Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Житніка Романа Леонідовича

на здобуття ступеня вищої освіти магістра

Метод врахування загроз безпеки на функціонування вузла мережі

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ. 230111.23.01.08 ПЗ

Виконав студент 2 курсу група КБЗІм-23-1 Роман ЖИТНІК
Керівник канд. техн. наук, доцент Ігор МУЛЯР
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
18 12 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

2 09 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Житніку Роману Леонідовичу

1 Тема роботи Метод врахування загроз безпеки на функціонування вузла мережі
Керівник роботи канд.техн.наук, доцент Ігор МУЛЯР
Затверджено наказом ректора університету від 26 08 2024 № 60
2 Строк подання студентом кваліфікаційної роботи на кафедру 2.12.2024
3 Вихідні дані до роботи

архітектура банківської мережі, статистика DDoS – атак

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Проведено аналіз чинників, що впливають на ефективне функціонування мережі, зокрема на надійність і стабільність її вузлів, враховуючи як технічні, так і кібернетичні загрози. Розроблено моделі надійності вузла, що враховує ці чинники, і дозволяє оцінити його готовність до різноманітних впливів. Модель точніше прогнозує поведінку вузлів при реальних умовах, зокрема, при різних типах атак або неполадках обладнання. Розроблено методу для експериментальної оцінки впливу таких атак на коефіцієнт готовності мережі. Останнім етапом є перевірка ефективності розроблених методів на реальних мережах, що дасть змогу оцінити їх працездатність в різних топологіях та підвищити стійкість мережі до зовнішніх і внутрішніх загроз.

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

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 2 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі		Виконано
Визначення змісту, структури кваліфікаційної роботи		Виконано
Підготовка першого розділу кваліфікаційної роботи		Виконано
Підготовка другого розділу кваліфікаційної роботи		Виконано
Підготовка третього розділу кваліфікаційної роботи		Виконано
Підготовка статті/тези за темою кваліфікаційної роботи		Виконано
Підготовка четвертого розділу кваліфікаційної роботи		Виконано
Підготовка та оформлення ілюстративного матеріалу		Виконано
Оформлення кваліфікаційної роботи		Виконано
Попередній захист кваліфікаційної роботи		Виконано
Захист кваліфікаційної роботи на засіданні ЕК		Виконано

Студент _____ Роман ЖИТНІК

Керівник кваліфікаційної роботи _____ Ігор МУЛЯР

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод врахування загроз безпеки на функціонування вузла мережі

Автор роботи: Житнік Роман Леонідович

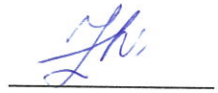
Керівник роботи: к.т.н., доц. Муляр Ігор Володимирович

Загальний обсяг роботи: 89 сторінок, 25 рисунків, 1 таблиця, 2 додатки, 65 посилань.

Ключові слова: захист інформації, вузли мережі.

Дослідження спрямоване на оптимізацію процесів забезпечення безперервної роботи корпоративних комунікаційних мереж через розроблення інноваційної методології аналізу кібернетичних впливів на інфраструктурні компоненти. Представлено принципово новий методологічний підхід до діагностування стану комунікаційних вузлів, який враховує ймовірнісні характеристики потенційних кіберзагроз та їхній безпосередній вплив на неперервність функціонування інформаційних сервісів.

Запропонована науково-методична розробка, доповнена рекомендаціями з проєктування резервних мережевих архітектур, надає комплексний інструментарій для всебічної оцінки мережевої інфраструктури, розроблення превентивних механізмів протидії кіберризикам та підтримання заданих параметрів системної стійкості.



2.12.2024

ANNOTATION

Theme of qualification work: Method for taking into account security threats to the operation of a network node

Author of the work: Zhytnik Roman

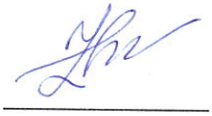
Supervisor: Candidate of Technical Sciences, Associate Professor Muliyar Ihor

Total amount of work: 89 pages, 25 figures, 1 table, 2 appendices, 65 references.

Keywords: information security, network nodes.

The study is aimed at optimising the processes of ensuring the continuous operation of corporate communication networks by developing an innovative methodology for analysing cyber impacts on infrastructure components. A fundamentally new methodological approach to diagnosing the state of communication nodes is presented, which takes into account the probabilistic characteristics of potential cyber threats and their direct impact on the continuity of information services.

The proposed scientific and methodological development, complemented by recommendations for designing redundant network architectures, provides a comprehensive toolkit for a comprehensive assessment of network infrastructure, development of preventive mechanisms to counter cyber risks, and maintenance of the specified parameters of system stability.



2.12.2024

ЗМІСТ

ВСТУП

З початку 2000-х років спостерігається тенденція до централізації інформаційних активів підприємств у всіх секторах економіки. Сьогодні ці процеси досягли свого піку, і автономне існування великих компаній стало неможливим. Відсутність зв'язку з дата-центром призвела до того, що додаткові офіси не в змозі забезпечити обслуговування клієнтів. Крім того, доступ до зовнішніх ресурсів, таких як кредитні бюро, списки осіб, пов'язаних з відмиванням грошей та фінансуванням тероризму, здійснюється через корпоративні телекомунікаційні мережі. Ці мережі також забезпечують подання звітності до Державної податкової служби, Національного банку України та інших контролюючих органів. Для цілей цього дослідження під корпоративними мережами в першу чергу розуміються мережі українських банківських установ, оскільки їх характеристики, статистика інцидентів та досвід впровадження є релевантними для підприємств банківської галузі. В той же час, результати впровадження показують, що ці мережі можуть і повинні використовуватися на підприємствах інших секторів економіки.

Активний розвиток мережевих технологій призводить до появи нових видів атак на комп'ютерні мережі. Різноманітні методи вторгнення та їх адаптація вимагають вдосконалення існуючих технологій та засобів захисту корпоративних мереж.

Використання сучасних інформаційних технологій є надзвичайно важливим для ефективного управління існуючими системами та об'єктами. Корпоративні комп'ютерні мережі служать універсальним інструментом, що забезпечує високу продуктивність і успішну роботу різних інформаційних систем.

Зі зростанням кількості користувачів та обсягів даних, що передаються в рамках комп'ютерних мереж, виникає ризик погіршення якості мережевих послуг через збільшення інтенсивності трафіку. Це підкреслює важливість вдосконалення засобів моніторингу та аналізу мережевого трафіку, які є

критично важливими для підтримки ефективності та надійності мережевої інфраструктури.

Проблема аналізу мережевого трафіку вивчається протягом значного часу, і для її вирішення проводяться численні наукові дослідження. Особливої актуальності ця проблема набуває в умовах швидких змін у мережевому середовищі. Сучасні методи та алгоритми можуть втрачати свою ефективність або навіть ставати непридатними, зокрема, в результаті збільшення трафіку та пропускної здатності. Це вимагає розробки нових алгоритмів, які зменшують обчислювальну складність і забезпечують швидкий аналіз трафіку без втрати точності.

Крім того, важливо впроваджувати новітні технології, такі як штучний інтелект і машинне навчання, в процеси моніторингу та аналізу. Це дозволяє автоматизувати виявлення аномалій і загроз, підвищити швидкість реагування на інциденти. Використання рішень для роботи з великими даними може значно підвищити ефективність аналізу, оскільки дає можливість обробляти великі обсяги інформації в режимі реального часу.

Таким чином, важливість розвитку нових технологій і алгоритмів моніторингу та аналізу мережевого трафіку є незаперечною і необхідною умовою забезпечення стабільності та безпеки корпоративних мереж. Орієнтація на проактивні заходи, такі як безперервний моніторинг та оцінка загроз, стає критично важливою для створення надійних механізмів захисту перед обличчям сучасних кібернетичних ризиків.

Основною вимогою до мереж є надання користувачам можливості доступу до вузлів і ресурсів усіх комп'ютерів, підключених до мережі. Це передбачає не тільки надійний доступ до даних і сервісів, а й дотримання високих стандартів безпеки для запобігання несанкціонованому доступу та витоку інформації. Дослідження та аналіз стану і постійний моніторинг телекомунікаційних мереж є актуальним завданням, оскільки сучасні загрози вимагають оперативного реагування на зміни в мережевій інфраструктурі та потенційні ризики.

Моніторинг дозволяє виявляти аномалії, аналізувати трафік, проводити аудит доступу та впроваджувати проактивні заходи безпеки. Сюди входить використання сучасних технологій, таких як системи виявлення вторгнень, антивірусні рішення і програми контролю доступу, які допомагають підвищити загальну надійність і відмовостійкість мережі.

Тому важливо не тільки забезпечити доступність ресурсів, але й гарантувати їх безпеку з метою збереження конфіденційності та цілісності даних, особливо в умовах зростаючих кіберзагроз.

Виходячи з вищевикладеного, перспективними для подальших досліджень є питання, пов'язані з інтеграцією традиційного поелементного підходу до оцінки показників надійності з сучасним макрорівневим підходом. Основним завданням цього дослідження буде створення єдиної математичної моделі, що поєднує характеристики надійності та інформаційної безпеки.

Для моделювання потоків управління подіями обох типів можуть бути використані марковські процеси та експоненціальний розподіл, за умови дотримання певних припущень.

Дослідження банківських корпоративних мереж буде здійснюватися шляхом перетворення мережевих структур у деревовидні графи, що дозволить візуалізувати зв'язки між елементами мережі та їх взаємодію. Такий підхід дозволить глибше зрозуміти динаміку мережевих процесів та виявити потенційні вразливості, які можуть вплинути на загальну безпеку та надійність корпоративної інфраструктури.

У дослідженнях, пов'язаних із поелементним підходом до оцінки показників надійності та інтеграцією характеристик інформаційної безпеки, активну участь беруть різні вчені та дослідники. Ось деякі з них: К. К. Квасневський – його роботи присвячені питанням надійності в комп'ютерних системах та інформаційних технологіях; А. І. Лапко – фахівець у сфері інформаційних систем, який досліджує методи оцінки надійності та безпеки інформаційних систем; С. С. Шевченко – автор публікацій, що стосуються моделювання складних систем, включаючи корпоративні мережі; М. В. Руденко

– його роботи стосуються математичного моделювання систем надійності, у тому числі у контексті інформаційних технологій; Т. А. Долгань – займається питаннями інтеграції інформаційної безпеки та надійності в інформаційних системах.

У зарубіжній науковій спільноті також є кілька відомих авторів, які проводять дослідження у сфері оцінки надійності та інформаційної безпеки, зокрема в контексті комп'ютерних мереж: Peter H. Feibelman – автор, що займається дослідженнями у сфері надійності програмного забезпечення та інформаційних систем; Avizienis A. – дослідник, який розробив концепції надійності, зокрема в системах з високими вимогами до безпеки; D. R. Stinson – відомий своїми дослідженнями в області теорії інформації та криптографії, а також безпеки інформаційних систем; B. Schneier – експерт з безпеки, що пише про інформаційну безпеку та технології захисту та інші.

Показником, який найкраще відображає характеристики надійності елементів корпоративної мережі, є коефіцієнт готовності. Існує практика стандартизації для корпоративних банківських мереж і ліній зв'язку в контексті мереж передачі даних. Однак існуючі стандарти не охоплюють корпоративні мережі передачі даних, які створюються на базі Інтернету. Це пов'язано з тим, що такі мережі частково абстраговані від конкретного постачальника послуг, що ускладнює їх стандартизацію.

Мета і задачі дослідження полягають в удосконаленні існуючих методів забезпечення ефективного функціонування корпоративних мереж шляхом розробки нових підходів до врахування впливу загроз інформаційній безпеці на функціонування вузлів мережевого зв'язку. Для досягнення поставленої мети в роботі вирішено наступні завдання:

– проведено аналіз існуючих правил та їх відповідності сучасним потребам корпоративних мереж, побудованих на основі інтернету;

– розроблено методику для оцінки коефіцієнту готовності, яка бере до уваги специфіку даних мереж;

– визначено основні загрози, які впливають на готовність вузлів банківської мережі, та оцінено їх вплив на сумарний коефіцієнт готовності;

– вдосконалено метод розрахунку впливу загроз доступності інформації на показник готовності вузлів мережі;

– розроблено систему моніторингу та керування ризиками, яка допоможе своєчасно виявляти та відповідно реагувати на загрози, підвищуючи ефективність функціонування банківської мережі.

Об'єктом дослідження є процеси, що відбуваються в корпоративних мережах у контексті загроз інформаційній безпеці.

Предметом дослідження виступають характеристики вузлів зв'язку, які впливають на ефективність роботи мережі.

Наукова новизна результатів кваліфікаційної роботи:

– вдосконалено марковську модель оцінки надійності вузла зв'язку мережі, за рахунок врахування впливу загроз, направлених на порушення доступності інформації;

– покращено метод дослідження мережі, заснований на моделюванні стану працездатності вузлів в умовах впливу атак на відмову в обслуговувані, за рахунок можливості кількісної оцінки їх впливу на ефективність роботи мережі.

Для дослідження продуктивності корпоративної мережі використовувалися різні методи. Одним з них є аналіз статистичних даних, який дозволяє вивчити історичні показники інцидентів безпеки, продуктивності мережі та їх взаємозв'язок із загрозами. Моделювання, як метод, допомагає створювати математичні або комп'ютерні моделі корпоративних мереж, що дає можливість імітувати різні сценарії загроз і оцінювати їх вплив на продуктивність мережі. Експертні висновки можуть бути використані для виявлення загроз і вразливостей, які можуть вплинути на мережу, а також для оцінки ефективності існуючих заходів безпеки. Тестування на проникнення допомагає виявити вразливості та оцінити реакцію системи безпеки. Безперервний моніторинг мережі за допомогою спеціалізованих інструментів допомагає виявляти аномалії та загрози в режимі реального часу.

Експериментальна перевірка здійснювалася шляхом виконання реальних експериментів із застосуванням як апаратного, так і програмного забезпечення, яке використовується на вузлах зв'язку в досліджуваній корпоративній мережі. Це включало налаштування і тестування різних компонентів мережі для оцінки їх продуктивності, надійності та стійкості до загроз інформаційної безпеки. Отримані результати дозволили проаналізувати ефективність існуючих заходів безпеки та виявити можливі вразливості, що впливають на загальний рівень захищеності мережі.

Запропонований метод базується на системному підході, що поєднує математичне моделювання, інтелектуальний аналіз даних з використанням AI і реальний моніторинг стану інфраструктури та .дозволяє проводити кількісну оцінку ефективності функціонування банківської мережі.

Теоретичні та практичні результати, здобуті в ході дослідження, були представлені й обговорені на міжнародних і всеукраїнських наукових конференціях. За матеріалами кваліфікаційної роботи опубліковано 2 тези.

1 АНАЛІЗ ФУНКЦІОНУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ У КОНТЕКСТІ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

1.1 Аналіз функціонування корпоративних мереж автоматизованих банківських систем

Теорія і практика в цій сфері відіграють важливу роль у процесі створення систем захисту автоматизованих банківських систем (АБС), які є невід'ємною частиною національних інформаційних ресурсів країни. Науково-методична база слугує основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення інформаційної безпеки (ІБ) держави на всіх рівнях. Ця база дозволяє адаптуватися до мінливих умов безпеки, оперативно реагувати на нові загрози та ризики, забезпечувати доступність, цілісність і конфіденційність інформаційних ресурсів [1]. Ці та інші вимоги регламентуються нормативними документами: НД ТЗІ 2.5-004-99; ДСТУ ISO/IEC 15408-1:2023 – ДСТУ ISO/IEC 15408-5:2023, та іншими [2, 3]. Застосування наукових підходів у цій області сприяє підвищенню ефективності управління ІБ, що, в свою чергу, забезпечує стабільність і безпечність фінансової системи держави.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» банківський сектор віднесено до об'єктів критичної інфраструктури [4]. Критична інфраструктура - це сукупність основних фізичних та організаційних структур, систем та активів, які є життєво важливими для функціонування суспільства та економіки. Порушення їх функціонування може призвести до серйозних наслідків, таких як загроза національній безпеці, економічним інтересам, здоров'ю населення або навколишньому середовищу [5].

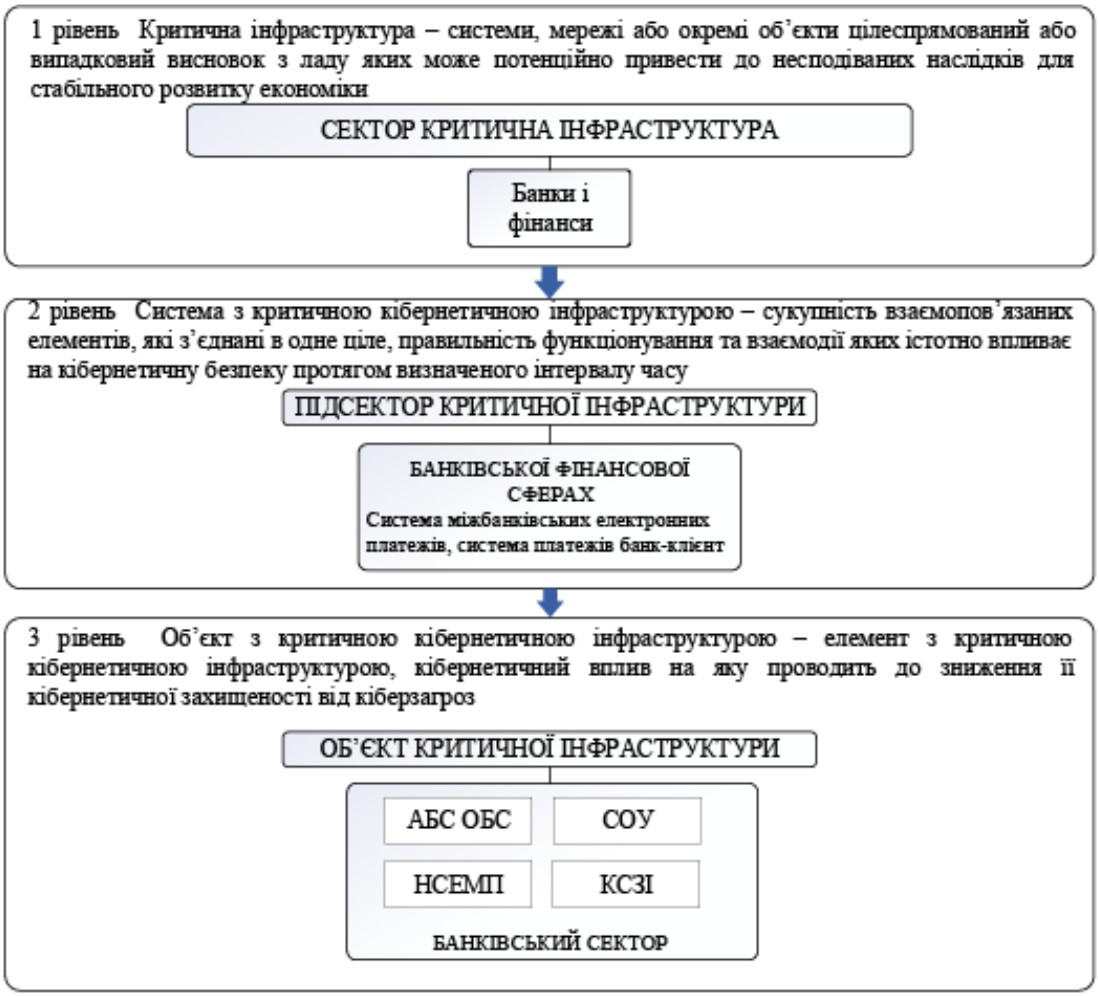


Рисунок 1.1 – Ієрархічна структура банківського сектору, як об'єкту критичної інфраструктури [6]

Перший крок - аналіз вимог до мережі. На цьому етапі визначаються специфікації, необхідні для забезпечення високої продуктивності, надійності та безпеки. Важливо врахувати кількість користувачів, обсяг даних, що передаються, та специфіку банківських операцій.

Наступний етап - проектування мережі, на якому створюється топологія, що включає фізичні та логічні компоненти. Це передбачає вибір відповідних мережевих технологій, таких як маршрутизатори, комутатори, брандмауери та інші елементи інфраструктури. Серед особливостей проектування також важливо розробити план резервного копіювання, щоб забезпечити безперервність роботи системи у випадку збоїв.

Після проектування наступним кроком є реалізація, яка включає в себе встановлення та налаштування мережевого обладнання, а також встановлення необхідного програмного забезпечення.

Завершальним етапом є тестування та оптимізація роботи мережі. Важливо забезпечити належний моніторинг мережевих активів для виявлення можливих загроз і аномалій в системі.

Успішна реалізація всіх цих етапів забезпечує надійне функціонування АБС, що є критично важливим для банківських установ, оскільки від цього залежить безпека фінансових операцій та даних клієнтів. Кінцевою метою є створення адаптивної та безпечної корпоративної мережі, здатної реагувати на змінні вимоги ринку та загрози інформаційної безпеки.

У сучасному бізнес-середовищі одним з найактуальніших питань для організацій є комплексна інформаційна безпека. Цей аспект має вирішальне значення для успішної роботи компанії. Інформаційні потоки, що передаються різними каналами, такими як телекомунікаційні лінії або розподільні інформаційні системи, можуть бути недостатньо захищені. Це підвищує ризик втрати корпоративної конфіденційної інформації. Витік важливої службової інформації стороннім особам може серйозно підірвати репутацію компанії. Зловмисники можуть використати ці дані для передачі їх конкурентам, тиску на керівництво організації або дискредитації її авторитету, зокрема через витік фінансової звітності та іншої чутливої економічної інформації.

Процеси захисту інформації в банківському секторі відіграють особливу роль у забезпеченні національної безпеки України, зокрема в економічній сфері. Автоматизовані банківські системи не лише спрощують процес статистичної звітності, але й легко адаптуються до змін, що запроваджуються НБУ [7]. Це розширює функціональність системи без потреби в значних програмних змінах (рис. 1.2).

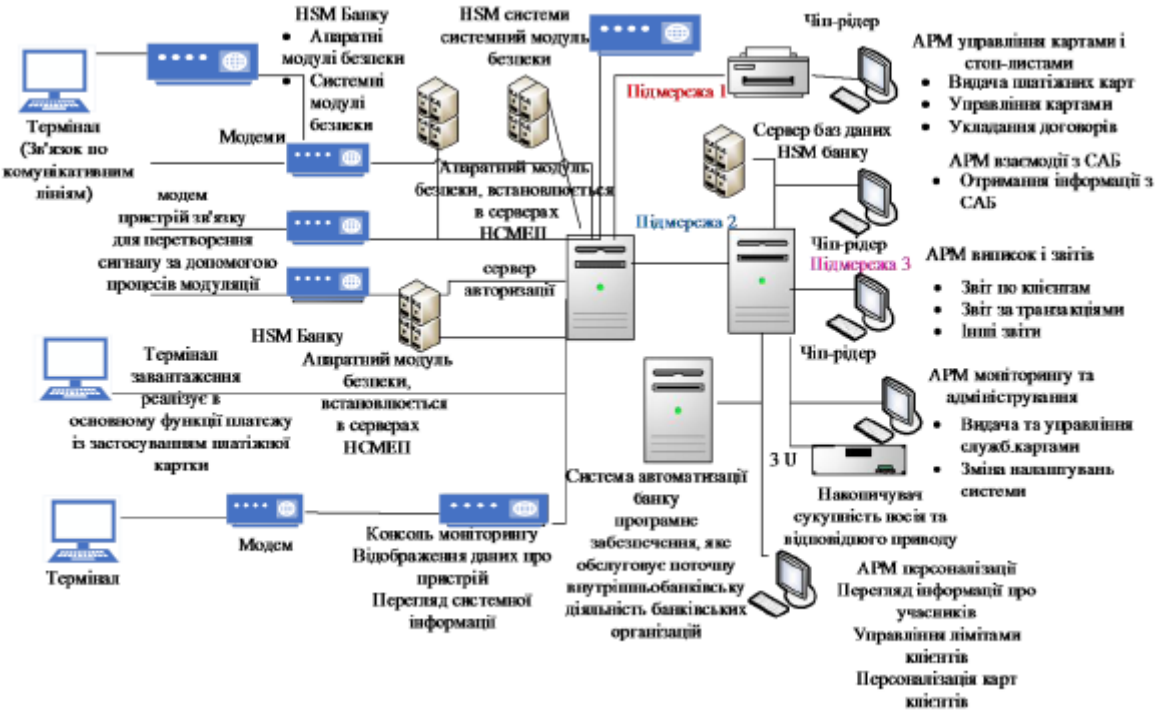


Рисунок 1.2 – Структура автоматизованої банківської системи

Таким чином, забезпечення інформаційної безпеки в банківському секторі є критично важливим для підтримки стабільності економіки та захисту інтересів національної безпеки.

1.2 Аналіз факторів, які впливають на функціонування мережі

Сучасні інформаційні системи стикаються з комплексними загрозами безпеки, що вимагає всебічного захисного підходу. Особливо вразливими стають кінцеві пристрої, які все частіше привертають увагу зловмисників.

Загрози можуть проникати різними шляхами - через електронні листи, вебсайти, сумнівні програми чи USB-носії. Типовий сценарій атаки включає поширення шкідливого коду та встановлення зв'язку з командним центром для подальших дій, як-от викрадення конфіденційних даних чи їх шифрування [8].

Захист забезпечується багаторівневою системою технологій, де кожен метод доповнює інші. На рівні проникнення застосовуються різноманітні засоби:

перевірка репутації файлів, захист веб-браузера, фільтрація посилань, мережевий екран, контроль пристроїв та програм. Важливим елементом є усунення вразливостей в операційних системах та програмному забезпеченні для запобігання поширенню загроз.

Виробничі процеси характеризуються надходженням даних з різноманітних джерел через канали змінної якості. Це спричиняє затримки в отриманні інформації, що ускладнює ефективне управління та планування. Диспетчерські служби часто перевантажені ручною обробкою даних, рутинними операціями та постійною комунікацією по телефону.

Сучасні системи безпеки активно використовують технології машинного навчання для проактивного та реактивного аналізу шкідливого програмного забезпечення. Це дозволяє виявляти загрози як на етапі попереднього сканування, так і під час виконання програм.

Спеціалізовані детектори здійснюють постійний моніторинг оперативної пам'яті, забезпечуючи захист від експлойтів, особливо в застарілих версіях операційних систем, які можуть мати відомі вразливості. Паралельно працюють системи виявлення аномальної активності, які відслідковують програми з підозріло високим споживанням ресурсів та здатні запобігати несанкціонованому шифруванню користувацьких файлів.

Фінальний рівень захисту забезпечується через моніторинг мережевої активності за допомогою спеціалізованих командних центрів. Вони аналізують патерни трафіку, виявляють підозрілі з'єднання та блокують потенційні канали витоку даних [9].

Комплексна безпека комп'ютерних мереж починається з ретельного аналізу можливих векторів атак та вразливостей [10]. Це включає:

– оцінку наявної інфраструктури та її слабких місць;
– аналіз потенційних зовнішніх та внутрішніх загроз;
– визначення критичних активів, що потребують посиленого захисту;
– розробку багаторівневої стратегії захисту;
– впровадження систем раннього виявлення та реагування на інциденти;

– регулярний аудит та оновлення систем безпеки;

– навчання персоналу щодо кібербезпеки та правил інформаційної гігієни.

Такий комплексний підхід дозволяє створити ефективну систему захисту, здатну протистояти сучасним кіберзагрозам.

Для розуміння сучасних викликів мережевої безпеки необхідно провести детальний аналіз типової корпоративної мережі, розглядаючи її основні характеристики та вразливості. Такий аналіз дозволяє виявити потенційні слабкі місця та розробити ефективну стратегію захисту.

Сучасні мережеві атаки найчастіше базуються на різноманітних маніпуляціях з IP-протоколом. Зловмисники активно використовують спуфінг IP-адрес, здійснюють маніпуляції з маршрутизацією та перехоплюють діапазони IP-адрес. Також поширеними є несанкціоноване сканування мережевої інфраструктури, збір критичної інформації про мережеву топологію, компрометація DNS-серверів та проведення атак типу "людина посередині" [11].

Для створення надійної системи захисту першочергово рекомендується впровадження контролю доступу на рівні портів. Це включає реалізацію прив'язки IP-MAC адрес, впровадження динамічної інспекції ARP та використання технології Port Security [12]. Важливим аспектом є постійний моніторинг несанкціонованих підключень та автоматична блокування підозрілої активності.

Наступним важливим кроком є маскування мережевої інфраструктури. Це досягається через впровадження NAT/PAT технологій, використання проксі-серверів та правильну сегментацію мережі. Впровадження VLAN та використання VPN для віддаленого доступу також значно підвищують рівень захисту мережевої інфраструктури [13].

Особливу увагу слід приділити управлінню доступом. Це передбачає створення та підтримку актуальних списків контролю доступу, впровадження рольової моделі та сегментацію мережі за рівнем доступу. Регулярний моніторинг та аудит доступу, впровадження систем AAA та періодичний перегляд політик доступу є необхідними елементами безпечної мережевої

інфраструктури [14].

Додатково рекомендується впровадження систем виявлення та запобігання вторгнень, проведення регулярного аудиту безпеки мережі та постійний моніторинг мережевого трафіку. Створення резервних каналів зв'язку, впровадження систем резервного копіювання та систематичне навчання персоналу основам мережевої безпеки доповнюють комплексний підхід до захисту.

Такий всебічний підхід до захисту мережевої інфраструктури дозволяє суттєво підвищити рівень безпеки та мінімізувати ризики успішних атак. При цьому важливо регулярно оновлювати та адаптувати заходи безпеки відповідно до нових викликів та загроз, що постійно з'являються в світі кібербезпеки.

1.2 Підходи до дослідження захищеності функціонування вузлів мережі

Ефективна оцінка стану інформаційної безпеки є фундаментальним етапом у побудові надійної системи захисту. Сучасна практика виділяє два принципово різні підходи до такої оцінки: метод "знизу вгору" та метод "зверху вниз", кожен з яких має свої переваги та обмеження [14].

Метод "знизу вгору" передбачає активне тестування системи безпеки через симуляцію потенційних атак [15]. Адміністратори безпеки виступають у ролі етичних хакерів, намагаючись виявити вразливості системи через проведення контрольованих атак. Цей підхід має суттєву перевагу в тому, що дозволяє виявити реальні, практичні вразливості системи. Проте він має значні обмеження: неможливість передбачити всі можливі вектори атак, обмеженість ресурсів для тестування та ризик пошкодження систем під час тестування. Крім того, цей метод може пропустити складні, багатоетапні атаки або нові, ще невідомі вектори загроз.

Метод "зверху вниз" представляє собою системний аналітичний підхід, який починається з всебічного вивчення інформаційної архітектури організації.

Цей метод включає детальне картографування інформаційних потоків, ідентифікацію критичних активів та аналіз існуючих механізмів захисту. Особлива увага приділяється класифікації інформаційних ресурсів за рівнями важливості та вимогами до їх захисту. Перевагою такого підходу є його комплексність та можливість виявити системні проблеми в архітектурі безпеки. Однак він може бути більш часозатратним [15].

Найбільш ефективним рішенням є комбінований підхід, який об'єднує переваги обох методів. Такий підхід дозволяє не лише виявити практичні вразливості, але й забезпечити системне розуміння ризиків та загроз [16-18].

Завершальним етапом оцінки є комплексний аналіз ризиків. Цей процес виходить за межі простого множення ймовірності атаки на потенційні збитки. Він повинен враховувати:

- прямі фінансові втрати від порушення безпеки;
- репутаційні ризики та втрату довіри клієнтів;
- можливі юридичні наслідки та штрафи;
- витрати на відновлення систем;
- втрати від простою бізнес-процесів;
- потенційний витік інтелектуальної власності;
- вплив на конкурентоспроможність організації.

Важливо регулярно переглядати та оновлювати оцінку безпеки, враховуючи появу нових загроз, зміни в інфраструктурі та бізнес-процесах організації. Це повинен бути безперервний процес, а не одноразова подія.

Крім того, результати оцінки повинні бути основою для розробки стратегії безпеки, включаючи планування інвестицій в засоби захисту, навчання персоналу та розробку політик безпеки. Важливо також забезпечити баланс між рівнем захисту та зручністю використання систем, оскільки надмірно жорсткі заходи безпеки можуть негативно впливати на ефективність роботи організації.

Процес формування оцінки захищеності комп'ютерної системи базується на циклічному підході, що відповідає методології Демінга-Шухарта (рис 1.3) [19].

Це забезпечує постійне вдосконалення системи захисту через регулярні переоцінки та коригування захисних механізмів.

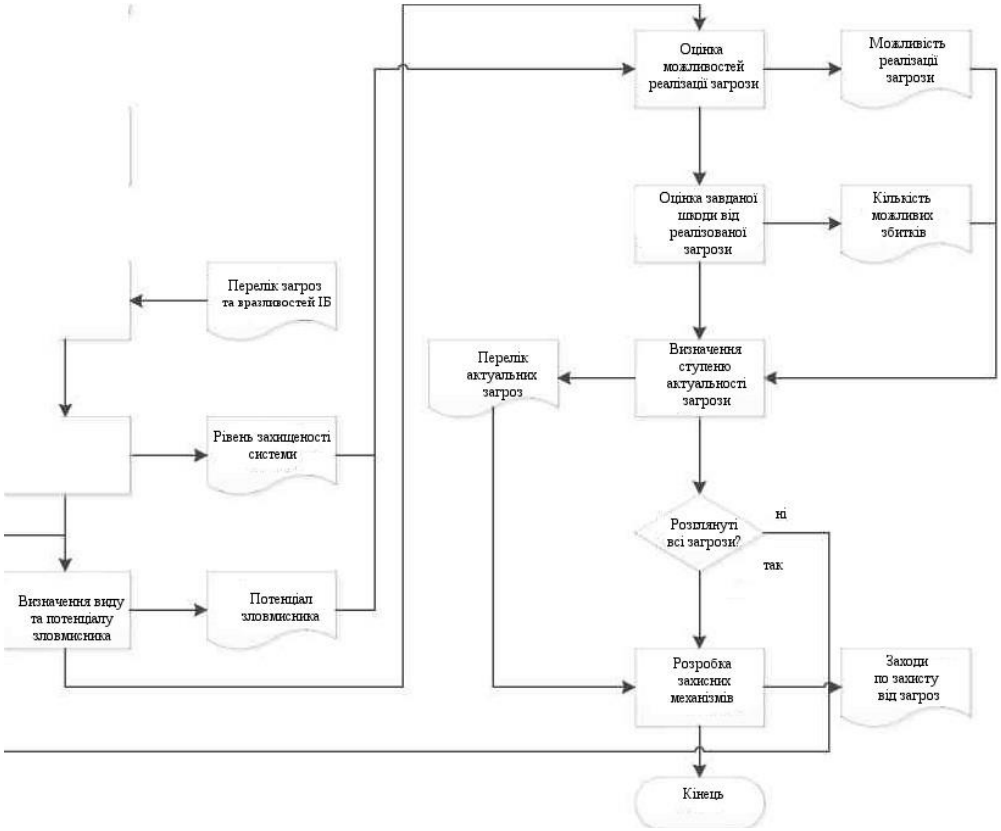


Рисунок 1.3 – Алгоритм оцінки захищеності мережі

Однак сучасні реалії кібербезпеки створюють значні виклики для такого підходу. Основна складність полягає у необхідності постійної актуалізації оцінки загроз в умовах надзвичайно динамічного характеру кіберзагроз. Інформаційно-комунікаційні системи стикаються з постійно еволюціонуючими загрозами, що вимагає безперервного моніторингу та оновлення методів захисту. Наразі відсутні повноцінні автоматизовані рішення для проведення такої комплексної оцінки, що суттєво ускладнює процес регулярного перегляду рівня захищеності.

З точки зору теорії дослідження операцій, оцінка ефективності інформаційно-комунікаційних систем представляє собою багатокритеріальну оптимізаційну задачу. Метою є визначення такої конфігурації системи, яка перевершує еталонні показники за визначеними критеріями в заданих умовах експлуатації.

Використання сертифікованих рішень для шифрування переданої інформації є важливим кроком у захисті від загроз, зосереджених на конфіденційності та цілісності даних. Це зменшує ймовірність того, що зловмисники зможуть отримати доступ до конфіденційної інформації шляхом перехоплення трафіку. Проте загрози, спрямовані на порушення інформаційної доступності, реалізуються за залишковим принципом, переважно через резервування каналів зв'язку. Це рішення ефективне для захисту від випадкових або незначних загроз, таких як пошкодження ліній зв'язку або відключення електроенергії на проміжних вузлах. Водночас перехід до Інтернету як основного середовища передачі даних несе нові ризики, зокрема, можливість атак на вузли зв’язку, які можуть вразити не лише основний канал, а й резервний. Це значно знижує ефективність резервування каналів як методу захисту від загроз доступності інформації. Зловмисники можуть цілеспрямовано атакувати будь-який мережевий вузол, який є частиною глобальної інфраструктури Інтернету, і таким чином паралізувати як основний, так і резервний канали зв’язку. Дане дослідження присвячене розробці методики оцінки ефективності захисту телекомунікаційних мереж від загроз ІБ, спрямованих на порушення доступності інформації. Зокрема, це дозволить створити алгоритми прогнозування потенційних ризиків і розробити більш ефективні методи захисту з урахуванням нових умов функціонування мережі в умовах глобалізації та відкритості Інтернету.

У роботі аналізуються загрози інформаційній безпеці, спрямовані на порушення нормального функціонування банківської мережі. Зі списку можливих загроз розглядаються ті, що відповідають наступним критеріям: По-перше, загроза має бути спрямована на порушення доступності інформації, тобто її реалізація повинна викликати тимчасове або повне припинення доступу до даних, що передаються через мережу. По-друге, об’єктами цієї загрози є вузли зв’язку, їх компоненти та телекомунікаційне обладнання, встановлене на цих вузлах у межах досліджуваної мережі. Іншими словами, вплив буде спрямований на критичні елементи мережі, які забезпечують передачу інформації. По-третє,

реалізація загрози відбувається в рамках існуючої інфраструктури ТСМ, тобто загроза реалізується за допомогою існуючих технологій і ресурсів, які є частиною мережі, і може бути викликана як внутрішніми, так і зовнішніми факторами. Таким чином, ці критерії визначають обсяг загроз, які будуть досліджуватися в контексті забезпечення стабільності та надійності телекомунікаційної мережі в умовах впливу потенційних атак на доступність її ресурсів (рис. 1.4).

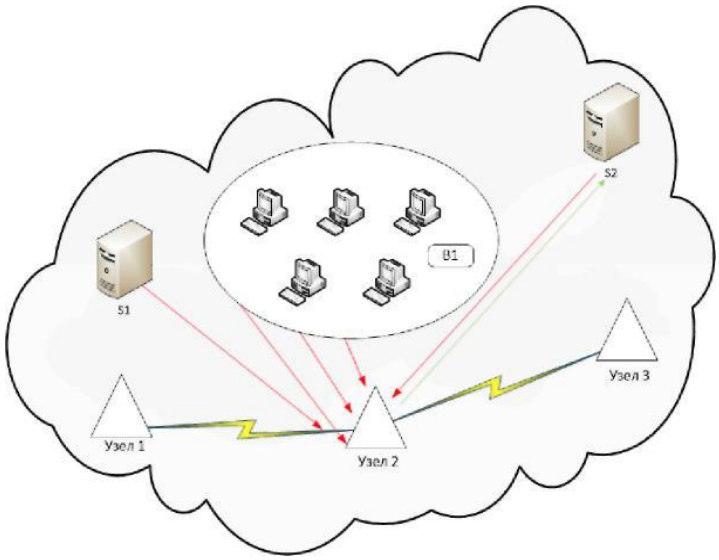


Рисунок 1.4 – Механізм здійснення DDOS атак

Особливу важливість має правильний вибір системи показників якості. Сучасний підхід передбачає використання ієрархічної структури показників, де локальні показники відображають специфічні аспекти функціонування системи:

- показники надійності захисних механізмів;
- метрики швидкодії та продуктивності;
- параметри доступності системи;
- показники цілісності даних;
- метрики виявлення та реагування на інциденти;
- економічні показники ефективності захисту.

Глобальний показник ефективності формується через інтеграцію цих локальних метрик з урахуванням їх взаємозв'язків та відносної важливості [20]. При цьому важливо забезпечити:

– об'єктивність оцінки через використання вимірюваних параметрів;

– можливість порівняння різних варіантів захисту;

– врахування специфіки конкретної організації;

– адаптивність до змін у середовищі загроз;

– економічну обґрунтованість впроваджуваних заходів.

Для підвищення ефективності оцінки необхідно розвивати автоматизовані системи аналізу захищеності, які могли б [21-23]:

– здійснювати постійний моніторинг стану безпеки;

– автоматично виявляти нові загрози та вразливості;

– прогнозувати потенційні ризики;

– забезпечувати оперативне реагування на інциденти.

Таким чином, сучасна оцінка захищеності комп'ютерних систем вимагає комплексного підходу, що поєднує методологічну базу, автоматизовані засоби аналізу та експертну оцінку для забезпечення адекватного рівня захисту в умовах динамічного ландшафту кіберзагроз.

Процес обробки інформації на мережевому вузлі являє собою складний багатоетапний процес, який суттєво впливає на загальну ефективність передачі даних в мережі. Коли інформація надходить від передавача до мережевого вузла, вона проходить через декілька критичних етапів обробки, кожен з яких може створювати певні затримки в загальному процесі передачі (рис.1.5) [24].

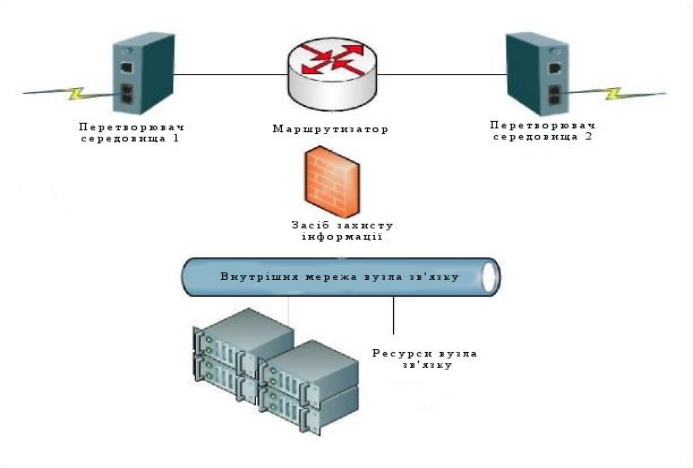


Рисунок 1.5 – Обробка трафіку

Початковим етапом є прийом даних від передавача, після чого відбувається конвертація форматів інформації відповідно до вимог мережевих протоколів та специфікацій. Наступним важливим етапом є аналіз та обробка мережевого трафіку, що включає перевірку цілісності даних, фільтрацію пакетів та оцінку пріоритетності передачі. На основі цього аналізу приймається рішення про маршрутизацію - визначається оптимальний шлях подальшої передачі даних до кінцевого одержувача [25-27].

Латентність на кожному етапі обробки значною мірою залежить від технічних характеристик обладнання. Ключову роль відіграє продуктивність процесорів, об'єм та швидкодія оперативної пам'яті, пропускна здатність інтерфейсів та загальна архітектура мережевих компонентів. Не менш важливими є характеристики самого трафіку: його загальний обсяг, інтенсивність потоку пакетів, розмір окремих пакетів та їх пріоритетність [28].

Особливу увагу варто приділити специфіці процесів обробки даних. Складність алгоритмів маршрутизації, необхідність шифрування та дешифрування інформації, вимоги до перевірки безпеки, процеси буферизації та операції конвертації форматів – усі ці фактори суттєво впливають на загальну затримку обробки даних на вузлі [29-32].

Для оптимізації роботи мережевого вузла критично важливим є правильне балансування навантаження між компонентами, вдосконалення алгоритмів обробки та впровадження ефективних механізмів кешування. Особливу роль відіграє пріоритезація критичного трафіку та постійний моніторинг продуктивності системи.

Сучасні тенденції розвитку мережевих технологій вимагають все більш ефективної обробки зростаючих обсягів даних. Це досягається через використання спеціалізованих процесорів, впровадження технологій віртуалізації та застосування методів штучного інтелекту для оптимізації маршрутизації. Важливу роль також відіграють технології розподіленої обробки даних та системи адаптивного управління ресурсами [33-36].

Глибоке розуміння особливостей процесу обробки даних на мережевому вузлі є фундаментальним для проектування ефективних мережевих архітектур, оптимізації їх продуктивності та забезпечення належної якості обслуговування. Це також критично важливо для планування розвитку інфраструктури та своєчасної діагностики проблем продуктивності.

Таким чином, ефективність роботи мережевого вузла залежить від комплексного врахування всіх факторів, що впливають на обробку даних, та своєчасного впровадження сучасних технологій оптимізації мережевого трафіку. Постійний моніторинг та аналіз продуктивності дозволяє вчасно виявляти потенційні проблеми та вживати необхідних заходів для їх усунення.

Найбільші виробники мережевого обладнання розробляють спеціалізовані рішення, спрямовані на забезпечення всебічного захисту корпоративних мереж. Одним із таких рішень є технологія NAC (Network Access Control) від компанії Cisco [38, 39]. Ця технологія забезпечує контроль доступу, перевіряючи пристрої та користувачів під час підключення до корпоративної мережі. Вона також здатна блокувати доступ пристроїв, які не відповідають встановленим політикам безпеки. До таких пристроїв належать системи, інфіковані вірусами чи шкідливим програмним забезпеченням, пристрої без актуальних антивірусних баз, а також ті, що не мають необхідних оновлень операційної системи. Це дозволяє ефективно знижувати ризики та підтримувати високий рівень безпеки в мережі.

1.4 Постановка задачі

Цифрова оцінка ефективності роботи вузлів мережі має принципове значення для розвитку сучасних корпоративних інформаційних систем. Його реалізація дозволяє досягти кількох критично важливих цілей. По-перше, кількісні методи оцінки значно підвищують точність прогнозування можливих збоїв обладнання та наслідків кіберзагроз. Це досягається за рахунок

використання математичних моделей і методів статистичного аналізу, які забезпечують об'єктивність отриманих результатів на відміну від суб'єктивних експертних оцінок. По-друге, цифровий підхід до оцінки ефективності дозволяє створити комплексну систему моніторингу стану мережевої інфраструктури. Це забезпечує можливість раннього виявлення потенційних проблем і своєчасного вжиття профілактичних заходів, що значно підвищує загальну надійність системи. По-третє, математичні методи оцінки створюють основу для прийняття оптимальних управлінських рішень щодо розвитку та модернізації мережевої інфраструктури. Це дозволяє ефективно розподіляти ресурси та інвестиції в найбільш критичні компоненти системи.

Теоретична основа дослідження охоплює ключові аспекти архітектури корпоративних мереж, принципи побудови систем захисту інформації та методології оцінки їх ефективності. Особливу увагу приділено аналізу функціональних характеристик вузлів зв'язку як базових елементів мережевої інфраструктури.

Дослідження включає детальний аналіз властивостей інформації, яка може бути скомпрометованавм різними кіберзагрозами. Це дозволило створити комплексну модель оцінки вразливостей та ризиків, яка враховує специфіку сучасних інформаційних систем та актуальні вектори атак.

Такий системний підхід забезпечує цілісне розуміння проблематики захисту корпоративних мереж та створює методологічне підґрунтя для розробки ефективних механізмів протидії сучасним кіберзагрозам. Практичне значення отриманих результатів полягає в можливості їх безпосереднього застосування для вдосконалення систем управління інформаційною безпекою в організаціях різного розміру та галузевої приналежності.

В рамках дослідження необхідно виконати наступні завдання:

– провести аналіз існуючих правил та їх відповідності сучасним потребам корпоративних мереж, побудованих на основі інтернету;

– розробити методику для оцінки коефіцієнту готовності, яка б брала до уваги специфіку даних мереж;

– визначити основні загрози, які впливають на готовність вузлів банківської мережі, і оцінити їх вплив на сумарний коефіцієнт готовності;

– вдосконалити метод оцінки впливу загроз доступності інформації на показник готовності вузлів мережі;

– розробити систему моніторингу та керування ризиками, яка допоможе своєчасно виявляти та відповідно реагувати на загрози, підвищуючи ефективність функціонування банківської мережі.

2 МОДЕЛЮВАННЯ ПРОЦЕСУ ФУНКЦІОНУВАННЯ МЕРЕЖІ

2.1 Математичне моделювання оцінки стану пристроїв

Математичне моделювання рівня захищеності інформаційних систем є складним та багатокритеріальним завданням, яке вимагає комплексного підходу. Процес оцінки базується на використанні математичного апарату, що дозволяє кількісно оцінити ефективність впроваджених засобів захисту та визначити оптимальну конфігурацію системи безпеки.

Процес математичної оцінки починається з формування системи критеріїв та метрик, які повинні враховувати специфіку конкретної організації. Ці метрики можуть включати показники надійності системи, час відгуку на інциденти, рівень доступності сервісів, показники виявлення вторгнень та інші параметри, що характеризують ефективність захисту [40].

Важливим аспектом є врахування взаємозалежності різних компонентів системи захисту. Наприклад, посилення одного аспекту безпеки може негативно вплинути на інший. Тому математична модель повинна враховувати ці взаємозв'язки та дозволяти знаходити оптимальний баланс між різними параметрами.

Вибір оптимального варіанту захисту здійснюється на основі багатокритеріальної оптимізації, де враховуються не лише технічні параметри, але й економічні фактори, такі як вартість впровадження та підтримки системи захисту, потенційні збитки від можливих атак, витрати на навчання персоналу тощо.

Перспективним напрямком розвитку є використання інформаційно-орієнтованого підходу, який дозволяє адаптувати систему оцінки під конкретні потреби організації. Цей підхід особливо актуальний для великих підприємств, де традиційні методи оцінки можуть бути недостатньо гнучкими.

Сучасні методи математичної оцінки також повинні враховувати динамічний характер загроз безпеці. Це означає, що модель повинна бути адаптивною та здатною враховувати нові типи загроз та вразливостей. Важливим

елементом є також можливість прогнозування потенційних ризиків на основі історичних даних та аналізу тенденцій.

Для підвищення точності оцінки доцільно використовувати методи машинного навчання та штучного інтелекту, які дозволяють автоматизувати процес аналізу великих обсягів даних про безпеку та виявляти приховані закономірності. Це особливо важливо в умовах постійного зростання складності кіберзагроз.

Процес формування оцінки захищеності повинен бути циклічним та включати постійний моніторинг ефективності впроваджених заходів, їх корегування та оптимізацію. Важливо також забезпечити можливість порівняння різних варіантів захисту та їх комбінацій для вибору найбільш ефективного рішення [41-43].

При цьому необхідно враховувати не тільки технічні аспекти, але й людський фактор, оскільки навіть найдосконаліша система захисту може бути скомпрометована через помилки або недбалість персоналу. Тому математична модель повинна включати оцінку ризиків, пов'язаних з людським фактором.

Таким чином, математична оцінка рівня захисту є комплексним завданням, яке вимагає врахування множини факторів та використання сучасних методів аналізу даних. Постійне вдосконалення методів оцінки та їх адаптація до нових викликів є необхідною умовою забезпечення ефективного захисту інформаційних систем.

Для створення моделі станів вузлів корпоративної мережі та оцінки їхнього впливу на мережу в цілому, необхідно виконати кілька етапів. Спочатку слід визначити можливі стани, у яких можуть перебувати окремі вузли мережі, а також ідентифікувати причини, що призводять до переходів між цими станами. Це можуть бути фактори, пов’язані з апаратними збоями, перевантаженнями, оновленнями програмного забезпечення чи кіберзагрозами [44].

Далі потрібно вибрати ключовий показник, що характеризує загальний стан мережі. Він має залежати від станів окремих вузлів, наприклад, пропускна здатність, затримки в передачі даних, рівень доступності або показники безпеки.

Для визначення поточних станів вузлів збираються експериментальні дані за допомогою засобів моніторингу, таких як системи аналізу трафіку чи журналів подій.

Наступним етапом є побудова графа мережі. У цьому графі вершини відповідають окремим вузлам, а ребра - зв’язкам між ними. На основі отриманого графа та даних про стан вузлів можна розрахувати значення обраного ключового показника для всієї мережі, використовуючи методи статистичного аналізу чи машинного навчання [45].

Отримана модель дозволяє не лише аналізувати вплив станів окремих вузлів на загальний стан мережі, але й прогнозувати її поведінку у разі змін умов. При необхідності модель можна уточнювати, додаючи нові можливі стани вузлів, причини переходів між ними або додаткові показники, що впливають на якість мережі.

Цей підхід забезпечує комплексний підхід до оцінки стійкості та надійності корпоративної мережі, дозволяючи ефективно ідентифікувати її слабкі місця та підвищувати загальну ефективність і безпеку мережевої інфраструктури.

Стандартним підходом до розрахунку коефіцієнта готовності *Fa* для мереж складної топології є її декомпозиція на підмережі з лінійною структурою. Цей процес триває, поки залишкові компоненти мережі не набудуть вигляду паралельно-послідовних схем. Такий метод дозволяє спростити аналіз складних топологій і зробити розрахунок більш керованим.

Для визначення коефіцієнта готовності послідовно з'єднаних пристроїв застосовується теорема про ймовірності незалежних подій. Вона передбачає, що ймовірність безвідмовної роботи всіх елементів у послідовному з'єднанні визначається як добуток їхніх індивідуальних ймовірностей готовності. Формула для розрахунку коефіцієнта готовності в такому випадку виглядає наступним чином:

$$Fa_{\text{посл}} = Fa_{\text{х}} \cdot Fa_2 \cdot \ldots \cdot Fa_{n.} \qquad (2.1)$$

де Fa_i — коефіцієнт готовності кожного окремого пристрою в послідовному з’єднанні.

Аргументуючи цей підхід, можна зазначити, що в послідовно з'єднаній системі відмова будь-якого елемента призводить до відмови всієї системи. Таким чином, показник готовності мережі значно залежить від надійності кожного з її компонентів.

Для складніших паралельно-послідовних структур коефіцієнт готовності розраховується з урахуванням імовірностей безвідмовної роботи як для паралельних, так і для послідовних частин мережі. Такий методичний підхід дозволяє точно оцінити надійність мереж складної архітектури, що особливо важливо для критично важливих систем, де безперервність роботи є ключовою вимогою.

Коефіцієнт готовності паралельно з'єднаних вузлів розраховується по формулі (2.2) [46, 47]:

$$Fa_{\text{парал}} = 1 - (1 - Fa_x) \cdot (1 - Fa_2) \cdot \ldots \cdot (1 - Fa_n), \qquad (2.2)$$

де Fa_i коефіцієнт готовності паралельно з’єднаних вузлів.

Для оцінки характеристик надійності мережі складної топології можна скористатися методом декомпозиції, розбиваючи її на підмережі з лінійною топологією. Ці підмережі моделюють шляхи передачі трафіку між вершинами графа, які виступають у ролі передавача та кінцевого приймача інформації. Такий підхід дозволяє спростити розрахунок надійності складної системи шляхом аналізу її простіших компонентів.

Зібравши статистичні дані про функціонування пристроїв банківської мережі, можна визначити частоту їх відмов і час, проведений у працездатному та неробочому стані. Це досягається шляхом моніторингу та аналізу подій, таких як збої або періоди технічного обслуговування. Важливо врахувати, що вузли

мережі є відновлюваними об'єктами, тобто після відмови їх можна повернути до працездатного стану.

На рисунку 2.1 представлено схему станів обладнання. У ній початковий стан (1) відповідає працездатному режиму об’єкта, тоді як кінцевий стан (2) відповідає відмові вузла. Параметри μ (інтенсивність відновлень) і λ (інтенсивність відмов) характеризують імовірнісні переходи між цими станами. Ці показники можна використовувати для побудови марковських моделей, що дозволяють прогнозувати поведінку мережі та оцінювати її надійність у різних сценаріях.

Аргументуючи важливість цього підходу, слід зазначити, що він забезпечує не лише глибоке розуміння процесів, які впливають на надійність мережі, але й дозволяє виявляти її слабкі місця. Це, у свою чергу, сприяє розробці заходів для підвищення стійкості та ефективності мережевої інфраструктури.

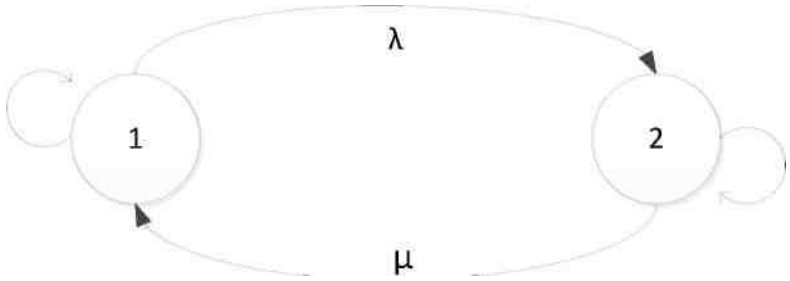


Рисунок 2.1 –Графічне представлення вузла мережі

Відповідно до [48], інтенсивність потоку відмов λ(t) визначається як відношення кількості неробочих пристроїв до середнього числа працездатних пристроїв у заданому часовому інтервалі. Формула для її обчислення має вигляд

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

де:

– Δt – інтервал часу;

– $n(t)$ — кількість пристроїв, які перебувають у непрацездатному стані в інтервалі часу Δt;

– Nср — середня кількість працездатних пристроїв протягом інтервалу часу.

Альтернативна форма запису інтенсивності потоку відмов базується на використанні ймовірності виявлення непрацездатного вузла:

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

де:

– N_0 – кількість працездатних вузлів на початок інтервалу;

– а (t) – середня вірогідність виявлення пристрою в непрацездатному стані.

Середня ймовірність виявлення пристрою в непрацездатному стані розраховується за формулою (2.5):

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

де:

– $n\ (t)$ – кількість непрацездатних пристроїв протягом інтервалу часу;

– N_0 – кількість працездатних пристроїв;

– $\bar{t_в}$ – середній час перебування пристрою в непрацездатному стані;

– Δt - тривалість інтервалу часу.

Такий підхід дозволяє чітко оцінити інтенсивність потоку відмов, враховуючи як кількісні характеристики, так і часову динаміку. Він є ефективним інструментом для аналізу надійності мережевої інфраструктури, дозволяючи виявити вузькі місця, прогнозувати поведінку системи та розробляти стратегії її оптимізації.

Враховуючи випадковий характер відмов вузлів, точне визначення кількості працездатних вузлів у мережі є складним завданням. У зв'язку з цим використовується прогнозування числа працездатних вузлів за формулою:

$$N(\Delta t) = N0 \times (1 - \frac{n(\Delta t) \times \bar{t}_{\text{в}}}{\Delta t}), \quad (2.6)$$

де:

– $n\ (\Delta t)$ – кількість пристроїв, які вийшли з ладу протягом інтервалу часу;

– $\bar{t}_{\text{в}}$- середній час відмови пристрою;

– N_0 - кількість працездатних вузлів на початку інтервалу;

– Δt - тривалість інтервалу часу.

Середнє число вузлів, що знаходяться у робочому стані протягом інтервалу, визначається як середнє арифметичне між початковою кількістю працездатних вузлів та прогнозованим значенням:

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

Середній час відновлення вузла визначається на основі статистичних даних, отриманих шляхом спостережень за процесом відновлення елементів мережі. Для цього будують графік апроксимуючої функції, яка описує закон розподілу часу відновлення. Значення обчислюється за формулою:

$$\bar{t}_{\text{в}} = \frac{1}{\text{i}} \int_{\text{i}}^{1} f(i), \quad (2.8)$$

де:

– i - число прецедентів відновлення працездатності вузла;

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

Коефіцієнт оперативної готовності визначається як ймовірність того, що об'єкт, перебуваючи в стані очікування, буде працездатним у будь-який момент

часу [49]. Він також враховує, що від моменту перевірки об’єкт залишатиметься у працездатному стані протягом заданого періоду. Цей показник є важливим індикатором для оцінки ефективності мережі в режимі реального часу та її здатності забезпечувати безперервність роботи.

Запропонований підхід дозволяє враховувати як прогнозовані, так і фактичні характеристики мережі, забезпечуючи більш точну оцінку її надійності та готовності.

Важливими інтегральними характеристиками надійності є показники, що враховують загальну та питому трудомісткість технічного обслуговування та ремонту. Вони включають середню загальну трудомісткість обслуговування, яка визначається як математичне сподівання загальних витрат праці на обслуговування за певний період експлуатації. Також враховується середня сумарна трудомісткість ремонтів, яка відображає сумарні витрати праці на всі види ремонтів за певний період експлуатації системи, та середні сумарні витрати на технічне обслуговування, які є математичним сподіванням усіх витрат на утримання та відновлення об'єкта під час його експлуатації.

Для цих показників використовуються конкретні значення, розраховані як відношення середніх загальних витрат до математичних сподівань загального часу роботи об'єкта за певний період. Крім того, важливими характеристиками є коефіцієнт відновлення, який відображає ймовірність повернення об'єкта в робочий стан після відмови, і коефіцієнт відновлення ресурсу, який враховує здатність системи зберігати працездатність після ремонту.

Показники експлуатаційної ефективності також є важливим аспектом, оскільки вони описують витрати, пов'язані з підготовкою об'єктів до експлуатації, плановим обслуговуванням під час експлуатації та завершенням робіт після експлуатації. Такі витрати включають витрати на оплату праці, витрати на початкову підготовку, технічне обслуговування під час експлуатації та післяопераційні дії, такі як консервація або утилізація. Цілісний підхід до оцінки цих показників дозволяє забезпечити оптимальну економічну ефективність технічного обслуговування та ремонту, а також підвищити загальну надійність і

стійкість систем протягом усього життєвого циклу. Це особливо важливо для складних технічних систем, де експлуатаційні витрати складають значну частку загальних витрат.

Час між відмовами телекомунікаційного пристрою визначається як період його безперервної роботи від початку роботи до першої відмови. Цей показник є ключовим для оцінки надійності обладнання, оскільки дозволяє прогнозувати тривалість ефективної роботи системи без необхідності втручання або ремонту. Коефіцієнт миттєвої доступності відображає ймовірність того, що пристрій знаходиться в робочому стані в певний час. Ця характеристика є динамічною і залежить від ряду факторів, включаючи частоту відмов і тривалість відновлення працездатності. Фізичний зміст коефіцієнта миттєвої доступності полягає в тому, що він демонструє працездатність системи забезпечувати виконання своїх функцій у будь-який момент часу, що критично важливо для телекомунікаційних мереж з високими вимогами до безперебійності.

Зв'язок між коефіцієнтом доступності вузла мережі, кількістю відмов обладнання та тривалістю його відновлення дозволяє проводити розрахунки на основі статистичних даних, зібраних протягом обмеженого періоду. Використання цих даних дозволяє формувати прогнозні моделі, які враховують реальні умови роботи та приймати обґрунтовані рішення щодо оптимізації роботи мережі. Такий підхід дозволяє підвищити ефективність телекомунікаційної інфраструктури, забезпечити її безперервність і мінімізувати ризики, пов’язані з поломками обладнання [50].

Враховуючи середній коефіцієнт готовності на інтервалі часу з t_1 до t_2 (2.9):

$$Fa = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} e^{-\lambda \times t}\, dt, \tag{2.9}$$

Використання експоненціального закону розподілу для аналізу впливу загроз інформаційній безпеці, спрямованих на порушення доступності інформації, потребує додаткового обґрунтування. Це пов'язано з тим, що

недостовірність даних про частоту і тривалість аварій істотно ускладнює визначення характеру поширення цих загроз. Відсутність достовірної інформації не дозволяє однозначно встановити, чи відповідає характер впливу загроз експоненціальному закону розподілу чи іншим моделям. Для вирішення цього питання в рамках магістерського дослідження в третьому розділі розроблено методику врахування впливу загроз інформаційній безпеці на коефіцієнт доступності вузла телекомунікаційної мережі. Цей підхід базується на аналізі статистичних даних та адаптації моделі до специфіки умов експлуатації. Завдяки цьому метод обліку загроз дозволяє точніше оцінити надійність вузлів і їх здатність забезпечувати інформаційну доступність навіть в умовах недостатньо повної або недостовірної інформації про загрози. Такий підхід має важливе практичне значення, оскільки дозволяє приймати обґрунтовані рішення щодо підвищення стійкості системи до загроз інформаційній безпеці, зокрема щодо доступності інформації. Це сприяє формуванню більш надійних телекомунікаційних мереж і знижує ризики, пов'язані з можливими збоями.

2.2 Використання резервування для підвищення коефіцієнту готовності

Використання резервування є одним із найефективніших методів підвищення доступності телекомунікаційних систем та інших критичних інфраструктур [51]. Це досягається шляхом дублювання ключових компонентів системи, що дозволяє зберегти її працездатність навіть у разі відмови одного або кількох елементів. Основною перевагою резервування є зменшення впливу збоїв на загальну продуктивність і доступність системи. Якщо основний елемент виходить з ладу, резервний автоматично або з мінімальними затримками бере на себе його функції. Це скорочує час простою, що є критичним для забезпечення безперебійної роботи телекомунікаційних мереж, банківських систем або інших послуг, які вимагають високого рівня доступності. Існують різні види резервування, такі як холодне (резервні компоненти активуються лише за

необхідності), гаряче (резервні компоненти працюють одночасно з основними) і комбіноване. Вибір методу залежить від специфіки системи, її критичності та вимог до продуктивності. Наприклад, гаряче резервування забезпечує найшвидшу реакцію на збій, але вимагає більшого споживання енергії та ресурсів. Додатковою перевагою резервування є підвищена гнучкість системи. Якщо необхідно, запасні елементи можна тимчасово використовувати для інших цілей, наприклад для тестування нових функцій або обробки пікових навантажень.

Однак слід зазначити, що впровадження резервування супроводжується збільшенням витрат на обладнання, енергію та обслуговування. Це вимагає ретельного аналізу економічної доцільності впровадження резервних елементів. Резервування також має бути інтегровано в загальну стратегію надійності, яка включає профілактичне обслуговування, моніторинг працездатності системи та швидке усунення несправностей [52]. Тільки комплексний підхід дозволяє досягти оптимального балансу між надійністю, продуктивністю і вартістю.

Використання каналів резервування є важливим засобом забезпечення безперебійної роботи банківських мереж, оскільки дозволяє підтримувати систему навіть у разі збоїв основних каналів зв'язку або проміжних пристроїв. Такий підхід значно підвищує стійкість мережі до зовнішніх і внутрішніх загроз, а також знижує ймовірність простоїв, які можуть вплинути на критичні процеси. Оскільки коефіцієнт доступності є імовірнісною величиною, його розрахунок базується на математичній теорії ймовірності і враховує вплив як окремих вузлів, так і всієї мережі в цілому. У практичних розрахунках прийнято кілька основних положень. По-перше, коефіцієнт доступності кожного вузла є обмеженим значенням, і його значення безпосередньо впливає на зниження загального коефіцієнта доступності мережі. По-друге, загрози мережевій безпеці розглядаються переважно на вузлах зв’язку, оскільки саме активне мережеве обладнання є основною мішенню для атак або збоїв. Для аналізу впливу різних факторів на коефіцієнт доступності та стійкість мережі до збоїв доцільно провести дослідження типових топологій. Наприклад, можна розглянути

варіанти зіркоподібної, кільцевої або комбінованої топології з резервуванням. Для кожного з них можна визначити вплив параметрів резервованих каналів і пристроїв на загальний показник доступності. Подібним чином можна вивчати й інші топології, враховуючи особливості їх архітектури. Такий підхід дозволяє не тільки оцінити ефективність впровадження резервованих каналів, але й сформулювати рекомендації щодо оптимального проектування мереж, спрямованих на забезпечення високої доступності та стійкості до загроз.

Тому дослідження впливу топології на надійність корпоративної мережі полягає в аналізі стійкості різних варіантів структурно-логічних схем підключення активних вузлів, зокрема, при реалізації кіберзагроз [53]. Оскільки топологія мережі безпосередньо впливає на її здатність протистояти різноманітним загрозам, важливо оцінити, як різні варіанти підключення елементів мережі можуть змінити рівень її надійності та стабільності. При проектуванні мережі на основі певної топології необхідно враховувати різні фактори, які можуть виникнути під час атаки або несанкціонованого доступу до мережі. Для цього необхідно змоделювати сценарії можливих кіберзагроз, таких як збої вузлів, зловмисні атаки або порушення цілісності даних. Таким чином, вибір топології визначає не тільки ефективність передачі даних, але й здатність мережі протистояти атакам без істотних втрат у функціонуванні. Різні типи топологій, наприклад, зірка, кільце або дерево, мають різні рівні відмовостійкості. У топології, де вузли мають кілька можливих шляхів для з’єднання, мережа буде більш стійкою до збоїв порівняно з одношляховими з’єднаннями, де навіть незначний збій у вузлі може призвести до відключення частини мережі. З іншого боку, зіркоподібна топологія може бути вразливою до збоїв у центральному вузлі, що робить її менш стійкою до збоїв цього компонента. Щоб оцінити стійкість мережі до кіберзагроз, важливо враховувати не лише топологію, але й динамічні фактори, такі як можливість резервування каналів, використання алгоритмів шифрування та моніторинг аномалій у реальному часі [54]. Усі ці аспекти необхідно об’єднати в єдину модель, яка

дозволить ефективно оцінити та підвищити надійність корпоративної мережі, зменшивши ймовірність негативних наслідків від кіберзагроз.

Використавши формули (2.1) та(2.2) коефіцієнт готовності, з топологією мережі «кільце» (рис. 2.2) для маршруту між вузлами 1 і 3, спростивши можна подати як (2.10).

$$Fa_{1-3}^{\text{Кільце}} = Fa_{\text{у}}^2 \times (1 - (1 - Fa_{\text{р}}^2 \times Fa_{\text{у}})^2), \quad (2.10)$$

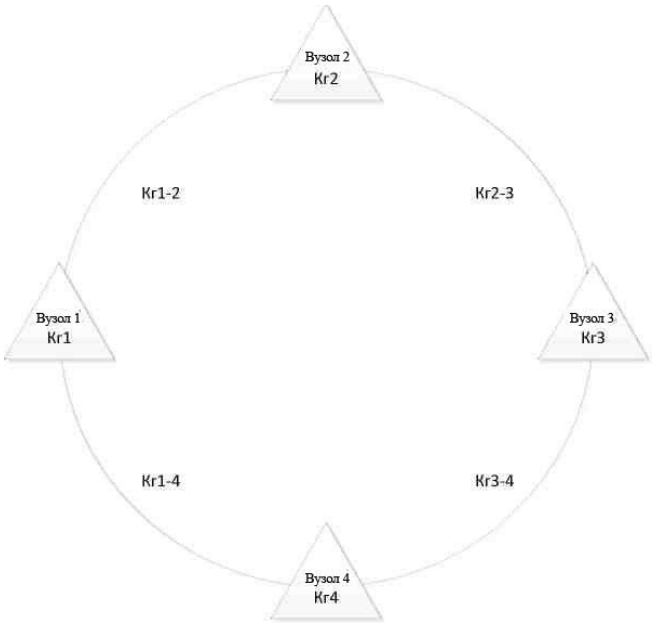


Рисунок 2.2 - Топологія мережі «кільце»

Використавши ті ж формули для коефіцієнту готовності з топологією «кільце з резервним горизонтальним ребром» (рис. 2.3) для маршруту між вузлами 1 і 3 можна записати як (2.11).

$$Fa_{1-3}^{\text{К.ГР.}} = Fa_{y}^2 \times (1 - \left(Fa_{\text{р}}^2 \times Fa_{\text{у}})^2 \times \left(1 - Fa_{\text{р}}\right)\right), \quad (2.11)$$

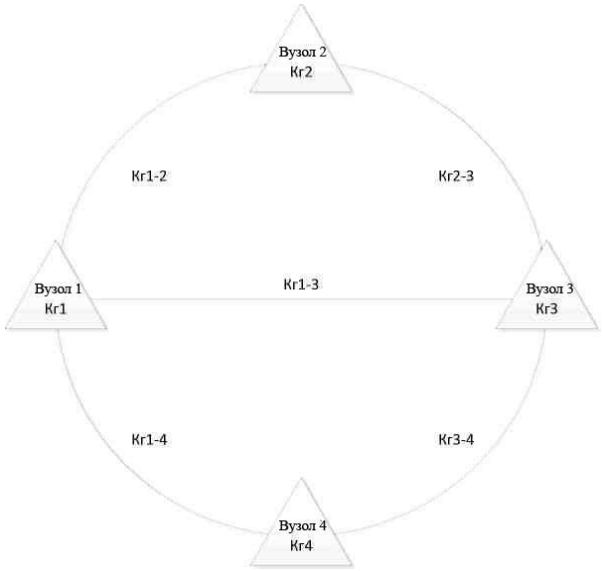


Рисунок 2.3 – Топологія «кільце з горизонтальним резервним ребром»

Для лінійної топології (рис. 2.4) коефіцієнт готовності можна записати як (2.12).

$$Fa_{1-3}^{Л} = Fa_{у}^{3} \times Fa_{р}^{2}, \quad (2.12)$$

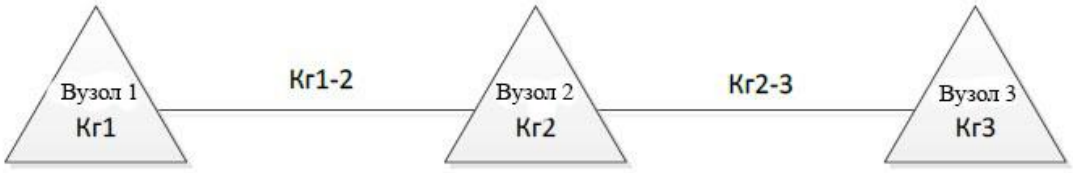


Рисунок 2.4 – Лінійна топологія мережі

Для лінійної топології з резервним ребром (рис. 2.5) коефіцієнт готовності можна записати як (2.13).

$$Fa_{1-3}^{Л+РР} = Fa_{у}^{2} \times (1 - (1 - Fa_{р}) \times (1 - Fa_{р}^{2} \times Fa_{у})), \quad (2.13)$$

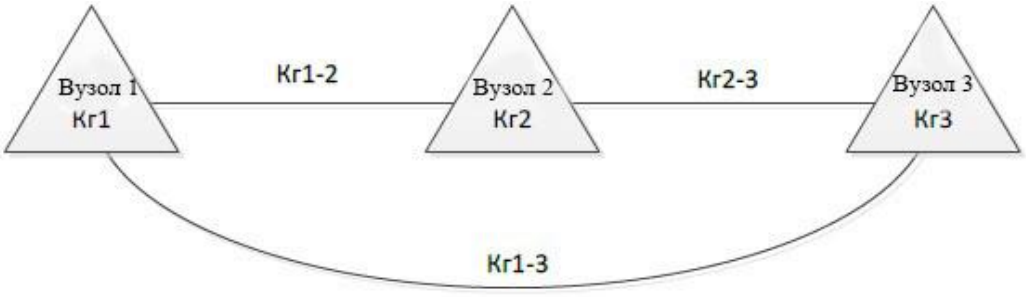


Рисунок 2.5 – Лінійна топологія мережі з резервним ребром

Таким чином, коефіцієнт формалізованої топології можна уявити як функцію від коефіцієнта готовності вузлів мережі і коефіцієнта готовності ребер мережі. Ця функція відображає залежність загальної надійності мережі від характеристик окремих компонентів.

Форма функції залежить від топології мережі і має бути визначена відповідно до специфікацій даної архітектури. Наприклад, у зірковій топології, де кожен вузол з’єднаний лише з одним центральним пристроєм, коефіцієнт готовності ребра матиме вирішальний вплив на загальний коефіцієнт готовності. У таких випадках, навіть невеликі відмови в центральному вузлі можуть значно знижувати загальну надійність мережі. У кільцевій або деревоподібній топології, де є альтернативні шляхи для передачі даних, коефіцієнт готовності мережі може бути вищим за рахунок наявності додаткових ліній і пристроїв для резервування.

Завдяки формалізації топології можна детально оцінити вплив окремих компонентів мережі на загальний рівень готовності. Така оцінка є особливо важливою для проектування надійних і стійких до відмов систем, а також при моделюванні різних загроз ІБ.

Таким чином, використання функції дозволяє проводити ефективні розрахунки, що стосуються оцінки надійності мережі на підставі реальних даних про стан вузлів і ліній зв'язку. Це також є важливим інструментом для прийняття рішень щодо оптимізації архітектури мережі, визначення пріоритетів у реалізації заходів із забезпечення безпеки та підвищення загальної стійкості мережевих систем.

Тому функція Fa буде залежати від топології мережі та визначатися згідно-(2.14).

$$Fa_{\text{ККМ}} = f\left(Fa_{\text{р}}; Fa_{\text{в}}\right). \qquad (2.14)$$

З математичної точки зору, банківська мережа може бути представлена як сукупність двох основних видів елементів: вузлів зв'язку та каналів зв'язку. Кожен з цих елементів має свою роль у забезпеченні функціонування мережі, а також може впливати на її надійність та ефективність у разі відмов чи впливу зовнішніх загроз. мережу можна описати як граф, де вузли є вершинами, а канали зв'язку - ребра, які з'єднують ці вершини [55]. Для такого графа можна визначити різні функції надійності, що враховують як стан окремих вузлів, так і стан каналів між ними. Врахування цих елементів дозволяє створити математичні моделі, що точно відображають поведінку мережі при зміні її топології, відмовах або впливі загроз на окремі елементи мережі.

Для побудови графіка при розрахунку приймемо, що коефіцієнт готовності змінюються в діапазоні від 0,99 до 0,9998 з кроком 0,00098

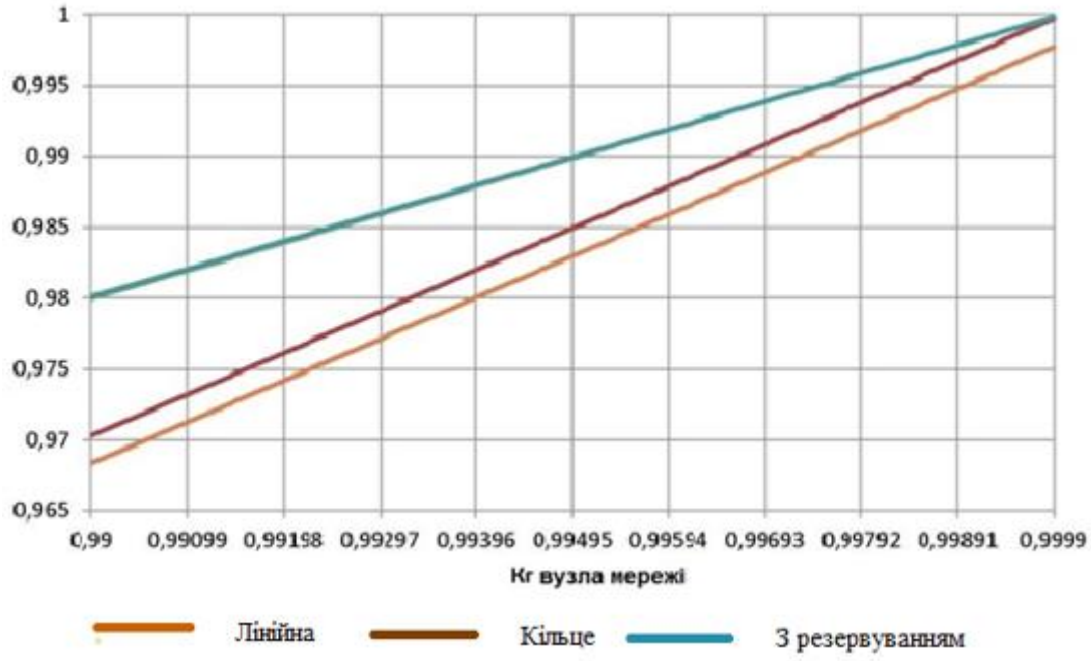


Рисунок 2.6 – Залежності коефіцієнту готовності різних топологій

Тому для досягнення високих показників надійності телекомунікаційної інфраструктури в умовах обмежених ресурсів необхідно зосередитися на забезпеченні надійної роботи вузлів. Це дозволить не тільки підвищити загальну стабільність системи, а й знизити ризики, пов'язані з відмовою окремих елементів, що критично важливо для підтримки безперебійної роботи мережі в цілому. Оскільки вузли банківської мережі є ключовими компонентами, їх стабільність і надійність безпосередньо впливають на ефективність обробки даних, передачі інформації та здатність мережі відновлюватися після збоїв. Тому, враховуючи фактори ризику, необхідно впроваджувати стратегії моніторингу, регулярного обслуговування та резервного копіювання для забезпечення високої доступності та стабільності цих вузлів, що, у свою чергу, забезпечить надійну роботу всього телекомунікаційного середовища.

2.3 Висновки

Було створено математичну модель, яка точно визначає ймовірність того, що досліджуваний елемент знаходиться в працездатному або непрацездатному стані, враховуючи відмови технічних пристроїв. Основою аналізу є розрахункова формула для коефіцієнта готовності, яка залежить від кількості відмов і часу перебування вузла мережі в працездатному або непрацездатному стані. Такий підхід дозволяє глибше оцінити структурну надійність технічних комп'ютерних систем і розробити ефективні стратегії для їх покращення.

Дослідження показує, що на коефіцієнт готовності банківської мережі найбільше впливає коефіцієнт доступності вузлів, тоді як коефіцієнт доступності каналів зв'язку має менший вплив. Це підкреслює важливість забезпечення стабільної роботи вузлів мережі для досягнення високих показників надійності в цілому. Враховуючи, що вузли є ключовими елементами в обробці даних і маршрутизації, їх продуктивність безпосередньо визначає загальний стан мережі, особливо при реалізації різних типів загроз.

З цієї точки зору дослідження підтверджує актуальність магістерського дослідження, яке спрямоване на підвищення надійності вузлів мережі.

Вузли банківської мережі є критичними елементами, від стабільності та надійності яких залежить ефективність обробки даних, передача інформації та швидке відновлення після збоїв. З огляду на потенційні ризики, важливо впроваджувати стратегії моніторингу, регулярного технічного обслуговування та резервного копіювання. Це сприятиме забезпеченню високої доступності та стабільності вузлів, що є основою для надійного функціонування всієї телекомунікаційної інфраструктури.

Для досягнення високого коефіцієнта готовності мережі необхідно оптимізувати не тільки характеристики каналів зв'язку, але й забезпечити безперебійну роботу активних елементів мережі. Такий підхід допоможе не тільки підвищити стійкість мережі до збоїв, але й знизити ризики, пов'язані з можливими відмовами вузлів, що критично важливо для корпоративних мереж, де висока надійність є основною вимогою.

На основі проведених розрахунків встановлено, що коефіцієнт готовності досліджуваних мережевих топологій можна підвищити як шляхом збільшення надійності їх елементів, так і через оптимізацію топології шляхом додавання резервних з’єднань у різних конфігураціях. Це підтверджує доцільність використання топологічних методів для підвищення ефективності функціонування телекомунікаційних мереж.

3 ОЦІНКА ВПЛИВУ ЗАГРОЗ ДОСТУПНОСТІ ІНФОРМАЦІЇ НА ПОКАЗНИК ГОТОВНОСТІ ВУЗЛІВ МЕРЕЖІ

3.1 Розрахунок впливу атак на відмову в обслуговувані на безпеку мережі

В умовах війни з російськими окупантами Україна повинна забезпечувати повний контроль над своїм інформаційним простором.

Розподілені атаки на відмову в обслуговуванні (DDoS) є однією з найбільш критичних загроз для сучасної мережевої інфраструктури. Їх сутність полягає у цілеспрямованому перевантаженні цільових систем масованим потоком мережевого трафіку, що призводить до порушення нормального функціонування сервісів.

DDoS-атаки особливо небезпечні через свою розподілену природу. Зловмисники використовують мережі скомпрометованих пристроїв (ботнети), які можуть включати як традиційні комп'ютери, так і різні пристрої Інтернету речей [56]. Така різнорідність джерел атак ускладнює виявлення та блокування шкідливого трафіку.

Механізм формування ботнету базується на масовому зараженні пристроїв спеціалізованим шкідливим програмним забезпеченням. Це дозволяє зловмисникам встановити віддалений контроль над зараженими системами, перетворюючи їх на «ботів» - слухняних виконавців команд зловмисника. Централізоване управління ботнетом забезпечує координацію роботи всіх скомпрометованих пристроїв.

Ця комбінація факторів - розподіленість атаки, різноманіття джерел трафіку, використання легітимних протоколів та складність відокремлення шкідливих запитів від нормального трафіку - робить DDoS-атаки одним з найбільш ефективних інструментів порушення доступності мережевих сервісів. Це вимагає розробки комплексних систем захисту, здатних виявляти та блокувати подібні атаки на ранніх стадіях їх розвитку.

2023 рік виявився досить багатим на події та тенденції у сфері кібербезпеки. Ми стали свідками появи нового терміну «білий шум», розвиток штучного

інтелекту призвів до збільшення активності ботів, що суттєво вплинуло на комерційні компанії. Ми виявили ознаки відродження популярності комерційних DDoS-атак. Впровадження технологій «віддаленого офісу» призвело до розширення каналів комунікації і, як наслідок, збільшення інтенсивності атак. Четвертий квартал минулого року, статистики компанії Qrator Labs [56] не приніс жодних сюрпризів з точки зору розподілу змішаних атак за векторами. UDP-флуд знову очолив список з показником 60,20%. На другому місці - IP-флуд з показником 16,86%. Мультивекторні атаки також увійшли до трійки лідерів з показником 13,36%. (рис. 3.1)

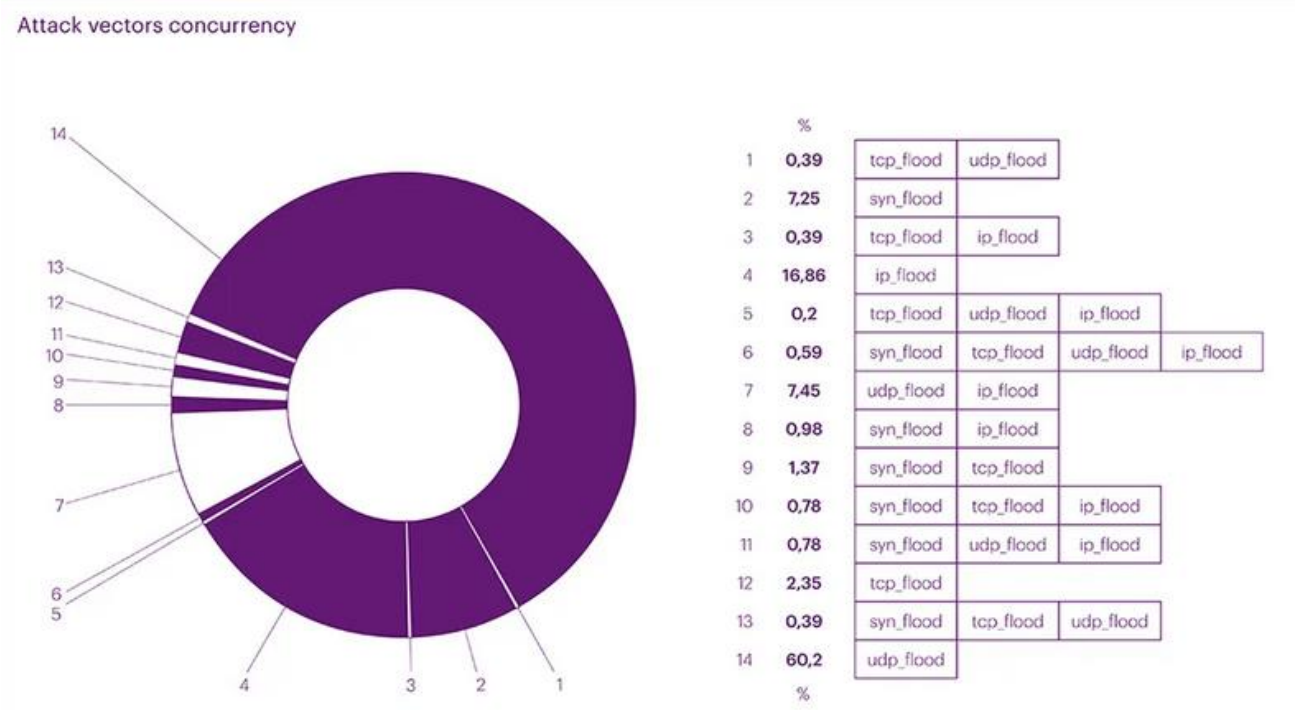


Рисунок 3.1 – Основні вектори DDoS в 2023 році

На рівні сегментів основними мішенями зловмисників стали банки - 28,31%, які традиційно піддаються атакам у періоди активного просування сезонних банківських продуктів - кредитів і депозитів. До топ-5 також увійшли дошки оголошень - 15,04%, освітні платформи - 9,57%, інтернет-магазини - 8% та платіжні системи - 7,05%, що не дивно. Розвиток електронної комерції останнім часом був величезним. Сьогодні більшість товарів та послуг можна

отримати онлайн. Крім того, як ми вже неодноразово згадували, розширення каналів зв'язку, перехід на нові протоколи для оптимізації роботи віддалених офісів, а також простота і дешевизна організації DDoS-атак призвели до відродження тенденції комерційних атак, які є ефективним інструментом впливу на бізнес, що використовується зловмисниками з усіма витікаючими звідси наслідками (рис. 3.2).

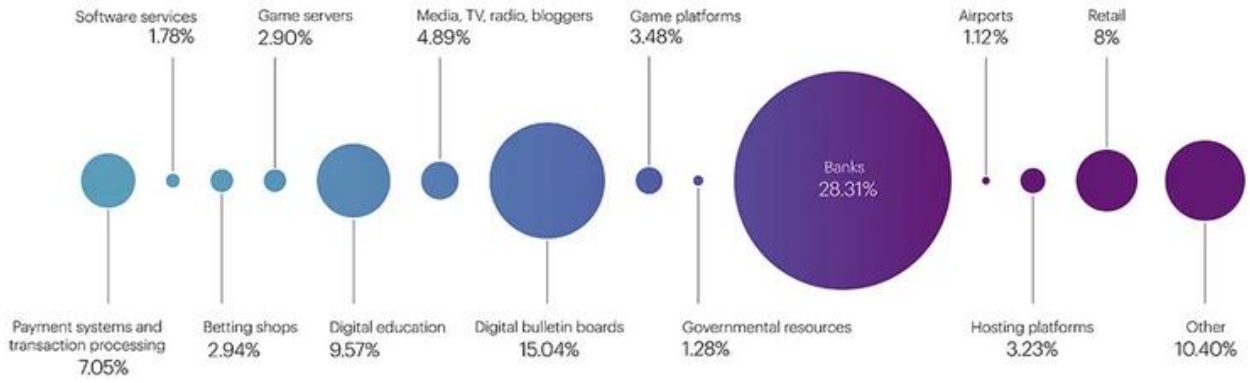


Рисунок 3.2 – Розподіл атак по сегментах

Статистика розподілу DDoS атак за географічними джерелами в четвертому кварталі підкреслює, що зловмисники успішно навчилися обходити блокування GeoIP, і значна частина атакуючого трафіку тепер генерується локальними джерелами.

Загальна кількість заблокованих IP-адрес зросла на 32,15% порівняно з третім кварталом - з 40,15 до 53,06 млн. Це найвищий показник за 2023 рік.

Як і раніше, в четвертому кварталі список Топ-20 очолила країна терорист, де було заблоковано 22,3 млн адрес (42,03% від загальної кількості). До трійки лідерів знову увійшли США і Китай з 6,23 (11,76%) і 2,65 (5%) мільйонами заблокованих адрес відповідно (рис. 3.3).

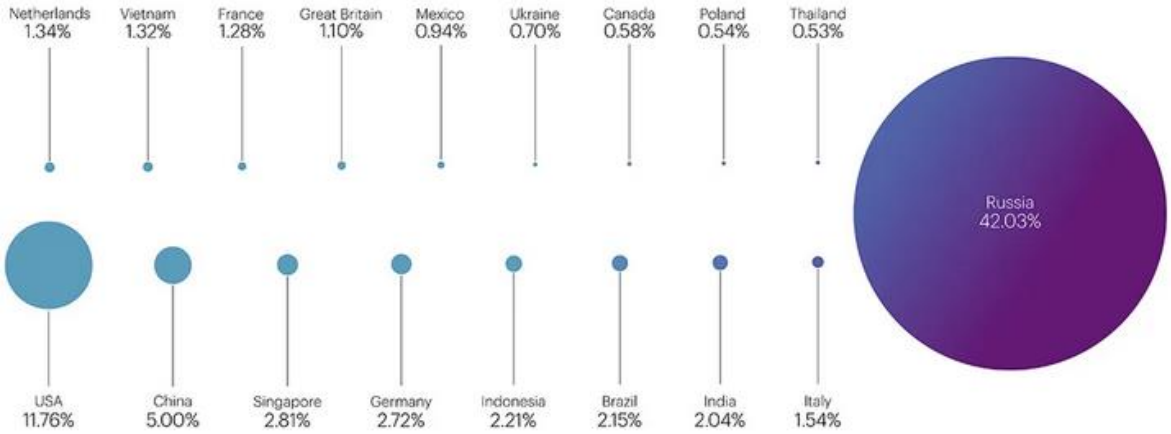


Рисунок 3.3 – Географічний розподіл атак

Найбільший у світі вендор Check Point Software Technologies Ltd, запустив світову мапу кіберзагроз ThreatCloud World Cyber Threat Map, яка відображає в режимі реального часу, де наразі у світі відбуваються кібератаки [57] (рис. 3.4).

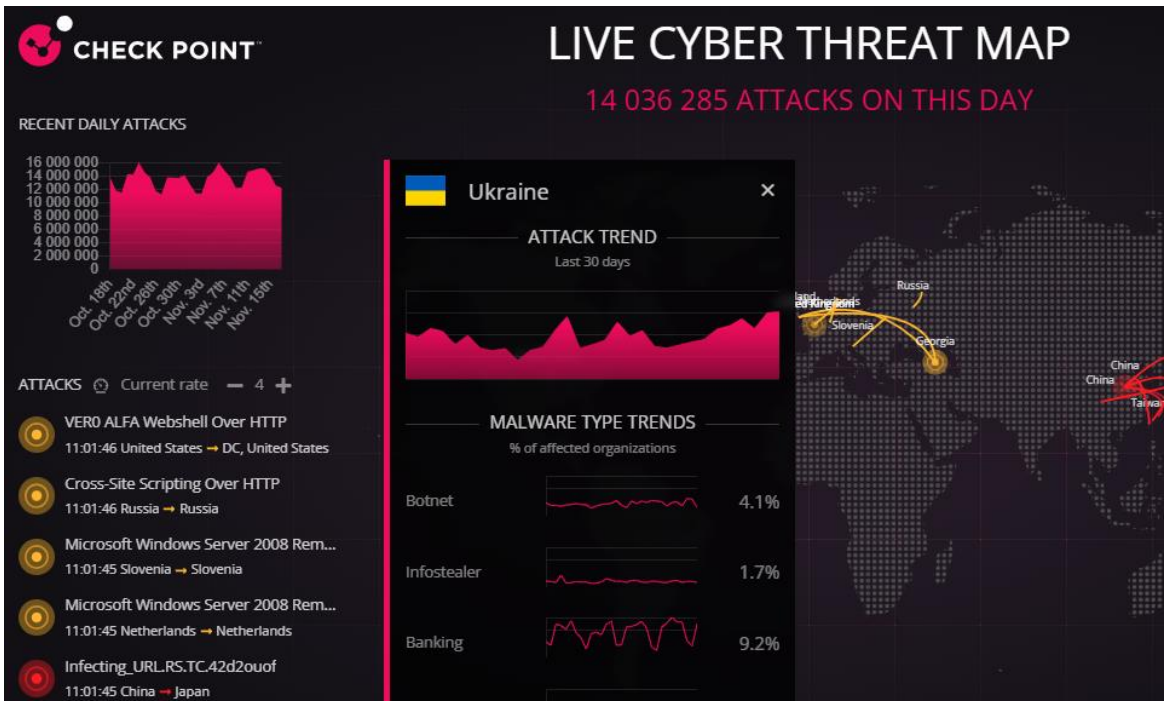


Рисунок 3.4 – Статистика атак на Україну 18.11.2024 в першій половині дня

Під час атаки кожен бот генерує потік запитів до певної цілі. Кумулятивний ефект від багатьох одночасних запитів створює критичне навантаження на цільову систему. Той факт, що кожен окремий бот використовує легальні

мережеві протоколи і може мати легальну IP-адресу, робить протидію таким атакам особливо складною. Ми бачимо, що за статистикою саме розподілені атаки на відмову в обслуговувані найбільш поширені. Тому розробимо метод для розрахунку кількісної оцінки коєфіцієнту готовності вузла банківської мережі в умовах DDoS.

Комплексним засобом забезпечення надійності інформаційної інфраструктури є система оцінки ефективності вузлів мережі, заснована на порівняльному аналізі коефіцієнтів доступності корпоративної мережі. Методичним обґрунтуванням такого підходу є використання коефіцієнта доступності як основного кількісного показника, що відображає здатність системи виконувати свої функції в певний момент часу. Порівняльний аналіз різних варіантів стану обладнання дозволяє глибоко зрозуміти вплив окремих факторів на загальну продуктивність мережі. У процесі оцінки враховується широкий діапазон можливих станів вузла зв'язку, включаючи стандартний режим роботи обладнання, часткове погіршення продуктивності, повний вихід з ладу компонентів, вплив зовнішніх факторів і наслідки потенційних кібератак. Такий багатофакторний аналіз дає повне розуміння надійності системи.

Коефіцієнт готовності мережі може бути визначений за кількома підходами, залежно від врахування впливу загроз та засобів захисту інформації. У першому випадку цей показник обчислюється без урахування загроз, які впливають на рівень безпеки мережі. У другому підході коефіцієнт готовності враховує вплив загроз, проте не враховує ефективність використання засобів захисту інформації. Третій підхід є найбільш комплексним, оскільки передбачає врахування як впливу загроз на безпеку мережі, так і ефективності застосованих засобів захисту інформації.

Якщо трафік проходить послідовно всі пристрої вузла, задіяні в інформаційному обміні то коефіцієнт готовності розрахуємо по формулі:

$$Fa_{\text{у}} = Fa_1 \times Fa_2 \times \ldots \times Fa_n, \tag{3.1}$$

де $Fa_1 \ldots Fa_n$ – відповідні коефіцієнти готовності елементів вузла

Вузлові елементи вважаються пристроями, які забезпечують функціональність на рівнях 1-3 еталонної моделі OSI. До таких пристроїв належать модеми, маршрутизатори, адаптери, брандмауери, пристрої оптимізації трафіку, шлюзи тощо. Для визначення коефіцієнта доступності цих елементів необхідно використовувати методологію, наведену у другому розділі дослідження. Він передбачає врахування основних характеристик працездатності кожного пристрою, включаючи частоту відмов і тривалість їх усунення. Це дозволяє отримати об'єктивну оцінку надійності функціонування вузлів мережі.

Зважаючи на те, що потоки подій, які впливають на стан досліджуваного вузла зв’язку банківської мережі, характеризуються експоненціальним розподілом, для визначення ймовірностей безвідмовної роботи елементів мережі доцільно застосувати математичний апарат марківських випадкових процесі. Марківський процес являє собою тип випадкового процесу, в якому майбутня динаміка системи залежить виключно від її стану в конкретний момент часу, не враховуючи попередніх станів [58-60]. Це дає змогу спростити аналіз складних систем, таких як вузли зв’язку, та обґрунтовано моделювати їхню надійність. В нашому випадку цими станами є:

– готовність вузла;
– відмова вузла через DDoS;
– відмова вузла через несправність.

Графова модель представлення станів наведено на рисунку 3.5

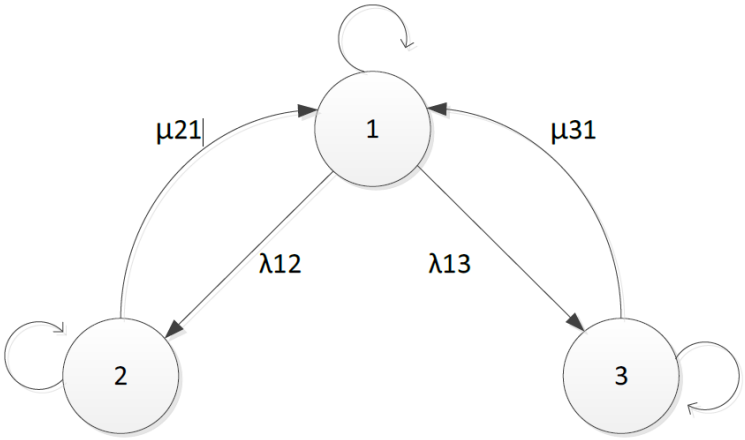


Рисунок 3.3 - Графова модель представлення станів вузла

Для опису математичної моделі процесу використаємо систему рівнянь Колмогорова-Чепмена:

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

де:

– $P_1(t)$, $P_2(t)$, $P_3(t)$ – ймовірність знаходження пристрою в одному з вище описаних станів;

– λ_{12}, λ_{13} – інтенсивності відмов мережного пристрою;

– μ_{21}, μ_{21} – інтенсивності відновлень мережного пристрою.

Розв’язавши цю систему рівнянь отримаємо імовірності перебування вузла в одному зі станів:

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

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

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

Таким чином, ймовірність безвідмовної роботи мережевого пристрою за умови впливу лише загроз інформаційній безпеці відображає ймовірність того, що пристрій не перейде в стан непрацездатності внаслідок реалізації загрози, спрямованої на порушення доступності. інформації. Цей показник є ключовим для оцінки стійкості пристрою до деструктивних впливів, спрямованих на обмеження доступу до інформаційних ресурсів і сервісів:

$$\bar{P}_2 = \frac{\mu_{21} \times (\lambda_{13} + \mu_{31})}{\mu_{21} + \mu_{31} + \lambda_{12} + \mu_{31} + \lambda_{13} + \mu_{21}}. \quad (3.6)$$

Для того щоб загроза інформаційній безпеці призвела до порушення доступності вузла корпоративної мережі, необхідно, щоб відбулася та реалізувалася низка послідовних подій. Ці події можуть включати виникнення вразливості в системі, ініціацію атаки зловмисником, подолання засобів захисту інформації, безпосередній вплив на елементи вузла і, як наслідок, вихід його з ладу. Лише при виконанні всього ланцюга таких умов можна говорити про реалізацію загрози, яка впливає на доступність вузла.

Для моделювання впливу розподілених атак на відмову в обслуговувані на надійність вузла банківської мережі будуть розглядатися два сценарії. Перший сценарій передбачає, що вузол оснащений лише базовими мережевими пристроями, без впровадження спеціалізованих рішень у сфері кібербезпеки. Другий сценарій включає наявність додаткових засобів захисту інформації, інтегрованих у маршрутизатор або представлених у вигляді окремого обладнання. Аналіз цих сценаріїв дозволить оцінити ефективність впровадження додаткових заходів безпеки, визначити їх вплив на зменшення наслідків атак і підвищення загальної надійності роботи мережевого вузла.

3.2 Метод врахування впливу загроз доступності інформації на функціонування вузла мережі

Наразі основним аспектом регулювання є оцінка на основі експертних висновків адекватності існуючої системи захисту інформації. Однією з ключових проблем оцінки ефективності мережевих технічних комплексів є відсутність прямого зв’язку між технічними характеристиками мережі та її показниками ефективності. Це зумовлює необхідність переходу до інформаційно-центричного підходу до оцінювання. Використання цього підходу полягає в оцінці загальних показників, які відображають загальну ефективність роботи мережі, а не окремих технічних параметрів, таких як затримка або пропускна здатність. Це пояснюється тим, що зміни одного технічного параметра не завжди істотно впливають на загальну ефективність мережі, тоді як одночасне погіршення кількох характеристик може призвести до значного зниження її продуктивності або навіть втрати функціональності.

У рамках нашого підходу ефективність мереж можна оцінити за такими показниками, як час виконання регулярних операцій, кількість помилок у виробничих процесах та іншими показниками. Однак через індивідуальні особливості мереж для кожної організації ці показники не підлягають стандартизації на рівні державного регулювання. Безпеку вузла мережі можна оцінити на основі комплексного аналізу його здатності протистояти різним загрозам і забезпечувати надійний захист даних. Перш за все, варто звернути увагу на конфіденційність інформації, яка обробляється цим вузлом. Важливо оцінити, як дані шифруються, як контролюється доступ до них і чи використовуються багаторівневі методи автентифікації. Іншим важливим фактором є здатність вузла забезпечувати цілісність даних. Для цього використовуються механізми виявлення будь-яких змін в інформації, такі як криптографічні підписи або хешування. По-перше, давайте скористаємося допомогою ШІ, щоб розробити наш метод.

Наявність вузла також є критичною характеристикою. Важливо оцінити, чи має він резервування та механізми захисту від DDoS. Необхідно проаналізувати здатність швидко відновлюватися після збоїв або атак. Автентифікація, тобто перевірка користувачів і пристроїв, що підключаються до вузла, повинна забезпечуватися надійними механізмами, такими як цифрові сертифікати або токени. Також важливо перевірити, наскільки ефективно вузол контролює доступ до своїх ресурсів, чи існують відповідні політики доступу та чи відстежуються дії користувачів у мережі [60, 61].

Узагальнений підхід до оцінки захищеності вузла банківської мережі, який запропонував AI наведено на рисунку 3.4

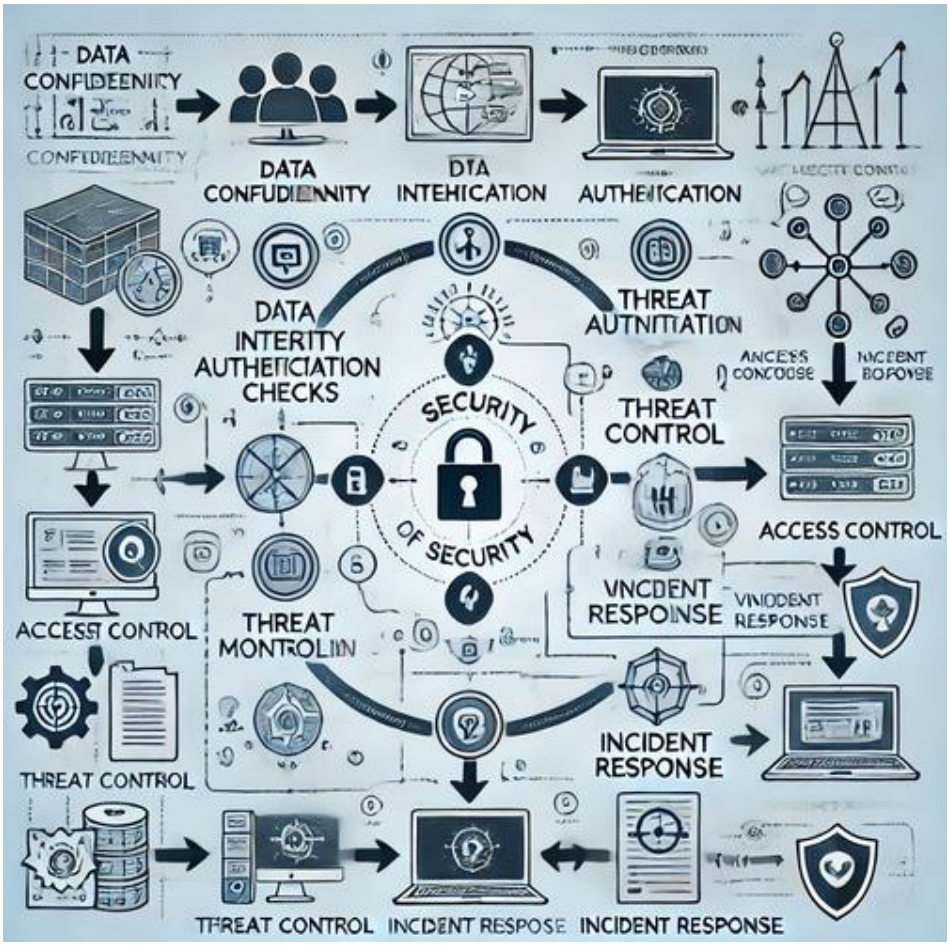


Рисунок 3.4 – Підхід до оцінки захищеності вузла мережі, запропонований AI

На схемі показано основні кроки, такі як конфіденційність даних, перевірка цілісності, процеси автентифікації, моніторинг загроз, контроль доступу, аналіз

вразливостей, реагування на інциденти та стійкість мережі. Кожен елемент описує, як він впливає на загальну оцінку безпеки сайту. Моніторинг і виявлення загроз відіграють ключову роль у забезпеченні безпеки сайту. Ось схема моніторингу загроз, запропонована AI, яка ілюструє основні компоненти системи, такі як виявлення загроз, збір даних, аналіз і кореляція, генерація сповіщень, реагування на інциденти та зворотний зв'язок для безперервного вдосконалення (рис.3.5).

Рисунок 3.5 – Підхід до моніторингу загроз, запропонований AI

Ця схема демонструє, як різні елементи взаємодіють у процесі моніторингу загроз. Необхідно оцінити, чи реалізовані системи для виявлення аномальної активності та вторгнень, і як вони інтегровані в загальну архітектуру безпеки. Крім того, важливо мати системи відстеження та аудиту подій для реєстрації всіх дій і подій для подальшого аналізу та швидкого реагування на інциденти. Останнім етапом оцінки є здатність сайту забезпечувати безперервність обслуговування та його стійкість до можливих збоїв або атак.

Методи захисту від DDoS-атак можна розділити на дві групи: це методи, що передують початку атаки, які спрямовані на запобігання самого факту атаки, і методи, які використовуються після початку атаки, це способи активної протидії та пом'якшення результатів нападу. До методів попередження нападу можна віднести організаційні та правові заходи. Наприклад, неприпустимість втягування в конфліктні ситуації, або заходи, спрямовані на усунення результатів, яких хоче досягти зловмисник, наприклад, розмежування та маскування критичних ресурсів. Також на цьому етапі здійснюється усунення вразливостей та підтримка в актуальному стані задіяного апаратно-програмного комплексу. Деякі типи мережевих атак спрямовані саме на використання різного роду вразливостей. Це можуть бути уразливості в програмному забезпеченні сервера. Або вразливості, пов’язані з використанням неоптимізованих програмних скриптів, які можуть надмірно споживати ресурси сервера. У цьому випадку для досягнення бажаного ефекту зловмисникові необхідно організувати менш потужну атаку.

Після початку нападу застосовуються активні заходи протидії нападу. Основними з цих заходів є нарощування ресурсів і фільтрація трафіку. Нарощенню ресурсів передує детальний аналіз навантаження на сервер і мережевий сегмент для виявлення вузьких місць. Наприклад, якщо в нормальному режимі роботи сервер займає значну частину каналу зв'язку, можна припустити, що в разі атаки зловмисник може досягти повного заповнення каналу шкідливими запитами. У цьому випадку доцільно заздалегідь збільшити пропускну здатність каналу зв'язку. Виявлені в результаті аналізу «вузькі місця» забезпечені додатковими ресурсами. Якщо основним споживачем ресурсів на фізичному сервері є сервер баз даних, його можна порекомендувати розмістити на окремому виділеному сервері або навіть створити розподілений кластер серверів баз даних. Те ж саме можна зробити і з іншими службами. Якщо продовжувати розглядати веб-сервер як об'єкт атаки, то, крім баз даних, підвищене навантаження може створювати сам вебсервер або розміщені на ньому скрипти. У цьому випадку необхідно збільшити ресурси самого сервера:

додаткову пам'ять, більш потужний процесор і т. д. Або за допомогою спеціальних засобів виділити веб-сервер в окремий кластер. Наприклад, це можна зробити за допомогою комбінації веб-серверів Apache і Nginx [63].

Такий підхід до збільшення ресурсів не є панацеєю від мережевих атак, крім того, він має ряд недоліків: збільшення ресурсів пов'язане зі зміною апаратного комплексу і не може бути здійснено швидко в момент атаки; збереження надлишкових ресурсів економічно недоцільно в період очікування атаки. Для подолання цих недоліків оптимальним використанням хмарних технологій є збільшення ресурсів за потреби. Наприклад, зараз ринок пропонує хостинг-провайдерам надавати послуги хмарного хостингу / В результаті надання послуг клієнтам надається необхідний на даний момент обсяг ресурсів. У разі збільшення навантаження, це може бути як збільшення кількості легальних користувачів, так і збільшення шкідливих запитів, для обробки кожного запиту надається додаткова потужність. Як наслідок, збою сервера немає. Єдиним недоліком такого підходу є його економічна складова. Оскільки клієнту хмарного хостингу потрібно платити за додаткові потужності, тобто, по суті, платити за обробку шкідливих запитів.

Для оцінки впливу кіберзагроз на працездатність вузлів корпоративної мережі доцільно застосувати кількісний метод аналізу стану мережевих пристроїв. Цей підхід дає можливість чисельно оцінити рівень збоїв у роботі мережі, спричинених реалізацією загроз, які порушують доступність інформаційних ресурсів.

Метод передбачає аналіз змін таких показників, як пропускна здатність вузлів, затримка передачі даних і відсоток втрат пакетів у процесі моделювання кіберзагроз. Порівняння цих параметрів до атаки та під час її реалізації дозволяє отримати кількісну оцінку впливу загроз на функціональність мережі.

Застосування цього методу, доповнене оптимізацією параметрів систем захисту, сприяє підвищенню стійкості мережі до загроз порушення доступності інформаційних ресурсів, що виникають унаслідок кібератак. Це забезпечує більш

ефективне управління ризиками інформаційної безпеки та покращує загальну працездатність інфраструктури .

Методика оцінки безпеки мережі під впливом атак на відмову в обслуговувані включає низку ключових етапів, які забезпечують комплексний аналіз та розробку заходів щодо мінімізації ризиків. Спочатку проводиться повна інвентаризація мережевих пристроїв, служб і ресурсів, а також їх взаємозв'язків. Наступним кроком є визначення можливих типів атак на відмову в обслуговувані, що включає аналіз трафіку, виявлення аномалій та виявлення найбільш уразливих компонентів мережі. Далі виконується перевірка наявних вразливостей у мережевих операційних системах, програмному забезпеченні та службах, які можуть стати мішенню для зловмисників. Виявлені вразливості аналізуються шляхом моделювання можливих сценаріїв атак, включаючи оцінку того, як їх можна реалізувати. На основі отриманих даних розробляються сценарії атак на відмову в обслуговувані, що дозволяють оцінити здатність мережі протидіяти загрозам і ефективність застосовуваних заходів захисту. При цьому аналізуються ймовірність, наслідки атак і критичні вектори загроз. Останніми кроками є формулювання рекомендацій щодо посилення захисту мережі, впровадження систем моніторингу для швидкого виявлення аномалій трафіку та регулярне оновлення стратегій безпеки відповідно до нових загроз і технологічних тенденцій. Цей підхід забезпечує проактивну стратегію захисту мережі від атак на відмову в обслуговувані.

Найбільш помітною ознакою атак на відмову в обслуговувані є раптове зниження швидкодії або повна недоступність вебсайту чи сервісу. Однак схожі проблеми можуть виникнути через легітимний сплеск трафіку, тому для точного діагностування зазвичай необхідно провести детальніше розслідування.

Інструменти аналізу мережевого трафіку допомагають виявити характерні ознаки DDoS-атаки, зокрема:

– аномально високий обсяг трафіку, що надходить із певної IP-адреси або діапазону адрес;

– одноманітна поведінка користувачів, наприклад, однакові геолокація, тип пристрою чи версія браузера;

– несподівані піки звернень до окремих сторінок або ресурсів;

– нетипові закономірності в потоці даних, такі як різкі сплески у незвичні години чи регулярні ритмічні підйоми трафіку (наприклад, кожні 10 хвилин).

Запропонований AI процес виявлення DDoS-атак HTTP GET flood складається із наступних етапів (рис. 3.6):

– захоплення трафіку спеціалізованим ПЗ і накопичення лог-файлу із даними по вхідних запитах на сервер;

– відправка лог-файлу до обчислювального комплексу;

– визначення кількості ентропії за допомогою використання моделей *AI*, та прийняття рішення (рис. 3.6).

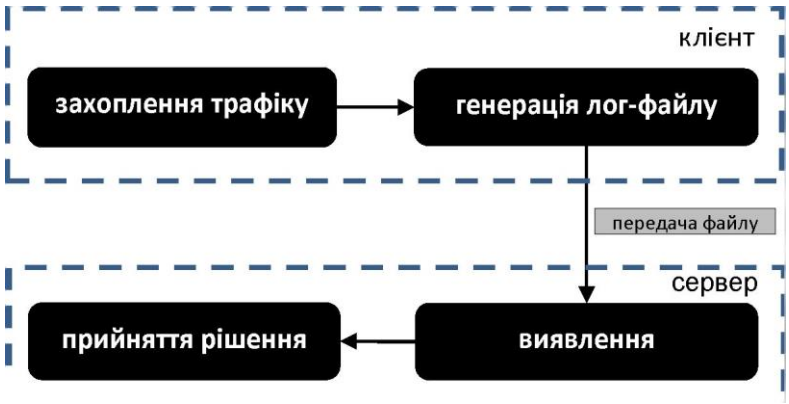


Рисунок 3.6 - Схема роботи методу виявлення HTTP GET flood

Лог-файл містить дані про кожне звернення, включаючи значення критеріїв, обраних для оцінки, адресу відправника та отримувача, а також часову мітку і тип протоколу, який використовувався. Така структура дозволяє фіксувати всі важливі аспекти мережевої активності, забезпечуючи можливість аналізу дій, маршруту передачі даних та характеристик взаємодії між вузлами. Зібрана інформація є основою для моніторингу, діагностики мережі, а також оцінки її безпеки та ефективності.

Для забезпечення безпеки мережі використовується запропонований метод

оцінки безпеки, який забезпечує поетапний підхід до аналізу та підвищення її стійкості (рис. 3.7).

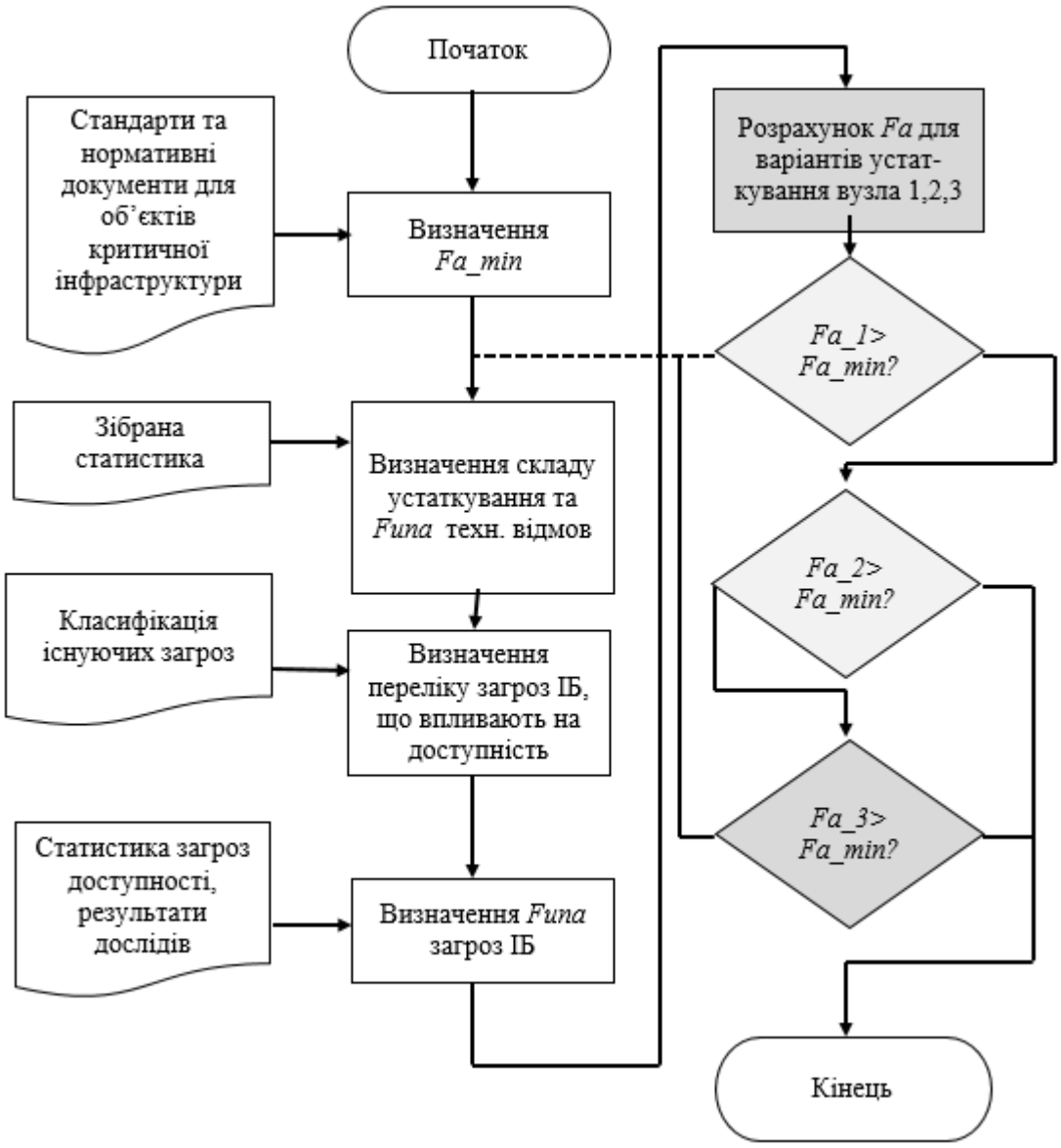


Рисунок 3.7 – Блок-схема алгоритму кількісної оцінки захищеності мережі

На першому етапі проводиться детальний аналіз мережевої інфраструктури з використанням ШІ з визначенням можливих типів атак на відмову в обслуговувані, які можуть порушити її роботу. Це дозволяє визначити слабкі сторони та ключові аспекти, які можуть бути під загрозою. Далі оцінюється реакція мережі на атаки, аналізується різними моделями ефективність існуючих заходів безпеки та рівень готовності до різних сценаріїв. Цей етап дозволяє

виявити критичні вразливості та розробити відповідні стратегії захисту. Щоб підготуватися до реальних загроз, створюються реалістичні сценарії атак на відмову в обслуговувані. Це дозволяє перевірити здатність мережі витримувати навантаження, аналізувати наслідки та перевіряти ефективність захисних заходів. Першочерговими завданнями є виявлення найбільш вразливих сегментів мережі та розробка відповідних заходів щодо їх захисту. Особливу увагу приділено критично важливим вузлам і компонентам.

Заключним етапом є впровадження систем постійного моніторингу для виявлення аномалій у трафіку, а також регулярне оновлення стратегій захисту з урахуванням нових загроз і технологій . Це забезпечує адаптивність мережі до змін і підвищує її стійкість до атак. Регулярне проведення таких заходів гарантує належний рівень безпеки мережі, її готовність протистояти атакам на відмову в обслуговувані та іншим кіберзагрозам.

Детальніше метод виглядає наступним чином:

– спочатку встановлюється мінімально допустимий коефіцієнт готовності сегмента банківської мережі відповідно до вимог;

– визначається склад обладнання вузлів банківської мережі, і на основі цього виконується розрахунок коефіцієнта неготовності обумовленого технічними відмовами обладнання;

– створюється модель загроз інформаційної безпеки, яка враховує можливі вектори атак і їхній вплив на доступність інформації;

– здійснюється перерахунок коефіцієнта неготовності з урахуванням впливу загроз DDoS-атаки.

– обчислюється загальний коефіцієнт готовності досліджуваного сегмента мережі, інтегруючи результати попередніх етапів;

– порівнюється отримане значення коефіцієнта готовності з мінімально допустимим. У випадку, якщо коефіцієнт готовності менший за встановлену норму, необхідно повернутися до етапу 2, щоб переглянути склад обладнання та вибрати більш відповідні мережеві пристрої, які відповідають критеріям захисту;

– аналізуються результати роботи мережі за умови використання лише маршрутизатора. Якщо коефіцієнт готовності *Fa_2* більший *Fa_min*, це означає, що маршрутизатор ефективно справляється із загрозами;

– проводиться порівняння результатів за двома сценаріями: із використанням лише маршрутизатора та з додатковими засобами захисту. Якщо коефіцієнт готовності *Fa_3* більше за *Fa_min*, робиться висновок, що обране рішення з додатковими засобами захисту є ефективним і забезпечує необхідний рівень захищеності інформації.

– для фільтрації шкідливого трафіку використовуються різноманітні програмні й апаратні засоби, що базуються на методах кількісного та якісного аналізу трафіку. Основою ефективного реагування є вирішення двох взаємопов’язаних завдань.

Перше завдання полягає у своєчасному виявленні початку атаки. Це дозволяє мінімізувати негативний вплив на мережеву інфраструктуру та швидко вжити заходів для захисту.

Друге завдання полягає у визначенні джерела атаки, тобто місць, звідки надходить шкідливий трафік. Ідентифікація джерел атаки дозволяє застосовувати більш таргетовані заходи протидії, такі як блокування або перенаправлення небезпечного трафіку.

Ефективність таких рішень залежить від точності аналізу трафіку, можливості адаптивного реагування та взаємодії між різними рівнями захисної інфраструктури.

3.3 Висновки

В третьому розділі розроблено методику оцінки готовності сегмента мережі до кіберзагроз, яка передбачає визначення мінімально допустимого коефіцієнта готовності, аналіз складу мережевого обладнання, моделювання загроз інформаційної безпеки та розрахунок впливу цих загроз на готовність.

Порівняння отриманих результатів із нормативними вимогами дозволяє виявити, чи достатньо ефективне існуюче обладнання, чи потрібні додаткові засоби захисту. Аналіз ефективності захисту проводиться для сценаріїв із базовим маршрутизатором і з додатковими засобами захисту, що забезпечує оптимізацію мережевої стійкості до загроз.

Практичне значення цього методу проявляється в можливості точного визначення критичних точок відмови, оцінки резервів надійності системи, оптимізації конфігурації обладнання та планування заходів з модернізації інфраструктури. Аналітичний потенціал порівняння коефіцієнтів готовності розкривається через можливість виявлення прихованих залежностей, оцінки ефективності захисних механізмів та визначення оптимальних режимів роботи обладнання. На основі отриманих даних формуються конкретні рекомендації щодо вдосконалення мережевої інфраструктури.

Під час атаки на відмову пропускна здатність мережевого вузла суттєво зменшується через саму природу такої атаки. Однак використання засобів захисту на вузлі зв’язку дає змогу забезпечити безперебійне функціонування мережі зі зниженими, але прийнятними параметрами.

Застосування такого комплексного підходу до оцінки ефективності створює надійну методологічну базу для прийняття виважених рішень щодо розвитку та захисту мережевих вузлів. Це особливо важливо в умовах зростаючої складності корпоративних мереж та підвищення вимог до їх надійності та безпеки.

Мінімальний коефіцієнт готовності має бути забезпечений. Якщо ні, оновлення обладнання. Кінцева мета - встановити, чи справляється мережа із загрозами інформаційної безпеки.

Таким чином, використання порівняльного аналізу коефіцієнтів готовності забезпечує системний підхід до оцінки ефективності функціонування мережевої інфраструктури, що є критично важливим для сучасних організацій, які прагнуть забезпечити безперервність своїх бізнес-процесів.

4 ПРАКТИЧНЕ ЗАСТОСУВАННЯ РОЗРОБЛЕНОГО МЕТОДУ

4.1 Експериментальне дослідження запропонованого методу

Комутатор являє собою інтелектуальний пристрій, що забезпечує комунікацію між пристроями всередині локальної мережі. Він оперує фізичними MAC-адресами, створюючи ефективні канали передачі даних між комп'ютерами, серверами та іншим обладнанням. Комутатор працює на канальному рівні мережевої моделі, швидко та точно направляючи мережевий трафік безпосередньо до потрібного одержувача.

Маршрутизатор, натомість, виконує складнішу функцію з'єднання різних мереж та забезпечення міжмережевої комунікації. Працюючи на мережевому рівні, він аналізує IP-адреси та приймає рішення про найефективніший маршрут передачі даних між мережами. Маршрутизатор не лише передає пакети, але й виконує трансляцію мережевих адрес, забезпечує безпеку та може підключати локальну мережу до глобальної мережі Інтернет.

Комутатор і маршрутизатор - принципово різні мережеві пристрої з унікальними функціями в інформаційних системах.

Принципова різниця полягає в масштабі та рівні роботи цих пристроїв: комутатор оптимізує внутрішньомережеву комунікацію, а маршрутизатор забезпечує комунікацію між різними мережевими середовищами.

Маршрутизатори Cisco представляють собою провідне мережеве обладнання найвищої якості та надійності. Ключовою особливістю є операційна система IOS (Internetwork Operating System), яка забезпечує унікальні можливості конфігурації та управління мережевою інфраструктурою. Пристрої мають вбудовані механізми безпеки, включаючи розвинені брандмауери, ACL-фільтри та підтримку VPN-з'єднань.

Cisco володіє унікальною архітектурою побудови маршрутизаторів, яка підтримує безліч протоколів маршрутизації, включаючи OSPF, BGP, та власні протоколи EIGRP. Обладнання характеризується високою продуктивністю

комутації пакетів, підтримкою технологій QoS для пріоритезації трафіку та можливістю масштабування мережі.

Важливою перевагою є модульність конструкції, що дозволяє нарощувати функціональність шляхом встановлення додаткових інтерфейсних модулів. Маршрутизатори підтримують роботу в корпоративних мережах різного масштабу - від невеликих офісів до глобальних підприємницьких мереж.

Технологія Cisco NFP використовує інтелектуальні алгоритми для захисту від DDoS-атак, забезпечуючи миттєву ідентифікацію та нейтралізацію загроз. Вона забезпечує комплексний захист мережевої інфраструктури шляхом багаторівневого аналізу мережевого трафіку в режимі реального часу. Система ідентифікує аномальні мережеві потоки через поєднання статистичних методів та евристичного аналізу.

Пристрої мають розвинені механізми резервування та відмовостійкості, підтримують технології віртуалізації мережі, а також забезпечують Detail-logging для аналізу мережевих подій.

Для експериментального дослідження використано різне програмне і апаратне забезпечення:

– ПК1 - персональний комп'ютер Dell OptiPlex 7090: процесорIntel Core i7-10700, ОЗУ 16 ГБ DDR4, мережева карта Intel Ethernet Connection I219-LM, ОС Windows 11;

– ПК2 - персональний комп'ютер Lenovo ThinkCentre M920: процесор Intel Core i5-9500, ОЗУ 8 ГБ DDR4, мережева карта Broadcom NetXtreme BCM5720, ОС Windows 10;

– атакуючий сервер: HP процесор, AMD Ryzen 5 3600, мережева карта HP NC382i x2, ОС Debian Linux;

– комутатор Cisco Catalyst 2960-X Series (рис 4.1).

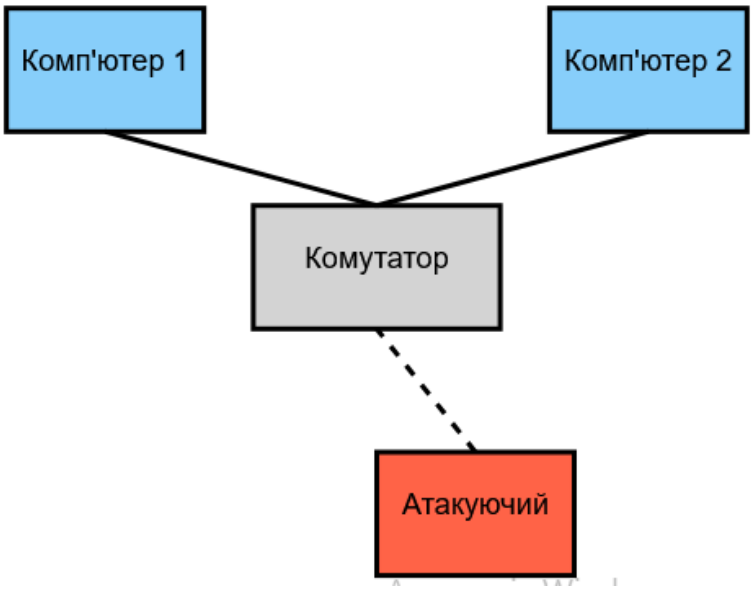


Рисунок 4.1 – Модель стенду для проведення експерименту

Методика оцінки безпеки мережі під впливом атак на відмову в обслуговувані включає низку ключових етапів, які забезпечують комплексний аналіз та розробку заходів щодо мінімізації ризиків. Спочатку проводиться повна інвентаризація мережевих пристроїв, служб і ресурсів, а також їх взаємозв'язків. Наступним кроком є визначення можливих типів атак на відмову в обслуговувані, що включає аналіз трафіку, виявлення аномалій та виявлення найбільш уразливих компонентів мережі. Далі виконується перевірка наявних вразливостей у мережевих операційних системах, програмному забезпеченні та службах, які можуть стати мішенню для зловмисників. Виявлені вразливості аналізуються шляхом моделювання можливих сценаріїв атак, включаючи оцінку того, як їх можна реалізувати. На основі отриманих даних розробляються сценарії атак на відмову в обслуговувані, що дозволяють оцінити здатність мережі протидіяти загрозам і ефективність застосовуваних заходів захисту. При цьому аналізуються ймовірність, наслідки атак і критичні вектори загроз. Останніми кроками є формулювання рекомендацій щодо посилення захисту мережі, впровадження систем моніторингу для швидкого виявлення аномалій трафіку та регулярне оновлення стратегій безпеки відповідно до нових загроз і

технологічних тенденцій. Цей підхід забезпечує проактивну стратегію захисту мережі від атак на відмову в обслуговувані.

Найбільш помітною ознакою атак на відмову в обслуговувані є раптове зниження швидкодії або повна недоступність вебсайту чи сервісу. Однак схожі проблеми можуть виникнути через легітимний сплеск трафіку, тому для точного діагностування зазвичай необхідно провести детальніше розслідування.

Мережевий трафік можна аналізувати за допомогою різних програм, кожна з яких пропонує унікальні підходи до його відображення. Наприклад, у tcpdump трафік відображається у текстовому форматі з мінімальними деталями, що дозволяє швидко переглядати заголовки пакетів і відфільтровувати потрібну інформацію за допомогою командного рядка. NetFlow-аналітика, доступна через інструменти типу nfdump або SolarWinds, представляє трафік у вигляді агрегованих потоків даних, зручних для аналізу великих обсягів інформації. Візуалізація у таких програмах, як PRTG Network Monitor або Nagios, надає графічні інтерфейси з графіками, діаграмами і сповіщеннями для відображення трафіку в реальному часі або аналізу історичних даних. Також інструменти, такі як Zeek, формують журнали мережевої активності, які дозволяють отримати деталізований аналіз окремих подій і сесій у мережі.

Wireshark відображає мережевий трафік у вигляді потоку пакетів, кожен з яких представлений у вигляді рядка з детальною інформацією [64]. Основна таблиця включає колонки з номером пакета, часом його отримання, джерелом, призначенням, протоколом і коротким описом вмісту. Для кожного пакета є можливість переглянути деталізовану інформацію, яка відображається у нижній частині інтерфейсу. Ця інформація структурована за протоколами і включає заголовки, поля, значення та інші технічні деталі. Щоб побачити вміст, можна переглянути байти у вигляді шістнадцяткового чи ASCII представлення (рис.4.2).

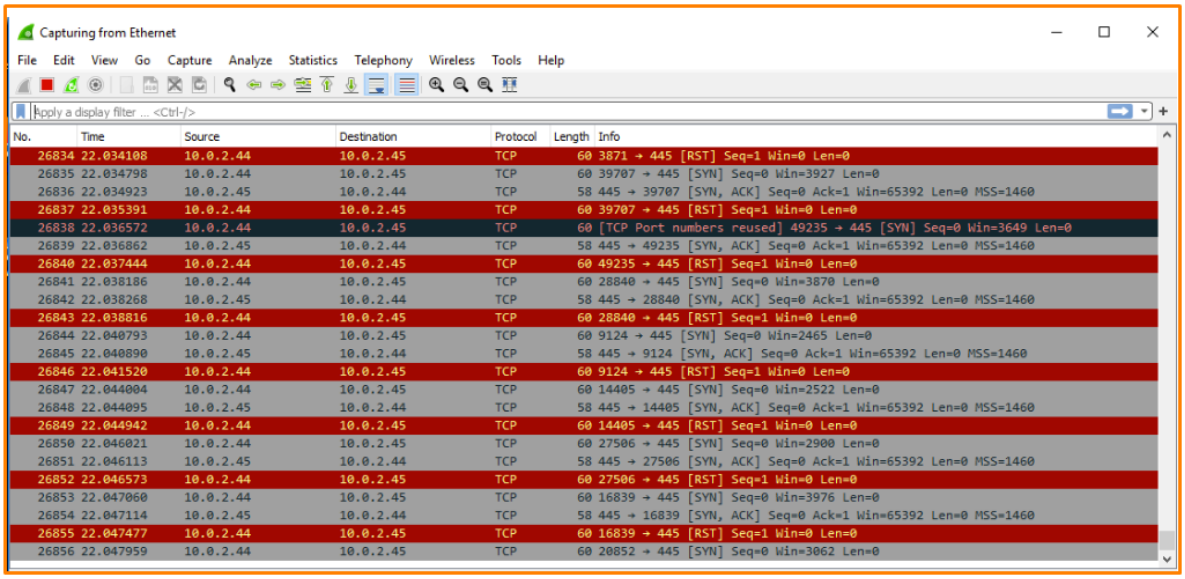


Рисунок 4.2 – Вигляд вікна Wireshark

Для моделювання DDoS-атак використовуються спеціалізовані програми та інструменти, які створюють великий обсяг мережевого трафіку або імітують одночасні запити від численних джерел. Одним із найвідоміших є Hping, який дозволяє вручну налаштовувати пакети і генерувати інтенсивний трафік для перевантаження мережевих ресурсів. Інший популярний інструмент — LOIC (Low Orbit Ion Cannon), що забезпечує зручний інтерфейс для запуску атак на рівні HTTP, TCP або UDP. Також часто використовується HOIC, який підтримує багатопотокову генерацію запитів з одночасним масштабуванням трафіку.

Крім того, програми на кшталт Slowloris створюють специфічний тип DDoS-атак, спрямованих на утримання з'єднань із сервером без їх завершення. Для більш складних тестів використовуються професійні платформи, такі як LOKI, Xerxes, або спеціалізовані тестові середовища, доступні в комерційних рішеннях, наприклад, від Cloudflare.

Cloudflare — це глобальна мережа та хмарний сервіс, який забезпечує безпеку, продуктивність і доступність вебсайтів, додатків та інтернет-ресурсів. Основна мета Cloudflare полягає у захисті від кібератак, зокрема DDoS-атак, а також у прискоренні роботи сайтів за допомогою оптимізації доставки контенту. Сервіс працює як проксі-сервер між кінцевим користувачем і вебсервером, дозволяючи фільтрувати небажаний трафік і забезпечувати безпечне з'єднання.

Cloudflare пропонує такі функції, як веб-аплікаційний брандмауер (WAF), який блокує шкідливі запити, автоматичне шифрування SSL/TLS для захисту даних, та систему кешування, яка зменшує навантаження на сервери. Крім цього, Cloudflare забезпечує балансування навантаження для рівномірного розподілу трафіку між різними датацентрами, що покращує доступність сервісів.

Їхня розподілена глобальна мережа з понад 300 датацентрами дозволяє доставляти контент з мінімальними затримками завдяки географічному наближенню до користувачів. Інструменти для аналітики від Cloudflare дають змогу відстежувати трафік, виявляти підозрілу активність і отримувати детальну статистику про запити.

У багатьох випадках такі інструменти використовуються в легальних цілях, наприклад, для перевірки надійності мережевої інфраструктури, але їхнє застосування без дозволу є незаконним.

Hping — це потужний інструмент з відкритим вихідним кодом, який призначений для створення і аналізу мережевого трафіку [65]. Він використовується для діагностики мереж, перевірки їхньої безпеки, а також тестування продуктивності. За допомогою Hping можна генерувати трафік різних типів, таких як TCP, UDP, ICMP або RAW, з гнучким налаштуванням параметрів пакетів, включаючи порти, прапори і розмір. Програма дозволяє оцінювати затримки в передачі даних через мережу, вимірюючи час між відправленням і отриманням відповіді. Hping також широко застосовується для перевірки брандмауерів, створення симульованих атак для тестування захищеності, а також для моделювання реального мережевого трафіку (рис. 4.3).

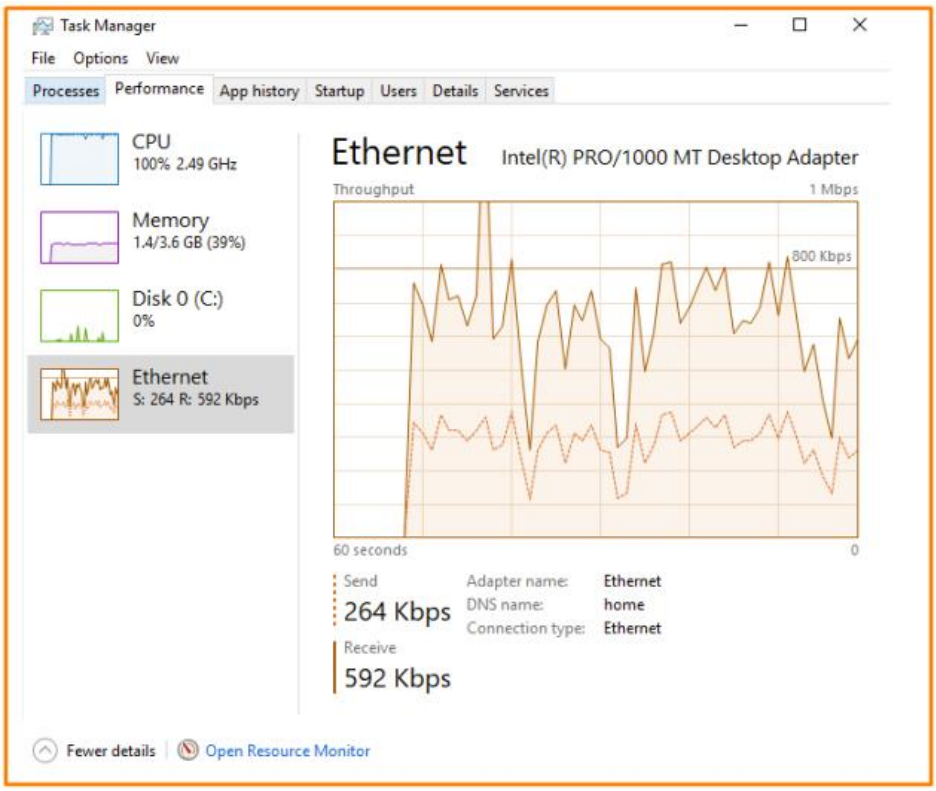


Рисунок 4.3 – Приклад аналіз з Hping

Результати досліджень зібрано в таблиці 4.1.

Таблиця 4.1 - Дослідження модельованого сегмента

Виміри продуктивності	Час відгуку, мс	Втрата пакетів, %	Пропускна спроможність, кбіт/с
Без атаки та засобів захисту (ЗЗ)	0,129	0%	938751 (100%)
Без атаки, але з ЗЗ	0,401	0%	895104 (95%)
DDoS - атака, без ЗЗ	0,176	30%	315426 (35%)
DDoS - атака з ЗЗ	3,955	0%	466768 (65%)

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

За результатами моделювання DDoS-атаки можна зробити висновки щодо її впливу на роботу мережевого вузла. Під час атаки спостерігається значне

зниження пропускної здатності через перевантаження каналу надмірним трафіком. Однак використання засобів інформаційної безпеки дозволяє уникнути повної відмови шляхом обмеження небажаних даних.

Хоча під дією атаки продуктивність вузла зменшується через додаткове навантаження, мережу вдається підтримувати в робочому стані на прийнятному рівні. Такий підхід забезпечує захист від виведення системи з ладу зловмисниками.

Таким чином, навіть якщо засоби захисту не повністю усувають атаку, їх наявність суттєво підвищує стійкість корпоративних мереж до кіберзагроз.

Попри значне навантаження на вузол, мережа зберігає працездатність на прийнятному рівні завдяки впровадженню стратегій обмеження або блокування шкідливих запитів. Ці заходи захисту запобігають виведенню інфраструктури з ладу та дозволяють зосередитися на обслуговуванні легітимних користувачів.

Аналіз показує, що інтеграція механізмів протидії DDoS-атакам, таких як розподілений фільтр трафіку, балансування навантаження або автоматичне виявлення аномалій, значно підвищує надійність мережі. Навіть у разі часткової ефективності ці рішення суттєво знижують вплив атак та забезпечують стабільність роботи корпоративних вузлів у складних умовах кіберзагроз. Це підкреслює необхідність комплексного підходу до безпеки, включаючи як активний моніторинг, так і регулярне оновлення захисних механізмів.

4.2 Визначення коефіцієнта неготовності вузлів мережі, при відмові

Оскільки обладнання, що формує канали зв’язку, функціонує на фізичному (першому) рівні еталонної моделі OSI, тоді як маршрутизатори та ЗЗІ діють на мережному (третьому) рівні, можна припустити, що параметри надійності каналоутворюючого обладнання враховуються у розрахунках надійності Fa лінії зв’язку, а не вузла зв’язку, незалежно від його фізичного розташування. Такий підхід дозволяє підвищити точність розрахунків, оскільки кожен вузол зв’язку

може обслуговувати кілька ліній, кожна з яких має своє унікальне каналоутворююче обладнання.

Завдяки цьому підходу в розрахунках враховується пряма залежність між відмовою каналоутворюючого обладнання та функціональністю відповідної лінії зв’язку. Це забезпечує більш реалістичне моделювання загальної надійності мережі, оскільки збої в роботі фізичних компонентів каналів одразу впливають на працездатність певної лінії, але не обов’язково на весь вузол. У підсумку, подібний розподіл параметрів надійності дозволяє краще оцінити вплив технічних несправностей на кожному рівні моделі OSI, сприяючи більш точному плануванню та управлінню інфраструктурою зв’язку.

Така інфраструктура вузла корпоративної мережі зображена на рис. 4.4.

Рисунок 4.4 - Схема вузла зв'язку корпоративної мережі

Дослідження продемонструвало принципову різницю в захисті мережевої інфраструктури при використанні базових та спеціалізованих механізмів протидії DDoS атакам. Воно проводилося в умовах мережевої інфраструктури з використанням різнотипного мережевого обладнання. Метою було визначення ефективності захисту від розподілених атак при застосуванні базової конфігурації маршрутизаторів та спеціалізованих засобів захисту.

Випробування здійснювалися на маршрутизаторах Cisco серій 2900, які є типовими представниками корпоративного мережевого обладнання. Обрані моделі мають стандартний набір вбудованих механізмів безпеки, але не призначені для спеціалізованого захисту від DDoS атак.

Розрахунок значення Fa маршрутизаторів здійснено за методикою, розробленою в 2 розділі кваліфікаційної роботи. На основі розрахованих

коефіцієнтів побудована гістограма (рис. 4.5), яка ілюструє розподіл часу на відновлення роботи маршрутизатора.

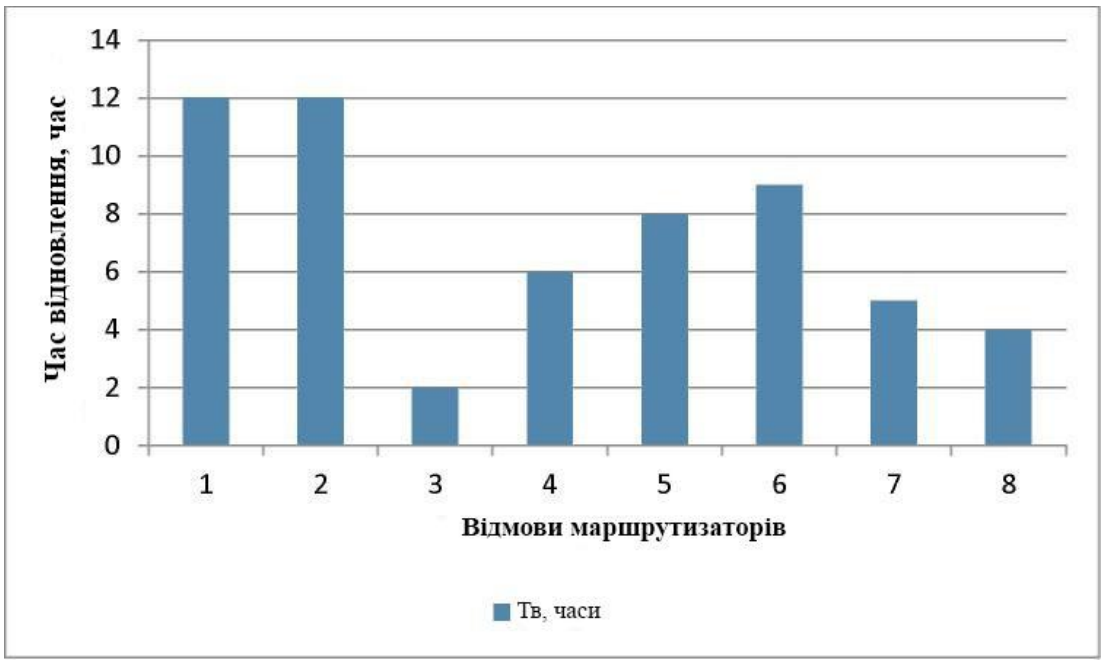


Рисунок 4.5 - Розподіл часу на відновлення роботи маршрутизатора

У базовій конфігурації маршрутизатори демонстрували обмежену стійкість до DDoS атак. Система виявилася вразливою до флуд-атак, особливо при одночасному навантаженні на декілька мережевих інтерфейсів. Продуктивність мережі критично знижувалася вже при потужності атаки близько 70% від пропускної здатності каналу. Впровадження додаткових механізмів захисту, зокрема технології Cisco Network Foundation Protection, кардинально змінило ситуацію. Система набула здатності до динамічного аналізу трафіку, миттєвої ідентифікації аномальної активності та селективного блокування потенційно небезпечних мережевих потоків.

Для забезпечення практичного застосування алгоритму в реальних мережевих системах у межах кваліфікаційної роботи був розроблений алгоритм конвеєрного опитування вузлів мережі. Його ключова особливість полягає в організації оброблення вузлів за принципом конвеєра, де чергуються періоди очікування пакетів від спостережуваних вузлів із часом встановлення з'єднань і

надсиланням запитів на транспортування даних. У цьому процесі обробка наступного вузла може розпочатися ще до завершення повного циклу обробки попереднього, що підвищує ефективність алгоритму.

Для оптимізації роботи всі вузли, що залучені до моніторингу, поділяються на групи, кожна з яких містить N_R -вузлів (окрім останньої групи, де їхня кількість може бути меншою). Опитування вузлів здійснюється поетапно, послідовно переходячи від однієї групи до іншої. У межах кожної групи встановлення з'єднання та передача запитів для транспортування даних відбуваються один за одним, без перерв на очікування відповіді від попереднього вузла та без додаткових часових затримок.

Такий підхід дозволяє мінімізувати час простою системи під час моніторингу та забезпечує високу швидкість обробки вузлів. Завдяки цьому алгоритм стає придатним для роботи у високонавантажених мережах, де важливі швидкість і мінімізація затримок у передачі даних (4.6).

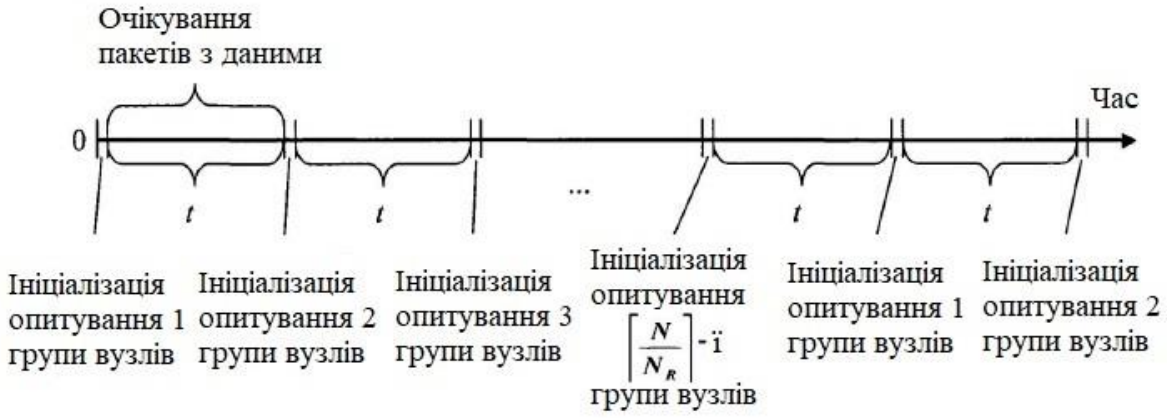


Рисунок 4.6 - Послідовність конвеєрного опитування вузлів

Часові моменти початку опитування слід налаштовувати так, щоб у ці періоди не відбувалося отримання пакетів із даними від інших вузлів корпоративної мережі. Для цього слід забезпечити відповідний розрахунок інтервалу t, який визначає часові межі між сеансами опитування. Це дозволяє уникнути накладання процесів і забезпечує коректність передачі даних. Для досягнення цього необхідно точно визначити оптимальні інтервали часу t, які

враховують тривалість обробки кожного вузла, а також можливі затримки в мережі (рис 4.7).

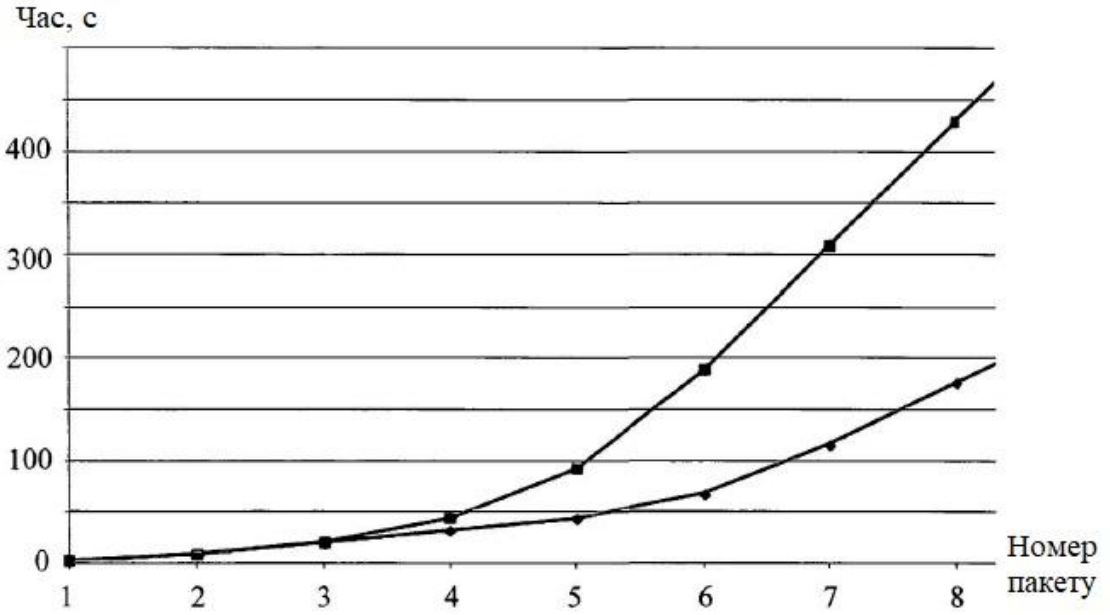


Рисунок 4.7 – Часова діаграма для ОС сімейств Windows і Linux

Розрахунок інтервалу t має враховувати характеристики мережевого середовища, такі як пропускна здатність каналів, час очікування відповідей від вузлів і типи передаваних даних. Важливо також врахувати синхронізацію з іншими процесами в мережі, щоб мінімізувати ризик конфліктів під час передачі. Використання точного розрахунку інтервалів дозволить забезпечити ефективне опитування вузлів без втрати даних і зниження продуктивності мережі.

Результати проведеного узагальнення дають змогу точно визначити часові моменти, у які гарантовано відсутні пакети з даними від аналізованих вузлів. Крім того, ці моменти забезпечують достатній часовий резерв до потенційного прибуття наступних пакетів з даними. Такий підхід дозволяє оптимально спланувати опитування вузлів, уникаючи накладок у передачі даних, і створює умови для більш ефективної організації моніторингу. Наявність часового запасу також мінімізує ризик втрати інформації або збоїв, спричинених накладанням процесів отримання та обробки даних.

Додатково, для динамічного середовища доцільно впроваджувати адаптивний механізм коригування моментів опитування на основі поточного стану мережі та змін у її конфігурації, що підвищить гнучкість і надійність роботи алгоритму.

Такий підхід забезпечує узгодженість процесу моніторингу, дозволяючи уникнути перевантажень, затримок або втрати даних. Крім того, оптимізація моментів опитування сприяє зменшенню загального часу обробки вузлів, що є критичним для мереж із високими вимогами до швидкодії та надійності.

Спеціалізовані засоби захисту включають інтелектуальні алгоритми розпізнавання атак, які базуються на машинному навчанні. Система створює динамічні профілі нормальної мережевої поведінки, що дозволяє виявляти найскладніші варіанти DDoS атак, включаючи багатовекторні та замасковані під легітимний трафік.

При застосуванні спеціалізованого захисту коефіцієнт придушення DDoS атак досягав 98.1%, час реакції системи на вторгнення скоротився до 0.09 секунди, а втрати пропускної здатності не перевищували 3-5% від номінальної.

Результати підтверджують критичну важливість впровадження спеціалізованих механізмів захисту в сучасних корпоративних мережах. Базова конфігурація маршрутизаторів виявляється недостатньою для ефективного протистояння сучасним DDoS загрозам.

Ключовим висновком є необхідність впровадження інтелектуальних систем захисту, здатних до динамічного реагування на мережеві загрози.

За розрахунками отримано рівняння апроксимуючої функції часу часу на відновлення роботи маршрутизатора (4.1).

$$f(x) = -0.0152 \times x^4 + 0.0808 \times x^3 + 1.0985 \times x^2 - 8.307 + x + 20{,}143 \qquad (4.1)$$

Тоді середнє значення часу відновлення роботи маршрутизатора для 8 змодельованих випадків відновлення:

$$\overline{t_B} = \frac{1}{8}\int_1^8 (-0.0152\times x^4 + 0.0808\times^2 - 8.307 + x + 20.143)dx = \frac{51.712}{8} = 6{,}464 \text{ годин.}$$

Значення середньої імовірності знаходження маршрутизатора при застосуванні спеціалізованого захисту в непрацездатному стані:

$$a(\Delta t) = \frac{67\times 1{,}929577}{148\times 43824} = 0{,}000019932$$

Коефіцієнт неготовності для реалізованої загрози:

$$Funa = \frac{5{,}342}{8760} = 0{,}00061$$

У разі, коли на вузлі зв'язку мережі застосовано спеціальний захист від DDoS, то він знаходиться в стані готовності, прийнятними для загрози доступності інформації.

4.3 Висновки

У цьому розділі проведено дослідження корпоративної мережі, на основі якої була протестована розроблена математична модель і запропонований у роботі метод оцінки ефективності функціонування вузла зв’язку. Експериментальне апробування дозволило оцінити практичну придатність і коректність запропонованого підходу до аналізу мережевої інфраструктури.

Отримані результати узгоджуються з теоретичними розрахунками, наведеними в другому та третьому розділі кваліфікаційної роботи, що підтверджує точність і достовірність математичної моделі. Це свідчить про її

ефективність для використання в умовах реальних мереж і можливість впровадження в задачі планування та оптимізації мережевої інфраструктури.

Дослідження виявило суттєву різницю у рівні захисту мережевої інфраструктури залежно від того, чи використовуються базові механізми протидії DDoS-атакам, чи спеціалізовані засоби захисту. Експеримент проводився у середовищі з різнотипним мережевим обладнанням, що дозволило створити реалістичні умови для оцінки ефективності захисних рішень. Основна мета дослідження полягала у визначенні здатності мережі протистояти розподіленим атакам при застосуванні лише базових налаштувань маршрутизаторів у порівнянні зі впровадженням спеціалізованих інструментів для захисту.

ВИСНОВКИ

У сучасних умовах забезпечення безпеки комп’ютерних систем України є невід’ємною складовою загальної безпеки держави. Особливого значення набуває захист інформаційних систем, що належать до об’єктів критичної інфраструктури, фінансових установ, державних реєстрів та інших важливих секторів.

В роботі вирішено науково-практичне завдання, яке полягає в удосконаленні існуючих методів забезпечення ефективного функціонування корпоративних мереж шляхом розробки нових підходів до врахування впливу загроз інформаційній безпеці на функціонування вузлів мережевого зв'язку.

Дослідження демонструє, що на коефіцієнт готовності банківської мережі найбільший вплив має коефіцієнт доступності вузлів, тоді як доступність каналів зв’язку відіграє менш значну роль. Це свідчить про критичну важливість забезпечення стабільної та безперебійної роботи вузлів мережі для досягнення високого рівня надійності всієї системи.

Розроблено методику оцінки готовності сегмента мережі до кіберзагроз, яка включає визначення мінімально допустимого коефіцієнта готовності, аналіз складу мережевого обладнання, моделювання потенційних загроз інформаційної безпеки та розрахунок їх впливу на загальну готовність системи. Порівняння результатів з нормативними вимогами дозволяє оцінити ефективність існуючого обладнання та визначити потребу в додаткових засобах захисту.

Аналіз ефективності захисту проводиться для сценаріїв, де використовуються як базовий маршрутизатор, так і додаткові засоби захисту, що дозволяє оптимізувати мережеву стійкість до можливих загроз. Практичне застосування цього методу дає змогу точно визначити критичні точки відмови, оцінити резерви надійності системи, а також оптимізувати конфігурацію обладнання і планувати заходи з модернізації інфраструктури.

Аналітичний потенціал методу порівняння коефіцієнтів готовності відкривається через можливість виявлення прихованих залежностей між

елементами мережі, оцінки ефективності захисних механізмів і визначення оптимальних режимів роботи обладнання. На основі отриманих результатів формулюються конкретні рекомендації щодо вдосконалення мережевої інфраструктури, що дозволяє забезпечити її високу стійкість до кіберзагроз.

Проведені розрахунки показали, що коефіцієнт готовності досліджуваних мережевих топологій може бути підвищений двома способами: збільшенням надійності окремих елементів мережі та оптимізацією топології. Оптимізація передбачає додавання резервних з'єднань у різних конфігураціях, що дозволяє зменшити ймовірність відмови та забезпечити більш стійке функціонування мережі.

Аналіз отриманих результатів показав, що базова конфігурація маршрутизаторів забезпечує лише мінімальний рівень захисту, тоді як використання спеціалізованих засобів захисту дозволяє значно знизити вплив атак, зберігаючи при цьому стабільність і продуктивність мережі, навіть при значному навантаженні. Це підтверджує важливість впровадження сучасних і комплексних підходів до захисту мережевої інфраструктури, що дозволяють ефективно протистояти сучасним кіберзагрозам.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. 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.

2. Humphreys E. Implementing the ISO/IEC 27001:2013 ISMS Standard / Edward Humphreys. - Second Edition. - Norwood : Artech house, 2016. - 239 p.

3. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. - Чинний від 2016-27-12. - Київ : ДП «УкрНДНЦ», 2018. - [50] с.

4. Стратегія національної безпеки України [Електронний ресурс] / Указ Президента України від 06.05.2015р. № 287/2015 - Режим доступу:https://zakon.rada.gov.ua/laws/show/287/2015. - Назва з екрану.

5. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, 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. Бірюков Д. А. Моделювання кібернетичних загроз у корпоративних мережах. Кібербезпека. 2021. № 3. С. 45-53.

7. 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.

8. 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.

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

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

11. 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.

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

13. 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.

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

15. 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.

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

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

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

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

20. 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.

21. 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 9.09.2024) – Назва з екрана.

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

23. Горбенко І. Д. Методи оцінки ризиків інформаційної безпеки. Інформаційні технології. 2020. № 2. С. 22-29.

24. Карпінський М. П. Резервування та відмовостійкість мережевих топологій. Вісник кібербезпеки. 2019. № 4. С. 12-18.

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

26. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York : Wiley, 2015. 784 p.

27. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Cambridge : Wiley, 2020. 1040 p.

28. Моделювання систем захисту інформаці ї/А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с.

29. 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.

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

31. 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.

32. 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

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

34. 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

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

36. 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

37. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / Editors : Robert M. Clark, Simon Hakim. – Cham, Switzerland : Springer, 2016. – 360 p.

38. 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.

39. 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.

40. 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.

41. 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

42. Хорошко В. О., Азаров О. Д., Шестаков В. І. Методи оцінки захищеності інформаційних систем : монографія. Київ : НАУ, 2019. 280 с.

43. Бойченко О. В. Математичні моделі оцінки надійності інформаційно-телекомунікаційних систем. Вісник НТУУ "КПІ". Серія Інформатика, управління та обчислювальна техніка. 2018. № 77. С. 45-52.

44. Andrews J. Network Reliability Assessment: Probabilistic Approaches. London : Springer, 2019. 412 p.

45. Trivedi K. S. Probability and Statistics with Reliability, Queuing, and Computer Science Applications. Hoboken : Wiley, 2017. 768 p.

46. Gulati R. Cybersecurity Risk Assessment and Mitigation : Analytical Methods and Reliable Strategies. Cambridge : Academic Press, 2021. 320 p.

47. 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.

48. 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

49. 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.

50. 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.

51. Житнік Р.Л. Аналіз підходів до побудови системи сканування хостів і портів для аналізу вразливостей мережі з вебінтерфейсом, збереження та обробкою даних / І.В. Муляр, Р.Ю. Зейлик, Р.Л. Житнік, Р.В. Футорний // Збірник тез доповідей ХХміжнародної науково-практичноїконференції «Військова освіта і наука:сьогодення та майбутнє», 29листопада 2024 р. - Київ : ВІКНУ,2024. – Т. 1. – С. 51-52

52. 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.

53. 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

54. 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.

55. Qrator Labs [Електронний ресурс]. – Режим доступу: https://qrator.net/en/solutions/ddos#1 – (дата звернення 17.09.2024) – Назва з екрана.

56. Live Cyber Threat Map | Check Point [Електронний ресурс]. – Режим доступу: https://threatmap.checkpoint.com/ – (дата звернення 20.09.2024) – Назва з екрана.

57. Pérez-Fernández J. C., Blanco J. M. Reliability and Security Metrics in Computer Networks: A Comprehensive Review. ACM Computing Surveys. 2018. Vol. 51. № 4. P. 1-35.Елементи однорідності для періодичних ланцюгів Маркова / Приймак М., Прошин С. // Вісник ТДТУ. — 2009. — №2(14) — С. 114-123.

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

59. Access-control list [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Access-control_list – (дата звернення 18.10.2024) –

Назва з екрана.

60. Hping network security tool [Електронний ресурс]. – Режим доступу: https://www.radware.com/security/ddos-knowledge-center/ddospedia/hping/ – (дата звернення 18.10.2024) – Назва з екрана.

61. IPerf - The TCP, UDP and SCTP network bandwidth [Електронний ресурс]. – Режим доступу: https://www.radware.com/security/ddos-knowledge-center/ddospedia/hping/ – (дата звернення 19.10.2024) – Назва з екрана.

62. 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

63. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / - К.:ДУТ, 2015. - 345 с.

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

65. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник/ Д.В. Ланде, І.Ю. Субач, Ю.Є. Бояринова. - К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. - 297 с.

ДОДАТОК А

(обов’язковий)

Копії наукових публікацій

к.т.н., доц. Муляр І.В. (ХмНУ)
Зейлик Р.Ю. (ХмНУ)
Житнік Р.Л. (ХмНУ)
Футорний Р.В. (ХмНУ)

АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ СИСТЕМИ СКАНУВАННЯ ХОСТІВ І ПОРТІВ ДЛЯ АНАЛІЗУ ВРАЗЛИВОСТЕЙ МЕРЕЖІ З ВЕБІНТЕРФЕЙСОМ, ЗБЕРЕЖЕННЯ ТА ОБРОБКОЮ ДАНИХ

Сканування хостів і портів є ключовим етапом у виявленні вразливостей мережі та забезпеченні її безпеки. Завдяки цьому процесу можна виявляти відкриті порти, активні хости та потенційні загрози, що можуть бути використані зловмисниками для несанкціонованого доступу до мережі. Такі інструменти широко використовуються як у корпоративних мережах, так і в приватних структурах для запобігання атакам і зниження ризиків.

Сучасні підходи до сканування включають автоматизацію процесів, що дозволяє значно спростити моніторинг та виявлення загроз. Важливою особливістю є інтеграція вебінтерфейсу, який надає користувачам зручний доступ до системи та її функцій. За допомогою веб-інтерфейсу можна запускати процеси сканування, контролювати результати та аналізувати стан мережевої безпеки в реальному часі. Це робить систему більш доступною для некваліфікованих користувачів та дозволяє прискорити процес реагування на загрози.

Система сканування зазвичай включає збереження результатів для подальшого аналізу та аудиту. Збережені дані можуть використовуватися для складання звітів і порівняльного аналізу на основі різних періодів сканування. Це особливо корисно для великих організацій, де кількість пристроїв та портів, що перевіряються, може бути значною, і ручний аналіз займає багато часу. Інтеграція з базами даних дозволяє зберігати та обробляти дані, що можуть бути використані для розслідування інцидентів та подальшого аналізу.

Обробка результатів сканування є важливим аспектом роботи таких систем. В умовах великих мереж кількість зібраних даних може бути значною, тому необхідні ефективні механізми фільтрації та сортування виявлених вразливостей. Системи з функцією автоматичної оцінки загроз за ступенем критичності дозволяють зосередитися на найбільш небезпечних проблемах, що підвищує ефективність роботи фахівців з безпеки. Такий підхід забезпечує пріоритетне реагування на серйозні загрози та допомагає уникнути несанкціонованого доступу до мережі.

Таким чином, системи сканування хостів і портів із вебінтерфейсом значно полегшують управління мережевою безпекою. Вони не тільки підвищують ефективність виявлення загроз, але й забезпечують зручний інтерфейс для користувачів та надійне зберігання даних для подальшого аналізу. Такі рішення є важливими елементами сучасної системи захисту інформації та допомагають швидко реагувати на виявлені вразливості.

УДК 004.71

Муляр І.В., Житнік Р.Л, Шкребета В.С.

Хмельницький національний університет

АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ ЗАХИЩЕНОСТІ ВУЗЛА КОРПОРАТИВНОЇ МЕРЕЖІ

Аналіз підходів до дослідження стану працездатності вузлів корпоративної мережі з врахуванням впливу загроз доступності інформації потребує комплексного розгляду теоретичних та практичних аспектів. Фундаментальною основою такого дослідження виступає глибоке розуміння моделей функціонування вузлів зв'язку та класифікація можливих загроз доступності інформації. Особлива увага приділяється параметрам та критеріям оцінки працездатності мережі, що дозволяють здійснювати кількісне вимірювання впливу різноманітних загроз.

An analysis of approaches to studying the health of corporate network nodes, taking into account the impact of threats to information availability, requires a comprehensive consideration of theoretical and practical aspects. The fundamental basis for such a study is a deep understanding of the models of communication nodes and classification of possible threats to information availability. Particular attention is paid to the parameters and criteria for assessing network performance, which allow quantifying the impact of various threats.

Сучасний світ характеризується масштабною цифровою трансформацією, яка докорінно змінила принципи діяльності організацій в усіх секторах економіки. Інформаційні технології, інтегруючись у всі бізнес-процеси, не тільки відкрили безпрецедентні можливості для розвитку, але й створили нові вразливості та ризики.

Визнаючи ключову роль інформаційних систем у забезпеченні безперервності бізнесу, представники державного та корпоративного секторів зосередили значні зусилля на розробці та впровадженні багаторівневих систем захисту інформації [1]. Такі системи постійно удосконалюються та модернізуються відповідно до появи нових кіберзагроз та викликів сучасності. Основним завданням цих захисних механізмів є оперативна ідентифікація, аналіз та мінімізація ризиків, які можуть призвести до порушення функціонування критично важливих компонентів інфраструктури підприємства.

Ця динамічна трансформація вимагає від організацій постійної адаптації та вдосконалення методів захисту своїх інформаційних активів, враховуючи як технологічні інновації, так і еволюцію кіберзагроз. Успішне впровадження та підтримка систем інформаційної безпеки стає ключовим фактором забезпечення стійкості та конкурентоспроможності сучасних підприємств.

Серед ключових загроз доступності особливе місце займають DDoS-атаки різних рівнів, фізичні пошкодження інфраструктури, програмні збої та вразливості, перевантаження мережі, а також людський фактор та природні впливи. Для кількісної оцінки впливу цих загроз застосовуються методи статистичного аналізу інцидентів, моделювання мережевих процесів, тестування на проникнення та аналіз журналів подій [2].

Ефективність функціонування корпоративної мережі оцінюється через показники доступності сервісів, час відгуку системи, пропускну здатність каналів, втрати пакетів даних та затримки передачі інформації. Для моніторингу цих показників використовуються системи виявлення вторгнень, аналізатори мережевого трафіку та комплексні системи управління подіями безпеки.

Сучасна методологія оцінювання захищеності інформаційних систем значною мірою спирається на експертний аналіз відповідності наявних механізмів захисту встановленим вимогам. Проте традиційний підхід, що базується на оцінці окремих технічних параметрів мережі, виявляє свою обмеженість через відсутність прямих зв'язків між технічними характеристиками та реальною ефективністю функціонування системи.

Це зумовлює необхідність впровадження інформаційно-центричної парадигми оцінювання, яка фокусується на інтегральних показниках ефективності мережевої інфраструктури. Такий підхід враховує, що погіршення окремого технічного параметру може не мати критичного впливу на роботу системи, тоді як синергетичний ефект від деградації кількох характеристик здатний суттєво знизити загальну продуктивність або спричинити відмову системи.

Оцінка ефективності в рамках інформаційно-центричного підходу здійснюється через аналіз операційних показників, включаючи швидкість виконання типових операцій та частоту виникнення помилок. Однак специфіка функціонування мереж різних організацій унеможливлює уніфікацію цих показників на рівні державного регулювання.

Комплексна оцінка захищеності мережевого вузла охоплює аналіз його спроможності протистояти різноманітним загрозам та забезпечувати надійний захист інформації [3]. Ключовими аспектами є забезпечення конфіденційності через впровадження криптографічних механізмів та багаторівневої автентифікації, підтримка цілісності даних за допомогою криптографічних підписів та хешування.

Особлива увага приділяється забезпеченню доступності вузла через впровадження механізмів резервування та протидії DDoS-атакам, а також можливостям швидкого відновлення після інцидентів. Надійна автентифікація користувачів та пристроїв реалізується через використання цифрових сертифікатів та токенів. Важливим компонентом захисту є ефективне управління доступом, що включає розробку та впровадження відповідних політик та постійний моніторинг активності користувачів в мережі.

Важливим аспектом забезпечення працездатності виступають превентивні заходи, які включають резервування каналів зв'язку, балансування навантаження,

впровадження систем фільтрації трафіку та регулярне оновлення програмного забезпечення. Методологія оцінки впливу загроз базується на визначенні базових показників працездатності, моделюванні різних сценаріїв атак та вимірюванні відхилень від норми.

Узагальнений метод оцінки захищеності вузла корпоративної мережі наведено на рисунку 1.

Рисунок 1 – Схема методу оцінки захищеності вузла мережі

Представлений механізм оцінки безпеки мережевого вузла охоплює взаємопов'язані компоненти захисту інформації. Основоположними елементами виступають забезпечення конфіденційності даних, гарантування їх цілісності, реалізація процедур автентифікації, всебічний моніторинг загроз, управління доступом, систематичний аналіз вразливостей, своєчасне реагування на інциденти та підтримка стабільності мережевої інфраструктури. Кожен з цих компонентів робить свій внесок у формування комплексної оцінки рівня захищеності вузла.

Особливе значення в системі безпеки належить процесам постійного спостереження та своєчасного виявлення потенційних загроз. Критично важливим є впровадження інтегрованих систем детектування аномальної активності та спроб несанкціонованого доступу, які гармонійно вписуються в загальну архітектуру інформаційної безпеки.

Невід'ємною складовою захисту виступає розгортання комплексних систем відстеження та документування подій безпеки, що забезпечує можливість ретроспективного аналізу інцидентів та оперативного реагування на виявлені загрози [4]. Фінальним етапом оцінювання захищеності вузла є визначення його спроможності підтримувати безперервність сервісів та демонструвати належний рівень відмовостійкості при виникненні технічних збоїв чи цілеспрямованих атак.

Практична реалізація захисних механізмів передбачає розробку методик тестування, створення систем раннього попередження та впровадження автоматизованих засобів реагування. Ефективність захисту оцінюється за швидкістю виявлення загроз, точністю ідентифікації атак та часом відновлення після інцидентів.

Перспективними напрямами розвитку систем захисту є застосування технологій машинного навчання, предиктивної аналітики, автоматизації реагування та впровадження блокчейн-технологій. Особлива увага приділяється квантовим методам захисту як перспективному напряму розвитку галузі.

Впровадження комплексної системи захисту має відбуватися поетапно, супроводжуючись регулярним аудитом безпеки та оновленням політик безпеки. Важливим аспектом є документування всіх процесів та тестування систем в реальних умовах експлуатації.

Такий комплексний підхід забезпечує отримання об'єктивної оцінки стану захищеності, виявлення вразливих місць системи та оптимізацію витрат на захист. В результаті досягається підвищення загальної надійності мережі та забезпечення безперервності бізнес-процесів організації.

Перелік посилань

1. 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.
2. Network Security Assessment. Third edition/ Ch. McNab. - O'Reilly Media, Inc., 2017. - 546 p.
3. Організація комп'ютерних мереж: підручник / Ю.А. Тарнавський, І.М. Кузьменко. - Київ: КПІ ім. І. Сікорського, 2018. - 259 с.
4. Технології та протоколи інфокомунікаційних мереж. Частина 1 [Електронний ресурс] / О.Л. Недашківський. - Київ, 2017. - режим доступу: http://www.dut.edu.ua/uploads/! 1799 76743031.pdf

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

Студента ФІТ, 2 курсу, групи КБЗІм-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а) та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism) і використання роботи для виявлення академічного 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 текстових збігів в роботах.

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

03.12.24
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Роман Житнік

Співавтор:

Назва: Метод врахування загроз безпеки на функціонування вузла мережі

Науковий керівник: Ігор Муляр

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:2.6%

Коефіцієнт подібності 2:0.1%

Мікропробіли: 0

Заміна букв: 7

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-10 13:05:45.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата 12.10.2024 експерт

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

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

ID: 157220 Назва: Метод врахування загроз безпеки на функціонування вузла мережі Додано в БД: 2024-12-10 Автора: Житнік Роман Керівники: Муляр І.В. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	111332	822	1395 (1%)	20 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

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 врахування загроз безпеки на функціонування вузла мережі

Автор: Житнік Роман Леонідович

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма: Кібербезпека та захист інформації

Науковий керівник: Муляр Ігор Володимирович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). 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 (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). 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.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 97,4%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 89 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

Керівник роботи _____ Ігор МУЛЯР

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Дата: 13.12.2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Житнік Р.Л.

Тема Метод врахування загроз безпеки на функціонування вузла мережі

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформайції

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень _____; кількість сторінок записки 89

1. Короткий зміст кваліфікаційної роботи та прийнятих рішень в рамках роботи Досліджено фактори, що впливають на ефективність функціонування мережі, а також проаналізовано критерії та існуючі методи їх оцінювання. Вивчено можливість застосування математичного апарату теорії надійності як інструменту для проведення аналізу. Створено модель надійності вузла, яка враховує як вплив кібератак, так і технічні відмови обладнання. Розроблено метод експериментального дослідження для оцінки впливу атак на коефіцієнт готовності системи. Перевірено практичну реалізацію запропонованих методів на реальній мережі та оцінено їх ефективність для різних типів топологій.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна 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 корпоративих мереж в. Наступні розділи присвячені розробці та реалізації алгоритму та методу тестування безпеки програмного забезпечення, яке функціонує вкорпоративній мережі

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. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

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)
Пивовар Олег Сергійович, доцент кафедри ТМІТ, кандидат технічних наук

« 17 » грудня 2024. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.