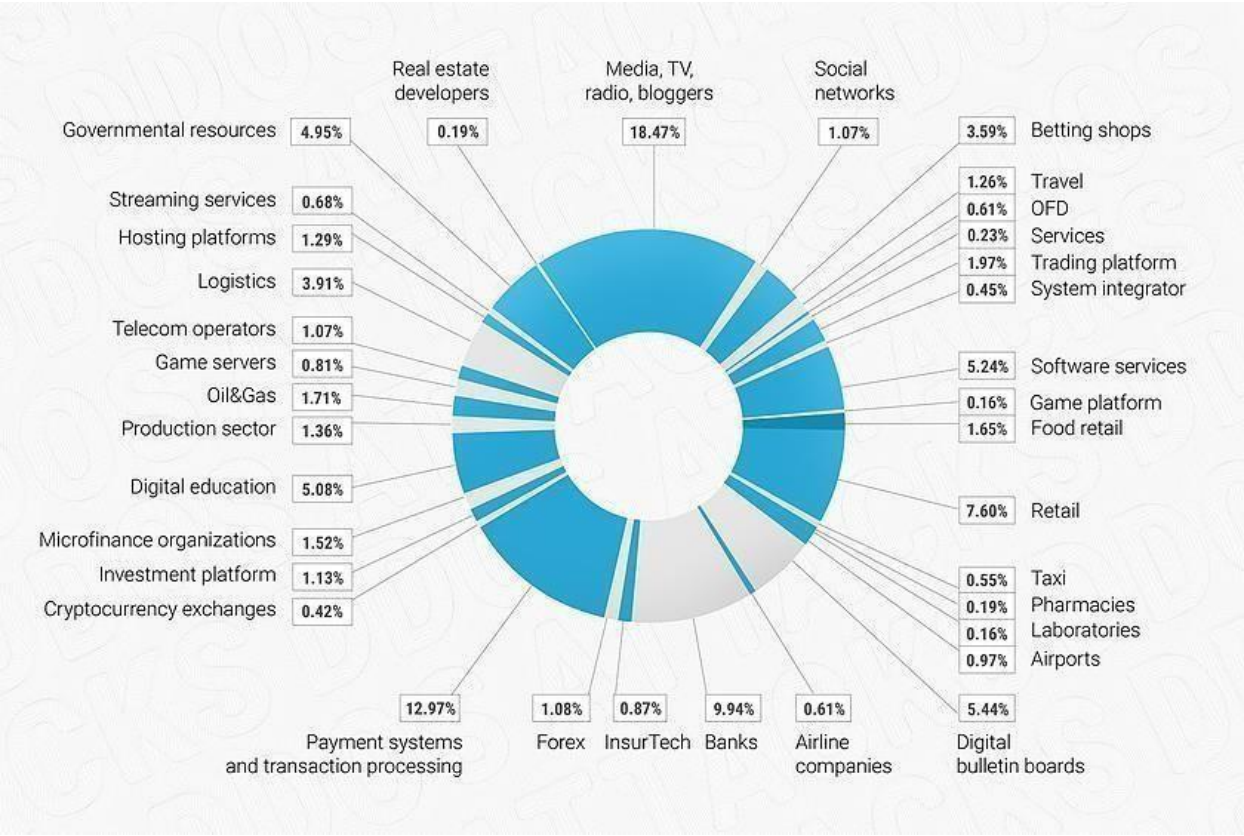


Рисунок 3.1 – Статистика DDoS-атак у 2022 р

DDoS-атака стала б неможливою без масового захоплення десятків тисяч пристроїв, що розташовані по всьому інтернету. Ці пристрої, без відома їх власників, стають знаряддям для відправки безглуздих запитів на вибрані зловмисниками сайти. Зазначено, що у останній час все частіше до цієї категорії пристроїв належать різноманітні пристрої Інтернету речей (IoT), такі як IP-камери, онлайн-каси, Wi-Fi-маршрутизатори та інші. Ці пристрої потрапляють під контроль зловмисників і стають часткою ботнету, який використовується для проведення масштабних DDoS-атак.

Список вразливих пристроїв можна також знаходити на сайті shodan (рис. 3.1). Варто зауважити, що цей список не є повністю актуальним і оновлюється з певною затримкою. Також, не завжди він може бути абсолютно точним через обмежену можливість негайного виявлення нових вразливостей. Тим не менш, цей ресурс надає приблизну картину ситуації і може бути важливим інструментом для виявлення потенційно небезпечних пристроїв, що можуть використовуватися для організації DDoS-атак та інших кіберзлочинних дій.

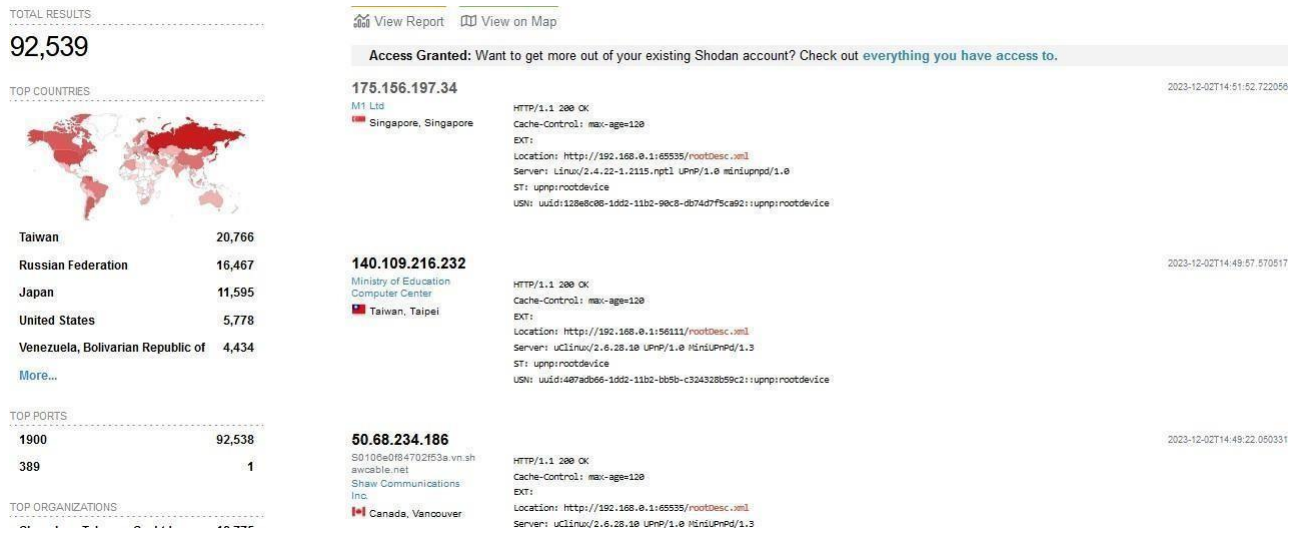


Рисунок 3.2 – Виявлення вразливих пристроїв за допомогою сервісу Shodan

За допомогою shodan можна визначити відкриті мережеві порти, служби та програмне забезпечення, що працює на підключених пристроях. Це дозволяє визначити ризики та вразливості в мережах та пристроях, допомагаючи впроваджувати заходи забезпечення та захисту.

Щодня в світі реєструється тисячі кібератак. Компанія Check Point розробила онлайн-карту DDoS-атак, яка надає можливість відстежувати активність в реальному часі [50]. За допомогою цієї картографії можна переглядати інформацію про те, між якими країнами зараз відбуваються атаки, визначити галузі, які найбільше піддаються удару хакерів, а також дізнатися кількість DDoS-атак за поточний день.

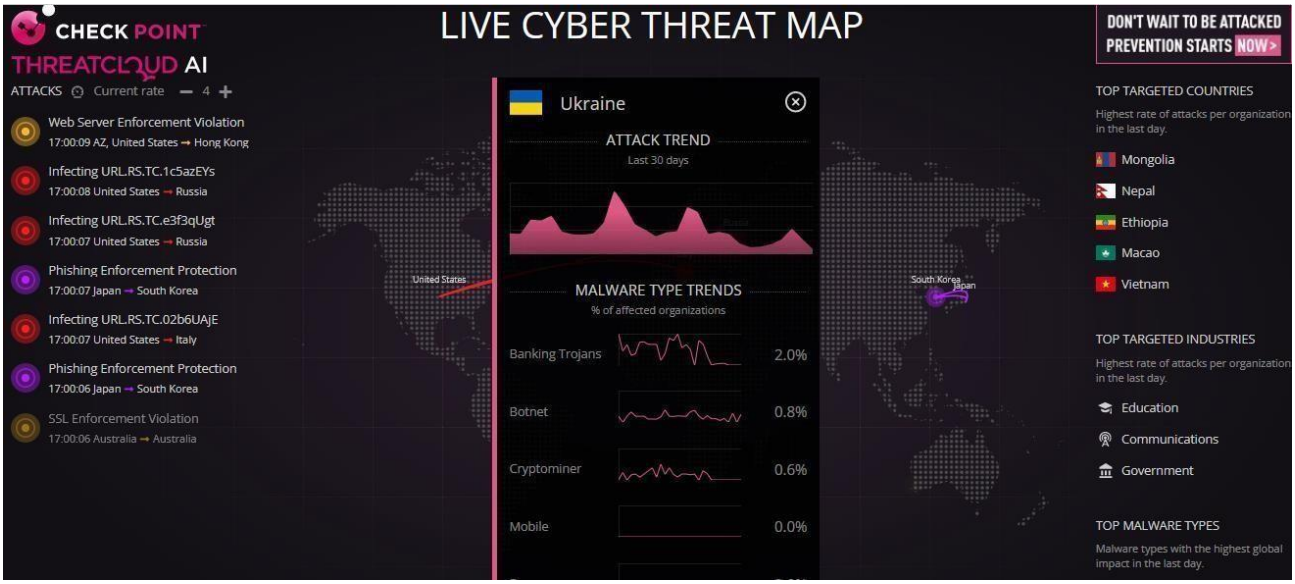


Рисунок 3.3 – Онлайн-карта DDoS-атак

Оцінка ефективності функціонування базується на порівнянні коефіцієнту готовності, розрахованого для різних варіантів. Кожен з цих варіантів відображає потенційний стан вузла зв'язку та встановленого на ньому обладнання. Аналіз мережі для кожного варіанту надає глибокий інсайт у можливості оптимізації надійності та стійкості мережі.

Цей підхід дозволяє визначити та порівняти рівень готовності для різних конфігурацій вузла зв'язку та інфраструктури, що допомагає здійснити вибір оптимального варіанту. Оцінка ефективності дозволяє точно визначити, як вибрані конфігурації впливають на загальну надійність та доступність мережі.

1. Коефіцієнт готовності мережі визначається, не враховуючи впливу на рівень безпеки мережі.

2. Коефіцієнт готовності мережі обчислюється з урахуванням впливу, проте без врахування застосування засобів захисту інформації.

3. Коефіцієнт готовності мережі визначається з врахуванням впливу загроз на рівень безпеки та ефективність застосування засобів захисту інформації.

Кожен елемент характеризується своїм власним коефіцієнтом готовності. Крім того, встановлено, що трафік пройде послідовно через всі пристрої вузла зв'язку мережі, які беруть участь у взаємодії. Цей підхід до оцінки включає аналіз готовності кожного окремого елемента та його впливу на процес передачі трафіку в мережі. При цьому передбачено, що інформаційний обмін в мережі відбувається за умови послідовного проходження трафіку через всі задіяні пристрої вузла зв'язку. Це дозволяє враховувати ефективність кожного компонента в системі та визначати загальну готовність мережі для оптимального обміну інформацією.

Таким чином, коефіцієнт готовності вузла мережі на основі (2.1) буде:

$$Кг_у = Кг_1 \times Кг_2 \times ... \times Кг_n, \quad (3.1)$$

де $Кг_1 ... Кг_n$ – коефіцієнти готовності мережних пристроїв.

Зазначений підхід до оцінки включає у себе детальний аналіз готовності кожного конкретного елемента вузла зв'язку, де в ролі елементів виступають пристрої, які функціонують на рівнях 1-3 еталонної мережевої моделі OSI [51].

На кожному з цих рівнів відбувається обмін інформацією, і кожен пристрій, що бере участь у вузлі зв'язку, має свій власний коефіцієнт готовності. Цей коефіцієнт враховує функціональність, доступність та надійність кожного пристрою на відповідному рівні мережевої моделі.

При передачі трафіку кожен елемент вузла зв'язку обробляє інформацію та передає її на наступний рівень. Аналіз готовності кожного елемента на кожному рівні дозволяє визначити, наскільки ефективно відбувається обмін інформацією в мережі.

Цей підхід також передбачає, що трафік проходить через всі пристрої вузла зв'язку послідовно, забезпечуючи повністю інтегрований підхід до аналізу готовності та ефективності мережі на рівнях фізичної, канальної та мережевої взаємодії.

На фізичному рівні вузла зв'язку працюють пристрої, які вирішують основне завдання - забезпечення фізичного з'єднання мережевих пристроїв. Це може бути, наприклад, хаб, який просто об'єднує пристрої в одну локальну мережу, чи повторювач, який відновлює і підсилює сигнали для їх передачі на великі відстані.

На канальному рівні знаходяться пристрої, які керують передачею даних на рівні каналів зв'язку. Мережеві мости можуть об'єднувати дві локальні мережі, а мережеві комутатори ефективно пересилають пакети даних, враховуючи адреси пристроїв. Мережеві контролери доступу, такі як точки доступу Wi-Fi, забезпечують контроль доступу до мережі.

Мережевий рівень включає в себе маршрутизатори, які визначають оптимальний шлях для передачі даних між різними мережами. Мережеві файрволи використовуються для фільтрації трафіку та захисту мережі від небажаних доступів, тоді як проксі-сервери можуть обробляти запити і транслювати мережевий трафік.

Ці пристрої взаємодіють, створюючи вузол зв'язку, де кожен з них виконує свою унікальну роль у забезпеченні стабільної та ефективної роботи мережі. Їхні

функції охоплюють всі аспекти від фізичного з'єднання до ефективного обміну даними та забезпечення безпеки мережі.

Розрахунок коефіцієнта готовності цих вузлів будемо проводити за методикою описано в розділі 2.

Враховуючи, що події, які впливають на стан розглянутого вузла зв'язку в мережі, розгортаються за експоненціальним сценарієм, для оцінки ймовірностей безвідмовної роботи компонентів мережі ми використовуватимемо математичний інструментарій марківських випадкових процесів.

Марківський процес - це випадковий процес, в якому подальша поведінка системи після певного моменту часу залежить виключно від поточного стану системи і не залежить від її попереднього стану [52]. Це дозволяє моделювати експоненціальні характеристики подій в мережі, спрощуючи аналіз і визначення ймовірностей надійності елементів мережі.

В рамках дослідження вказаних питань можна виділити такі стани вузлів мережі:

- вузол мережі у стані готовності;
- стан неготовності через реалізацію кіберзагрози, метою якої є порушення доступності інформаційних ресурсів;
- стан неготовності вузла мережі через відмову обладнання.

Перехід між станами можна охарактеризувати імовірностями конкретних подій. Для математичного моделювання цього процесу зручно скористатися апаратом марківських ланцюгів чи системою диференціальних рівнянь Колмогорова для обчислення ймовірностей станів. На основі моделі можна аналізувати надійність вузла за умови певних впливів.

Граф станів вузлів мережі наведено на рис. 3.4.

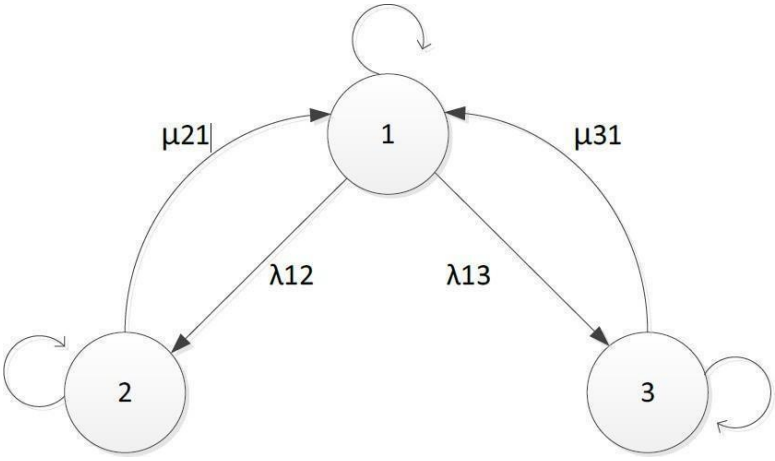


Рисунок 3.4 – Можливий граф станів вузлів

Математична модель процесу переходів між станами вузла, може бути описана за допомогою системи диференціальних рівнянь Колмогорова-Чепмена.

Ця система дозволяє обчислити ймовірності знаходження системи в кожному з можливих станів у довільний момент часу. Вона встановлює зв'язок між похідними цих ймовірностей та перехідними інтенсивностями процесу.

Розв’язуючи рівняння Колмогорова-Чепмена, можна простежити динаміку зміни ймовірностей різних станів вузла з плином часу. Це дозволяє детально проаналізувати його надійність з урахуванням імовірностей відмов та атак. Отримані результати можуть бути використані для подальшої оптимізації параметрів системи [53].

$$\begin{aligned} \frac{dP_1(t)}{dt} &= -(\lambda_{12} + \lambda_{13}) \times P_1(t) + \mu_{21} \times P_2(t) + \mu_{31} \times P_3(t) \\ \frac{dP_2(t)}{dt} &= \lambda_{12} \times P_1(t) - \mu_{21} \times P_2(t) \\ \frac{dP_3(t)}{dt} &= \lambda_{13} \times P_1(t) - \mu_{31} \times P_3(t) \end{aligned} \quad (3.2)$$

де $P_i(t)$ – імовірність знаходження вузла в одному з вище описаних станів;

μ_{21}, μ_{31} – інтенсивності відновлень вузла;

λ_{12}, λ_{13} – інтенсивності відмов вузла.

Враховуючи, що сума цих трьох імовірностей рівна 1, вирішивши систему рівнянь маємо формули ймовірності знаходження вузла в одному з станів:

$$P_1 = \frac{\mu_{21}+\mu_{31}}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}, \quad (3.3)$$

$$P_2 = \frac{\lambda_{12}+\mu_{31}}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}, \quad (3.4)$$

$$P_3 = \frac{\lambda_{13}+\mu_{21}}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}. \quad (3.5)$$

Отже, ймовірність безвідмовної роботи мережного пристрою, при умові впливу лише загроз інформаційної безпеки, визначає ймовірність того, що він не потрапить у стан неготовності через реалізацію загрози захищеності. Ця загроза спрямована на обмеження доступності інформації. Розрахунок цієї імовірності проводиться:

$$P_2 = \frac{\mu_{21}\times(\lambda_{13}+\mu_{31})}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}. \quad (3.6)$$

Для того, щоб загроза безпеці інформації призвела до порушення доступності вузла корпоративної мережі, мають статися та реалізуватися певні послідовні події.

По-перше, зловмисники повинні розробити та реалізувати комплекс технічних заходів для атаки на даний вузол. По-друге, наявні в системі засоби захисту інформації мають виявитися неефективними та не змогти запобігти чи нейтралізувати реалізацію загрози.

І по-третє, в результаті успішної кібератаки відбувається безпосереднє порушення працездатності вузла мережі на певний час, протягом якого він

перебуває у стані неготовності та не може виконувати свої функції відповідно до вимог.

Таким чином, лише за умови конкретизації та настання всіх трьох фаз можливий вплив кіберзагрози на доступність інформаційних ресурсів корпоративної мережі.

Тому потрібно визначити коефіцієнт неготовності (*Кнг*) вузла, що враховує вплив загроз захищеності мережі, які направлені на обмеження доступності інформації.

Коефіцієнт неготовності має складатися з трьох складових [34, 35]:

– $П_B$, імовірності виникнення загрози доступності вузлів зв'язку досліджуваної мережі;

– $П_P$, імовірності реалізації загрози доступності вузлів зв'язку, якахарактеризує недосконалість застосовуваних засобів захисту інформації;

– $Кнг^{П.В}$, імовірність викликаного реалізацією загрози, яка описує час, коливузол знаходиться в стані неготовності.

Загальна ймовірність настання трьох залежних подій:

$$Кнг_{В(i)} = П_B \times П_{P|B} \times Кнг^{П.В} \quad (3.7)$$

Коефіцієнт неготовності вузла визначається часом його перебування в неробочому стані внаслідок реалізації кіберзагрози. Наприклад, це може бути інтервал, необхідний для активації зовнішніх засобів захисту від DDoS-атак, якщо вбудовані механізми безпеки виявилися неефективними.

Для подальшого моделювання впливу DDoS-атак на надійність вузла розглядатимуться два сценарії:

– вузол має лише базові мережеві пристрої без спеціалізованих рішень кібербезпеки;

– наявні додаткові засоби захисту інформації на базі маршрутизатора або окремого обладнання.

Аналіз обох випадків дасть уявлення про ефективність залучення додаткових систем безпеки для мінімізації наслідків атак та підвищення надійності функціонування мережевого вузла.

Маршрутизатор - це пристрій, який забезпечує маршрутизацію трафіку в комп'ютерній мережі на основі певних алгоритмів. Він працює на 3 рівні еталонної моделі взаємодії відкритих систем OSI [53].

На фізичному рівні маршрутизатор приймає та передає двійкові сигнали по фізичному середовищу передачі даних за допомогою мережевих інтерфейсів.

На канальному рівні відбувається упакування даних в кадри, адресація пристроїв, кодування та модуляція сигналів, контроль помилок.

Основна функція маршрутизації реалізується на мережевому рівні - тут відбувається вибір оптимальних шляхів для пакетів між вузлами мережі на основі алгоритмів маршрутизації.

Таким чином, саме на 3 рівні моделі OSI маршрутизатор приймає рішення про подальше спрямування трафіку для реалізації основної функції - маршрутизації.

Маршрутизатори Cisco мають такі ключові особливості:

- висока продуктивність, масштабованість, здатність обробляти великі обсяги трафіку без втрати пакетів за рахунок апаратного прискорення;
- гнучкість налаштування складних схем маршрутизації з використанням різних протоколів RIP, OSPF, BGP, маршрутизація на основі політики;
- підтримка резервування компонентів, оперативне перемикання на резерв без втрати сесій;
- вбудовані засоби мережевої безпеки: міжмережеві екрани, система запобігання вторгненням, VPN;
- можливість централізовано керувати розподіленими пристроями за допомогою єдиної платформи управління;
- інтеграція з хмарними рішеннями та сервісами Cisco;
- гнучке масштабування продуктивності мережі.

Саме ці можливості роблять маршрутизатори Cisco оптимальним вибором для побудови надійних корпоративних мереж будь-якого масштабу. Для забезпечення повноцінного захисту від атак типу DDoS на маршрутизаторах Cisco необхідно додатково придбати та активувати ліцензійний пакет Security Technology Package License. Цей пакет дозволяє використовувати розширені засоби та функціональність безпеки, спрямовані на виявлення та захист від DDoS атак, що може бути важливим аспектом для ефективного функціонування мережевого обладнання.

Маршрутизатори Cisco мають кілька можливостей для захисту від DDoS атак:

– обмеження швидкості вхідного трафіку (rate limiting) для запобігання перевантаженню;

– фільтрація трафіку за допомогою ACL (Access Control List) [54] для блокування пакетів з підроблених IP-адрес, непотрібних протоколів, портів тощо;

– використання технології Cisco Network Foundation Protection для ідентифікації та блокування DDoS атак в режимі реального часу;

– моніторинг стану ресурсів маршрутизатора - процесора, пам'яті, де при перевищенні порогів спрацьовують алгоритми захисту;

– можливість швидкого перенаправлення трафіку на резервні канали в разі перевантаження основних ліній зв'язку;

– застосування цих та інших функцій дозволяє ефективно протидіяти DDoS атакам безпосередньо на рівні мережевих пристроїв Cisco.

Для експеременту по дослідженню сегменту мережі використано таке програмне і апаратне забезпечення:

– ПК1, комп'ютер HP DC7800SFF: CPU Intel Core 9 2.53 GHz, 16 GB ОЗУ, Windows 11;

– ПК2, комп'ютер HP DC7700SFF CPU Intel Core 7 2.26 GHz, 16 GB ОЗУ, Windows 11;

– атакуючий ПК - сервер Сервер HP ProLiant DL380 Gen9 (24 SFF) 16 GB ОЗУ, LAN HP NC382i x2, ОС Debian Linux;

– PoE-комутатор H3C S5024PV3-EI-HPWR (LS-5024PV3-EI-HPWR-GL).

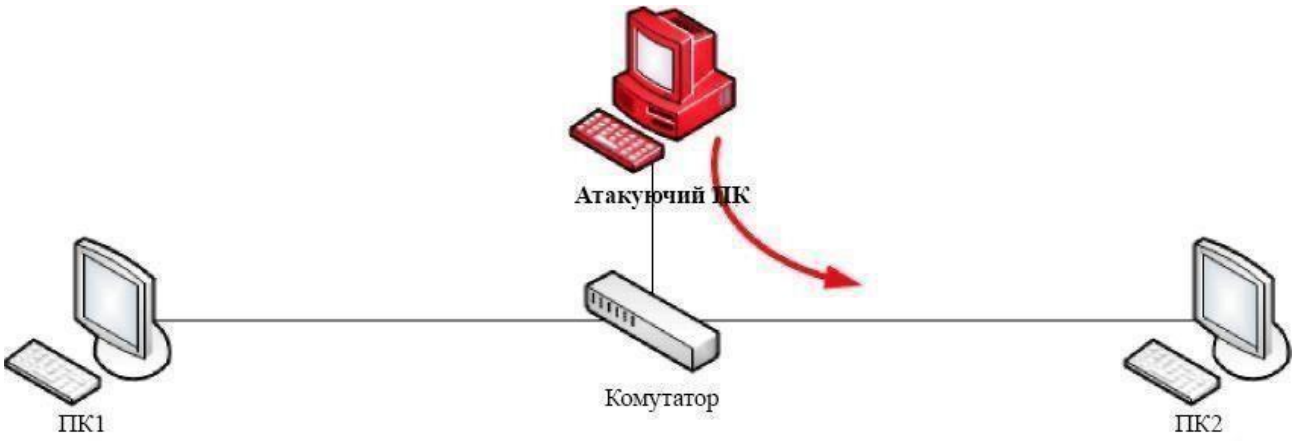


Рисунок 3.5 – Дослідження характеристик сегмента мережі

Таким чином, переходимо до пристрою, на якому встановлено операційну систему Windows, та відкрийте програму Wireshark. Після цього обираємо потрібний мережевий інтерфейс і розпочинаємо моніторинг, натискаючи кнопку "Пуск". Wireshark відобразить потік мережевого трафіку, який надходить з даного пристрою, інформацію щодо якого буде відображено на екрані, як показано на знімку екрану (рис 3.6).

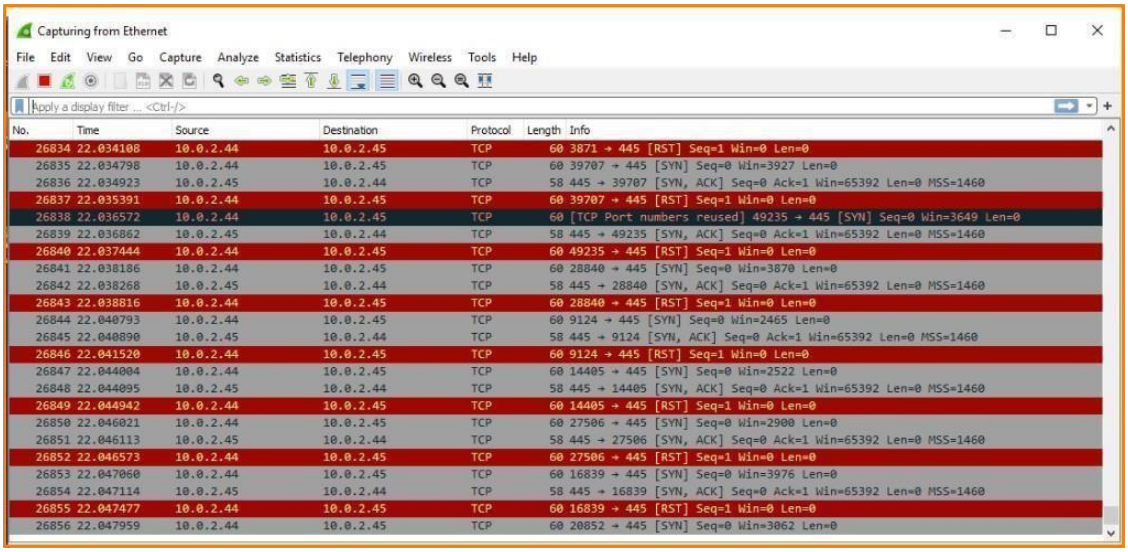


Рисунок 3.6 – Емуляція DDoS атаки за допомогою програму Wireshark

Hping - це відкрите програмне забезпечення для генерування мережевого трафіку та вимірювання його параметрів. Воно дозволяє оцінити затримки при проходженні пакетів через мережу.

Основні можливості Hping [55]:

- генерування TCP/IP пакетів різних типів (TCP, UDP, ICMP) з заданими параметрами (розмір, порти, прапорці);
- відправка трафіку з високою інтенсивністю для стрес-тестування мережі;
- вимірювання часу проходження (RTT) окремих пакетів в обидві сторони з точністю до мілісекунд;
- оцінка відсотка втрачених пакетів, їх порядку, затримок;
- аналіз відповідних пакетів і реакції мережевого обладнання (рис 3.7).

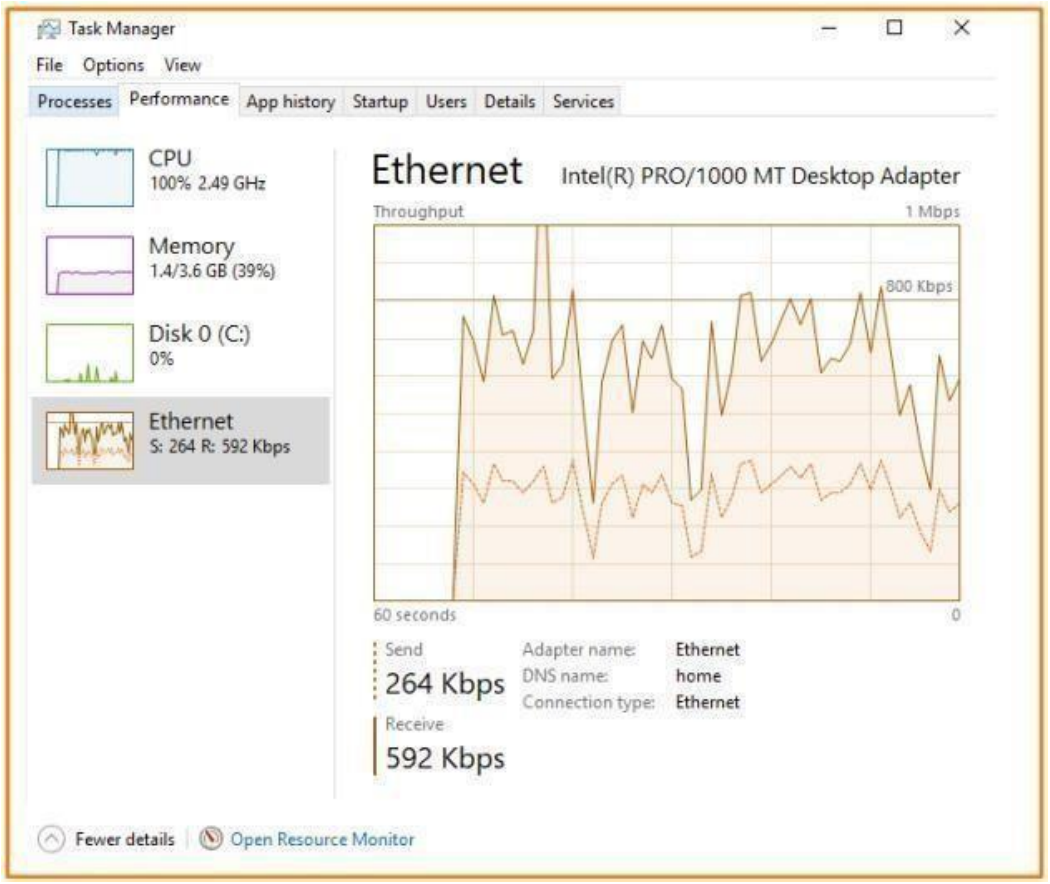


Рисунок 3.7 – Статистика Hping

Зібрана Hping статистика дозволяє проаналізувати якість обслуговування мережі та виявити вузькі місця, що впливає на затримки доставки даних.

Після ініціації програми, яка імітує DDoS атаку, відбувається замір часу відгуку та пікової пропускної здатності каналу зв'язку в умовах навантаження. Крім того, здійснюється підрахунок кількості втрачених пакетів, що не досягли адресата.

Для визначення граничного значення пропускної спроможності використовується спеціалізоване програмне забезпечення IPerf [56]. Воно дозволяє провести виміри максимальної смуги пропускання каналу при різних режимах навантаження та типах трафіку.

Аналіз цих показників у сукупності надає уявлення про якість обслуговування та стійкість лінії зв’язку до перевантажень в умовах, що імітують кібератаку.

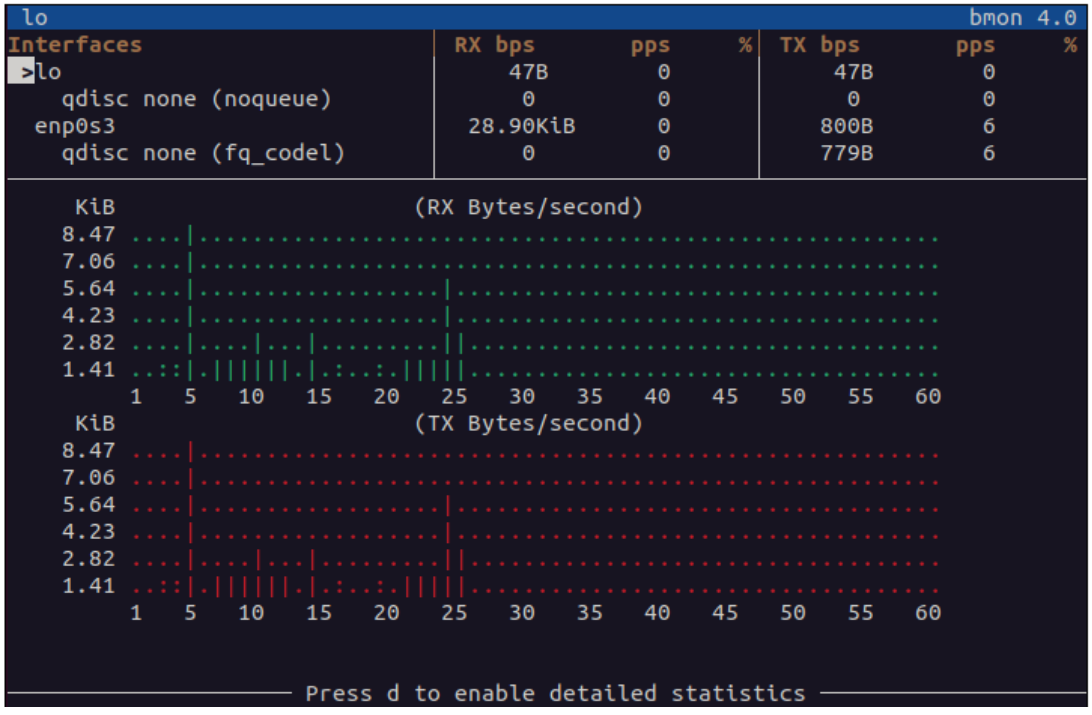


Рисунок 3.8 – Використання програмного забезпечення IPerf

Результати досліджень представлено в таблиці 3.1.

Таблиця 3.1 - Продуктивність сегмента корпоративної мережі

Тип	Час відгуку, мс	Втрата пакетів, %	Пропускна здатність, кбіт/с
Без загроз та без засобів захисту	0,149	0	938751 (100%)
Без загроз, з засобами захисту	0,448	1	895201 (94%)
DDoS - атака, без засобів захисту	0,172	29%	316216 (35%)
DDoS - атака з засобами захисту	7,966	0%	466768 (48%)

За підсумками проведеного моделювання DDoS атаки можна зробити такі висновки щодо її впливу на роботу мережевого вузла:

В умовах атаки відбувається істотне падіння пропускної здатності вузла, оскільки канал перевантажується надлишковим трафіком. Проте застосування засобів захисту інформації дозволяє запобігти повній відмові шляхом обмеження непотрібного трафіку.

Хоча характеристики вузла знижуються через додаткове навантаження, вдається забезпечити безперервне функціонування мережі на прийнятному рівні. Такі заходи захисту дають можливість уникнути виведення мережі з ладу зловмисниками.

Отже, наявність засобів протидії DDoS, навіть якщо вони не нейтралізують атаку повністю, значно підвищує стійкість роботи вузлів корпоративної мережі в умовах кіберзагроз.

3.2 Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

Для аналізу впливу кіберзагроз на працездатність вузлів корпоративної мережі можна застосувати кількісний метод оцінювання стану мережевих

пристроїв. Він дозволяє чисельно визначити ступінь відмови у роботі мережі внаслідок реалізації загроз порушення доступності інформаційних ресурсів.

Суть методу полягає в аналізі зміни таких показників як пропускна здатність вузлів, час затримки передачі даних, відсоток втрачених пакетів при моделюванні кібератак. Порівняння цих характеристик до та під час атаки дає уявлення про глибину впливу загроз на безперервну роботу мережі.

Такий підхід разом з подальшою оптимізацією параметрів систем захисту сприяє підвищенню стійкості мережі до ризиків порушення доступності внаслідок кібератак [57].

Метод оцінки захищеності мережі в умовах впливу DDoS-атак включає такі основні етапи:

– складається реєстр всіх пристроїв, сервісів, інформаційних ресурсів в мережі та зв'язків між ними;

– проводиться ретельний аналіз, який ідентифікує можливі типи DDoS-атак, які можуть вплинути на мережу, що включає аналіз трафіку, виявлення аномальних патернів та визначення потенційно вразливих точок;

– здійснюється сканування на предмет відомих вразливостей мережевих ОС, сервісів, програмного забезпечення, які можуть бути використані зловмисником;

– на основі моделей порушника аналізуються імовірні способи реалізації атак з використанням виявлених вразливостей;

– створюється реалістичний сценарій DDoS-атак, які можуть виникнути в конкретному середовищі, що дозволяє оцінити, наскільки добре мережа може витримати подібні атаки та які заходи безпеки виявляються найефективнішими;

– здійснюється аналіз ймовірності та наслідків потенційних атак, визначаються критичні вектори загроз;

– розробка рекомендацій щодо посилення захисту та зниження ризиків;

– впровадження систем моніторингу для постійного спостереження за трафіком та виявлення аномалій, та регулярне оновлення стратегій захисту відповідно до нових загроз та технологічних рішень.

Для забезпечення найвищого рівня захищеності ми використовуємо запропонований метод оцінки безпеки мережі.

На початку ми проводимо ретельний аналіз та ідентифікацію можливих типів DDoS-атак, які можуть вразити нашу мережу. Це дозволяє нам розуміти, які саме аспекти можуть бути під загрозою.

Далі ми вивчаємо, як наша мережа реагує на атаки, оцінюємо ефективність існуючих заходів безпеки та визначаємо, наскільки ми готові до різних сценаріїв атак. Це надає нам змогу розробити стратегії захисту, приділяючи увагу найбільш критичним аспектам нашої мережі.

Для більш точної підготовки до можливих атак, ми створюємо реалістичні сценарії, щоб переконатися, що ми готові до різноманітних викликів.

Основною частиною процесу є визначення та приділення пріоритетів заходів безпеки, фокусуючись на найбільш вразливих і критичних областях мережі.

Останніми етапами є встановлення систем постійного моніторингу та регулярне оновлення стратегій захисту відповідно до нових загроз та технологічних рішень. Все це спрямовано на створення стійкої мережі, яка може ефективно впоратися з DDoS-атаками та залишатися надійною в умовах зростаючих загроз.

Надаються конкретні заходи щодо підвищення стійкості мережі до загроз.

Такий аналіз має проводитися на регулярній основі для моніторингу захищеності мережі. Алгоритм оцінки захищеності мережі наведено на рис. 3.9.

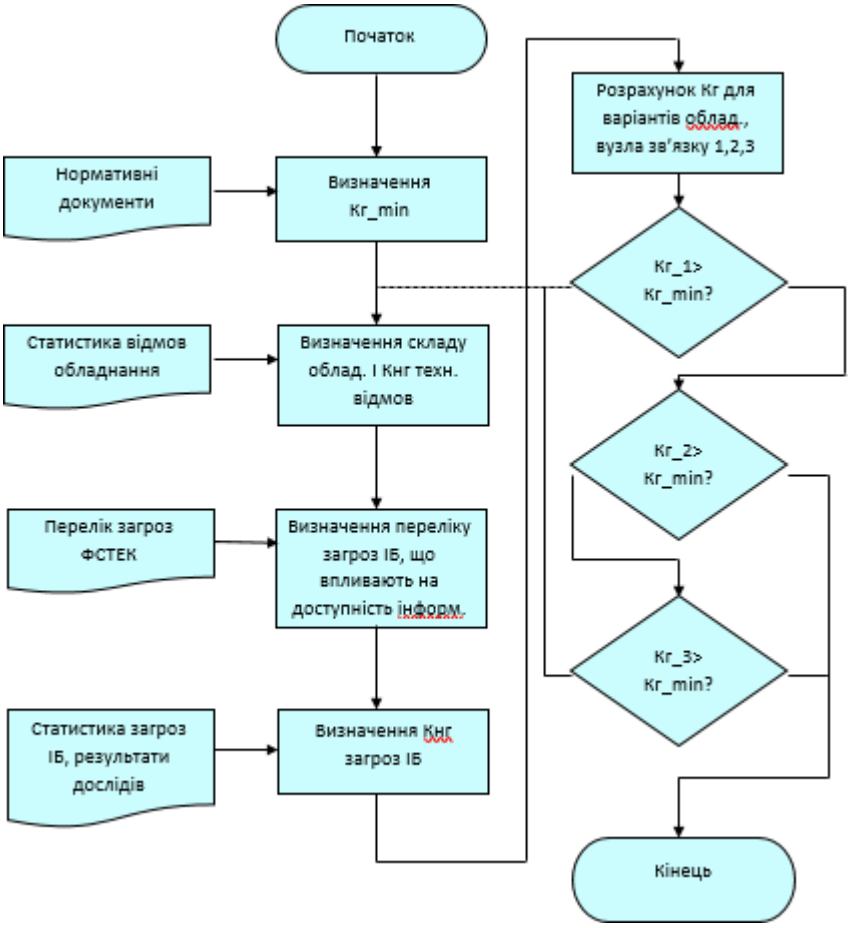


Рисунок 3.8 – Алгоритм оцінки захищеності мережі

1. На першому етапі встановлюється мінімально припустимий рівень готовності сегмента мережі, який відповідає нормативам комплексної системи захисту інформації.

2. Визначається склад обладнання вузлів мережі, і проводиться розрахунок коефіцієнта неготовності.

3. Відповідно до рекомендацій, сформульованих вище будується модель загроз інформаційної безпеки.

4. Розраховується коефіцієнт неготовності, враховуючи вплив загроз доступності інформації.

5. За допомогою методу повного перебору проводиться диференційний розрахунок коефіцієнту готовності усього досліджуваного сегмента мережі.

6. Здійснюється порівняння коефіцієнта готовності з граничним. У разі, коли результат менше заданого, переходимо до етапу 2, замінюючи обладнання, щоб відповідати критеріям захисту.

7. Аналізуються результати, використовуючи лише маршрутизатору без додаткових засобів захисту, щоб оцінити, чи маршрутизатор справляється з загрозами інформаційної безпеки.

8. Порівнюються результати при використанні маршрутизатора та додаткового засобу захисту інформації. Якщо значення *Кг_3* перевищує *Кг_min*, то обране рішення ефективно вирішує завдання.

3.3 Висновки

Використовуючи математичний апарат марківських процесів було створено граф станів вузла мережі, що визначає його працездатність в умовах впливу загроз безпеки. Математична модель ефективності вузла реалізована у вигляді системи рівнянь Колмогорова-Чепмена, яка враховує три стани вузла: готовність, неготовність та атакований стан впливу атак на доступність інформації. Крім того, розроблений метод дозволяє враховувати імовірність знаходження вузла мережі в різних станах, таких як готовність, неготовність та атакований стан впливу загроз ІБ, що забезпечує більш повний аналіз його функціонування в умовах небезпеки.

За результатами дослідження можна зробити деякі висновки щодо впливу DDoS-атаки на функціонування елементів мережі. Умови DDoS-атаки призводять до значного зниження пропускної здатності вузла мережі, що пояснюється самою природою таких атак. Проте, використання засобів захисту інформації на вузлі зв'язку дозволяє забезпечити неперервне функціонування мережі із зниженими, але прийнятними характеристиками.

Розроблений метод обрахунку ймовірності перебування вузла мережі в стані непрацездатності викликаного впливом загроз доступу до інформації. Робота методу промодельовано реальним експериментом. Згідно з цим методом,

ймовірність перебування вузла у стані неготовності представляє собою суму ймовірності загрози безпеки, ймовірності реалізації загрози, а також середнього часу перебування вузла в режимі неготовності.

Отримані в ході дослідження результати надають підставу вважати, що розроблений метод є ефективним і відповідно використовується для оцінки імовірності відмови вузла мережі в умовах впливу DDoS-атак та загроз безпеки інформації.

4 ПРАКТИЧНЕ ВИКОРИСТАННЯ ЗАПРОПОНОВАНОГО МЕТОДУ ДЛЯ ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Дослідження функціонування розробленого методу

Як вказано у третьому розділі, у межах розробленої моделі надійності вузол зв'язку досліджуваної мережі може перебувати у одному з трьох імовірних станів: працездатному, непрацездатному через технічні відмови обладнання, і непрацездатному через реалізації загроз інформаційної безпеки, направлених на порушення доступності інформації. Подальше дослідження включатиме аналіз ймовірностей та часу перебування вузла в кожному з цих станів для оцінки його надійності та стійкості.

Для апробації запропонованого методу врахування впливу загроз безпеці, спрямованих на порушення доступності інформації на ефективність функціонування мережі проведено дослідження на мережі Старосинявського відділення 10022/099 - Ощадбанк, Хмельницька область.

Була зібрана інформація щодо причин відмов та часу відновлення працездатності обладнання. Мережа використовує різноманітне обладнання, зокрема, маршрутизатори виробництва компанії Cisco, які забезпечують роботу всіх вузлів мережі без використання спеціалізованих засобів захисту від атак типу DDoS. Також проводилося дослідження ефективності застосування засобів захисту від DDoS-атак після активації додаткового ліцензійного пакета Security Technology Package License. Дослідження включало в себе оцінку реакції мережевого обладнання на навантаження, що характерне для DDoS-атак, як до, так і після впровадження зазначеного пакета.

Security Technology Package License (STPL) - це ліцензія, яка активує додаткові можливості безпеки на маршрутизаторах та комутаторах Cisco [58].

Використання STPL дозволяє отримати такі переваги:

– активація функцій брандмауера, фільтрації трафіку, VPN без необхідності придбання окремих пристроїв чи ПЗ;

– захист від атак шляхом аналізу трафіку та виявлення загроз в режимі реального часу;

– моніторинг стану пристроїв, систем оповіщення про інциденти безпеки;

– управління політиками безпеки на рівні всієї мережі з єдиної консолі;

– зниження витрат на побудову системи захисту мережі.

За допомогою STPL можливо швидко розгорнути комплексну систему кібербезпеки, що працює на рівні мережевого устаткування. Це суттєво підсилює захищеність корпоративних мереж від кіберзагроз. Орієнтовна вартість для окремих моделей маршрутизаторів, наприклад Cisco ISR 4000 - близько $300 за 1 пристрій.

Під час експериментів були враховані такі параметри, як пропускна здатність мережі, час відновлення працездатності після атаки, кількість втрачених пакетів та загальна стійкість мережі до DDoS -атак. Також вивчалася взаємодія між активованим захистом і різними типами DDoS-атак для визначення його ефективності у різних сценаріях.

Оскільки обладнання, що утворює канали зв'язку, функціонує на фізичному рівні моделі OSI, а маршрутизатори та засоби захисту - на мережевому, вважатимемо характеристики надійності каналоутворюючих пристроїв складовою показника готовності самої лінії зв'язку, а не окремого мережевого вузла. Такий підхід обґрунтований тим, що один вузол може обслуговувати декілька ліній, кожна з яких має власне обладнання. Отже, відображаючи відмову каналоутворювача як відмову відповідного каналу, підвищуємо точність розрахунків показників безперервної роботи мережі.

Розрахунок відповідних коефіцієнтів готовності, як з використанням спеціалізованого обладнання, так і без нього, здійснюється відповідно до методики, яка була представлена у пункті 2.3 магістерської роботи. Статистика про відмови маршрутизаторів, їх причину та час відновлення була зібрана та визначена шляхом проведення експериментів (рис 4.1).

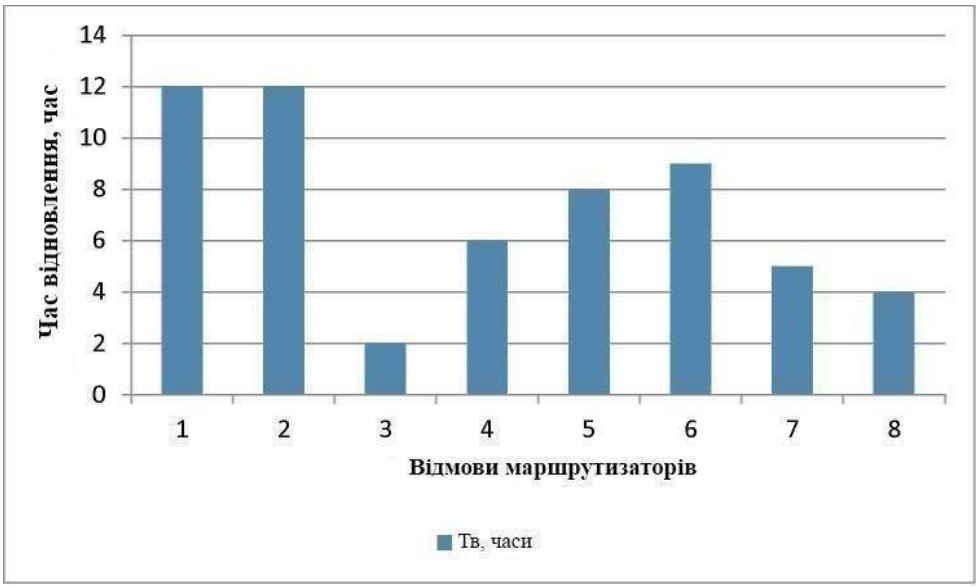


Рисунок 4.1 – Орієнтований час відновлення маршрутизаторів

Роз

Таблиця 4.1 – *Кнг*, визваний непрацездатністю обладнання

Склад обладнання	$K_{нг}^{(3)}$	λ
Маршрутизатор	0,000004	0,00000000019255
Маршрутизатор та засіб захисту STPL	0,0000143	0,00000000062892

У цьому контексті, загрози, що призводять до переходу системи в стан "відмова в обслуговуванні", та посилення впливу на обчислювальні ресурси користувачів за допомогою сторонніх серверів, об'єднані під загальним терміном "атака типу "відмова в обслуговуванні".

Таблиця 4.2 - *Кнг*, визваний впливом DDoS-атак

Склад обладнання	$П_В$	$П_{Р\|В}$	$Кнг_{п.в.}$	$K_{нг}^{(2)}$
Маршрутизатор	1	1	0,00063	0,00063
Маршрутизатор та засіб захисту STPL	1	0,1	0,00062	0,000062

4.2 Визначення чисельних значень коефіцієнта готовності вузла мережі

Розрахунок коефіцієнта готовності здійснюється для трьох різних сценаріїв:

1. Без врахування впливу загроз безпеки та без використання засобів захисту мережі.
2. З врахуванням впливу загроз безпеки, але без використання засобів захисту мережі.
3. З врахуванням впливу загроз безпеки та використання засобів захисту мережі.

Це дозволяє врахувати різні умови та фактори для оцінки ефективності готовності мережі в різних сценаріях.

Для першого випадку (без урахування впливу загроз та з одним маршрутизатором) коефіцієнт готовності ($K_г^{вузла(1)}$) розраховується за розраховується за формулою (4.1):

$$K_г^{вузла\,(1)} = \frac{1}{t_1 - t_2} \int_{t_1}^{t_2} e^{-\lambda_{м-р} \times t}\, dt, \tag{4.1}$$

$$Кг^{\,м-р} = \frac{1}{43824} \int_{0}^{43824} e^{-0{,}0000000001749 \times t}\, dt = 0{,}999996.$$

Для 2 випадку (з урахуванням впливу загроз безпеки і з одним маршрутизатором в складі обладнання) коефіцієнт готовності вузла розраховується за (4.2):

$$K_г^{вузла\,(2)} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} e^{-\lambda_{м-р} \times t}\, dt - P_{B} \times P^{м-р}_{P|B} \times Кнг^{\,р.у.}, \tag{4.2}$$

$$K_{г}^{вузла\,(2)} = \frac{1}{43824}\int_{0}^{43824} e^{-0,0000000001749\times t}\,dt - 0,514\times 1\times 0,00118 = 0,999996 - 0,00061 = 0,999386.$$

Для 3 випадку (з урахуванням впливу загроз безпеки, з одним маршрутизатором в складі обладнання та засобом захисту STPL) коефіцієнт готовності вузла ($K_{г}^{вузла(3)}$) розраховується за формулою (4.3):

$$K_{г}^{вузла\,(3)} = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} e^{-\lambda_{м-р}\times t}\,dt \times \int_{t_1}^{t_2} e^{-\lambda_{ФПСУ}\times t}\,dt - П_{В} \times П_{Р|В}^{м-р} \times Кнг^{П.В.}, \qquad (4.3)$$

$$K_{г}^{вузла\,(3)} = \frac{1}{43824}\int_{0}^{43824} e^{-0,0000000001749\times t}\,dt \times 0,514 \times \frac{1}{43824}\int_{0}^{43824} e^{-0,000000000282\times t}\,dt - 0,514 \times$$

$$\times 0,1\times 0,00118 = 0,999996 - 0,00061 = 0,999925.$$

Таким чином, врахування *Кнг*, що спричинили атаки DDoS-атаки, дозволяє покращити точність розрахунків (на величину $K_{(н)г}^{(2)}$ за рахунок врахування впливу помилок другого роду.

Занесемо отримані результати до таблиці 4.3

Таблиця 4.3 – Значення *К*г і *Кнг* мережевих вузлів

Тип моделювання	Обладнання вузла зв'язку	$K_{г}^{(1)}$ стан 1	$K_{нг}^{(3)}$ Стан 3	$K_{нг}^{(2)}$ Стан 2
1	2	3	4	5
Без впливу загроз ІБ $K_{г}^{вузла\,(1)}$	Маршрутизатор	0,999994	0,000003	0

Кінець таблиці 4.3 – Значення *К*г і *Кнг* мережевих вузлів

1	2	3	4	5
З урахуванням впливу загроз безпеки ($К_{г}^{вузла(2)}$)	Маршрутизатор	0,999385	0,000003	0,00062
З урахуванням впливу загроз безпеки ($К_{г}^{вузла(3)}$)	Маршрутизатор, засіб захисту STPL	0,999924	0,000015	0,000062

Виходячи з припущення про експоненціальний розподіл потоку відмов обладнання, можна на основі запропонованої математичної моделі здійснювати як короткострокові, так і довгострокові прогнози показника готовності з урахуванням впливу кіберзагроз.

Зокрема, модель дозволяє розрахувати ймовірність перебування вузла мережі у працездатному стані на заданому інтервалі часу в майбутньому з врахуванням імовірності реалізації атак, спрямованих на порушення доступності інформаційних ресурсів.

Крім цього, на підставі статистичних даних можна оцінити середній час перебування вузла в неробочому стані як через технічні неполадки обладнання, так і внаслідок успішних кібератак. Це надає можливість аналізувати ризики та планувати заходи щодо посилення стійкості мережі.

4.3 Аналіз впливу атак на показники надійності сегментів мережі

Для впровадження обрано ділянку мережі наступної топології (рис. 4.2).

Наведена схема демонструє топологію підключення філій до централізованих сервісів та ресурсів ЦОД. У цій мережі виділено основний (I) та

резервний (II) шлюзи, які з'єднані з ЦОД високошвидкісними лініями підвищеної надійності.

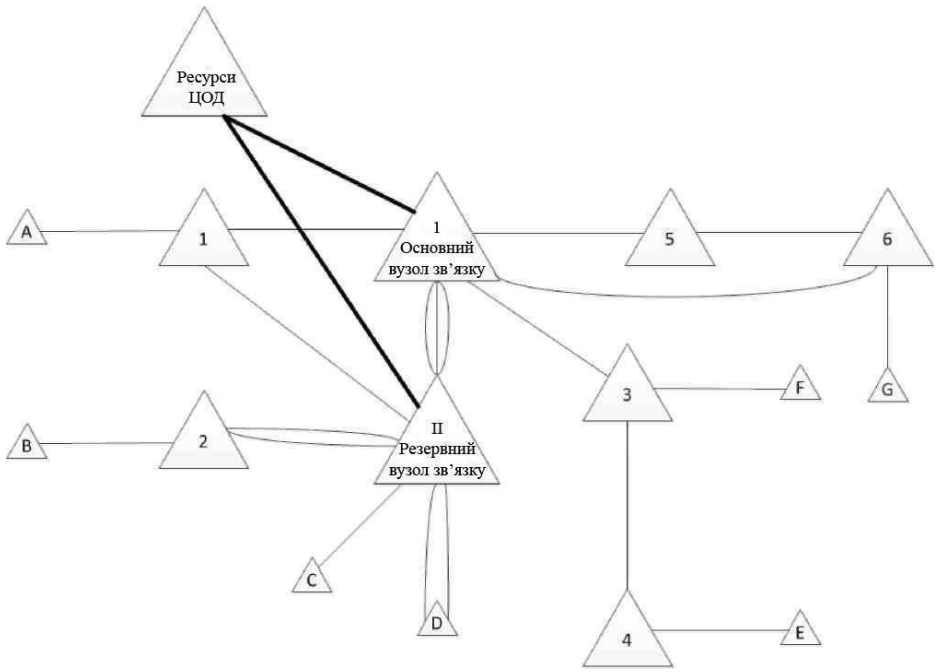


Рисунок 4.3 – Фрагмент досліджуваної мережі

Вузли 1-6 є проміжними, через них можливе підключення як безпосередньо кінцевих користувачів, так і інших вузлів мережі. Вузли A-G - кінцеві, що забезпечують доступ користувачам філій до корпоративних сервісів.

В рамках впровадження системи проводиться розрахунок показника готовності на шляху від кінцевих вузлів A-G до ЦОД. Це дозволяє оцінити ймовірність стабільного доступу користувачів до критичних IT-сервісів та запланувати заходи для підвищення надійності мережі.

В запропонованій схемі використовуються наступні способи резервування каналів зв'язку:

– розподілений (A), при цьому основний та резервний канал обслуговуються відповідно в основному та резервному ЦОД

– комутатитивний (B, C, D), при ньому основний та резервний канал зв'язку обслуговуються на основному або резервному вузлах зв'язку можливим резервуванням каналу;

– з резервуванням (G) за допомогою додаткового резервного ребра;

– без використання резервування (E,F).

Для забезпечення зв'язку між основним та резервним вузлами зв'язку використовуються 3 лінії, які працюють незалежно один від одного. *Кг* лінії каналу I-II обраховується по (2.2) і дорівнює $Кг_{I-II}$ = 0,9999999. Всі величини, необхідні для подальшого розрахунку зведені в таблиці 4.4

Таблиця 4.4 - Розрахунок коефіцієнтів готовності вузлів мережі

Змінна	Значення
Кг каналу зв'язку між кінцевими вузлами	$Кг_л = 0,997$
Кг каналу зв'язку між основним або резервним вузлами та ЦОД	$Кг_{ЦОД} = 0,9999$
Кг каналу зв'язку між основним та резервним пристроями	$Кг_{I-II} = 0,9999999$
Кг без урахування впливу загроз	$Кг_г^{ВУЗЛА(1)} = 0,999996$
Кг з врахуванням впливу загроз атак «відмова в обслуговувані»	$Кг_г^{ВУЗЛА(2)} = 0,999386$
Кг з урахуванням впливу загроз ІБ і використання додаткових засобів захисту	$Кг_г^{ВУЗЛА(3)} = 0999925$

Проведемо розрахунок показників готовності окремих сегментів корпоративної мережі для аналізу її надійності. Використовуватиметься метод повного перебору всіх можливих шляхів передачі даних від кінцевих вузлів до ЦОД [59].

Для спрощення обчислень формалізуємо топологію, тобто приймемо однаковими значення показників складових вузлів і ліній згідно з наведеною таблицею [60]. Розглядатимуться 3 сценарії з різними вихідними значеннями ймовірності готовності вузла, що дозволить проаналізувати вплив надійності окремих пристроїв на безперервну роботу мережі в цілому.

Отримані коефіцієнти готовності для кожного шляху передачі даних надалі можуть бути використані для визначення оптимальних маршрутів та планування заходів підвищення стійкості критичних ділянок мережі до збоїв та кібератак.

Відповідно до вимог, мінімально допустимий коефіцієнт готовності має бути не менший $K_{г\,min} = 0{,}996$.

Для зручносты коефіцієнти готовності досліджуваного сегменту мережі для різних станів кожного сегменту наведено на рис 4.5.

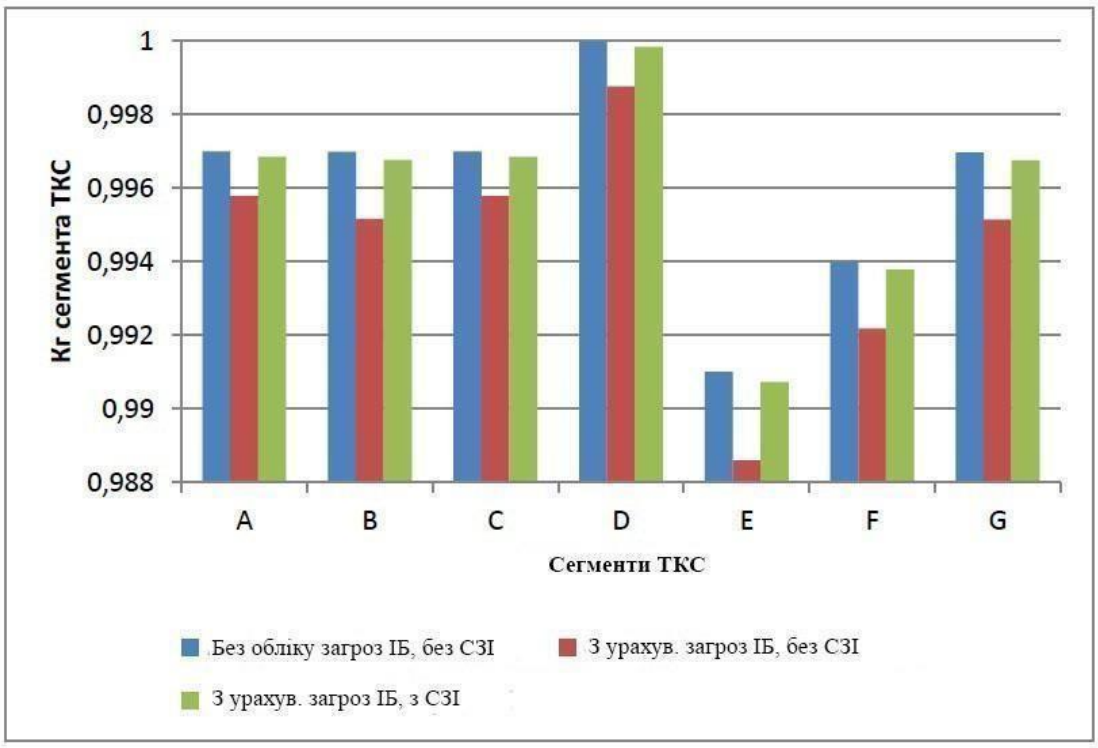


Рисунок 4.5 – Гістограма відображення впливу загроз на коефіцієнти готовності

Отримані числові значення коефіцієнтів готовності для різних сегментів мережі відповідають теоретичним розрахункам, наведеним у другому розділі дослідження. Зокрема, результати узгоджуються із значеннями показників для типових топологічних структур (послідовне, паралельне з'єднання пристроїв).

Ця відповідність підтверджує адекватність та достовірність запро понованої автором математичної моделі для оцінювання впливу кіберзагроз на коефіцієнт готовності корпоративної мережі. Модель коректно враховує особливості топології мережі, ймовірнісні характеристики вузлів та зв’язків між ними.

Отже, її можна використовувати для аналізу стану та прогнозування надійності реальних корпоративних мереж, а також як інструментарій при прийнятті рішень щодо забезпечення їх безперервного та стабільного функціонування.

На графіку, розташованому на рис. 4.5 чітко видно, що при використанні додаткового захисту від загроз на доступність інформації тип резервування не грає вагому роль. Але при зниженні коефіцієнта готовності без використання додаткових засобів захисту від DDoS атак, додаткове резервування каналів зв'язку суттєво впливає на надійність роботи корпоративної мережі.

Варто зауважити, що впровадження резервованих топологій корпоративної мережі, на відміну від незарезервованих, потребує додаткових фінансових витрат. Оцінка економічної ефективності запропонованих рішень виходить за рамки даного дослідження, проте економічний чинник не може не враховуватись при прийнятті рішень.

З розглянутих топологій можна виділити кільцеву структуру з вертикальним резервним каналом. Вона може бути реалізована на одному фізичному вузлі у вигляді двох незалежних комплектів обладнання та ліній зв'язку - основного і резервного. Така архітектура дозволяє оптимізувати витрати на резервування за рахунок об'єднання декількох функцій в межах одного пристрою.

4.4 Висновки

У даному розділі проведено дослідження корпоративної мережі Старосинявського відділення 10022/099 - Ощадбанк, Хмельницька область.

З метою практичної перевірки запропонованої математичної моделі та методики оцінювання ефективності функціонування мережевих вузлів.

Підтверджено відповідність отриманих значень показника готовності окремих топологій теоретичним розрахункам, що свідчить про адекватність розробленої моделі.

Встановлено, що вплив кіберзагроз на коефіцієнт готовності вузлів є вагомішим за вплив технічних факторів. Отже обґрунтовано пріоритетність заходів із забезпечення кібербезпеки для підвищення ефективності функціонування мережі.

Проведено оцінку впливу на коефіцієнт готовності факторів, викликаних непрацездатністю обладнання (0,0014%), а також впливом загроз, які можна формалізувати як «відмова в обслуговувані» (0,061%).

Запропоновано рекомендації з оптимізації окремих топологій шляхом резервування, що у деяких випадках дозволяє підвищити стійкість мережі до загроз без додаткових засобів захисту.

Отримані результати дозволяють зробити висновки про ефективність застосованих заходів захисту від DoS-атак після впровадження додаткового ліцензійного пакета Security Technology Package License, а також надають рекомендації для підвищення стійкості мережі до подібних атак.

ВИСНОВКИ

У даній роботі було вирішено наукове завдання, а саме, удосконалено метод визначення стану працездатності вузлів мережі в умовах впливу загроз доступності інформації. Однією з особливостей цього підходу є можливість проведення кількісної оцінки впливу загроз на ефективність функціонування корпоративної мережі.

Основні результати магістерського дослідження:

1. Проведено огляд та аналіз актуальних методів оцінювання стійкості мереж до кібератак, спрямованих на порушення доступності інформаційних ресурсів.
2. Обґрунтовано можливість застосування апарату теорії надійності та показника готовності для аналізу ефективності функціонування мережевих вузлів.
3. Розроблено математичну модель з трьома станами вузла та системою диференціальних рівнянь для врахування впливу розподілених кібератак на корпоративну мережу, представлену у вигляді графа.
4. Вдосконалено метод оцінювання ефективності роботи окремого вузла в умовах реалізації загроз порушення доступності інформаційних ресурсів.
5. Розроблено алгоритм підвищення ефективності комунікаційних вузлів в умовах хакерських атак.
6. Запропоновано підхід до побудови внутрішньої топології вузла у вигляді кільця з вертикальним резервуванням, що дозволяє суттєво підвищити показник його готовності.
7. На прикладі фрагменту мережі корпоративної мережі Старосинявського відділення 10022/099 - Ощадбанк, Хмельницька область, практично апробовано запропоновану модель та методику оцінки готовності вузлів. Підтверджено їх адекватність та ефективність.

8. Проведено оцінку впливу на коефіцієнт готовності факторів, викликаних непрацездатністю обладнання (0,0014%), а також впливом загроз, які можна формалізувати як «відмова в обслуговувані» (0,061%).

9. Встановлено, що вплив кіберзагроз істотніше знижує показник готовності вузлів порівняно з технічними факторами. Обґрунтовано пріоритетність реалізації заходів кібербезпеки для підвищення надійності функціонування мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Defensive Security Handbook/ Lee Brotherston, Amanda Berlin. - O'Reilly Media, Inc., 2017. - 247 p.

2. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. - К.: КУБГ, 2019. - 218 с.

3. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення/ Бурячок В. Л. та ін. /Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. - №3. - С. 48-61.

4. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник,

5. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. - Львів: Видавництво Львівської політехніки, 2019. - 580 с.

6. Network Security Assessment. Third edition/ Ch. McNab. - O'Reilly Media, Inc., 2017. - 546 p.

7. Avizienis, A. The architecture of a resilience infrastructure for computing and communication systems / A. Avizienis // 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). - 2013. - P. 1-2.

8. Чинчик Д., Коробейнікова Т., Захарченко С. Методи та засоби комплексного захисту корпоративної мережі. InterConf. 2021. №84. С.433-450.

9. Яциковська У. О. Модель захищеної архітектури клієнт-сервер [Текст] / У. О. Яциковська, І. В. Васильцов, М. П. Карпінський // Вісник Східноукраїнського національного університету імені Володимира Даля. - 2010. - № 9 (151). - С. 74-79.

10. Комп'ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. - К.: НПУ імені М.П. Драгоманова, 2015 р. - 141 с.

11. Якименко І. З. Критерії оцінки рівня захисту комп 'ютерних мереж з

врахуванням їх архітектури // Інформатика та математичні методи в моделюванні, 2013. - Т. 3 - №1 - С. 82-90.

12. Проектування та монтаж локальних комп'ютерних мереж/ І. М. Журавська. - Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. - 396 с.

13. Моделювання систем захисту інформації/А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с.

14. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. - Software Architecture. - 2016. - P. 274-290.

15. Комп'ютерні мережі. Книга 1/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. - Львів, «Магнолія 2006», 2013. - 256 с.

16. Комп'ютерні мережі. Книга 2/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. - Львів, «Магнолія 2006», 2014. - 312 с.

17. The Practice of System and Network Administration. Volume 1. Third Edition/ Th. A. Limoncelli, Ch. J. Hogan, S. R. Chalup. - Virtual.NET Inc., Lumeta Corporation, 2017. - 1426 p.

18. Відкритий проект захисту веб-додатків (OWASP). Стандарт оцінювання відповідності безпеки додатків 3.0 [Електронний ресурс]. - 2023. – режим доступу: https://owasp.org/ www-pdf-archive/ASVS_3_0_Ukrainian_Beta.pdf. – (дата звернення 9.09.2023) – Назва з екрана.

19. Універсальній метод захисту веб-додатків/ І.В. Василенко. – Системи обробки інформації. – 2016. – вип.1 (138). – С. 122-124.

20. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. - Львів, «Магнолія 2006», 2016. - 256 с.

21. Operating System Concepts Essentials. Second Edition/ A. Silberschatz, P. B. Galvin, G. Gagne. - John Wiley & Sons, Inc, 2014. - 760 p.

22. ISO/IEC 15408-3:1999 – Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements.

23. CEM-97/017. Common Evaluation Methodology for Information

Technology Security - Part 1: Introduction and general model.

24. ISO/IEC 15408-2:1999 - Information technology - Security techniques - Code ofpractice for information security management.

25. Моделювання систем захисту інформації/А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с.

26. Bondavalli, A. Foundations of measurement theory applied to the evaluation of dependability attributes / A. Bondavalli, A. Ceccarelli, L. Falai, M. Vardusi // Dependable systems and networks. – 2007. – №7. – P. 522–533.

27. Longo, F. Dependability modeling of software defined networking / F. Longo, S. Distefano, D. Bruneo, M. Scarpa // Computer Networks. – 2015. – №83. – P. 280–296.

28. Методичні вказівки до лабораторних робіт з курсу «Мультисервісні технології в комп'ютерних мережах» / Укладачі: Марценко С.В., Поливана У.В. - Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 - 20 с.

29. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар - Чернівці: Чернівецький національний університет, 2018. - 252 с

30. Гребенніков В.В. Комплексні системи захисту інформації: проєктування, впровадження, супровід. / В.В. Гребенніков – Ужгород: Ужгородський національний університет, 2013. — 161 с.

31. Y. Borsukovskyi, «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 3», Кібербезпека: освіта, наука, техніка, вип. 4, вип. 8, с. 34-48, Чер 2020

32. Організація комп'ютерних мереж: підручник/ Ю.А. Тарнавський, І.М. Кузьменко. - Київ: КПІ ім. І. Сікорського, 2018. - 259 с.

33. Cisco AVVID Network Infrastructure Overview [Електронний ресурс] - Режим доступу до ресурсу: https://www.cisco.com/web/offer/CAT4500/toolkit/comin_ov.pdf – (дата звернення 19.10.2023) – Назва з екрана.

34. Cisco Webex Plans and Pricing [Електронний ресурс] - Режим доступу до ресурсу*:* https://www. webex. com/pricing/index. Html – (дата звернення 17.10.2023) – Назва з екрана.

35. Теорія ймовірностей та математична статистика: навч. посіб. У 2 ч. Ч. 1. Теорія ймовірностей / А.О. Рамський, Н. М. Самарук, О. А. Поплавська [та ін.]. – Хмельницький: ХНУ, 2020. – 219 с.

36. Теорія систем масового обслуговування: навч. посібник/ А. Л. Литвинов. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 141 с.Теорія ймовірностей, теорія випадкових процесів та математична статистика (частина I). / І.А. Рудоміно-Дусятська, Л.М. Козубцова, О.Ю. Пояркова, Т.В. Соловйова, В.Є. Сновида, Л.М. Цитрицька – К.: ВІТІ, 2018. – 187 с.

37. Моделювання систем: навчальний посібник/ І. П. Гамаюн, О. Ю. Чередніченко. – Харків: Факт, 2015. – 228 с. Tippenhauer, N.O. Automatic generation of security argument graphs / N.O. Tippenhauer, W.G. Temple, A.H. Wu, B. Chen, D.M. Nicol, Z. Kalbarczyk W.H. Sanders // Dependable Computing (PRDC) Pacific Rim International Symposium. – 2014. – P. 33–42.

38. Основні метрики якості мереж передавання даних / Н.В. Горячий, Г.М. Осухівська, А.М. Луцків, В.В. Яцишин – Матеріали VI науково-технічнийI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (12-13 грудня 2018 року) –Тернопіль, ТНТУ – 2018 – с. 65

39. Моделювання систем захисту інформації/ А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с."DDoS, Machine Learning, Measures". // "Understanding Denial-of-Service Attacks". / , 2016. - (Taylor & Francis Group). - (ISBN:13: 978-1-4987-2965-9). - С. 12-34.

40. Famous DDoS Attacks | The Largest DDoS Attacks Of All Time [Електронний ресурс] –Режим доступу до ресурсу: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/ – (дата звернення 16.10.2023) – Назва з екрана.

41. Гнатюк С.О. Базові аспекти захисту конфіденційної інформації на

об’єктах критичної інформаційної інфраструктури/ Гнатюк С.О., Сидоренко В.М., Сотніченко Ю.О./ Кібербезпека:освіта, наука, техніка - №1 (9) – 2020. – с.170-181.

42. Муляр І.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи ./ С.В.Ленков, В.М.Джулій, І.В. Муляр -Сучасна спеціальна техніка. Науково практичний журнал. - ДНДІ МВС України, 2016 - Вип. №2(45). - С.59-66

43. Інструментарій для раннього виявлення розподілених атак / І. В. Муляр, О. В. Мірошніченко, І. З. Якименко, Я. В. Соколюк // Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє", 27 листоп. 2020 р. – Київ : ВІКНУ, 2020. – Т. 1. – С. 51–52.

44. Барабаш О. В. Забезпечення функціональної стійкості складних технічних систем / О. В. Барабаш, Б. В. Дурняк, Д. М. Обідін // Моделювання та інформаційні технології : зб. наук. праць ІПМЕ ім. Г. Є. Пухова. - 2012. - Вип. 64. - С. 36-41.

45. . Newman M. E. The structure and function of complex networks / M. E. Newman // SIAM Review. – 2018

46. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. // Journal of Network and Computer Applications. - 2023. - С. 49-63.

47. Dobryshin M M Timing of occurrence of group denial of services (the services) under conditions of DDoS attacks, taking into account the possibilities offered by telecommunications services Certificate of registration of computer programs 2018610012

48. Прикладна математика: навч. посібн. / Н.Л.Сосницька, В.М.Малкіна, О.А.Іщенко, Л.В.Халанчук, О.Г.Зінов’єва. – Мелітополь : ТОВ “КОЛОР-ПРИНТ”, 2019. – 100 с.

49. Qrator Labs [Електронний ресурс]. – Режим доступу: https://qrator.net/en/solutions/ddos#1 – (дата звернення 17.09.2023) – Назва з

екрана.

50. Live Cyber Threat Map | Check Point [Електронний ресурс]. – Режим доступу: https://threatmap.checkpoint.com/ – (дата звернення 20.09.2023) – Назва з екрана.

51. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” *Int. J. Comput. Sci. Appl.,* vol. 6, no. 2, pp. 388-393, 2013

52. Елементи однорідності для періодичних ланцюгів Маркова / ПриймакМ., Прошин С. // Вісник ТДТУ. — 2009. — №2(14) — С. 114-123.

53. Комп’ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. - К.: НПУ імені М.П. Драгоманова, 2015 р. - 141 с.

54. Access-control list [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Access-control_list – (дата звернення 18.10.2023) – Назва з екрана.

55. Hping network security tool [Електронний ресурс]. – Режим доступу: https://www.radware.com/security/ddos-knowledge-center/ddospedia/hping/ – (дата звернення 18.10.2023) – Назва з екрана.

56. IPerf - The TCP, UDP and SCTP network bandwidth [Електронний ресурс]. – Режим доступу: https://www.radware.com/security/ddos-knowledge-center/ddospedia/hping/ – (дата звернення 19.10.2023) – Назва з екрана.

57. Аналіз захищеності вузлів мережі в умовах впливу атак / С.В. Лєнков, І.В. Муляр, О.Ю. Чемерис // XIX Міжнародній науково-практичній конференції «Військова освіта та наука: сьогодення та майбутнє», 10 листоп. 2023 р. – Київ : ВІКНУ, 2023. – С. 45–46.

58. CISCO Community [Електронний ресурс]. – Режим доступу: https://community.cisco.com/t5/routing/2921-k9-licensing/td-p/3016806 (дата звернення 16.09.2023) – Назва з екрана.

59. Протоколи, методи і технології захисту комп’ютерних мереж на транспортному рівні / Світличний В.А., Онищенко Ю.М. / Актуальні питання протидії кіберзлочинності та торгівлі людьми – Харків - 2018. - с.314-317

60. Поповський, В.В. Математичне моделювання надійності

інформаційно-комунікаційних мереж / В.В. Поповський, В.С. Волотка // Телекомунікаційні та інформаційні технології. – 2014. – №3. – С. 5–9.

ДОДАТОК А

Копії наукових публікацій

д.т.н., проф. Лєнков С.В. (ВІКНУ)
к.т.н., доц. Муляр І.В. (ХмНУ)
Чемерис О.Ю. (ХмНУ)

АНАЛІЗ ЗАХИЩЕНОСТІ ВУЗЛІВ МЕРЕЖІ В УМОВАХ ВПЛИВУ АТАК

Для ефективного захисту комп'ютерних мереж необхідно почати з проведення систематичного аналізу можливих загроз безпеці мережі. Загрози можуть набувати різних форм.

Під час забезпечення безпеки комп'ютерних мереж, важливо враховувати можливі випадкові загрози. Вони виникають, коли особа, яка не має відповідного розуміння правил і політики безпеки або з необережності, створює випадкові ризики. Такі загрози можуть бути спричинені неправильним налаштуванням системи, випадковим видаленням важливих файлів або помилками під час роботи з програмами. Важливо звернути увагу на навчання співробітників і розробку чітких політик безпеки, щоб мінімізувати можливість виникнення випадкових загроз.

Інший вид загроз безпеці мережі - несанкціоновані зміни. Оновлення, патчі та інші зміни в операційних системах, програмних додатках, конфігураціях, сумісності та обладнанні можуть створити неочікувані загрози для безпеки системи промислової автоматизації та управління або відповідного промислового процесу. Такі зміни можуть призвести до порушення роботи системи, витоку конфіденційних даних або недоступності сервісів.

Відкрита природа протоколів на рівні додатків створює ризики для безпеки, основним з яких є передача незашифрованої інформації. Під час використання таких протоколів, можливе перехоплення і доступ до конфіденційних даних. Це може призвести до витоку інформації та порушення конфіденційності.

Використання процедур ідентифікації та аутентифікації з подальшою авторизацією також вносить загрозу перехоплення або викрадення облікових даних і паролів. Якщо зловмисник отримує доступ до облікових даних, він може отримати несанкціонований доступ до системи і провести шкідливі дії.

Атаки типу DoS і DDoS на інформаційні системи також становлять значну небезпеку. Під час таких атак система стає недоступною для легітимних користувачів через перевантаження ресурсів. Це може призвести до втрати даних і серйозних проблем для бізнесу.

Для забезпечення ефективного захисту від загроз на рівні додатків необхідно створювати та впроваджувати комплексні системи інформаційної безпеки. Ці системи мають включати спеціалізовані механізми обмеження та контролю доступу до мережі, щоб запобігти несанкціонованому доступу. Також важливо забезпечити фізичний захист серверів і використовувати електронні цифрові підписи для забезпечення цілісності даних.

ДОДАТОК Б

Презентація кваліфікаційної робот

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Олександр ЧЕМЕРИС

Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

Науковий керівник
ст. викладач, к.т.н., доц., Ігор МУЛЯР

Метою магістерської роботи є удосконаленні методу врахування впливу загроз на функціонування вузла мережі
Об’єкт дослідження процес забезпечення ефективного функціонування корпоративних мереж
Предмет дослідження: є характеристики вузла зв'язку мережі

Задачі досліджень у роботі сформульовані наступним чином:

1. Провести аналіз факторів, які впливають на ефективне функціонування вузлів мережі.
2. Дослідити доцільність використання математичного апарату теорії надійності для аналізу доступності вузла в умовах впливу атак на відмову в обслуговуванні
3. Розробити математичну модель надійності вузла мережі в умовах впливу атак на відмову в обслуговуванні устаткування.
4. Дослідити вплив загроз доступності інформації в мережі на її коефіцієнт готовності.
5. Удосконалити метод врахування загроз доступності інформації на коефіцієнт готовності вузлів мережі.
6. Розробити алгоритм підвищення ефективності комунікаційних вузлів в умовах хакерських атак.
7. Оцінити ефективність комунікаційних вузлів існуючих мереж, та досліджено їх придатність для корпоративних мереж, з використанням різних фізичних топологій.

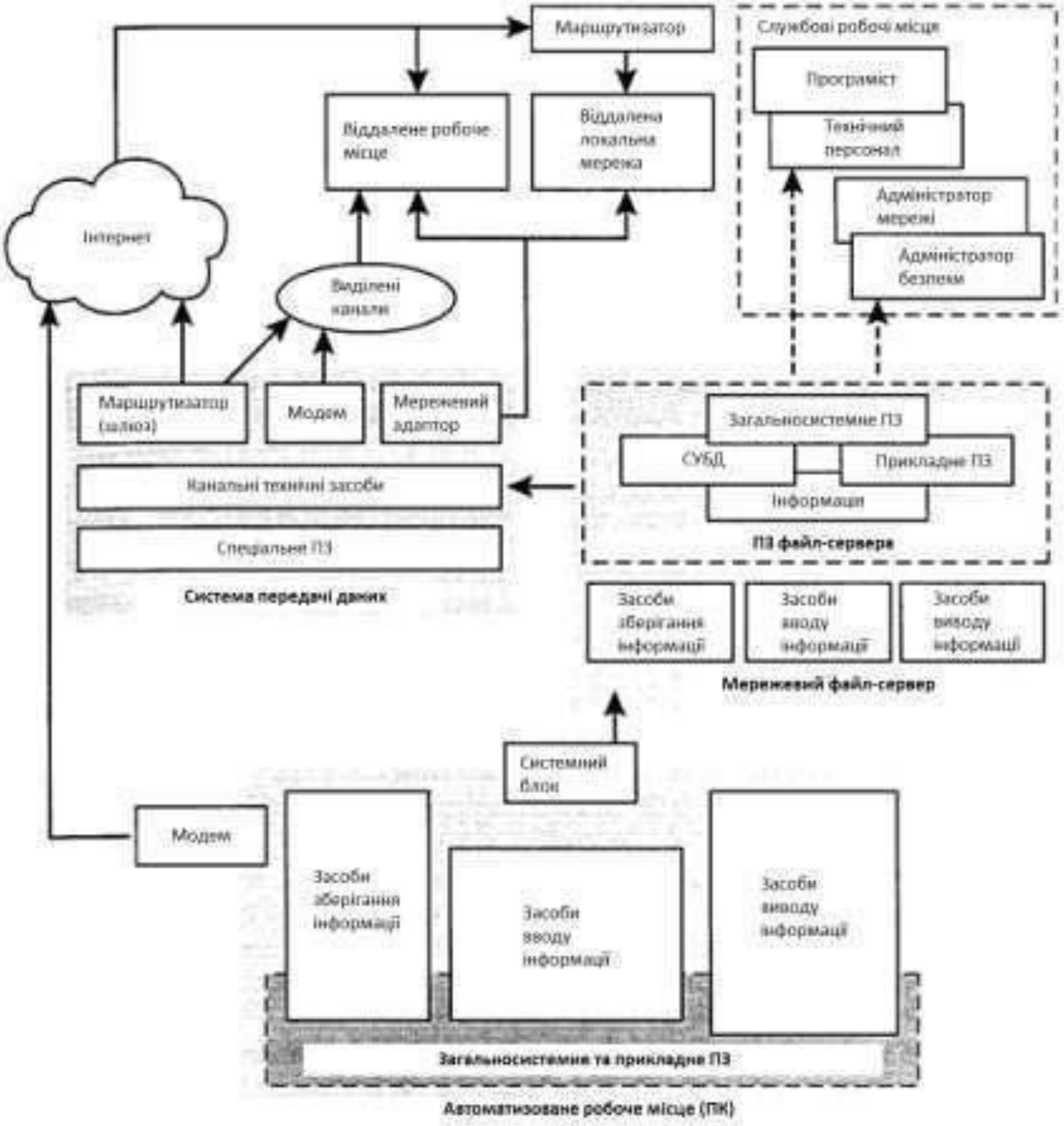
Наукова новизна роботи полягає в наступному:

1. Вдосконалена модель надійності комунікаційного вузла, яка вирізняється тим, що враховує вплив загроз пов’язаних з відмовою в обслуговувані.
2. Удосконалено метод дослідження мережі, заснований на моделюванні стану працездатності комунікаційних вузлів в умовах впливу атак на відмову в обслуговувані, який враховує кількісну оцінку ступеня впливу загроз безпеці доступності інформації.

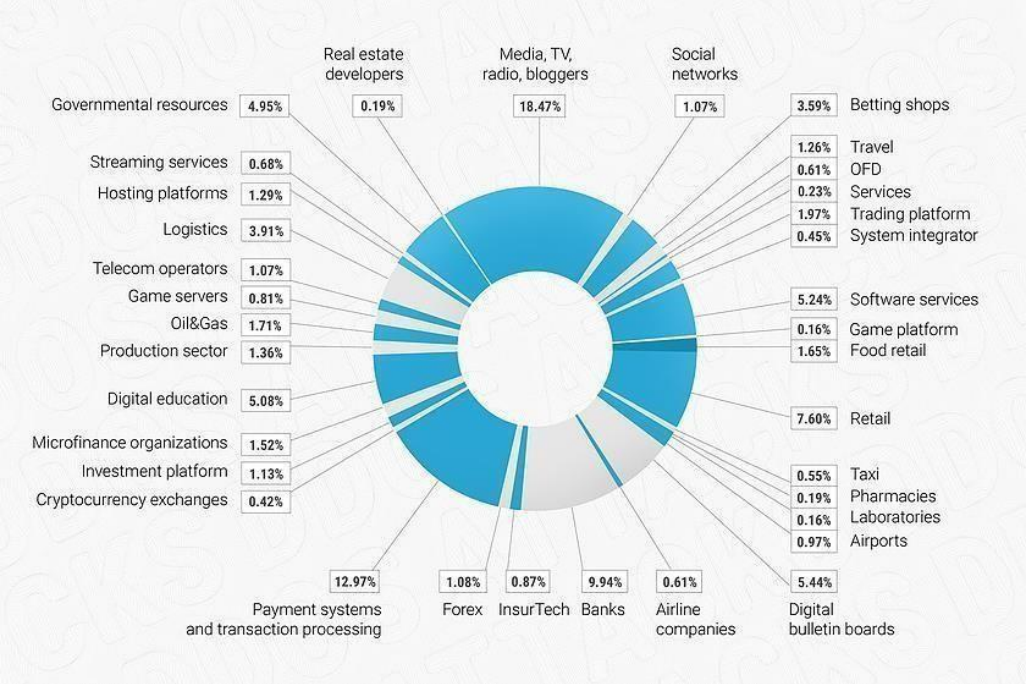
Практична цінність Практична реалізація розроблених у магістерській роботі моделей, та методу дозволило Це дозволило ефективно прогнозувати стан комунікаційних вузлів мережі в умовах впливу непрацездатності обладнання та загроз інформаційної безпеки.

Публікації. По темі магістерської роботи опубліковано 1 - теза доповідей XIX Міжнародній науково-практичній конференції «Військова освіта та наука: сьогодення та майбутнє» у Військовому інституті Київського національного університету імені Тараса Шевченка.

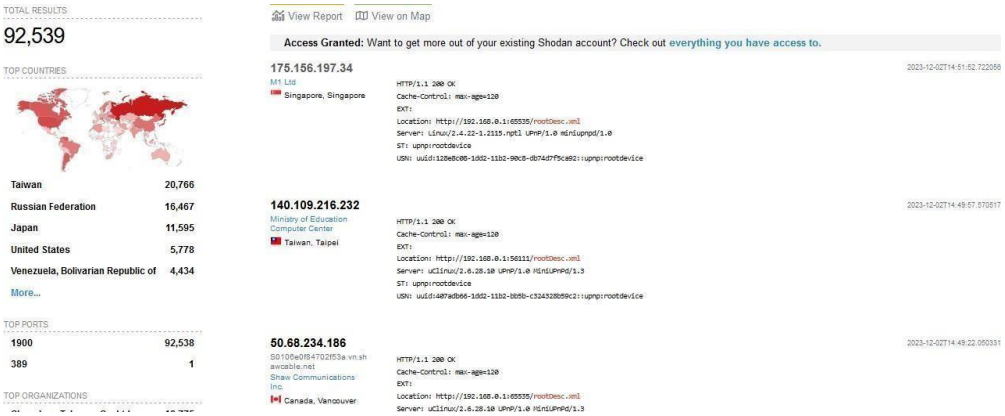
Модель корпоративної мережі



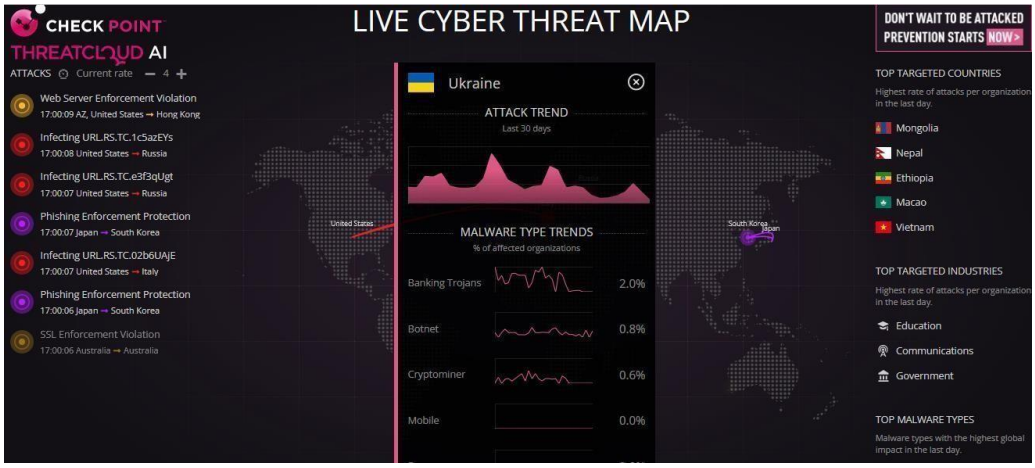
Аналіз впливу DDoS-атак на працездатність вузлів мережі



Статистика DDoS-атак у 2022 р

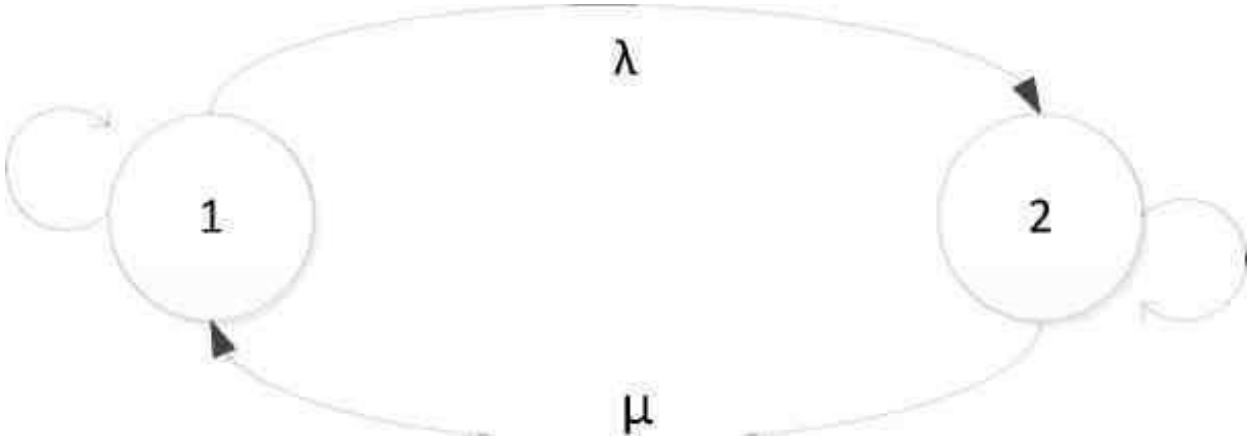


Виявлення вразливих пристроїв за допомогою сервісу Shodan



Онлайн-карта DDoS-атак

МАТЕМАТИЧНИЙ АПАРАТ ПРОГНОЗУВАННЯ ЧИСЛА ПРИСТРОЇВ, ЩО ЗНАХОДЯТЬСЯ В ПРАЦЕЗДАТНОМУ СТАНІ



Граф стану обладнання елемента мережі, де стан 1 відповідає працездатному стану об'єкта, стан 2 –несправному, λ - інтенсивність потоку відмов, μ - інтенсивність потоку відновлень.

інтенсивність потоку відмов буде розраховуватись

$$\lambda(t) = \frac{n(t)}{N\text{ср} \cdot \Delta t}$$

де, $n(t)$ – кількість пристроїв, що знаходяться в непрацездатному стані на інтервалі часу Δt,

Δt – інтервал часу.

$N\text{ср}$ – середнє число пристроїв, що знаходяться в працездатному стані на інтервалі часу Δt.

число пристроїв, що знаходяться в працездатному стані

$$N(\Delta t) = N0 \times (1 - \frac{n(\Delta t) \times \bar{t}\text{в}}{\Delta t}),$$

де $n\,(\Delta t)$ – пристрої які знаходяться в непрацездатному стані на інтервалі часу

$\bar{t}_{\text{в}}$- середній час знаходження пристрою в непрацездатному стані,

N_0 - число пристроїв, що знаходяться в працездатному стані

Δt - інтервал часу.

середній час відновлення

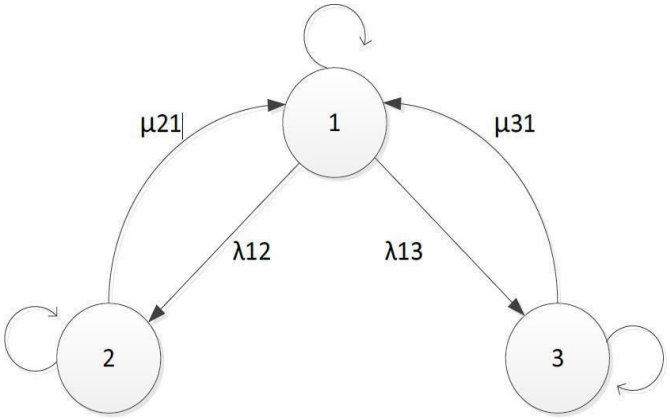
$$\bar{t} = \frac{1}{\text{i}} \int_{\text{i}}^{1} f(i),$$

де i - число випадків відновлення працездатності пристрою в аналізованому періоді.

$f\,(i)$ - функція розподілу часу відновлення.

МАРКІВСЬКА МОДЕЛЬ НАДІЙНОСТІ ВУЗЛА ЗВ'ЯЗКУ МЕРЕЖІ

Перший науковий результат



Граф станів вузла зв'язку мережі

Представлення математичної моделі вузла зв'язку мережі

В обробці трафіку задіяно багато обладнання, яке являє собою сукупність пристроїв, кожен з яких має власні технічні характеристики та показники, що характеризують його надійність (Кг). Також відомо, що трафік проходить послідовно всі пристрої вузла зв'язку, задіяні в інформаційномуобміні.

Таким чином, для розрахунку Кг вузла зв'язкурозраховується:

$Кг_у = Кг_1 \times Кг_2 \times ... \times Кг_n$,

де $Кг_1 ... Кг_n$ – Кг пристроїв вузла мережі.

1. Вузол зв'язку знаходиться в стані готовності.

2. Вузол зв'язку знаходиться в стані неготовності через реалізації загрози ІБ, спрямованої на порушення доступності інформації.

3. Вузол зв'язку знаходиться в стані неготовності через відмови обладнання.

Математична модель процесу, що визначається графом буде описуватися системою рівнянь Колмогорова-Чепмена :

$$\frac{dP_1(t)}{dt} = -(\lambda_{12} + \lambda_{13}) \times P_1(t) + \mu_{21} \times P_2(t) + \mu_{31} \times P_3(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_{12} \times P_1(t) - \mu_{21} \times P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda_{13} \times P_1(t) - \mu_{31} \times P_3(t)$$

Де $P_1(t), P_2(t), P_3(t)$ – ймовірність знаходження вузла зв'язку в першому, другому і третьому станах, якщо від початку процесу пройшов період часу (t);

$\lambda_{12}, \lambda_{13}$ – інтенсивність потоків відмов вузла зв'язку мережі;

μ_{21}, μ_{21} – інтенсивність потоків відновлень вузла зв'язку мережі.

Оскільки вузол зв'язку весь аналізований період знаходиться в одному з трьох описаних вище станів, слід ввести нормувальну:

$$P_1(t) + P_2(t) + P_3(t) = 1$$

Представлена математична модель вузла, що враховує вплив не тільки технічних відмов обладнання, але й загрози ІБ на Кг вузла зв'язку мережі. Під загрозою безпеки інформації розуміється сукупність умов та факторів, що створюють потенційну або реально існуючу небезпеку відмови в обслуговувані. В даній роботі, вважається, що атакам піддається активне обладнання вузла мережі.

ОПТИМІЗАЦІЇ МЕРЕЖЕВИХ ТОПОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖІ

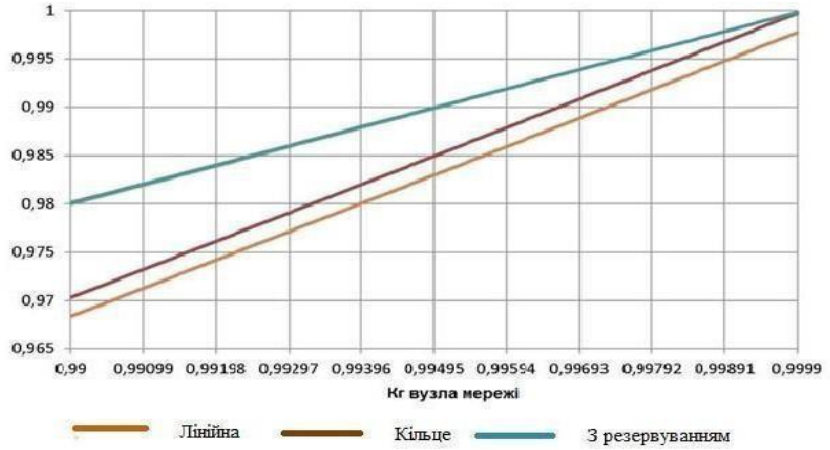
Залежність коефіцієнту готовності формалізованих топологій від коефіцієнту готовності вузла

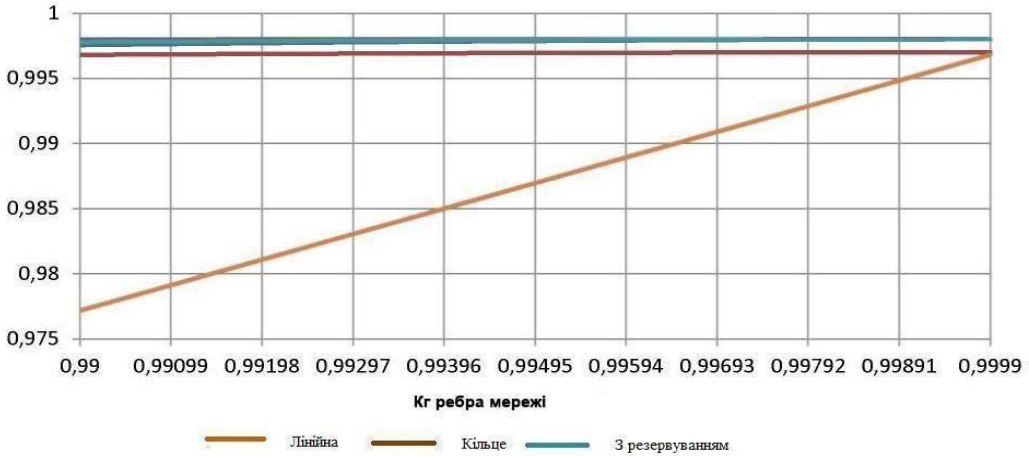
Кг	Кільце	З резервуванням	лінійна
0,99	0,979959	0,98009	0,968359
0,99099	0,981943	0,982052	0,971267
0,99198	0,983926	0,984016	0,974181
0,99297	0,985909	0,985982	0,977101
0,99396	0,987893	0,987951	0,980026
0,99595	0,989876	0,989921	0,982958
0,99594	0,99186	0,991892	0,985895
0,99693	0,993844	0,993866	0,988838
0,99792	0,995828	0,995842	0,991786
0,99891	0,997812	0,99782	0,994741
0,9999	0,999796	0,9998	0,997702

Залежність коефіцієнту готовності формалізованих топологій від коефіцієнту готовності ребра

Кг	Кільце	З резервуванням	лінійна
0,99	0,997566	0,997989	0,977163
0,99099	0,997644	0,997991	0,979118
0,99198	0,997714	0,997992	0,981075
0,99297	0,997777	0,997993	0,983034
0,99396	0,997832	0,997995	0,984996
0,99495	0,997879	0,997996	0,986959
0,99594	0,997918	0,997997	0,988924
0,99693	0,99795	0,997998	0,990891
0,99792	0,997975	0,997999	0,99286
0,99891	0,997991	0,998	0,994831
0,9999	0,998	0,998001	0,996804

Графіки залежності коефіцієнта готовності мережі в цілому від елемента

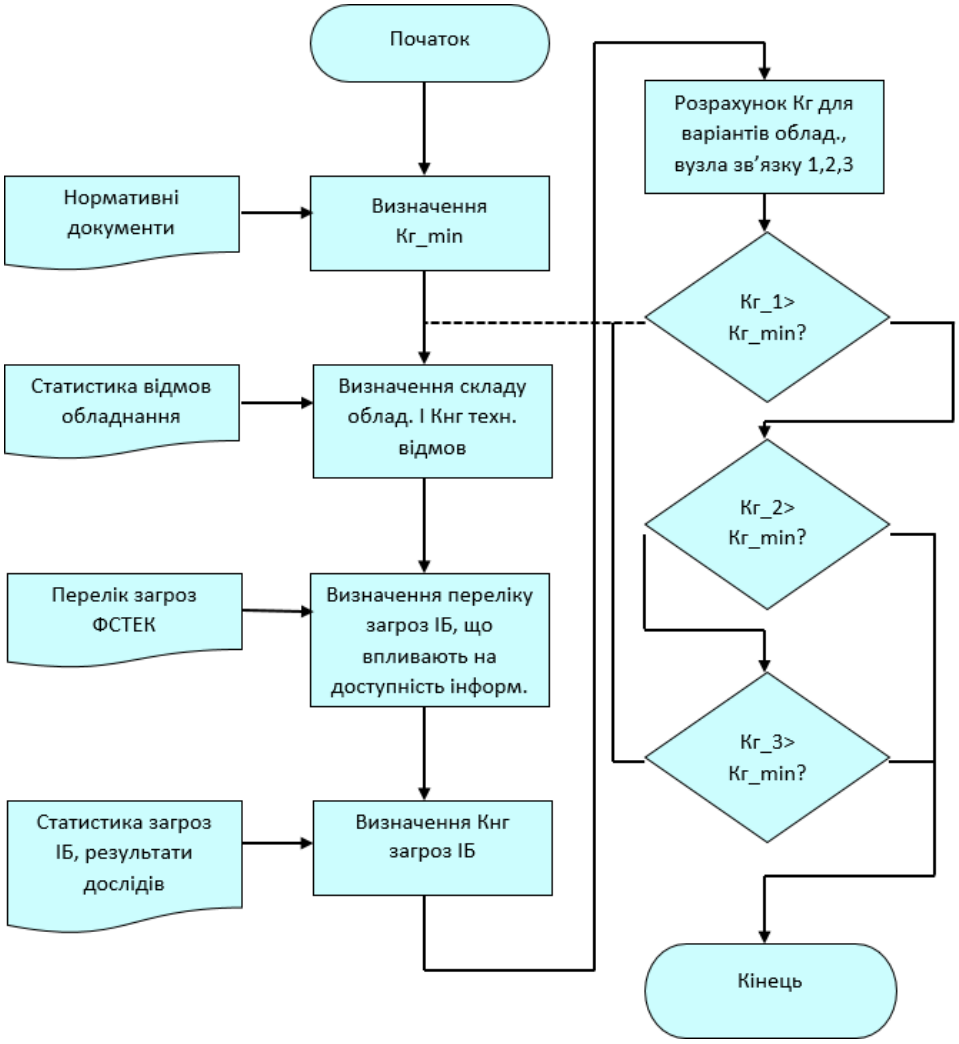




З графіка випливає що коефіцієнт готовності розглянутих топологій, що мають у своєму складі, резервування ліній зв'язку майже не реагують на зміну коефіцієнт готовності ребра. Це підтверджує доцільність врахування впливу загрози на ефективність функціонування мережі саме у значеннях коефіцієнту готовності вузла мережі.

ВДОСКОНАЛЕННЯ МЕТОДУ ОБЛІКУ ВПЛИВУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Другий науковий результат



Блок-схема алгоритму оцінки ефективності функціонування мережі

Оцінка захищеності відбувається в наступному порядку:

- ✓ Проводиться визначення мінімально допустимого Кг сегмента мережі (Кг_min) відповідно до вимог нормативних документів і державних стандартів.
- ✓ Визначається склад обладнання вузлів зв'язку, проводиться розрахунок Кнг, обґрунтованого технічними відмовами обладнання.
- ✓ Проведено формування переліку загроз інформаційній безпеці, що впливають на ефективність функціонування мережі в цілому.
- ✓ З використанням математичної моделі врахування впливу атак на Кг вузла зв'язку мережі, проводиться розрахунок Кнг, обґрунтованого впливом атак спрямованих на цілісність інформації.
- ✓ Проводиться порівняння розрахованого значення Кг_2 з Кг_min. У разі, коли значення Кг_2 більше значення Кг_min, тоді, виявлені атаки не завдають істотної шкоди на нормовані показники надійності функціонування телекомунікаційної мережі.

У випадку, коли вузол зв'язку піддається більш ніж одній загрозі, тоді Кнг буде розрахуватися:

$$\text{Кнг}_{\text{В}(i)} = \text{Р}_B \times \text{Р}_{P|B} \times \text{Кнг}^{\text{П.В}}$$

Р_B – ймовірність виникнення загрози ІБ,

Р_P – ймовірність реалізації загрози ІБ,

$\text{Кнг}_{\text{В}(i)}$ – коефіцієнт неготовності, обґрунтований реалізацією загрози;

$$\text{Кнг}_{\text{В}} = \text{Кг}_{\text{В}(1)} \times \text{Кг}_{\text{В}(2)} \times \ldots \times \text{Кг}_{\text{В}(n)},$$

де $\text{Кг}_{\text{В}1}$ ... $\text{Кг}_{\text{В}n}$ – Кг, що відображають вплив загроз ІБ відповідно до прийнятої моделі загроз.

$$\text{П}_P = \begin{cases} \left| \dfrac{t_{\text{експ}} - t_{\text{ср}}}{t_{\text{макс}} - t_{\text{ср}}} \right|, & t_{\text{експ}} < t_{\text{макс}}, \; t_{\text{експ}} \geq t_{\text{макс}}. \\ 1, \end{cases}$$

де $t_{\text{макс}}$ – максимально допустимий час виконання операції відповідно до вимог внутрішніх нормативних документів підприємства,

$t_{\text{ср}}$ - середній час виконання операції при відсутності впливу загроз ІБ,

$t_{\text{експ}}$ – середній час виконання операції безпосередньо під час атаки.

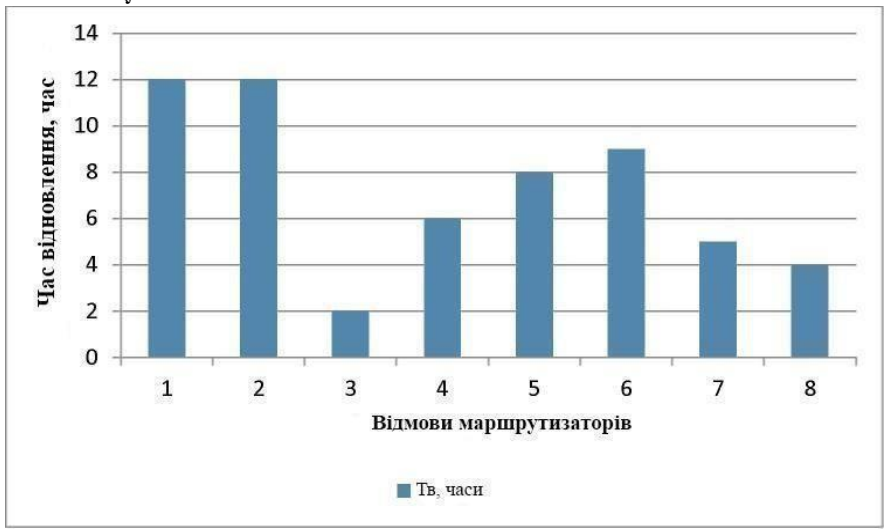
Використовуючи значення Кг вузла зв'язку мережі, можливо оцінити ефективність функціонування в різних умовах. Оцінка захищеності базується на порівнянні Кг мережі, розрахованого для наступних варіантів, кожен з яких відображає можливий стан вузла зв'язку та варіанти складу обладнання на ньому

РІВНЯННЯ АПРОКСИМУЮЧОЇ ФУНКЦІЇ ЧАСУ ВІДНОВЛЕННЯ РОБОТИ МАРШРУТИЗАТОРІВ

$$f(x) = -0.0152 \times x^4 + 0.0808 \times x^3 + 1.0985 \times x^2 - 8.307 + x + 20{,}143$$

Підставляючи в рівняння отримаємо значення середнього часу відновлення працездатності маршрутизатора для 8 випадків відновлення після відмов:

$$\overline{t_B} = \frac{1}{8}\int_{8}(-0.0152 \times x_4 + 0.0808 \times {}_2 - 8.307 + x + 20.143)dx = \frac{51.712}{8} = 6{,}464 \text{ годин.}$$

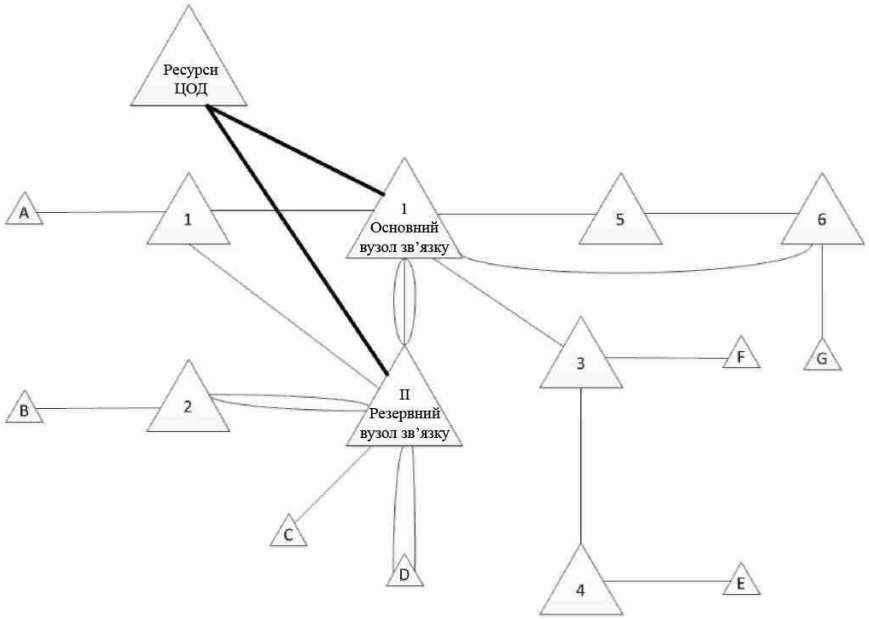


Розподіл часу відновлення працездатності маршрутизаторів

Кнг, визваний впливом DDoS-атак

Склад обладнання	$K_{нг}^{(3)}$	λ
Маршрутизатор	0,000004	0,00000000019255
Маршрутизатор та засіб захисту STPL	0,0000143	0,00000000062892

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ЗАСТОСОВАНІ НА ЧАСТИНІ МЕРЕЖІ



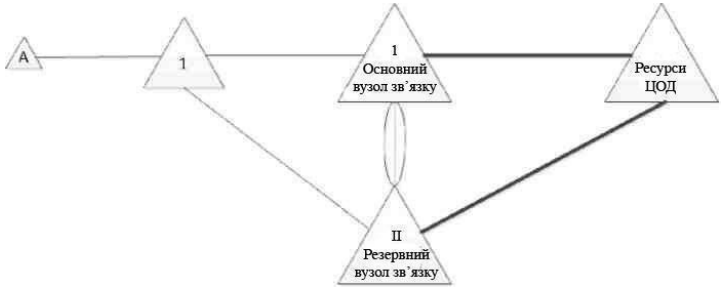
В представленій схемі використовуються наступні способи резервування ліній зв'язку:

– розподілений (A), при цьому основний та резервний канал обслуговуються відповідно в основному та резервному ЦОД

– комутатитивний (B, C, D), при ньому основний та резервний канал зв'язку обслуговуються на основному або резервному вузлах зв'язку можливим резервуванням каналу;

– з резервуванням (G) за допомогою додаткового резервного ребра;

– без використання резервування (E,F).



Даний сегмент, а саме, топологія А-ЦОД (розподілене резервування) має безпосереднє підключення як до основного, так і до резервного вузла зв'язкумережі.

ВИСНОВКИ

У даній роботі було вирішено наукове завдання, а саме, удосконалено метод визначення стану працездатності вузлів мережі в умовах впливу загроз доступності інформації. Однією з особливостей цього підходу є можливість проведення кількісної оцінки впливу загроз на ефективність функціонування корпоративної мережі.

Основні результати магістерського дослідження:

1. Проведено огляд та аналіз актуальних методів оцінювання стійкості мереж до кібератак, спрямованих на порушення доступності інформаційних ресурсів.
2. Обґрунтовано можливість застосування апарату теорії надійності та показника готовності для аналізу ефективності функціонування мережевих вузлів.
3. Розроблено математичну модель з трьома станами вузла та системою диференціальних рівнянь для врахування впливу розподілених кібератак на корпоративну мережу, представлену у вигляді графа.
4. Вдосконалено метод оцінювання ефективності роботи окремого вузла в умовах реалізації загроз порушення доступності інформаційних ресурсів.
5. Розроблено алгоритм підвищення ефективності комунікаційних вузлів в умовах хакерських атак.
6. Запропоновано підхід до побудови внутрішньої топології вузла у вигляді кільця з вертикальним резервуванням, що дозволяє суттєво підвищити показник його готовності.
7. На прикладі фрагменту мережі корпоративної мережі Старосинявського відділення 10022/099 - Ощадбанк, Хмельницька область, практично апробовано запропоновану модель та методику оцінки готовності вузлів. Підтверджено їх адекватність та ефективність.
8. Проведено оцінку впливу на коефіцієнт готовності факторів, викликаних непрацездатністю обладнання (0,0014%), а також впливом загроз, які можна формалізувати як «відмова в обслуговувані» (0,061%).
9. Встановлено, що вплив кіберзагроз істотніше знижує показник готовності вузлів порівняно з технічними факторами. Обґрунтовано пріоритетність реалізації заходів кібербезпеки для підвищення надійності функціонування мереж

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Чемерис О.Ю
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

11.12.2023
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 7%**

	Документ		Сумарний збіг по Базі Даних	
ID: 122069 Назва: Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні Додано в БД: 2023-12-07 Автора: Чемерис О.Ю. Керівники: Муляр І.В. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	88308	1366	853 (1%)	12 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015981303

Дата перевірки:
07.12.2023 17:48:27 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
07.12.2023 17:59:44 EET

ID користувача:
100008300

Назва документа: **Чемерис_магістерська_на плагіат**

Кількість сторінок: **81** Кількість слів: **13045** Кількість символів: **106273** Розмір файлу: **2.01 MB** ID файлу: **1015661485**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

4.45%
Схожість

Найбільша схожість: **2.63%** з джерелом з Бібліотеки (ID файлу: **1005683463**)

4.15% Джерела з Інтернету	216	Сторінка 83
3.16% Джерела з Бібліотеки	51	Сторінка 84

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	34
Підозріле форматування	13 сторінок

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

Автор: Чемерис Олександр Юрійович

Науковий керівник: Муляр Ігор Володимирович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 95,45%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Виявлені системою Unichek модифікації стосуються математичних формул і не є пошенням академічної доброчесності.

Керівник роботи І.В. Муляр

Гарант ОП В.Ю. Тітова

Завідувач кафедри кібербезпеки Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Чемерис О.Ю.

Тема Метод оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень ; кількість сторінок записки 86

1. Короткий зміст кваліфікаційної роботи та прийнятих рішень в рамках роботи Проаналізувано чинники, що впливають на забезпечення ефективного функціонування мережі, розглянути критерії та існуючі методи їх оцінки. Перевірено можливість використання математичного апарату теорії надійності як інструменту для проведення досліджень. Розроблено модель надійності вузла, яка враховує вплив атак і технічних відмов обладнання. Розроблено метод експериментального дослідження впливу атак на коефіцієнт готовності. Перевірено застосування розроблених методів до реальної мережі та дослідити їх ефективність для різних топологій.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна магістерська робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі висвітлюється актуальність теми роботи, дається аналіз досліджуваної проблеми і обґрунтовується застосовуваний підхід до її вирішення, формулюються цілі і завдання дослідження, описується наукова новизна і практична значимість отриманих результатів. У першому розділі розглядаються питання особливостей функціонування корпоративних мереж в умовах DDoS атак. Наступні розділи присвячені розробці та реалізації алгоритму та методу оцінки захищеності вузлів мережі в умовах впливу атак на відмову в обслуговуванні

4. Позитивні сторони роботи Кваліфікаційна робота містить ряд інноваційних рішень, зокрема запропонований підхід полягає в тому, що враховується стан готовності вузла, в умовах атаки на його доступність

5. Негативні сторони роботи Впровадження розробленої моделі та методу ускладняється масштабними та складними топологіями мережі.

6. Оцінка графічного оформлення та пояснювальної записки роботи
Пояснювальна записка відповідає нормам для її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційної роботи заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре»

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Завідувач кафедри ТМІТ д.т.н., проф Підченко С.К.

« 11 » грудня 2023. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.