Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА МАГІСТРА

Метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки
Назва теми

Галузь знань 11 – Математика та статистика

Спеціальність 113 – Прикладна математика

Шифр ДРПМ.000000.19.01.00 ПЗ

Виконав: студент 2 курсу, група ПМм-19-1 _____ Рикун В.В.
Підпис Ініціали, прізвище

Керівник _____ к.т.н., доц. Муляр І.В.
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри ТМІТ _____ д.т.н., проф. Підченко С.К.
Підпис, дата Ініціали, прізвище
9 12 2020 р.

Хмельницький, 2020

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра телекомунікацій, медійних та інтелектуальних технологій

Освітній рівень магістр

Галузь знань 11 Математика та статистика

Спеціальність 113 Прикладна математика

Освітня програма освітньо-професійна програма підготовки магістра

ЗАТВЕРДЖУЮ

Зав. кафедри С.К. Підченко

"3" 09 2020 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Рикуну В.В.
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки
2. Керівник проекту (роботи) к.т.н., доц. Муляр І.В
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.09.2020 р. № 118

2. Строк подання студентом проекту (роботи) на кафедру 01.12.2020

3. Вихідні дані до проекту (роботи)

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Провести аналіз факторів, які впливають на забезпечення ефективного функціонування мережі, критеріїв та існуючих методів оцінки. Проаналізувати можливість застосування методичного та математичного апарату теорії надійності як методу дослідження. Створити модель надійності вузла, що враховує вплив атак і відмов обладнання. Створити метод експериментального дослідження впливу атак на коефіцієнт готовності вузла зв'язку мережі. Застосувати розроблені методи до існуючої мережі, довести їх придатність для різних топологій

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Тема, мета магістерської роботи, об'єкт, предмет, задачі дослідження, наукова новизна, практична цінність, апробація роботи. Фактори що впливають на функціонування мережі. Алгоритм оцінки процесу захищеності. Марківська модель вузла звязку. Експериментальне визначення ймовірності проведення атаки. Вдосконалення методу обліку вплив загроз інформаційної безпеки. Результати дослідження застосовані на частині мережі. Порівняння коефіцієнта готовності оптимізованих топологій. Висновки

6. Консультанти розділів дипломного проекту (роботи)

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

7. Дата видачі завдання «__» _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики ДРМ з керівником	2.02.2020	
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	2.03.2020	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	1.04.2020	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	1.05.2020	
5	Робота над науковою статтею	1.06.2020	
6	Робота над розділом 3 – розробка алгоритмів та технологій, їх аналіз	1.09.2020	
7	Робота над розділом 4 – моделювання процесу, для вирішення поставленої задачі	1.10.2020	
8	Узгодження отриманих; оформлення пояснювальної записки згідно вимог	1.11.2020	
9	Оформлення графічної частини	11.11.2020	
10	Попередній захист ДР	15.11.2020	
11	Захист ДР на засіданні ЕК	12.12.2020	

Студент Підпис В. В. Гецко Ініціали, прізвище

Керівник проекту (роботи) Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема дипломної роботи: Метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки

Автор роботи: Рикун Валентин Володимирович

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

Загальний обсяг роботи: 81 сторінка, 23 рисунків, 7 таблиць, 2 додатки, 46 посилань,

КОРПОРАТИВНІ МЕРЕЖІ, КОЕФІЦІЄНТ ГОТОВНОСТІ, ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗПОДІЛЕНІ АТАКИ

Метою дипломної роботи є вдосконалення методу врахування загроз інформаційної безпеки на вузли мережі та їх впливу на функціонування вузла зв'язку корпоративної мережі.

Дана дипломна робота присвячена розробці методу дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації, особливістю якого є можливість кількісної оцінки ступеня впливу загроз на ефективність функціонування корпоративної мережі. Це дозволить прогнозувати стан мережі в умовах впливу непрацездатності обладнання та загроз, і оцінювати ефективність функціонування мережі у вигляді кількісного показника, тим самим підвищуючи якість оцінки.

ANNOTATION

a master's degree work of Rykun Valentyn

entitled «A method of assessing the effectiveness of the communication node of the corporate network, taking into account information security».

Mentor: Ihor Muliar

Total volume of work: 81 pages, 23 figures, 7 tables, 2 appendices, 46 references.

CORPORATE NETWORKS, PREPAREDNESS RATIO, INFORMATION SECURITY, DISTRIBUTED ATTACKS

The purpose of the thesis is to improve the method of taking into account information security threats to network nodes and their impact on the functioning of the communication node of the corporate network.

This thesis is devoted to the development of a method for studying the state of operation of network nodes in the face of threats to the availability of information, the feature of which is the ability to quantify the degree of impact of threats on the efficiency of the corporate network. This will allow predicting the state of the network in the face of equipment failures and threats, and assess the effectiveness of the network in the form of a quantitative indicator, thereby improving the quality of assessment.

Дата / Date 09.12 Підпис студента / Signature

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АЗ – апаратне забезпечення

ДЦ - дата-центр

ІТ - інформаційні технології

ІКС – інформаційно комунікаційна система

ІБ - інформаційна безпека

ЗЗІ - засоби захисту інформації

ЗБІ - загроза безпеці інформації

ККМ – корпоративна комп’ютерна мережа

ІС - інформаційна система

ПЗ - програмне забезпечення

СПЯ - система показників якості

DoS - Denial Of Service

DDoS - distributed denial of service

Fa - availability factor (коефіцієнт готовності)

Funa - unavailability factor (коефіцієнт неготовності)

ICMP - Internet Control Message Protocol

UNI - User-Network-Interface (інтерфейс користувач-мережа)

VPN - Virtual Private Networks (віртуальна приватна мережа)

WAN - Wide Area Network (великомасштабна територіальна мережа)

ВСТУП

Використання ресурсів у всіх сферах глобальної комунікаційної мережі сприяло тому, що зловмисники вже більше десяти років активно здійснюють різні правопорушення у сфері високих технологій [11] і в даний час активно розробляють різні способи та стратегії впливу інформаційних технологій. Вперше концепція впливу інформаційних технологій в юридичній літературі зустрічається в доктрині інформаційної безпеки України, цей ефект стосується негативного фактору, що впливає на стан інформаційної безпеки в нашій країні. Під інформаційними технологіями слід розуміти події, спрямовані на використання активів та можливостей інформаційних технологій та інших руйнівних впливів несанкціонованого зловмисника на об'єкти глобальної мережі, операційні процеси яких порушують стабільність його функціонування та інформаційну безпеку [15]. Таким чином, оскільки вплив інформаційних технологій може спричинити кібератаки [36], вартість яких дуже значна. Дані про фінансовий збиток, заподіяний різними кібератаками за 2019 рік [7], свідчать про те, що існуючі рішення, що забезпечують інформаційну безпеку, не в повній мірі здатні захистити від такого типу наслідків. Для захисту від загроз даних, що розробляються і широко використовуються різні системи виявлення та протидії кібератакам. Однак такі системи не враховують динаміку змін у мережі передачі даних і не враховують шкоду [12].

Аналіз тактики успішних кібератак на об'єкти показує, що злочинці, щоб досягти цієї мети, досить часто використовують різнорідні кібератаки [19]. Під різними атаками маються на увазі кібератаки, спрямовані на мережеву інфраструктуру жертви та захищену інформацію. Одним із можливих сценаріїв кібератак може бути атака, що полягає у впливі на систему виявлення та протидії кібератакам з подальшим проникненням у захищену локальну мережу або мережевий ресурс. Виклик мережевих кібератак - це часткове або повне вимкнення системи для виявлення та протидії атакам (як варіант DDoS-атаки). Атака на захищену локальну мережу, спрямована на викрадення або спотворення

інформації, що обробляється (як варіант введення SQL, введення шкідливого коду тощо). Ця тактика полягає в тому, що існуючі рішення не здатні ефективно виявляти та протистояти відповідно різним типам кібератак. Ці недоліки пов'язані з тим, що існуючі системи виявлення протидії кібератакам не використовують динамічно мінливі (регульовані) правила роботи та не враховують шкоду.

На актуальність рішення цієї важливої науково-технічної задачі наголошують багато повідних українських і зарубіжних вчених, зокрема П.П. Воробієнко, С.В. Лєнков, В.М. Б.А. Котельников, Л.Е. Назаров, А.Н. Колмогоров, Дж. Во-зенкрафт, А. Витерби, Р. Галлагер, У. Питерсон, Т. Кассами, Р. Блейхут і інші.

Розуміння природи та функцій кіберзлочинності та безпеки мережі; якісний описовий механізм є найбільш ідеальним засобом збору та аналізу даних завдяки гнучкості, адаптивності та безпосередності теми. Це призводить до властивої упередженості, але ще однією характеристикою таких досліджень є виявлення та моніторинг цих упереджень, включаючи, таким чином, їх вплив на збір та аналіз даних, а не спроби їх усунути. Нарешті, аналіз даних при інтерпретаційному якісному дослідженні є індуктивним процесом. Дані досить описові та суттєво сприяють цьому дослідженню.

В магістерській роботі під корпоративними комп'ютерними мережами (ККМ) розуміються в першу чергу ККМ установ банківської системи України, так як характеристики ККМ, статистичні дані про вторгнення, досвід впровадження безпосередньо відноситься до підприємств банківської сфери. У той же час, результати дослідження показали, що їх доцільно використовувати і на підприємствах в інших сферах економіки.

Оскільки системи зв'язку дуже важливі для нормального функціонування організації, вони стають пріоритетом для злочинців. Впливаючи на мережу, організовуються атаки, спрямовані на різні характеристики інформації. Загроза інформаційній безпеці - це сукупність умов та факторів, що створюють потенційну або фактичну загрозу інформації. Під час атак зловмисників існує ризик втрати, спотворення, блокування, копіювання, розповсюдження інформації, а також інших несанкціонованих дій із нею.

Незалежно від конкретних типів загроз, слід забезпечити такі основні властивості: цілісність, конфіденційність та доступність. Доступність - це можливість отримати необхідний інформаційний сервіс за розумний час.

Цілісність означає доречність та послідовність інформації, її захист від знищення та несанкціонованих змін.

Конфіденційність - це захист від несанкціонованого доступу до інформації.

Проблема цілісності та конфіденційності успішно вирішується завдяки використанню криптографічного захисту інформації. У цьому магістерському дослідженні запропоновано метод оцінки ефективності комунікаційного вузла корпоративної мережі з урахуванням інформаційної безпеки. Це дає можливість вжити заходів щодо їх нейтралізації та оцінити ефективність їх використання.

Основним завданням цього дослідження є поєднання характеристик надійності та інформаційної безпеки в єдину математичну модель. Процеси Маркова та експоненціальний розподіл можливих подій можуть бути використані для моделювання характеристик надійності та захисту інформації. Як показник, що безпосередньо характеризує властивості системи, доцільно використовувати коефіцієнт готовності (*Fa*). Класичним підходом до моделювання ККМ є приведення її до деревовидного графу. Одним з підходів є нормування *Fa* для ККМ та ліній зв'язку для мереж передачі даних, але існуючі правила не застосовуються до корпоративних мереж передачі даних, побудованих поверх Інтернету, оскільки мережа, сформована таким чином, частково абстрагується від певного постачальника послуг.

З врахуванням вищесказаного, розробка методу оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки є актуальним науково-технічним завданням.

Мета та завдання дослідження: вдосконалення методу врахування загроз ІБ на вузли мережі та їх впливу на функціонування вузла зв'язку корпоративної мережі

Для досягнення цієї мети в роботі потрібно вирішити наступні завдання:

1. Проаналізувати фактори, що впливають на ефективне функціонування ККМ,. Визначити критерії та фактори, що впливають на ефективність функціонування мережі з врахуванням загроз ІБ.

2. Дослідити можливість використання математичного апарату теорії надійності як методу дослідження ККМ для оцінки впливу загроз ІБ. Перевірити можливість підвищення ефективності функціонування мережі за рахунок топологічних засобів (зміна топології мережі).

3. Розробити модель надійності вузла ККМ з урахуванням впливу загроз ІБ та відмов обладнання.

4. Провести експериментальне дослідження впливу загроз доступності інформації на коефіцієнт готовності.

5. Удосконалити метод обліку впливу загроз ІБС на надійність та ефективність вузлів зв'язку.

6. Розробити спосіб підвищення ефективності вузлів зв'язку ККМ під впливом хакерських атак та забезпечити ІБ в корпоративних мережах топологічними засобами.

7. Провести оцінку ефективності комунікаційних вузлів існуючих ККМ, підтвердити їх придатність для різних фізичних топологій.

Об’єктом дослідження є процес функціонування корпоративних мереж в умовах загроз інформаційної безпеки

Предметом дослідження є властивості вузла зв'язку, що впливають на ефективність функціонування мережі.

Наукова новизна результатів магістерської роботи:

1. Вдосконалено модель надійності вузла зв'язку мережі, що відрізняється від відомих врахуванням впливу загроз інформаційної безпеки, спрямованих на порушення доступності інформації.

2. Удосконалено метод дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації, особливістю якого є можливість кількісної оцінки ступеня впливу загроз на ефективність функціонування корпоративної мережі.

Метод дослідження: для вирішення поставлених завдань використано методи теорії системного аналізу, теорії графів, теорія ймовірностей, математичної статистики, методи системного аналізу, математичного та імітаційного моделювання. Апробація проводилася шляхом проведення реальних експериментів.

Практичне значення роботи. реалізація розроблених у магістерському досліджені моделей, алгоритмів та методів дозволило прогнозувати стан ККМ в умовах впливу непрацездатності обладнання та загроз ІБ, та оцінювати ефективність функціонування ККМ у вигляді кількісного показника, тим самим підвищуючи якість оцінки

Публікації. За матеріалами магістерської роботи опубліковано 1 стаття у нефаховому журналі та 1 теза доповіді на міжнародній конференції.

1 ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ВРАХУВАННЯ ВПЛИВУ ЗАГРОЗ НА ЕФЕКТИВНІСТЬ ФУНКЦІОНУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Корпоративні мережі в банківській системі

Більшість сфер діяльності та підприємств сучасного суспільства істотно автоматизовані. Хоча розвиток технологій не має меж. Будь-яка організація - це сукупність взаємодіючих між собою підрозділів, кожен з яких може мати свою власну структуру. Елементи функціонально взаємопов’язані, тобто вони виконують певні види роботи в рамках одного бізнес-процесу, а також інформацію, обмін документами, факсами, письмовими та усними замовленнями тощо, крім того, ці елементи взаємодіють із зовнішніми системами та взаємодіють між собою. також може бути як інформаційним, так і функціональним. І така ситуація справедлива майже для всіх організацій, незалежно від того, якою діяльністю вони займаються - для державного органу, банку, промислового підприємства, комерційної фірми тощо.

Проблема зв'язку багатьох інфокомунікаційних систем полягає в тому, що кількість параметрів, необхідних для опису поведінки системи (системний розмір), дуже велика, і прийняти правильне рішення в таких мережах досить складно, враховуючи те, що інформація про стан мережа може бути досить суперечливою. Зростаючий вимір сучасних технологій є об’єктивною тенденцією, яку можна спостерігати історично протягом усього розвитку цифрової ІКС. Поява концепції інфокомунікаційних мереж нового покоління (NGN та FN - мережі майбутнього) дозволить користувачам значно розширити горизонти своєї діяльності, спектр послуг [41]. Однак шлях до переходу до мультисервісних мереж складний і тернистий. Тому питання полягає в тому, чи простіше продовжувати експлуатувати існуючі мережі до тих пір, поки існує попит на перелік послуг, які вже розроблені та піклуються про їх якість.

Звичайно, при швидкому розвитку мереж нового покоління можна назвати "проблемними точками" функціонування інфокомунікаційних мереж нового

покоління з точки зору оператора. Ключовими моментами в роботі мережі є її надійність та досконаліть системи управління. До «хворих точок» мереж нового покоління належать не стільки проблеми з використовуваними технологіями, скільки завдання забезпечення стабільної роботи мережевого обладнання, стикувальних протоколів, інтерфейсів різних провайдерів та інформаційної безпеки.

Забезпечення безпеки інформації в мережах наступного покоління загалом та їх системах управління є складним завданням. У міжнародних стандартах питання інформаційної безпеки вирішуються одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі.

В умовах ринкової економіки оператори зв'язку є операторами мережі та постачальниками послуг (постачальниками послуг). Вони забезпечують побудову комунікаційних мереж загального користування, які називають публічними мережами (Public Network). Ці мережі призначені для надання послуг зв'язку широкому колу користувачів різних категорій [30].

Приватні мережі - це мережі, що належать установам та компаніям, чиї ділові інтереси виходять за межі ринку телекомунікацій.

Характерною особливістю приватних мереж є те, що всі мережеві ресурси використовуються виключно працівниками компанії, яка володіє мережею. Крім того, термін "приватна" мережа також означає закриту мережу, призначену для конфіденційного спілкування. У цьому сенсі термін "приватна мережа" частіше використовується стосовно мереж великих корпорацій з філіями в різних містах, країнах і навіть континентах. Мережі малого бізнесу завжди сприймаються як приватні.

Поєднання комп’ютерів у мережі дозволяє компанії оптимізувати свою інформаційну інфраструктуру (програми, додатки, бази даних тощо), що в свою чергу підвищує ефективність бізнес-процесу в цілому. Залежно від масштабу виробничого підрозділу, в межах якого функціонує мережа, розрізняють мережі робочих груп, мережі відділів, мережі кампусів та корпоративні мережі [31].

Корпоративні мережі, як правило, належать великим компаніям, які складаються зі штаб-квартири (центрального офісу), або віддалених філій в інших містах, країнах або навіть на різних континентах. Кількість користувачів та комп'ютерів у такій мережі сягає кількох тисяч.

Корпоративні підрозділи можуть мати різний масштаб: від невеликого з одним або кількома працівниками до філії університетського містечка, а отже, інтеграція корпоративних підрозділів можлива лише за допомогою зовнішнього телекомунікаційного зв'язку, що не належить підприємству (рис. 1).

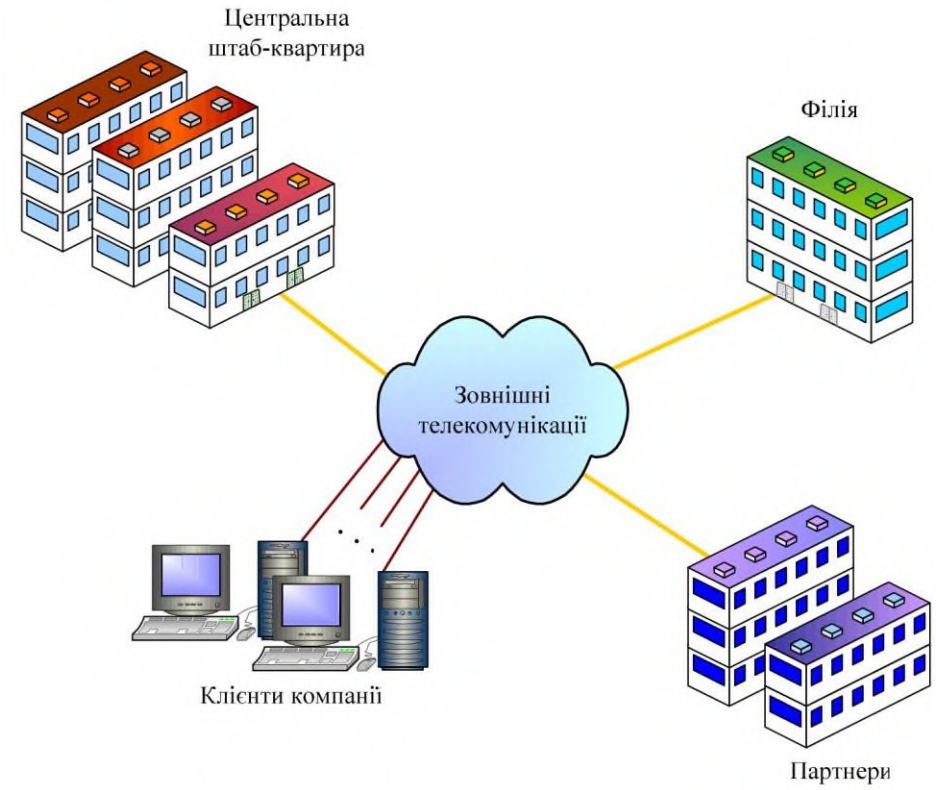


Рисунок 1.1- Корпоративна мережа

Корпоративна мережа може містити не тільки підрозділи певної великої компанії, але і деяку групу користувачів, до якої входять ділові партнери, співробітників компанії та ключові клієнти компанії. У будь-якому випадку, доступ до корпоративної мережі надають лише деякому контингенту користувачів, певній групі людей. До корпоративних мереж входить вся комунікаційну інфраструктура, що забезпечує безпосередньо взаємодію між користувачами: різні види термінальних пристроїв, кабельні комунікації в офісах,

глобальні системи на основі ресурсів мережних операторів та функціональні засоби керування мережею.

Банківські установи використовуються в цьому дослідження тому, що вони включають географічно розподілену інфраструктуру, об’єкти обслуговування якої поєднуються із використанням ККМ. В даний час, щоб розширити зону покриття та спростити введення в експлуатацію нових філій, ККМ будуються з широким використанням Інтернету та інших відкритих мереж.

В даний час внутрішні мережі компаній, зазвичай не ізольовані від зовнішнього оточення. Ділове листування, використання Інтернету, обмін миттєвими повідомленнями - це види комунікації співробітників. Сама компанія може мати декілька офісів, розташованих по місту, країні чи світі, а її співробітники можуть працювати віддалено вдома, так і у відрядженнях. В епоху інтенсивного обміну інформацією та стрімкого розвитку інформаційних технологій вся множина елементів мережі компанії - її сервери, мобільні комп’ютери, вебресурси та бази даних - є потенційними об’єктами зловмисників, і всі вони потенційно вразливі.

Побудова корпоративної системи захисту інформації розпочинається із забезпечення всебічного захисту кінцевих точок від шкідливого програмного забезпечення, мережних атак, несанкціонованого доступу та крадіжки даних. Архітектура сучасних загроз ІС вимагає багаторівневого підходу до побудови систем захисту. Актуальність та складність захисту кінцевих пристроїв посилюється тим фактом, що вони все частіше обираються в якості основних цілей зловмисників.

Ланцюжок атак може починатися з різних способів доставки: електронною поштою, через Інтернет або через загрозливий застосунок, USB-пристрої. Під час зараження шкідливе ПЗ намагається поширитися в поперечному напрямку, а іноді викликає командний центр для одержання керівної інформації про подальші дії: передачу конфіденційної інформації на зовнішні ресурси, шифрування, тощо.

Щоб охопити ланцюг ініціалізації загроз, необхідно використовувати різні технології, методи виявлення та захисту - якщо атака перенесе одну технологію,

вступить в дію інша. На етапі доставки відповідальність покладається на такі системи, як аналіз репутації файлів, захист браузера та фільтрація URL-адрес, локальний брандмауер, управління пристроями та контроль програм. Блокування відомих та невідомих вразливостей для виправлення експлойтів в операційних системах та застосунках - захищає від зараження та поширення по мережі [33]. Це захищає застарілі операційні системи, які не мають і не можуть мати жодних оновлень. Технології машинного навчання аналізують шкідливе програмне забезпечення як до, так і після запуску файлу. Крім того, на цьому кроці активується захист від використання експлойтів в оперативній пам'яті. Вимоглива технологія виявлення програм працює окремо і блокує шифрування файлів користувача. На останньому кроці аналіз репутації командних центрів знову вступає в силу і відстежується діяльність мережі.

Впроваджуючи сучасні застосунки для ефективного захисту робочих станцій та серверів, насамперед необхідно звертати увагу на їх властивість запобігати зараженню на кожному кроці. Крім того, крім безпосереднього виявлення поточних загроз, Endpoint Protection повинен відповідати таким вимогам, як низьке навантаження кінцевої точки та простота керування [17].

Канали зв'язку - доступніші зловмисникам елементи інформаційної інфраструктури в силу великої протяжності та фізичного розташування. Останнім часом, коли все більше і більше в якості каналів зв'язку використовується мережа Інтернет та бездротові засоби зв'язку, ситуація із загрозою доступності інформації стала ще більше небезпечною. За дослідженням для здійснення найпоширеніших атак, спрямованих на введення об'єктів ККМ у ситуацію DDoS зараз потрібен мінімальний поріг знань і повноважень. Ситуація загострилася через широке поширення Інтернет-банкінгу, яке надає кінцевому споживчому банківському продукту доступ до внутрішніх інформаційних ресурсів банківських установ. Ця послуга провокує до спроби несанкціонованого доступу до інших інформаційних ресурсів банку [27].

Корпоративна мережа банку - це окремий випадок корпоративної мережі великої компанії. Специфіка банківської сфери висуває жорсткі вимоги до систем

захисту інформації в інфраструктурі банку [7]. Не менш важливу роль у побудові корпоративної мережі банку відіграє необхідність забезпечити доступність і безперебійну роботу, оскільки навіть короткочасна відмова в її роботі може призвести до величезних втрат. Також вам потрібно забезпечити швидку та надійну передачу великих обсягів даних, оскільки багато банківських додатків повинні працювати у режимі реального часу. Виділяють такі основні вимоги до корпоративної банківської мережі:

- Мережа інтегрує у структуровану та керовану закриту систему всі інформаційні пристрої, що належать компанії: окремі комп'ютери та локальні мережі (LAN), робочі станції, хост-сервери, телефони, факси, офісні АТС, Інтернет-термінали, мережі банкоматів,

- Мережа забезпечує надійність її роботи та потужні системи захисту інформації. Тобто безперебійна робота системи гарантується як у разі помилок персоналу, так і в разі спроби несанкціонованого доступу.

- Існує налагоджена система комунікації між філіями банків різного рівня (як з міськими філіями, так і з міжміськими філіями).

Завдяки сучасним тенденціям розвитку банківських послуг (наприклад, телефонна послуга, цілодобовий доступ до банкоматів та Інтернет-терміналів, розвиток мереж швидкісних платіжних терміналів у торгових центрах, цілодобові операції з акціями клієнтів) необхідні особливі телекомунікаційні рішення для банків. Організація швидкого, надійного та безпечного доступу віддаленого клієнта до необхілних банківських послуг набуває значної ролі.

Щодо питання найкращої архітектури банківської мережі, можна зазначити, що найпоширенішою в європейських країнах і актуальною сьогодні для вітчизняних банків є «зіркова» топологія, проста або багаторівнева, головний офіс якої знаходиться в центрі і зв'язаний з регіональними відділеннями. Переважними факторами цієї топології є:

- Структура банківських організацій. (Наявність регіональних відділень та велика кількість інформації, що передається між ними.)

- Велика вартість оренди каналів зв'язку. Слід мати на увазі, що зазвичай при організації комунікації з віддаленими офісами не використовують комутовані телефонні канали зв'язку. Для цього потрібні високошвидкісні та надійні лінії зв'язку.

У Східній Європі та СНД є додатковий фактор на користь використання "зіркової" топології - недостатньо розвинена телекомунікаційна інфраструктура та пов'язані з цим труднощі з отриманням великої кількості каналів зв'язку. В цих умовах особливо важливо впроваджувати економічні рішення, що існують на світовому ринку, а іноді спеціально модифіковані відповідно до умов країн, що розвиваються [16].

У загальному випадку, коли існує потреба безпосередньо пов’язати регіональні відділення, актуальною стає індивідуальна топологія. По суті, ця топологія характеризується підвищеною надійністю та відсутністю перевантажень. На практиці можна використовувати численні змішані топології, як у випадку з «децентралізованим головним офісом», коли різні відділи центрального апарату банку - розрахунковий, кредитний, аналітичний, технічний чи будь-який інший - розташовані в різних будівлях.

У деяких європейських країнах реалізовані загальнонаціональні конфігурації, де корпоративні мережі окремих банків утворюють "суперзірку" з міжбанківським розрахунковим центром як вершиною ієрархії банківських телекомунікацій. Ці питання безпосередньо пов'язані з вибором системи міжбанківських розрахунків і будуть розглянуті нижче.

Коротко розглянемо рішення RAD Data Communications, безпосередньо орієнтоване на європейський ринок.

Дані, голос (телефонні розмови), відеоінформація та факси передаються по одному та тому ж каналу, що забезпечує багаторазове зменшення вартості оренди каналів або їх прокладання. Тут важливу роль приділяється на мережі банкоматів.

Технічно це робиться засобами мультиплексування, інтегрованої передачі та подальшого демультиплексування окремих потоків інформації. Різні види мультиплексорів дозволяють інтегрувати потоки інформації різного розміру, що

надходять як від невеликих віддалених офісів, так і від великих регіональних. У конкретних застосунках можна використовувати додаткові вбудовані механізми мультиплексорів, які збільшують ефективність смуги пропускання каналу зв'язку. Мультиплексори з опцією конфігурації день / ніч працюють з урахуванням різниці у властивостях денного та нічного трафіку (більше голосових каналів - вдень, а каналів даних - вночі). Адаптивні мультиплексори виділяють всю смугу голосового каналу для передачі даних, якщо немає голосового трафіку. Крім того, завдяки спеціальній технології придушення тиші, інші потоки даних, голос, факси та трафік локальної мережі передаються під час пауз у телефонних розмовах.

В результаті використання інтегрованої передачі, отримується істотна економія у використанні каналів зв'язку - найдорожчого ресурсу мережі.

Використання інтегрованої передачі інформаційних потоків безпосередньо дозволяє забезпечити всі робочі місця повним спектром інформаційних послуг за розумну ціну для їх підтримки. Крім того, телефонні розмови серед регіональних відділень перетворюються на внутрішньофірмові, які забезпечують кращий контроль та безпеку.

1.2 Аналіз загроз інформаційній безпеці, які впливають на функціонування мережі

Для забезпечення захисту комп’ютерних мереж спочатку необхідно провести систематичний аналіз можливих загроз безпеці мережі. Загрози характеризують можливі дії, які можуть бути здійснені щодо системи. Вони мають прояви в різних формах, але найпоширенішими є такі [8]:

- випадково: особа, яка не знайома з відповідними правилами та політикою або через неналежний догляд, створює випадковий ризик;

- несанкціоновані зміни: оновлення, виправлення та інші зміни в операційних системах, програмних додатках, конфігураціях, сумісності та обладнанні можуть становити несподівану загрозу безпеці систем промислової автоматизації та управління або відповідного промислового процесу.

Фактор загрози - це термін, що використовується для опису суб'єкта господарювання, який є загрозою. Загрозами можуть бути як зловмисники, так і порушники. Прикладами таких факторів є [8]:

- інсайдер: довірена особа, працівник, підрядник або постачальник, який має інформацію, яка загалом не відома громадськості. Інсайдер може становити загрозу навіть без зловмисних намірів;

- сторонній: особа або група осіб, які не мають права внутрішнього доступу. Для того, щоб визначити загальні тенденції змін у безпеці мережі, ми проведемо дослідження корпоративної мережі із загальними характеристиками.

Розглянемо перелік можливих атак, реалізація яких призведе до негативних наслідків мережі [12].

1. Scan Attacks - пошук можливих системних вразливостей:

1) Сніфери пакетів - перехоплення та аналіз трафіку;

2) Розгортки пінгу - пошук IP-адрес запущених комп'ютерів;

3) Сканер портів - сканування відкритих портів TCP та UDP;

4) Фішинг - метод отримання необхідної інформації від користувачів комп'ютерної мережі.

2. Веб-атаки:

1) Міжсайтові сценарії (XSS) - зловмисний збір інформації про користувача на сторінках веб-програми;

2) SQL Injection - один із поширених методів зламу сайтів та застосунків, що працюють з базами даних, заснований на реалізації довільного SQL-коду в запиті;

3) Обхід шляху - обробка зловмисником HTTP-запитів з метою обходу елементів керування доступом та переходу до інших каталогів та файлів у системі.

3. Спуфінг - заміна довіреної особи:

1) IP- спуфінг - використання чужої IP-адреси відправника з метою обходу системи безпеки;

2) DNS-спуфінг - підміна даних кешу доменних імен для призначення помилкової IP-адреси;

3) DHCP-спуфінг - заміна шлюзу за замовчуванням.

4. Атаки, спрямовані на одержання доступу до системи:

1) Парольні таки - злом пароля;

2) Trust Exploitation - компрометація надійного хоста, використання його для нападу на інших хостів у мережі;

3) атака "людина посередині" - компрометація каналу зв'язку, при якій зловмисник втручається в протокол передачі даних, видаляючи або підмінюючи інформацію.

5. Викрадення сесії - використання поточного комп'ютерного сеансу для одержання несанкціонованого доступу до послуг або інформації у комп'ютерній мережі.

6. Атака компрометованого ключа – безпосереднє перехоплення секретного ключа.

7. Спам - зловживання функціональністю електронної пошти.

8. Атака відмови в обслуговуванні (DoS) - лавиноподібна маршрутизації пакетів, що викликає перевантаження мережі і робить її недоступною.

9. Шкідливе програмне забезпечення (троянські програми, хробаки, віруси, ботнет тощо) - направлене на втручання в мережу, збір конфіденційної інформації або одержання доступу до приватних комп’ютерних систем і мереж.

10. Фізичний вплив зловмисника на мережу - призводить до руйнування або виходу з ладу фізичних компонентів, таких як апаратне забезпечення, роз’єми, датчики, контролери, пристрої зберігання програмного забезпечення,.

11. Розкриття інформації - навмисні або необережні дії користувача, внаслідок яких користувач, який не має доступу до цієї інформації, знайомиться з нею.

12. Необережні дії, помилки користувачів мережі - включають дії користувача, які здійснюються випадково, через незнання, необережність чи недбалість, з цікавості, але без зловмисних намірів.

13. Природні явища та техногенні явища (аварії, урагани, пожежі, землетруси, тощо).

Як при розробці комп’ютерної мережі, так і при формуванні політики

мережевої безпеки можна моделювати процес атаки, змінюючи значення впливу досліджуваних концепцій на систему, з метою оцінки результатів їх можливої реалізації.

Більшість атак на рівні мережі включають використання IP: заміна IP-адреси хоста, накладання неправильного маршруту, перехоплення інтервалу IP-адрес зловмисника та отримання інформації про логічну структуру мережі (IP-адреси хоста, імена доменів), один- проблеми з ідентифікацією часу IP.

Можна виділити наступні підходи до захисту від цих атак:

- формування прив'язок портів IP-MAC для запобігання заміні IP-адрес та несанкціонованому підключенню до мережі (основні підходи реалізовані на рівні каналу та були розглянуті в попередній статті циклу [1]),
- використання технології перекладу мережевих адрес (Network Address Translation - NAT [22]), щоб приховати від зовнішніх зловмисників діапазон IP-адрес організації та логічну структуру мережі,
- формування списків контролю доступу [21] для обмеження доступу до вузлів та протоколів / служб рівня додатків.

Протокол NAT застосовується для передачі пакетів з IP-адрес, призначених лише для внутрішнього використання, у зовнішні мережі та для вирішення проблеми приховування внутрішньої логічної архітектури мережі від зовнішніх мереж [43]. NAT надсилає лише той трафік, який відбувається між внутрішньою та зовнішньою мережею і призначений для передачі. Будь-який трафік, який не відповідає характеристикам передачі або який проходить між іншими інтерфейсами маршрутизатора, ніколи не транслюється та не пересилається через маршрутизацію. Слід зазначити, що протокол NAT лише перекладає адреси і не виконує функції фільтрації. Необхідно використовувати відповідні списки доступу, щоб запобігти передачі пакетів із зовнішніх у внутрішні мережі.

Відкритий характер протоколів прикладного рівня створює ряд загроз для основної проблеми цих протоколів - передачі інформації в незашифрованому вигляді. Використання програмних процедур ідентифікації та автентифікації з подальшою авторизацією також створює загрозу перехоплення або вибору

облікових записів та паролів. Віруси та шпигунські програми, що працюють на рівні застосунків DoS та DDoS атаки на інформаційні системи також становлять значну небезпеку.

Зазвичай, говорячи про засоби захисту на рівні застосунків, розглядаються два підходи: використання проксі-серверів [16] та використання механізмів управління сеансами (Statefull Inspection), основи яких обговорювались вище. Обидва ці підходи контролюють з'єднання, але не вирішують проблему аналізу вмісту пакетів та їх фільтрації з небажаним вмістом, що не перешкоджає поширенню вірусів електронною поштою, встановленню несанкціонованого ПЗ через Інтернет на робочих станціях, несанкціонованих змін вміст вебресурсу. Для захисту від таких порушень може використовуватися фільтрація вмісту, яка базується на аналізі підписів пакетів [13]. Цей механізм включає аналіз інформації в пакеті як за допомогою заголовка пакету, так і поля даних. Це дозволяє узгоджувати інформацію в полі даних та певних програмах, контролювати передачу даних між цими програмами та фільтрувати небажану інформацію. Через те, що інформація аналізується в групах, цей механізм не дозволяє повністю проаналізувати трафік мережних застосунків.

Можливість здійснювати ці атаки з віртуальної мережі значно обмежує використання традиційних методів захисту комп’ютерних мереж і вимагає розробки спеціалізованих рішень. Такі рішення можуть базуватися на вищезгаданих механізмах державної інспекції та механізмів фільтрації пакетів. Таким чином, [24] пропонує підхід до обмеження доступу, заснований на контролі віртуальних з'єднань та безпосередньому використанні прихованої фільтрації. Правила фільтрації можуть бути сформовані для різних рівнів опису потоку даних на основі заголовків каналів, мережі та застосунків.

Таким чином, враховуючи велику кількість та різноманітність протоколів на рівні додатків та програмних додатків, можна організувати ефективну протидію загрозам рівня застосунків, лише розробляючи та впроваджуючи комплексні системи інформаційної безпеки з використанням спеціалізованих механізмів

обмеження та контролю доступу до мережі, фізичний захист та електронні цифрові підписи.

1.3 Оцінка ефективності функціонування мережі та її захищеності

Інформаційна безпека оцінюється з початку інформаційних технологій. На цю тему існує багато робіт, але найбільш актуальними та фундаментальними роботами є нормативні документи, які внесли значний теоретичний та практичний внесок у вирішення проблем інформаційної безпеки, а саме: "Помаранчева книга" [24], яка викладає та систематизує критерії. оцінки захисту комп'ютерних систем; Європейські характеристики оцінки безпеки інформаційних технологій [13] з урахуванням усіх недоліків та обмежень, викладених у «Помаранчевій книзі»; Федеральні критерії США, спрямовані на усунення обмежень, незручностей практичного застосування та недоліків "помаранчевої книги"; Канадські критерії оцінки безпеки комп'ютерних систем [14]; Міжнародний стандарт IS0 / IEC 15408 - "Стандарти оцінки безпеки інформаційних технологій" [16]; Стандарт CEM-97/017 - "Загальна критерії оцінки безпеки інформаційних технологій" [19].

Розглянуті нормативні документи покладено в основу єдиної міжнародної науково-методичної бази для вирішення проблем інформаційної безпеки в інформаційних системах, ресурсах, та технологіях. Для вирішення проблем інформаційної безпеки поряд із формальними методами моделювання процесів та оцінки ефективності систем потрібно використовувати методи декомпозиції та структурування компонентів систем і процесів, неформальні критерії та методи оцінки ефективності операцій та прийняття рішень.

Як правило, для оцінки рівня захисту спочатку необхідно визначити поточний стан інформаційної безпеки. Сьогодні існує два різних підходи до оцінки стану інформаційної безпеки, а саме "дослідження знизу вгору" та навпаки, "дослідження зверху вниз".

Використовуючи перший підхід, адміністратори починають самі перевіряти систему безпеки на всі відомі типи атак. Таким чином, адміністратори виступають

як зловмисники, які намагаються зламати захист інформаційних ресурсів. Але відразу стає зрозуміло, що найкращі адміністратори не можуть знати всіх можливих методів злому, а також усього програмного та апаратного забезпечення хакерів.

Підхід зверху вниз ґрунтується на детальному аналізі всіх відомих схем зберігання та обробки даних. Спочатку визначаються інформаційні ресурси та потоки захисту, а потім досліджується сучасний стан систем захисту інформації з метою визначення впроваджених методів захисту інформаційних ресурсів, а також їх стану та рівня. Потім усі інформаційні ресурси та потоки захисту класифікуються за рівнями відповідно до вимог щодо конфіденційності, доступності та цілісності.

Останнім етапом є "оцінка ризику", яка полягає у визначенні розміру збитків організаці через порушення захисту кожного конкретного інформаційного ресурсу. Приблизний ризик є результатом "можливого збитку від атаки" на "імовірність цього нападу". Як правило, в оцінка ризику входить аналіз ризику та оцінка збитків.

Наступним кроком в аналізі ризиків є складання списку переважних загроз та переліку вразливих місць для них кожного інформаційного ресурсу, а потім обчислення ймовірності можливих загроз або атак. Згідно зі стандартом [23], загрози інформаційної безпеки мають подвійне тлумачення, наприклад: умова реалізації вразливості ресурсу (в даному випадку вразливості та загрози ідентифікуються окремо); загальна потенційна подія, яка може призвести до несанкціонованої спроби доступу до інформаційного ресурсу (коли можливість усвідомлення вразливості є загрозою).

Оцініть ризик, обчисливши його та порівнявши із заданою шкалою. Розмір ризику розраховується шляхом множення ймовірності несанкціонованого доступу до інформації або ресурсів на величину збитків компанії від цього. Встановлена величина ризику дозволяє визначити важливість для компанії кожного інформаційного ресурсу.

За п'ятибальною шкалою рівні оцінювання ідентифікованого ресурсу

виглядають як: “незначний”, “малий”, “середній”, “високий”, “дуже високий”. За трибальною шкалою - як “малий”, “середній”, “високий”.

Загальні критерії оцінки безпеки повинні розроблятися на єдиній загальній методологічній основі, заснованій на синтезі заходів безпеки, інструментів та послуг для мінімізації інформаційних ризиків. Експерти, розробники та замовники застосовують загальну методологію оцінки інформаційної безпеки для контролю безпеки інформаційних ресурсів [9].

Відповідно до загальної методів оцінки інформаційної безпеки вона повинна проводитися у три кроки: підготовчий, базовий, заключний.

На підготовчому етапі головними дійовими особами є замовник оцінки інформаційної безпеки та експерт. Замовник повідомляє всі сторони про необхідність оцінки профілю захисту, надає експерту всю необхідну документацію, матеріали щодо об'єкту оцінки. Головне завдання експерта - визначити можливість проведення успішної оцінки на підставі отриманих матеріалів, а при необхідності додатково вимагати допоміжні матеріали у замовника або розробника. Підсумком підготовчого етапу є укладення договору між замовником та експертом на виконання робіт з оцінки об'єкта або профілю захисту.

Підсумком основного етапу є розробка та подання експертом звіту про технічну оцінку, який містить причини рішення. На основному етапі експерт вивчає отримані матеріали, профіль захисту або об’єкт оцінки. Експерт готує комплект звітів з вимогами для надання пояснень щодо вимог контролюючого органу, виявлених недоліків чи недбалості та іншої інформації про хід оцінки. Контролюючий орган постійно керує процесом оцінювання відповідно до схеми оцінки.

На завершальному етапі проводиться поглиблений аналіз звіту про технічну оцінку інспекційним органом на предмет його відповідності загальним критеріям, методам та вимогам схем оцінки безпеки. На підставі технічного звіту складається остаточний звіт про оцінку з рішенням про відповідність необхідним поставленим

вимогам. Усі сторони, які беруть участь у процесі формування оцінки, переглядають остаточний звіт і мають можливість вимагати відповідних пояснень.

Фактично рівень захисту визначається як співвідношення ризиків в захищеній системі до ризиків у системі, яка не має захисту. Цей підхід дозволяє детальніше описати інформаційні ресурси через властиві їм вразливості, ціну самих ресурсів, ранжувати ризики і інформаційні ресурси відповідно до ступеня критичності їх загроз для організації.

Для проведення оцінки безпеки ми пропонуємо такі кроки:

- на першому кроці скласти перелік загроз з позицій інформаційної безпеки, визначити ймовірність загроз та ймовірність їх відображення системою захисту, вартості інформаційних ресурсів;

- на другому етапі вводяться обмеження щодо вартості побудови системи захисту інформації та щодо зниження рівня продуктивності комп'ютерної інформаційної системи;

- на третьому етапі проводиться оцінка за загальними математичними формулами рівня захисту комп'ютерної інформаційної системи запропонованими засобами;

- На четвертому етапі з розглянутих та оцінених варіантів обирається найкращий по відповідним критеріям, що відповідає вимогам і не виходить за встановлені рамки.

Властивості характеристик індивідуальні для кожної організації, яка використовує та не підлягає регулюванню державними регуляторами, оцінка ефективності з використанням інформаційно-орієнтованого підходу в даний час не використовується широко, але є перспективною для вивчення та використання великими підприємствами.

На рис. 1.3 зображено блок схему процесу формування оцінки захищеності комп'ютерної системи.

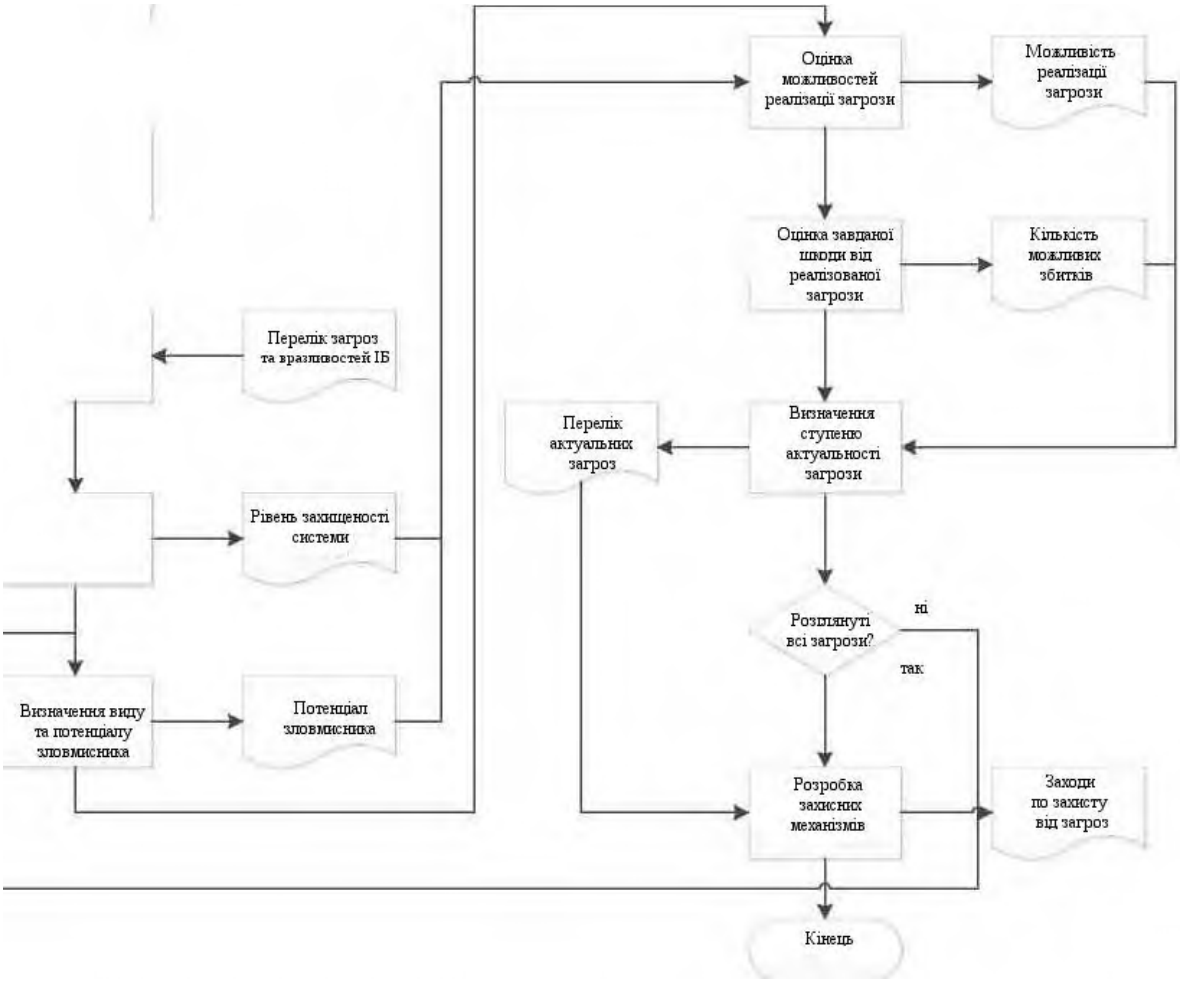


Рисунок 1.2 – Алгоритм процесу оцінки захищеності

Оскільки робота згідно з цим алгоритмом передбачає процес, описаний циклом Демінга-Шухарта, то в кінці роботи над введенням захисних механізмів проводяться повторні, а потім періодичні оцінки [32]. Очевидні недоліки цього процесу включають значну складність процесу регулярної періодичної переоцінки впливу загроз. Ця необхідність пов’язана з тим, що характер впливу загроз ІС змінюється досить динамічно, і для ефективної оцінки необхідно врахувати всі зміни, як у списках загроз, так і в поточній ситуації в галузі. На момент написання статті ми не знаємо про програмне забезпечення, яке дозволяє автоматизувати процес оцінки цим методом.

Завдання оцінки ефективності ІКС можна розглядати як одне із особливих завдань сучасної теорії дослідження операцій. При такому підході завдання оцінки ефективності такої системи можна сформулювати так: при заданих вихідних умовах потрібно визначити систему, що у порівнянні з еталонною є кращою

відносно заданого критерію [5].

Результат оцінки та її практична цінність значною мірою залежать від вибору критерію та системи показників якості (СПЯ). Поширеним підходом до розробки системи показників якості складних систем є формулювання багатьох локальних СПЯ, що відповідає сукупності властивостей системи, що впливають на виконання її завдань. Глобальний СПЯ, що характеризує спільне, єдине завдання, що стоїть перед інформаційно-комунікаційною системою, реалізується шляхом підключення оригінальних локальних систем показників якості.

Запропоновано метод формування системи показників якості, на відмінну від традиційного, пропонує на основі математичних методів теорії декомпозиції (функціональне та параметричне розкладання, факторизація) розглянути проблему функціонування ІКС загалом. Повнота такої СПЯ базується на тому, що вихідними даними для її формулювання є вимоги, запропоновані користувачем до ІКС, математично правильно розділені в інтересах їх подальшого використання [6].

Локальні системи критеріїв якості нижчого рівня ієрархії конкретизують внутрішні властивості системи, а глобальна СПЯ характеризує зовнішні властивості системи. Розмірність локальної СПЯ значно зменшується методом редукції, заснованим на оцінці ступеня лінійної незалежності критеріїв якості їх чутливості до змінного стану ІКС.

Основними зовнішніми властивостями ІКС є види та рівень інформаційних послуг, що надаються користувачам. Разом із процесом обміну інформацією в системі функціонує процес керування якістю обміну інформацією, структури, алгоритмів та параметрів мережі, який, характеризується сукупністю властивостей (якостей). Елементи системи інфокомунікацій - система обміну інформацією та система керування - мають спеціалізований набір основних внутрішніх властивостей (якостей). Зв'язок між властивостями системи та відповідними критеріями ефективності представлена на рис. 1.3.

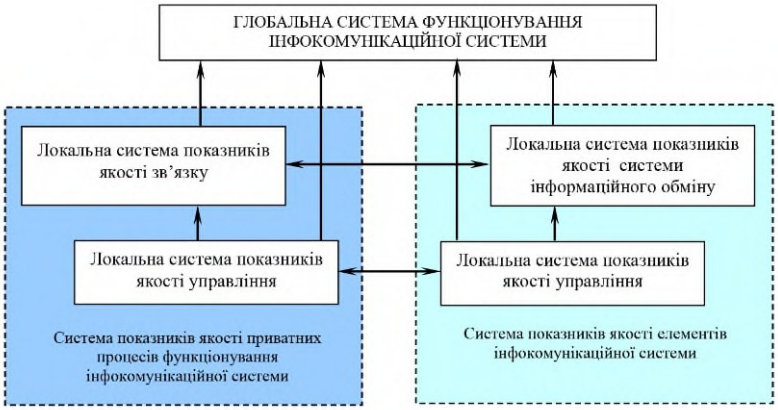


Рисунок 1.3 – Взаємозв'язок систем критеріїв якості в інфокомунікаційній системі

1.4 Фактори, що впливають на ефективність функціонування вузлів мережі під час атак

При аналізі інформаційних ризиків необхідно використовувати моделі системи захисту інформації, засновані на міжнародних стандартах. Розглянемо конкретну модель, побудовану відповідно до даних аналізу ризиків (ISO 17799 "Стандарт для побудови ефективної системи безпеки") та стандарту (ISO 15408 "Загальні параметри оцінки безпеки інформаційних технологій"). Ця модель відповідає спеціальним нормативним актам завдань інформаційної безпеки, прийнятим у нас, ISO / IEC 17799 "Управління інформаційною безпекою", міжнародному стандарту ISO / IEC 15408 "Інформаційні технології - методи захисту, критерії оцінки ІБ", а також враховує вимоги у українських нормативних документів бази даних про ІБ. [42].

Детальний опис загальної мети побудови охоронної системи об'єкта замовника виражається сукупністю чинників або критеріїв, що уточнюють мету. Сукупність чинників є основою для визначення вимог до системи (підбір альтернатив).

Під час оцінки інформаційної системи необхідно визначити її ресурси, та відокремити ці ресурси та зовнішні елементи, з якими відбувається взаємодія.

Ресурсами можуть бути комп’ютери, програмне забезпечення, апаратне забезпечення, дані. Прикладами зовнішніх елементів виступають мережі зв'язку.

Визначення взаємозв’язків між ресурсами є основою побудови загальної моделі інформаційної безпеки організації.

Об'єктивні фактори моделі:

- види загроз інформаційній безпеці підприємства, що характеризуються вірогідністю реалізації;

- вразливості інформаційної системи або система захисту інформації;

- ризик - фактор, який відображає можливу шкоду підприємства в результаті загрози інформаційній безпеці: витік та зловживання інформацією (ризик відображає вірогідні фінансові втрати - прямі чи непрямі).

Принципами побудови збалансованої системи інформаційної безпеки організації є:

- аналіз ризиків у сфері інформаційної безпеки,

- визначення оптимального рівня ризику для компанії на підставі зазначених критеріїв,

- забезпечення таких контрзаходів, які можуть гарантувати досягнення заданого рівня ризику.

Цей підхід дозволяє проаналізувати вимоги до інформаційної безпеки організації. Для досягнення цієї мети потрібно вирішення певних завдань:

- розподіл інформації за певними рівнями доступу;

- прогнозування та виявлення перешкод безпеці інформаційних ресурсів,

- створення умов, для безпеки інформаційних ресурсів;

- створення механізму та умов оперативної відповіді на загрози інформаційній безпеці, забезпечення проведення відновлювальних робіт у стислі терміни;

- створення механізму та засобів для максимально можливої компенсації та локалізації загрози, заподіяної незаконними діями певних фізичних та юридичних осіб;

- забезпечення оптимального вибору можливих контрзаходів;

- провести оцінку ефективності контрзаходів.

На основі побудованої моделі ви можете обґрунтовано вибрати систему контрзаходів, яка може знизити ризики до прийнятних рівнів. Обов’язковим елементом контрзаходів повинна бути регулярна перевірка ефективності системи, перевірка відповідності існуючого режиму захисту інформації політиці безпеки, перевірка відповідності сертифікації інформаційної системи (технології) на її відповідність вимогам певного стандарту безпеки.

У рамках магістерського дослідження розглядаються загрози ІБ, спрямовані на обмеженні доступності інформації в ККМ, таким чином, із наведеного переліку розглядаються загрози ІБ, які відповідають наступним критеріям:

1. Загроза спрямована на порушення доступності інформації.

2. Об'єктом загрози є вузли зв'язку, їх компоненти та телекомунікаційне обладнання, яке розташоване на вузлах зв'язку досліджуваного ККМ.

3. Загроза ІБ реалізується в рамках інфраструктури, що використовується в ККМ.

Атака на відмову в обслуговуванні (DoS (Denial-of-service) attack), розподілена атака, (DDoS attack, (Distributed)) — атака на комп'ютерну систему з метою зробити комп'ютерні ресурси певний час недоступними користувачам, для яких розроблена система була призначена [19].

Одним з найпоширеніших методів атаки є насичення атакованого комп’ютера або мережевого обладнання великою кількістю зовнішніх звернень (часто безглуздих або некоректно сформульованих), щоб атаковане обладнання не могло реагувати на користувачів або реагувати настільки повільно, що стає практично недоступним

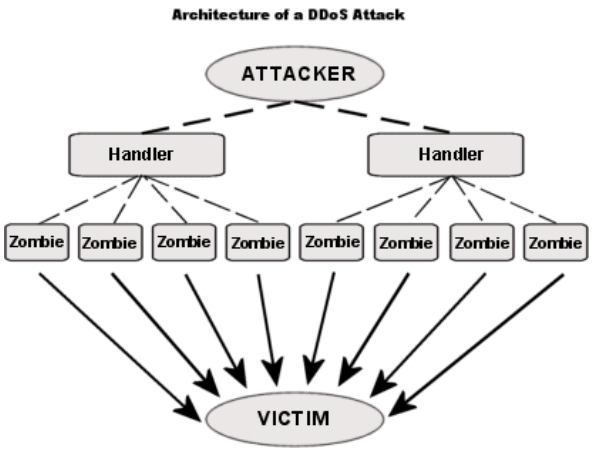


Рисунок 1.4 – Механізм здійснення атак типу «відмова в обслуговуванні»

Взагалі відмова в обслуговувані здійснюється:

- примусом атакованого устаткування до припинення роботи програмного забезпечення/устаткування або до можливих витрат наявних ресурсів, внаслідок чого прилади не можуть продовжувати роботу;
- заняттям комунікаційних каналів зв’язку між користувачами і атакованим устаткуванням, внаслідок чого якість зв’язку перестає відповідати вимогам

Загроза полягає у можливості відмовити дискредитованій системі у доступі законним користувачам із лавиною мережевих підключень до системи [28]. Ця загроза зумовлена тим, що система споживає частину своїх ресурсів для обробки кожного мережевого запиту, а також слабкими сторонами мережевих технологій, пов'язаними з обмеженою швидкістю обробки потоків мережних запитів, та відсутністю заходів контролю для управління з'єднаннями. Ключовим фактором успіху цієї загрози є кількість запитів, які порушник може надіслати за одиницю часу: чим більша ця кількість, тим більша імовірність успішної реалізації цієї загрози для системи дискредитації

Загроза порушення технологічного виробничого процесу через тимчасові затримки, внесені засобом захисту. Ця загроза пов'язана з тим, що кожен з пристроїв вузла зв'язку при проходженні через нього інформаційного потоку створює затримку і негативно впливає на характеристики сегмента ККМ.

Загрозою є можливість переведення системи в стан DoS або порушення нормального режиму роботи через тимчасові затримки в системах реального часу, що вводяться в передачу та обробку інформації, захищеної захистом інформації, спричиненою необхідність обробки переданої / обробленої інформації. інформація для виявлення та нейтралізації загроз інформаційній безпеці.

Обладнання вузла зв'язку безпосередньо приймає інформацію від передавача, перетворює формати переданої інформації, обробляє мережевий трафік, приймає рішення про напрямок подальшої передачі і тільки тоді передає дані одержувачу. Тому виникають затримки переданої інформації на вузлі зв'язку. Характеристики цих затримок залежить від швидкодії обладнання, обсягу трафіку, що проходить через нього, а також видів операцій, які виконуються з інформацією. Процес обробки мережевого трафіку на вузлі зв'язку зображено на рис. 1.5.

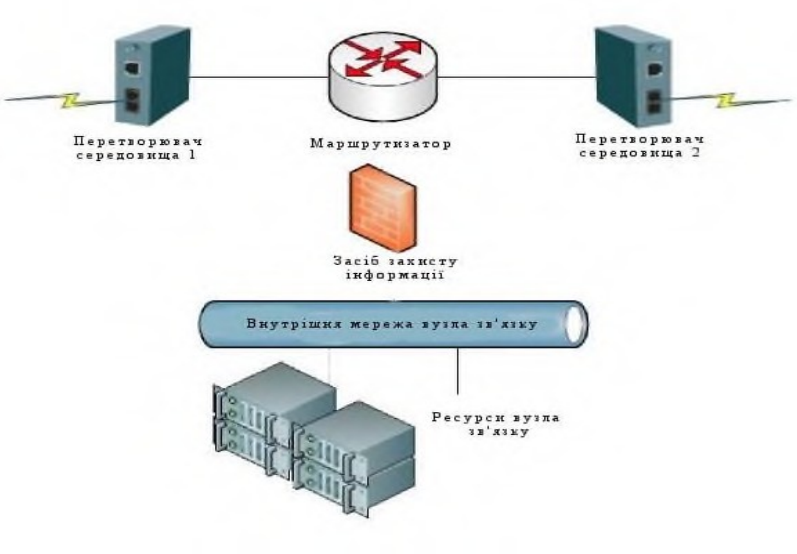


Рисунок 1.5 – Процес обробки мережевого трафіку на вузлі зв'язку

Вузол зв'язку, залежно від розташування може бути транзитним або кінцевим.

Великі виробники мережевого обладнання пропонують спеціалізовані рішення для вирішення задач комплексного захисту корпоративних мереж. Прикладом таких рішень є технологія NAC компанії Cisco [16]. Дана технологія дозволяє не тільки перевіряти пристрої та користувачів ще на етапі підключення до корпоративної мережі, а і заблокувати доступ комп’ютерів, які не відповідають

політиці безпеки (в тому числі заражених вірусами та шкідливими програмами, де не оновлено антивірусні бази, відсутні необхідні оновлення операційної системи тощо). Контроль відповідності політиці безпеки реалізується максимально близько до можливого джерела порушень - на порту комутатора, точки доступу Wi-Fi або маршрутизатора, які підтримують технологію NAC.

1.5 Постановка задачі

У першому розділі розглядаються основні теоретичні положення по проєктуванню корпоративних мереж, організації їх системи захисту, та оцінки ефективності функціонування.

Для формулювання постановки задачі було охарактеризовано ККМ, визначено властивості інформації, на які може бути направлено вплив загроз ІБ. Зі всього спектру загроз увага в цьому досліджені приділено формуванню специфічної для ККМ моделі загроз, що впливають на обмеження доступності інформації.

Сформулюємо основні завдання магістерського дослідження:

1. Проаналізувати актуальні методи дослідження мережі, що дозволяють проводити оцінку захисту від атак, спрямованих на порушення доступності інформації.
2. Довести можливість використання математичного та методологічного апарату теорії надійності як методу мережевих досліджень та коефіцієнта готовності як показника для оцінки ефективності вузлів зв'язку.
3. Розробити математичну модель, яка дозволяє врахувати вплив розподілених атак на систему, що описується графом трьох станів та відповідною системою рівнянь
4. Удосконалити метод дослідження корпоративної мережі, що дозволяє оцінити ефективність функціонування вузла зв'язку в умовах впливу розподілених атак, пов’язаних з доступністю інформації. На підставі отриманих розрахунків і цільового значення коефіцієнту готовності вузлів мережі, можливо прийняти

рішення про необхідність проведення заходів щодо підвищення ефективності функціонування мережі.

5. Розробити підхід до організації внутрішньої топології вузлів зв'язку мережі, що приводить її до форми кільця з вертикальним резервним фронтом, що дозволяє значно збільшити коефіцієнт готовності елементів.

6. Застосувати розроблені методи для оцінки ефективності функціонування вузлів зв'язку існуючої корпоративної мережі

2 МАТЕМАТИЧНА МОДЕЛЬ НАДІЙНОСТІ ВУЗЛА ЗВ'ЯЗКУ ККМ, ЩО ВРАХОВУЄ ВПЛИВ ЗАГРОЗ ІБ

2.1 Розрахунок нормованих показників надійності

Для визначення безпеки ККМ необхідно розробити математичну модель стану вузлів, на основі якої можна передбачити стан всієї мережі. Отже потрібно змоделювати набір станів вузлів досліджуваної системи, та визначити причини переходів між ними, і дослідити ступінь впливу стану на стан мережі в цілому..

Для вирішення цієї проблеми слід вибрати індикатор, за допомогою якого можна ідентифікувати стан досліджуваної ККМ. Виходячи із завдання та особливостей розглянутих загроз ІБ, вибір показника здійснено серед нормованих показників надійності мережі, пов'язаних з доступністю інформації. Вихідні дані про стан вузлів для побудови математичної моделі і можливості прогнозування стану вузлів і мережі в цілому потрібно отримувати експериментально.

З технічної точки зору через вузол ККМ проходить трафік в певному напрямку. В залежності від того чи це активний або пасивний мережевий пристрій, трафік може проходити через елемент ККМ лінійно, або більш складним маршрутом. Таким чином, модель ККМ можна зобразити у вигляді графу. В найпростішому випадку [37] шлях графа буде лінійним.

Надійність - це складна властивість, яка залежно від призначення об’єкта та умов його експлуатації складається з надійності, довговічності, ремонтопридатності, безпеки [22]

Надійність системи можна оцінити:

- аналітично;

- за допомогою імовірнісного моделювання;

- шляхом спільного використання аналітичних методів та методів моделювання при вирішенні однієї проблеми [32].

Розглянемо ці методи більш докладно. При оцінці надійності системи аналітичними методами результати рішення отримуються у вигляді виразів, які пов'язують надійність системи з факторами, що їх визначають, і дозволяють не тільки оцінювати показники, але і досліджувати вплив різних факторів. Це перевага аналітичних методів.

Імовірнісне моделювання успішно використовуються для аналізу надійності систем майже необмеженої складності з будь-яким законом розподілу різних випадкових величин. Ці методи дозволяють врахувати велику кількість різних реальних факторів. Результатом методів імовірнісного моделювання є отримана кількісна оцінка, а не математичні залежності, що використовуються при використанні аналітичних методів. Для отримання залежності надійності системи від різних факторів, що впливають на неї, необхідно використовувати багаторазове моделювання системи з певною модифікацією параметрів.

При застосуванні комбінованих методів завдання проектної оцінки надійності складної системи розбивається на декілька підзадач, кожна з яких вирішується методом (аналітичним або моделюючим), який є найбільш ефективним для специфічних особливостей даної конкретної задачі. Як результат, комбіновані методи завжди є більш ефективними, ніж аналітичні або моделюючі методи для вирішення складних проблем. Застосування методів цієї групи вимагає висококваліфікованого дослідника, який повинен добре знати загальну методологію аналізу надійності складних систем та весь арсенал відомих методів оцінки надійності.

Загальноприйнятим методом розрахунку [21] коефіцієнту готовності *Fa* мережі складної топології є метод її послідовного розкладання на набір мереж з лінійною топологією, поки залишкові структури не стануть паралельно-послідовними. Коефіцієнт готовності послідовно з'єднаних пристроїв згідно з теоремою про ймовірності незалежних подій розраховується по формулі (2.1)

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

де, $Fa_{\text{і}} \ldots Fa_n$ послідовно з'єднаних елементів.

Коефіцієнт готовності паралельно з'єднаних вузлів розраховується по формулі (2.2) [28]:

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

де, $Fa \ldots Fa_{\ n} - Fa_n$ паралельно з'єднаних елементів.

Отже, опираючись на (2.1) і (2.2), можна розрахувати характеристики надійності мережі складної топології, розбивши її на сукупність мереж з лінійною топологією, які моделюють шлях між вершинами графа, які є передавачем і кінцевим приймаючим елементом мережевого трафіку.

В результаті дослідження пристроїв ККМ, і збору статистики, можливо визначити кількість їх відмов вузлів та час перебування в працездатному та неробочому стані. Вузли ККМ є відновлюваним об'єктами. На рис. 2.1 зображено графічний стан обладнання, де початковий стан (1) відповідає працездатному режиму об'єкта, кінцевий стан (2) – вузлу, що вийшов з ладу, λ - інтенсивність відмов, μ - інтенсивність відновлень.

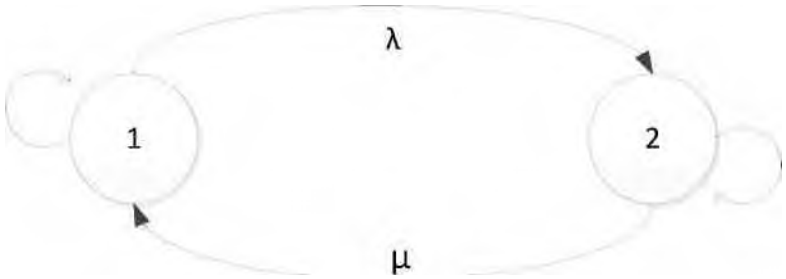


Рисунок 2.1 –Представлення вузла ККМ у вигляді графу стану

Відповідно до [43] інтенсивність потоку відмов буде розрахована по (2.3):

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

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

Δt – інтервал часу.

Nср – середнє число пристроїв, в працездатному стані на інтервалі часу Δt.

Тоді інтенсивність потоку відмов виразимо за формулою (2.4):

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

де N_0 – кількість працездатних вузлів

а (t) – середня імовірність виявлення вузла в неробочому стані.

Середня імовірність виявлення вузла в неробочому стані обчислюється по (2.5):

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

де $n\ (t)$ - кількість неробочих вузлів а інтервалі часу Δt,

$\bar{t}_в$- середній час знаходження вузла в неробочому стані,

N_0 – кількість працездатних вузлів,

Δt - інтервал часу.

Враховуючи, що відмови вузлів є випадковими подіями, достовірно визначити кількість працездатних вузлів неможливо. Тому зпрогнозуємо число працездатних вузлів, $N\ (\Delta t)$ (2.6):

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

де $n\ (\Delta t)$ – неробочі вузли на інтервалі часу,

$\bar{t}_в$- середній час відмови вузла,

N_0 - кількість працездатних вузлів,

Δt - інтервал часу.

Таким чином, середнє число пристроїв, що знаходяться в працездатному стані на заданому інтервалі часу Δt буде визначено по (2.7):

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

Під $\bar{t}_в$ - мається на увазі середній час відновлення вузла, оскільки процес відновлення починається відразу ж після відмови.

Середній час відновлення визначається експериментально, на підставі статистичних даних після спостережень за елементами мережі в певному інтервалі часу.

Для визначення величина $\bar{t}_в$ визначається будується графік апроксимуючої функції, яка описує відповідний закон розподілу Таким чином, $\bar{t}_в$ визначається по формулі (2.8):

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

де *i* - кількість випадків відновлення працездатності пристрою в інтервалі часу,

f (i) - функція розподілу часу відновлення.

Коефіцієнт оперативної готовності - вірогідність того, що об'єкт, перебуваючи у стані очікування, буде працездатним у будь-який момент часу, і, від цього моменту, буде функціонувати безвідмовно протягом заданого періоду часу.

Режим очікування - це стан об'єкта при повному або зменшеному навантаженні без виконання робочих дій. При цьому є вірогідність виникнення відмов, які потрібно усунути до відновлення працездатності певного об'єкта для виконання робочих функцій. Потрібно також врахувати, щоб у разі необхідності об'єкт був обов’язково працездатним.

Показники, що враховують загальну та конкретну загальну складність (вартість) технічного обслуговування та ремонту та є всебічними показниками надійності, включають наступне:

- середня загальна складність технічного обслуговування - математичне сподівання загальних трудових витрат на ремонт за деякий період експлуатації;

- середня загальна трудомісткість ремонту - математичне сподівання сукупних витрат праці на всі види ремонту об’єктів за деякий період експлуатації;

- середні загальні витрати на технічне обслуговування (ремонт) - математичне сподівання загальних витрат на технічне обслуговування об'єкта за деякий період експлуатації.

Для цих показників (разом із їх середніми значеннями) застосовуються специфічні значення, які розраховуються як відношення середніх загальних значень до відповідного математичного сподівання загального часу роботи об'єкта за деякий період експлуатації.

Важливими характеристиками є коефіцієнт відновлення та коефіцієнт відновлення ресурсу.

Показники експлуатаційної технологічності описують витрати на оплату праці, а також вартість підготовки машин до експлуатації, на планове обслуговування під час експлуатації, на роботу після експлуатації.

Час роботи при відмові телекомунікаційного пристрою - тривалість роботи машини до першої поломки. Імовірність безвідмовної роботи в момент часу t в цьому випадку визначається згідно [19] по формулі (2.9):

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

де λ - інтенсивність потоку відмов,

t - момент часу, в який визначається імовірність відмови.

Фізичний зміст миттєвого коефіцієнта готовності є імовірністю перебування пристрою в працездатному стані в розглянутий момент часу, використовуючи(2.9) подамо його як (2.10):

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

Тоді середній коефіцієнт готовності на інтервалі з t_1 до t_2 визначається за формулою (2.11):

$$Fa = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} Fa\,(t)dt, \tag{2.11}$$

Використовуючи (2.10)), середній коефіцієнт готовності на інтервалі з t_1 до t_2 (2.12):

$$Fa = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} e^{-\lambda \times t} \, dt, \tag{2.12}$$

Залежність (2.12) дозволяє розрахувати коефіцієнт готовності вузла мережі на підставі статистичних даних про кількість відмов устаткування і часу його відновлення на обмеженому інтервалі часу.

Однак використання закону експоненціального розподілу для вивчення впливу загроз ІБ, спрямованих на порушення доступності інформації, вимагає додаткового обґрунтування, оскільки неточність даних про аварії (частота та тривалість) не дозволяє зробити однозначний висновок про природу розподіл. Метод обліку впливу загроз ІС на елемент *Fa* СКК розроблений у розділі 3 цього дослідження.

Так як недостовірність даних про загрози (частота їх виникнення і тривалість) не дозволяє зробити однозначний висновок про той чи інший характер розподілу цих загроз. Тому використання експоненціального закону розподілу для впливу на порушення доступності інформації, вимагає додаткового обґрунтування, Метод обліку впливу загроз ІБ на коефіцієнт готовності вузла розроблено в третьому розділі магістерського дослідження.

2.2 Дослідження впливу резервування каналів зв'язку на коефіцієнт готовності

Резервува́ння у техніці —підхід до забезпечення надійності об'єкта за рахунок використання додаткових засобів або можливостей, надлишкових відносно мінімально необхідних для виконання потрібних функцій. Резервування є універсальним принципом підвищення характеристик безвідмовності функціонування, що знайшов широке застосовування безпосередньо у природі, техніці і технології, та й інших сторонах людського життя.

Використання каналів резервування дозволяє забезпечити функціонування ККМ в разі відмов як основних каналів зв'язку, так і проміжних пристроїв через які ці канали проходять.

Оскільки коефіцієнт готовності являє собою імовірнісну величину і його розрахунки спираються на математичну теорію імовірностей, для практичних розрахунків приймаємо [46]:

1. Коефіцієнт готовності вузла є кінцевою величиною і має вплив на зниження загального *Fa* ККМ.

2 Загрози захищеності мережі розглядаються тільки на вузлах зв'язку, оскільки можуть бути спрямовані тільки на активне мережеве обладнання

Проведемо дослідження деяких топологій, інші можна дослідити аналогічно.

Використавши (2.1) і (2.2) Коефіцієнт готовності ККМ, з топологією «кільце» (рис. 2.2) для шляху між вузлами 1 і 3 можна подати як (2.13). Спростивши (2.13), отримаємо (2.14).

$$Fa_{1-3}^{\text{Кільце}} = Fa_1 \times (1 - (1 - Fa_{1-2} \times Fa_2 \times Fa_{2-3}) \times (1 - Fa_{1-4} \times Fa_4 \times Fa_{4-3})) \times Fa_3 = Fa_{\text{у}}^2 \times (1 - (1 - Fa_{\text{р}}^2 \times -Fa_{\text{у}})^2), \quad (2.13)$$

$$Fa_{1-3}^{\text{Кільце}} = Fa_{\text{у}}^2 \times (1 - (1 - Fa_{\text{р}}^2 \times Fa_{\text{у}})^2), \quad (2.14)$$

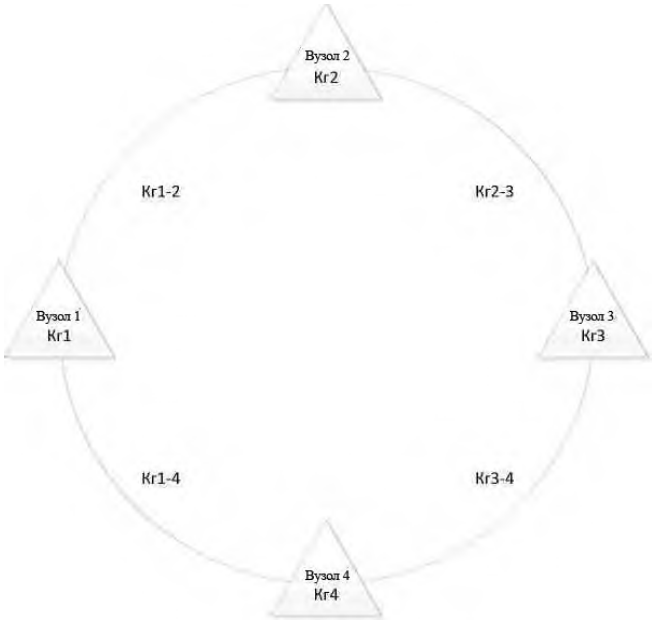


Рисунок 2.2 - Топологія «кільце»

Використавши (2.1) і (2.2) Коефіцієнт готовності ККМ, з топологією «кільце з горизонтальним резервним ребром» (рис. 2.3) для шляху між вузлами 1 і 3 можна записати як (2.14). Спростивши (2.15), отримаємо (2.16).

$$Fa_{1-3}^{\text{К.ГР.}} = Fa_1 \times (1 - (1 - Fa_{1-2} \times Fa_2 \times Fa_{2-3}) \times (1 - Fa_{1-4} \times Fa_4 \times Fa_{4-3}) \times (1 - Fa_{1-3}) \times Fa_3 \quad (2.15)$$

$$Fa_{1-3}^{\text{К.ГР.}} = Fa_{y}^{2} \times (1 - (Fa_{\text{р}}^{2} \times Fa_{\text{у}})^2 \times (1 - Fa_{\text{р}})), \quad (2.16)$$

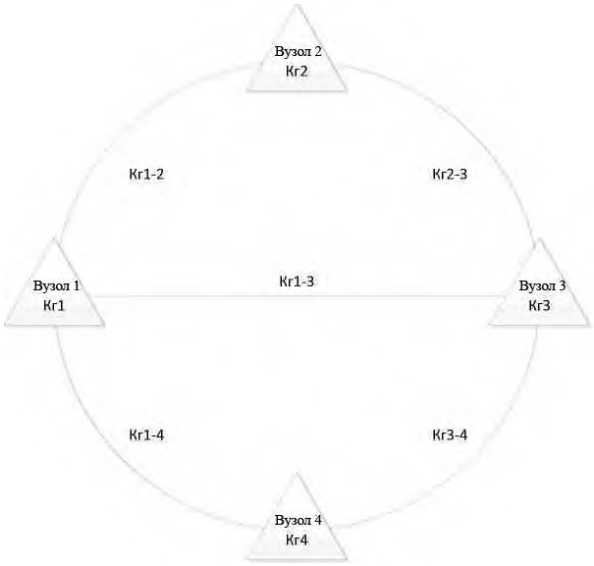


Рисунок 2.3 – Топологія «кільце з горизонтальним резервним ребром»

Використавши (2.1) і (2.2) коефіцієнт готовності ККМ, з топологією «лінійна» (рис. 2.4) можна записати як (2.17). Спростивши (2.17), отримаємо (2.88).

$$Fa_{1-3}^{\text{Л}} = Fa_1 \times Fa_{1-2} \times Fa_2 \times Fa_{2-3} \times Fa_3, \quad (2.17)$$

$$Fa_{1-3}^{\text{Л}} = Fa_{\text{у}}^{3} \times Fa_{\text{р}}^{2}, \quad (2.18)$$

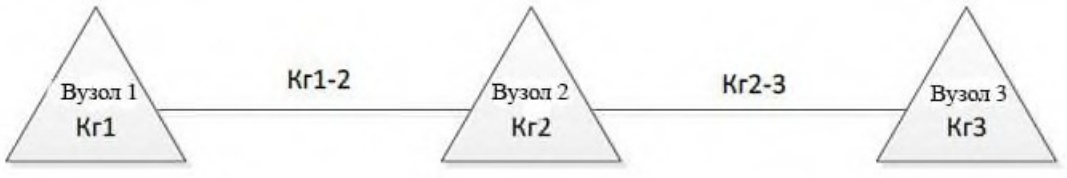


Рисунок 2.4 – Лінійна топологія

Використавши (2.1) і (2.2) коефіцієнт готовності ККМ, з топологією «лінійна з резервним ребром» (рис. 2.5) можна записати як (2.19). Спростивши (2.19), отримаємо (2.20).

$$Fa_{1-3}^{Л+РР} = Fa_1 \times (1 - (1 - Fa_{1-3}) \times (1 - Fa_{1-2} \times Fa_2 \times Fa_{2-3})) \times Fa_3, \quad (2.19)$$

$$Fa_{1-3}^{Л+РР} = Fa_{у}^{2} \times (1 - (1 - Fa_{р}) \times (1 - Fa_{р}^{2} \times Fa_{у})), \quad (2.20)$$

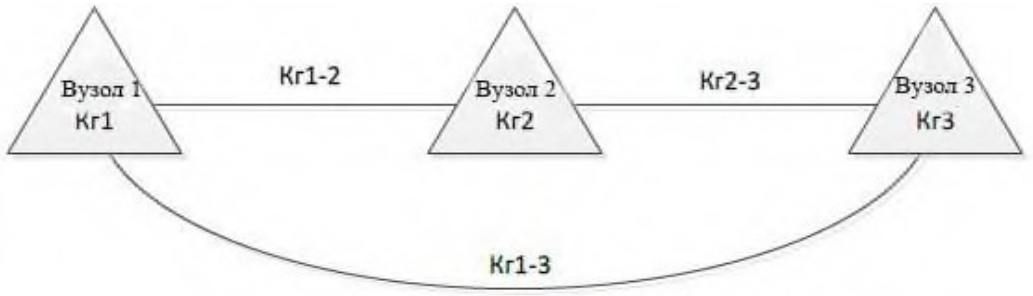


Рисунок 2.5 – Лінійна топологія з резервним ребром

Таким чином, коефіцієнт формалізованої топології ККМ можна уявити як функцію від $Fa_в$ вузла мережі і $Fa_р$ ребра мережі (2.27). Вид функції Fa ККМ буде залежати від її топології та визначатися (2.13) - (2.20).

$$Fa_{ККМ} = f(Fa_р; Fa_в). \quad (2.21)$$

2.3 Підвищення ефективності функціонування мережі за рахунок оптимізації топології

З математичної точки зору ККМ являє собою сукупність двох видів елементів: вузлів зв'язку та каналів зв'язку.

Для аналітичного розрахунку і побудови графіка приймемо коефіцієнт готовності вузла зв'язку ($Fa_в$), що змінюються в діапазоні від 0,99 до 0,9999 з

кроком 0,00099 відповідно до таблиці 2.1. Коефіцієнт готовності ребра мережі ($Fa_р$) приймемо стабілізованою на значенні 0,999. Результати розрахунку занесемо до таблиці 2.1

Таблиця 2.1 - Розрахунок Fa формалізованих топологій в залежності від $Fa_в$

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

Побудуємо графік залежності (рис. 2.5).

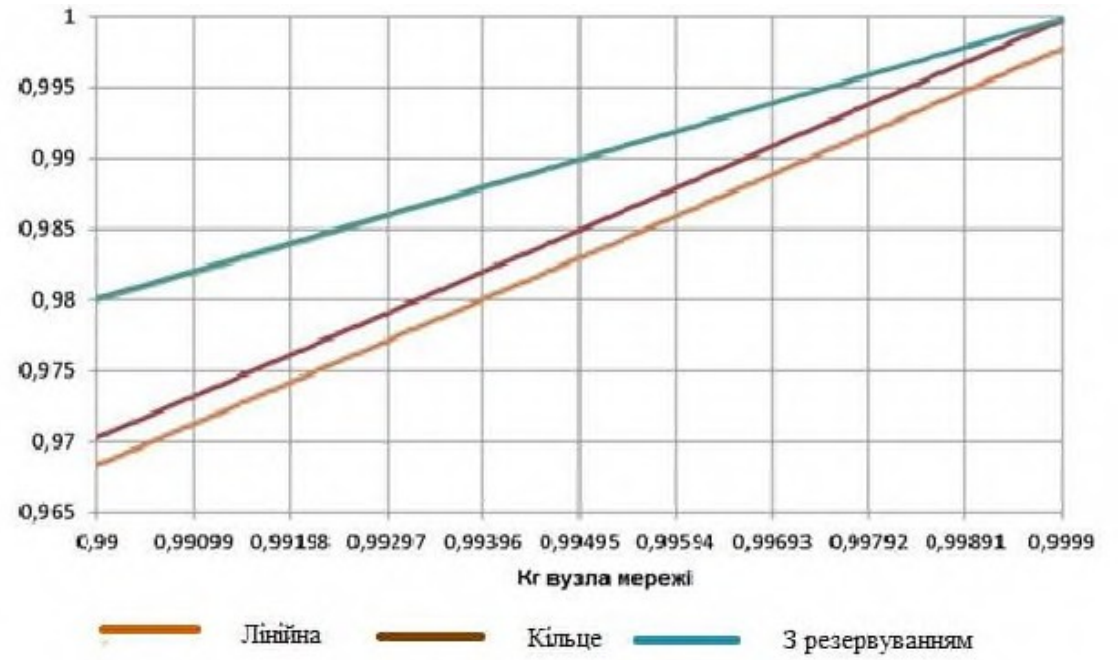


Рисунок 2.5 – Графік залежності коефіцієнту готовності формалізованих топологій в від $Fa_{в}$

Таблиця 2.2 - Розрахунок Fa формалізованих топологій в залежності від $Fa_{р}$

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

Побудуємо графік залежності (рис. 2.6).

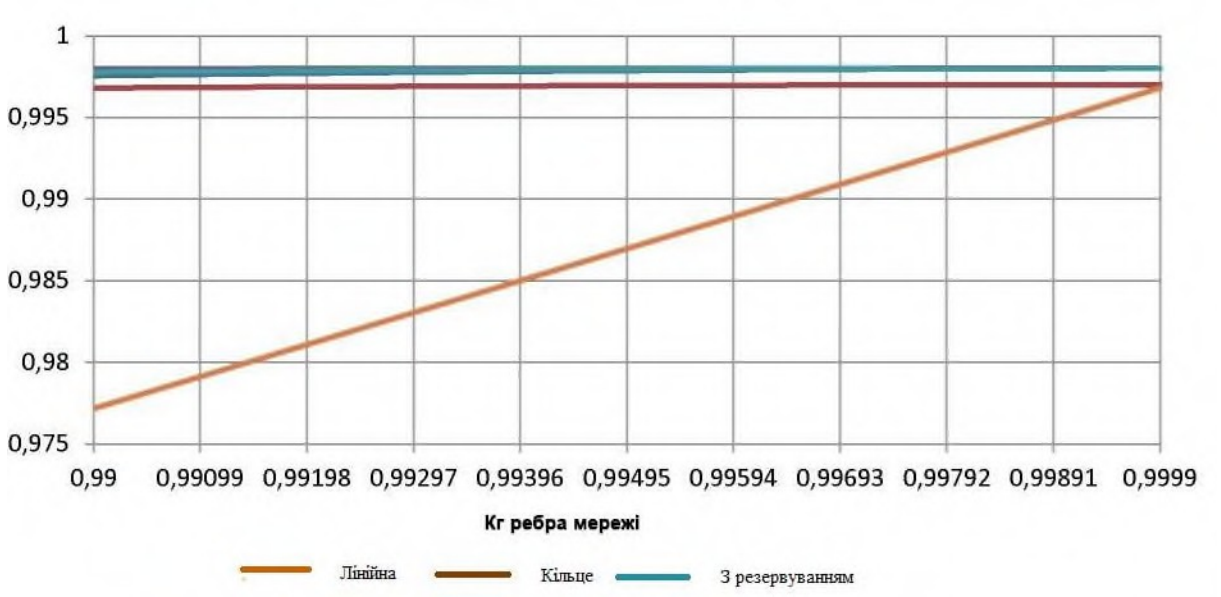


Рисунок 2.6 - Графік залежності коефіцієнту готовності від $Fa_{\text{р}}$

Отримані залежності відображають той факт, що найбільша залежність від $Fa_{\text{р}}$ коефіцієнта готовності є у лінійної топології. (рис. 2.6). Топології з резервуванням показують майже лінійний характер залежності від $Fa_{\text{р}}$. Коефіцієнт готовності з резервуванням в діапазоні мінімальних розглянутих значень $Fa_{\text{р}}$ мережі показує незначну залежність від $Fa_{\text{р}}$, але в той же час в діапазоні максимальних значень $Fa_{\text{р}}$ залежності практично нема.

Проведене дослідження доводить, що на коефіцієнт готовності мережі найбільший вплив має $Fa_{\text{в}}$, на відмінну від $Fa_{\text{р}}$. Отже, ще раз підтверджено актуальність магістерського дослідження, адже для забезпечення високих показників надійності, слід приділяти більшу увагу надійності функціонування вузлів ККМ [33].

2.4 Висновки

У цьому розділі проаналізовано математичного апарату теорії надійності для підрахунок структурної надійності ККМ з різними топологіями. Для визначення безпеки ККМ запропоновано математичну модель стану вузлів, на основі якої можна передбачити стан всієї мережі. Промодельовано набір станів вузлів досліджуваної системи, та визначено причини переходів між ними, і досліджено ступінь впливу стану на стан мережі в цілому.

Виходячи із завдання та особливостей розглянутих загроз ІБ, вибір показника здійснено серед нормованих показників надійності мережі, пов'язаних з доступністю інформації. Вихідні дані про стан вузлів для побудови математичної моделі і можливості прогнозування стану вузлів і мережі в цілому отримано експериментально.

Визначено порядок обчислення коефіцієнтів готовності складних топологій за допомогою методу повного пошуку маршруту. Отримані залежності відображають той факт, що найбільша залежність від $Fa_{\text{р}}$ коефіцієнта готовності є у лінійної топології. (рис. 2.6). Топології з резервуванням показують майже лінійний характер залежності від $Fa_{\text{р}}$. Коефіцієнт готовності з резервуванням в діапазоні мінімальних розглянутих значень $Fa_{\text{р}}$ мережі показує незначну залежність від $Fa_{\text{р}}$, але в той же час в діапазані максимальних значень $Fa_{\text{р}}$ залежності практично нема.

Проведене дослідження доводить, що на коефіцієнт готовності мережі найбільший вплив має $Fa_{\text{в}}$, на відмінну від $Fa_{\text{р}}$. Оскільки вплив загроз доступності інформації спрямований також на вузли зв'язку, питання оцінки та підвищення безпеки вузлів зв'язку є актуальним.

На основі розрахунків зроблено висновок про можливість впливу на коефіцієнт готовності досліджуваних ККМ як за рахунок збільшення компонентів коефіцієнт готовності її вузлів, так і за рахунок оптимізації топології шляхом додавання запасних ребер у різних конфігураціях.

3 ДОСЛІДЖЕННЯ ВПЛИВУ ЗАГРОЗ ІБ НА ХАРАКТЕРИСТИКИ ККМ

3.1 Модель впливу загроз, спрямованих на доступність інформації на коефіцієнт готовності

Як зазначено в розділі 1, загрози захищеності мережі можна поділити на загрози цілісності, конфіденційності та доступності інформації [3].

Найбільше зростання кількості DDoS-атак, на 836% в порівнянні з попереднім, був зафіксований в Україні на ринку онлайн-кас [23]. Атаки йдуть не на самі каси, а на ті сервери, на які вони відправляють дані. Реальне зростання числа атак спостерігається в страхуванні, букмекерських конторах, онлайн-іграх, а також у банків (рис.3.1).

Рисунок 3.1 – Статистика DDoS-атак у 2019 р

Причому DDoS-атака була б неможлива без десятків тисяч зламаних по всьому інтернету пристроїв, які без відома їх власників відправляють по команді

зловмисників безглузді запити на сайт обраної ними жертви. Останнім часом все частіше цими пристроями стають всілякі пристрої інтернету речей (Internet of Things, IoT): IP-камери, онлайн-каси, Wi-Fi-маршрутизатори та ін

Оцінка ефективності функціонування базується на порівнянні коефіцієнту готовності ККМ, розрахованих для різних варіантів, кожен з яких відображає можливий стан вузла зв'язку і обладнання на ньому:

1. Коефіцієнт готовності ККМ розраховується без врахування впливу на захищеність мережі.

2. Коефіцієнт готовності ККМ розраховується з урахуванням впливу, але без використання засобів захисту інформації.

3. Коефіцієнт готовності ККМ розраховується з урахуванням впливу загроз захищеннлсті і ЗЗІ.

Коефіцієнт готовності є характеристикою кожного елементу. Також визначено, що трафік проходить послідовно всі пристрої вузла зв'язку ККМ, задіяні в інформаційному обміні (рис. 3.2). Таким чином, коефіцієнт готовності вузла на підставі (2.1) можна записати

$$Fa_{\text{у}} = Fa_1 \times Fa_2 \times \ldots \times Fa_n, \qquad (3.1)$$

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

Рисунок 3.2 – Представлення математичної моделі вузла зв'язку ККМ

Під елементами вузла розуміються пристрої, як функціонують на 1-3 рівнях еталонної мережевої моделі OSI [45], наприклад пристрої модеми, маршрутизатори, адаптери, міжмережні екрани, пристрої оптимізації трафіку, шлюзи і т. д. Розрахунок коефіцієнта готовності цих елементів слід проводити за методикою розглянутою в розділі 2.

Взявши до уваги, що потоки подій, які впливають на стан досліджуваного вузла зв'язку ККМ, мають експоненціальний характер, для визначення імовірностей безвідмовної роботи елементів мережі використаємо математичний апарат марківських випадкових процесів.

Марківський процес – це випадковий процес, за якого майбутня поведінка системи після певного моменту часу безпосередньо залежить тільки від стану системи в цей конкретний момент і не залежить від стану системи в попередній період[32].

В рамках досліджувальної проблематики цими станами є [38]:

1. Вузол мережі в стані готовності.

2. Вузол в стані неготовності через реалізацію загрози захищеності, спрямованої на обмеження доступності інформації.

3. Вузол мережі я в стані неготовності через відмови обладнання.

Граф станів, в яких може перебувати вузол ККМ зображено на рис. 3.3.

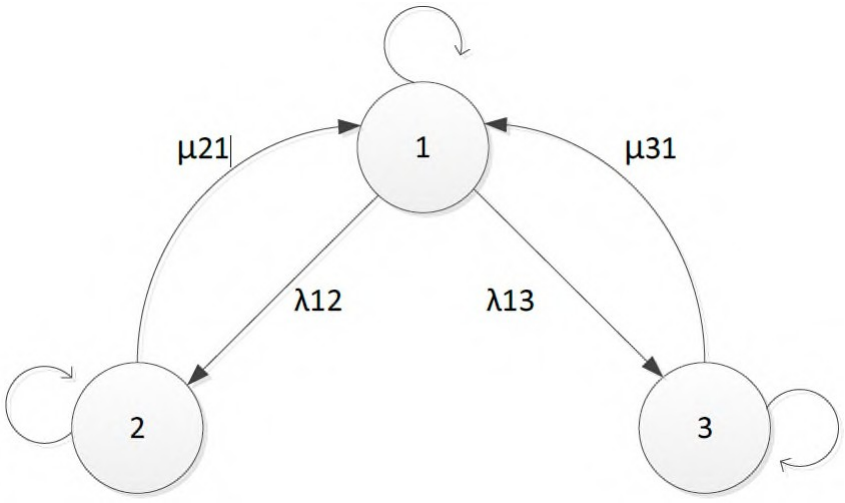


Рисунок 3.3 - Граф станів вузла мережі

Математична модель процесу, що визначається графом (рис. 3.2), можна описати системою рівнянь Колмогорова-Чепмена [27]:

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

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.

Сума імовірностей цих станів рівна одиниці.

В цьому випадку отримаємо систему алгебраїчних рівнянь:

$$\begin{cases} -(\lambda_{12} + \lambda_{13}) \times P_1 + \mu_{21} \times P_2 + \mu_{31} \times P_3 = 0 \\ \lambda_{12} \times P_1 - \mu_{21} \times P_2 = 0 \\ \lambda_{13} \times P_1 - \mu_{31} \times P_3 = 0 \\ P_1 + P_2 + P_3 = 1 \end{cases} \quad (3.3)$$

Її вирішення дає нам можливість отримати формули ймовірності знаходження мережного пристрою в одному з станів:

$$P_1 = \frac{\mu_{21}+\mu_{31}}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}, \quad (3.4)$$

$$P_2 = \frac{\lambda_{12}+\mu_{31}}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}, \quad (3.5)$$

$$P_3 = \frac{\lambda_{13}+\mu_{21}}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}. \quad (3.6)$$

Тому імовірність безвідмовної роботи мережного пристрою, за умови впливу на нього виключно загроз ІБ, відповідає ймовірності непотрапляння його в стані неготовності через реалізацію загрози захищеності, спрямованої на обмеження доступності інформації (2) і розраховується:

$$\bar{P}_2 = \frac{\mu_{21}\times(\lambda_{13}+\mu_{31})}{\mu_{21}+\mu_{31}+\lambda_{12}+\mu_{31}+\lambda_{13}+\mu_{21}}. \quad (3.7)$$

Отже 3.7 являє собою коефіцієнт неготовності *Funa (*unavailability factor) вузла ККМ, що враховує вплив загроз захищеності мережі, направлених на обмеження доступності інформації. При цьому допускається відсутність технічних відмов.

Коефіцієнт *Funa* буде складатися з трьох складових [19]:

- P_B, імовірність порушення доступності вузлів;

- P_P, імовірність що застосовані ЗЗІ не виявлять загрозу;

- $Funa^{\text{П.В}}$, що характеризує час, який вузол мережі знаходиться в стані неготовності.

Для того, щоб загроза ІБ вплинула на коефіцієнт готовності вузла ККМ, всі перераховані вище умови повинні виконуватися одночасно.

Загальна ймовірність настання всіх трьох подій:

$$Funa_{\text{В}(i)} = P_B \times P_{P\ B} \times Funa^{\text{П.В}} \quad (3.8)$$

Коефіцієнт неготовності визначається часом перебування вузла і цьому стані.. Це може бути інтервал, який потрібно для активізації зовнішніх засобів захисту, призначених захисту від DoS атак, якщо штатні ЗЗІ не впоралися з реалізованої атакою і не змогли від неї захистити.

У подальших розрахунках P_P загрози безпеці типу DoS буде розраховуватися для двох випадків - наявності в складі обладнання вузла зв'язку тільки маршрутизатора Cisco або крім того наявності ЗЗІ.

Маршрутизатор - це електронний пристрій, що використовується для підключення двох або більше мереж та управління процесом маршрутизації, тобто на основі інформації про топологію мережі та певних правил він вирішує пересилати пакети на рівні пакетів (рівень OSI 3) між різними сегментами мережі [17].

Для середньостатистичного користувача маршрутизатор - це мережевий пристрій, який з'єднується між Інтернетом та локальною мережею. Але маршрутизатор не обмежується лише передачею даних між інтерфейсами, а виконує й інші функції: розподіляє IP-адреси, захищає локальну мережу від

зовнішніх атак, обмежує доступ певних користувачів локальної мережі до Інтернет-ресурсів, шифрує трафік тощо.

Маршрутизатори функціонують на мережному рівні моделі OSI: вони можуть надсилати пакети між мережами. Для того, щоб відправляти пакети у бажаному напрямку, використовується таблиця маршрутизації. Вона зберігається в пам'яті маршрутизатора. Таблиця маршрутизації може будуватися за допомогою статичної або динамічної маршрутизації.

Крім того, ці пристрої можуть транслювати адресу відправника та одержувача, на основі певних правил фільтрувати транзитний потік даних, щоб обмежити доступ, шифрувати / дешифрувати відправлені дані тощо.

Маршрутизатори не можуть передавати широкомовні повідомлення, такі як запит ARP.

Маршрутизатором може бути спеціалізований пристрій або звичайний комп'ютер, який виконує функції звичайного маршрутизатора. Якщо в таблиці маршрутизації не вказано маршрут для адреси, пакет відкидається.

Існують інші варіанти визначення маршруту переадресації пакетів, коли, наприклад, визначається адреса відправника, протоколи верхнього рівня, які використовуються та інша інформація, яка знаходиться в заголовках пакетів мережного рівня.

На маршрутизаторах Cisco повноцінний захист від DoS атак вимагає придбання і активації додаткового ліцензійного пакета Security Technology Package License

Access Control List або ACL - список управління доступом, який визначає, хто або що може отримувати доступ до об'єкта (програма, процес або файл) та які саме операції дозволено або заблоковано суб’єкту (користувач, групи користувачів).

Якщо мережа зазнає DoS-атаки, ACL можуть бути ефективним методом скидання пакетів DoS до досягнення цільової мети. Використовуйте ACL безпеки, якщо атака виявлена з певного хоста.

У цьому прикладі хост 10.1.1.10 та весь трафік із цього хосту заборонені: Маршрутизатор (конфігурація) # access-list 101 заборонити ip хост 10.1.1.10 будь-який

Маршрутизатор (конфігурація) # access-list 101 дозволяє ip будь-який

Списки безпеки також захищають від підробки адрес. Наприклад, припустимо, що адреса джерела A знаходиться всередині мережі та інтерфейс комутатора, який вказує на Інтернет. Ви можете застосувати вхідний ACL до інтерфейсу комутатора Інтернету, який забороняє всі адреси з джерелом A (внутрішня адреса). Ця дія зупиняє атаки, коли зловмисники підробляють внутрішні адреси джерела. Коли пакет надходить на інтерфейс комутатора, він збігається на цьому ACL і скидає пакет, перш ніж він заподіє шкоду.

Коли комутатор використовується з модулем виявлення вторгнень Cisco (CIDM), ви можете динамічно встановлювати захисний ACL як відповідь на виявлення атаки зондуючим механізмом.

VACL - це інструмент забезпечення безпеки, заснований на інформації рівня 2, рівня 3 та рівня 4. Результатом пошуку VACL щодо пакету може бути дозвіл, відмова, дозвіл та захоплення або перенаправлення. Коли ви асоціюєте VACL з певною VLAN, весь трафік повинен бути дозволений VACL, перш ніж трафік буде дозволений у VLAN. VACL застосовуються в апаратному забезпеченні, тому за застосування VACL до VLAN не застосовується заборону.

Для проведення моделювання використано наступне програмне і апаратне забезпечення:

- PC1 - персональний комп'ютер HP DC7800SFF: CPU Intel Core 7 2.66 GHz, 8GB RAM,, ОС Windows 10;

- PC2 - персональний комп'ютер HP DC7700SFF CPU Intel Core 5 2.26 GHz, 8GB RAM, , ОС Windows 10;

- Атакуючий PC - сервер HP Proliant DL 360 G6 CPU Intel XEON E6540 x4 2.53GHz, 12GB RAM, LAN HP NC382i x2, ОС Debian Linux (з використанням технологій віртуалізації);

- Комутатор H3C S6500 .

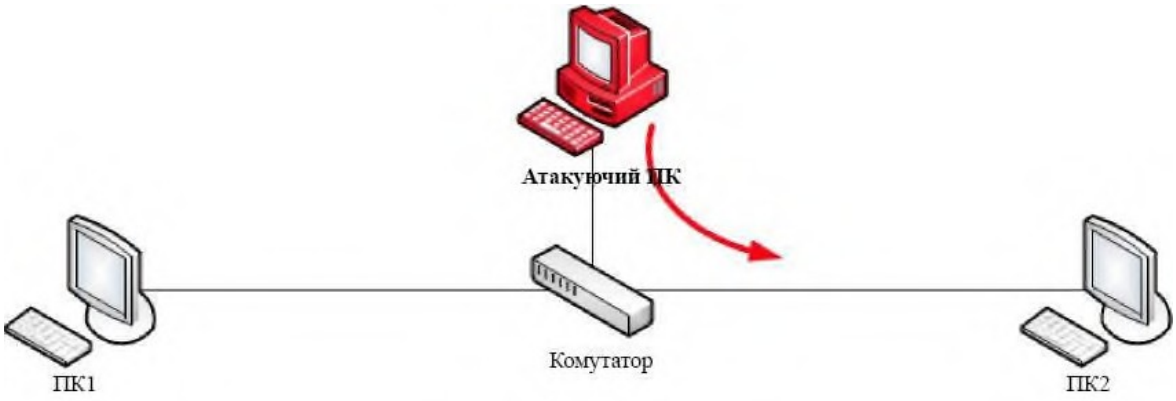


Рисунок 3.4 – Структура стенду для вимірювання характеристик сегмента ККМ

Для оцінки затримок при проходженні трафіку через телекомунікаційне обладнання використовується ПО «HRPing v5.07» Багато службових програм Ping вже доступні, одна навіть випускається з самою Windows, яка називається Ping. Але hrPing має деякі розширені функції, які інші Pings не мають. Графічне відображення результатів пінгу. Використовує таймери з високою роздільною здатністю, тому час пінгування відповідає використанню Також може пінгувати за допомогою пакетів UDP або повідомлень про мітки часу ICMP. Може мати кілька пінгів "у польоті", не потрібно чекати відповіді, перш ніж відправляти наступний пінг.

З hrPing можна зробити набагато більше, ніж із Windows Ping. Як і кожен пінг, hrPing надсилає пакети "ICMP Echo Request" на віддалений комп'ютер і прослуховує відповідні пакети "Echo response". Більше того, hrPing також може надсилати пакети UDP та пакети часової мітки ICMP. Не всі типи пакетів однаково легко проходять усі брандмауери та мережі. За допомогою hrPing ви можете змінюватись. Більше того, hrPing помножується на затримку туди і назад у мікросекундах (1/1000 мсек). Зазвичай це робиться за допомогою «Лічильника продуктивності» Windows, який має роздільну здатність дещо МГц. Ви навіть можете попросити hrPing використовувати "лічильник часу" центрального

процесора, який збільшується з тактовим циклом процесора. Сьогодні ви не можете отримати точніше зі стандартними ПК!

Наступне, що Windows Ping не може зробити, це одночасно надсилати більше одного пакета ping. Windows Ping завжди відправляє один пакет, чекає відповіді, потім друкує його вихідний рядок, повторює.

hrPing розсилає один пакет ping кожні x мілісекунд (ви можете налаштувати цей час за допомогою параметра -s) під час прослуховування вхідних відповідей та друку вихідних даних, якщо такі є.

Причина, по якій вам це сподобається, проста: при широкосмуговому зв’язку у вас часто виникає затримка близько 40 мсек, тоді як пропускна здатність всього з'єднання становить близько 500 кбайт / с. Отже, із "стандартним" пінг-пакетом у 60 байт (заголовок IP + заголовок ICMP + корисний набір пінгу) ви можете відправити тисячі пакетів, перш ніж отримати першу відповідь. Якщо ви хочете перевірити умови лінії, пропускну здатність тощо, цей "накладений" спосіб надсилання дуже корисний.

Крім того, hrPing має набагато кращу статистику, ніж Windows Ping. Ви також отримуєте час в обидва кінці для відповідей на повідомлення про помилку ICMP! Таким чином ви можете напр. контролювати затримку перевищення TTL. hrPing враховує відповіді та повідомлення про помилки окремо, тому глобальна статистика не псує одна одну. Плюс, для статистично схильних, hrPing також обчислює стандартне відхилення, щоб показати вам, наскільки величини "хитаються". hrPing показує стандартне відхилення часу, а також середній час.

hrPing відображає поле ідентифікації IP відповідей і таким чином дає можливість робити "тихі вимірювання навантаження";

При відправленні великої кількості пакетів "Зведений режим" hrPing стане в нагоді: він буде пригнічувати друк кожної відповіді у своєму рядку, але замість цього надрукує короткий опис усіх відповідей на даний момент та короткий зміст за останні 10 секунд (час може бути скоригований). Це дозволяє зберегти гарний загальний вигляд. (-y перемикач)

hrPing може надсилати пінги зі збільшеними розмірами: функція "Розгортка розміру", де після кожного надсилання розмір збільшується до досягнення максимуму, а потім скидається. Плюс, ми обчислюємо під час обробки відповідей та оцінюємо швидкість лінії, якщо дані є досить переконливими. (-l та -L перемикачі)

Після запуску програми, що імітує атаку, вимірюється час відгуку і пікової пропускної спроможності лінії зв'язку. Також збирається статистика числа втрачених пакетів Визначення пікової пропускної здатності проводиться засобами програмного забезпечення IPerf Measurement Tool.

Iperf це клієнт-серверна утиліта котороя дозволяти проводити виміри пропускної здатності каналу. Клієнт-серваная утиліта має на увазі під собою, що для перевірки швидкості між двома ПК необхідно буде запустити iperf на одному ПК в режимі «сервер», а на іншому ПК в режимі «клієнт». Швидкість вимірюється від клієнта до сервера, тобто якщо ви на своєму комп'ютері запустили iperf в режимі «клієнт», то результатом буде «виходить» швидкість. iPerf - це програмне забезпечення для активного вимірювання пропускної здатності, доступне для IP-мереж. Під загальною назвою iPerf мається на увазі саме iPerf3, випущений у відкритому коді та вільно завантажуваний з офіційної сторінки Github.

iPerf, завдяки підтримці всіх найпоширеніших операційних систем (включаючи мобільні, таких як Android та iOS) та можливості регулювання численних параметрів в аналізі продуктивності мережі для різних протоколів, безумовно, є одним із еталонних інструментів для діагностики мережі.

Iperf в unix-подібних система знаходиться у всіх репозиторіях і, щоб його встановити, необхідно запустити стандартну інсталяційну команду для вашого дистрибутива.

Серед програм для моніторингу пропускної здатності мережі iPerf3, безсумнівно, є однією з найбільш використовуваних також системними адміністраторами та адміністраторами мережі, завдяки можливості отримувати стандартні результати та легко перевіряти наявність будь-яких проблем із

мережею або підключенням для серверів Windows або Linux. Результати занесено до таблиці 3.1.

Таблиця 3.1 - Продуктивність сегмента ККМ

Виміри	Час відгуку, мс	Втрата пакетів, %	Пропускна спромож, кбіт/с
1 без загроз, без ЗЗІ	0,150	0	938651 (100%)
2 без загроз, з ЗЗІ	0,452	0	895101 (95%)
3 DoS-атака, без ЗЗІ	0,173	28%	316116 (34%)
4 dos-атака з ЗЗІ	7,966	0%	466668 (49%)

За результатами проведених експериментів можна зробити наступні висновки про вплив DoS атаки на функціонування вузла мережі

В умовах DoS атаки пропускна здатність вузла мережі значно знижується, що обгрунтовується самою природою атаки, проте застосування ЗЗІ на вузлі зв'язку, дозволяє організувати безперебійне функціонування мережі зі зниженими, але допустимими характеристиками.

3.2 Метод дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації

Для дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації, пропонується застосувати метод, особливістю якого є можливість кількісної оцінки ступеня впливу загроз на ефективність функціонування корпоративної мережі. Процес проведення оцінки захищеності ККМ зображена на рис. 3.5.

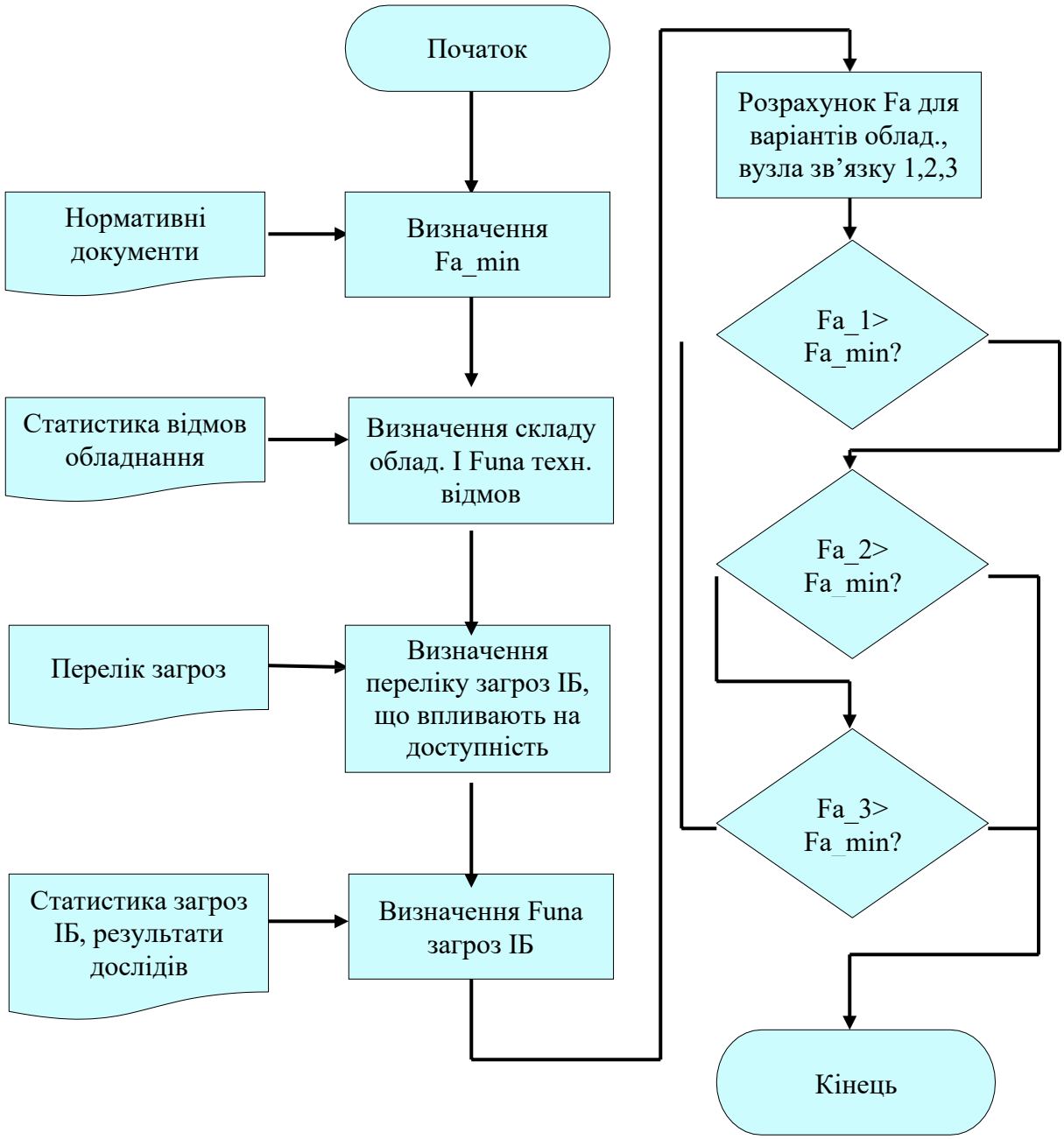


Рисунок 3.5 - Блок-схема процесу оцінки захищеності ККМ від загроз ІБ

1. На першому кроці визначається мінімально допустимий коефіцієнт готовності сегмента мережі, відповідно до нормативних вимог комплексної системи захисту інформації.

2. Визначається склад устаткування вузлів мережі, та проводиться розрахунок коефіцієнт неготовності.

3. Будується модель загроз інформаційної безпеки

4. Проводиться розрахунок коефіцієнт неготовності, з врахуванням впливу загроз доступності інформації.

5. Розраховується коефіцієнт готовності усього досліджуваного сегмента мережі.

6. Проводиться порівняння коефіцієнта готовності з мінімально допустимим. Якщо значення коефіцієнту готовності менше допустимого, необхідно повернутися до етапу 2 і замінити мережне устаткування, щоб задовольняло критерії захисту.

7. Аналізуються результати, при використанні тільки маршрутизатору. При умові, коли значення *Fa_2* перевищує значення *Fa_min*, робиться висновок, що маршрутизатор справляється з загрозами захищеності інформації

8. Порівнюються результати, коли в складі обладнання вузла зв'язку встановлений маршрутизатор і додатковий засіб захисту інформації. При умові, коли значення *Fa_3 перевищує значення Fa_min,* можна зробити висновок, що обране рішення ефективно справляється з поставленою задачею.

3.3 Висновки

За допомогою математичного апарату марківських процесів розроблено граф станів вузла мережі, який характеризує працездатність в умовах впливу загроз безпеці. Математичною модель стану ефективності вузла реалізовано у вигляді системи рівнянь Колмогорова-Чепмена, Вона враховує три його стани: стан готовності; стан неготовності,; атакований стан впливу загроз ІБ.

За результатами проведених експериментів можна зробити наступні висновки про вплив DDoS атаки на функціонування вузла мережі

В умовах DDoS атаки пропускна здатність вузла мережі значно знижується, що обгрунтовується самою природою атаки, проте застосування ЗЗІ на вузлі зв'язку, дозволяє організувати безперебійне функціонування мережі зі зниженими, але допустимими характеристиками

Розроблений метод визначення імовірності знаходження вузла мережі в стані непрацездатності, обґрунтовані впливом загроз доступу інформації, які промодельовано реальним експериментом. Відповідно до цього методу, імовірність знаходження вузда у стані неготовності (коефіцієнт неготовності) є сумою імовірності загрози безпеці, імовірності реалізації загрози, а також середнього часу знаходження вузла в режимі неготовності.

4 ЗАСТОСУВАННЯ МЕТОДУ ДЛЯ ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Практичне дослідження розробленого методу

Для апробації запропонованого методу врахування впливу загроз безпеці, спрямованих на порушення доступності інформації на ефективність функціонування мережі проведено дослідження на ККМ Старосинявської філії ПАТ «ПриватБанк». Мережа складається з 152 вузлів та має складну топологію. Було зібрано інформацію про причини відмов і часу відновлення працездатності устаткування.

В мережі використовується різний склад устаткування. Досліджувалися маршрутизатори виробництва компаній Cisco, що забезпечують функціонування всіх вузлів мережі без спеціалізованих засобів захисту від DoS атак. А також з використанням засобів захисту від DoS атак після активації додаткового ліцензійного пакета Security Technology Package License.

Схема розташування вузла зв'язку в корпоративній мережі наведена на рис. 4.1.

Рисунок 4.1 - Схема розташування вузла зв'язку в корпоративній мережі

Розрахунок коефіцієнтів готовності з використанням спеціалізованого обладнання і без нього проводиться за методикою викладеною в п. 2.3 магістерської роботи. Інформація про відмови маршрутизаторів, їх причину та час відновлення наведена в Додатку А.

На рис 4.2 зображено графік, що демонструє розподіл часу відновлення працездатності маршрутизатора.

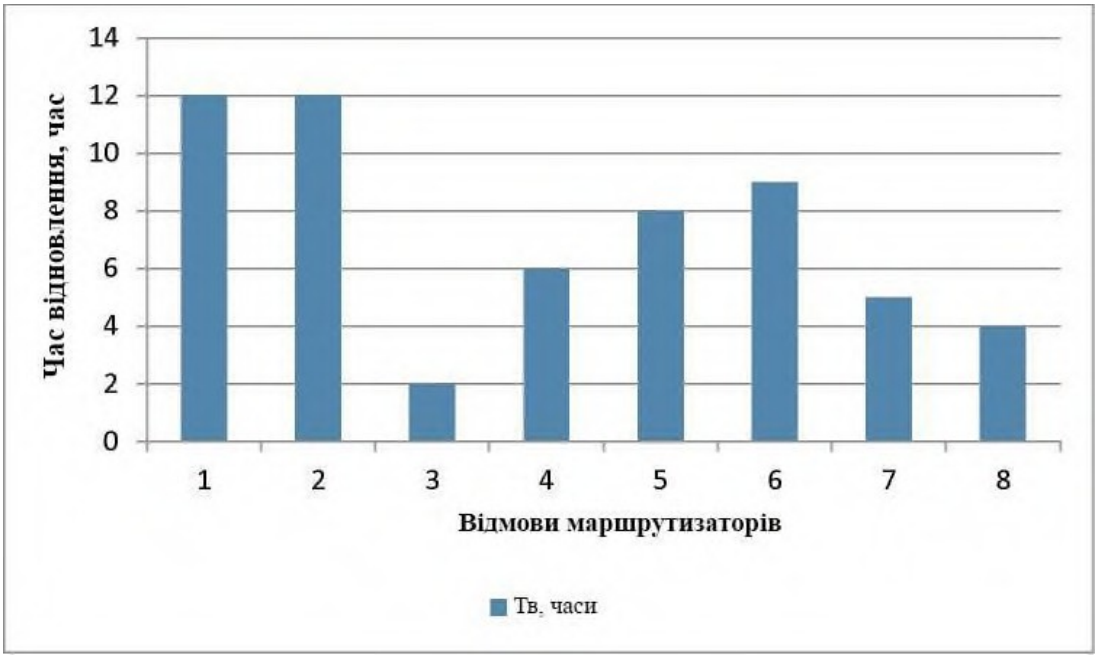


Рисунок 4.2 - Час відновлення маршрутизаторів

.

Значення коефіцієнту неготовності реалізованої загрози $F^{п.в.}_{ипа}$. Розрахунок проводиться на інтервалі часу, що дорівнює 1 календарному році ($\Delta T = 8760$ годин):

$$F^{п.в.}_{ипа} = \frac{5,342}{8760} = 0,00061$$

Таблиця 4.1 – середня тривалість атак типу «відмова в обслуговуванні»

Період 1	Частка атак φ_i для відповідного інтервалу часу DoS атаки						
	0-3 ч	4-8 ч	9-18 ч	19-49 ч	50-100 ч	101-150 ч	151-200 ч
	2	3	4	5	6	7	8
	t_{B1}= 2 ч	t_{B2}= 7 ч	t_{B3}= 14.5 ч	t_{B4}= 34.5 ч	t_{B5}= 74.5 ч	t_{B6}= 124.5 ч	t_{B7}=175 ч

Кінець таблиці 4.1 – середня тривалість DoS атак

1	2	3	4	56	6	7	8
III квартал 2019	0,7413	0,1461	0,0672	0,0453	0,0089	0,0008	0
IV квартал 2019	0,7334	0,1383	0,1284	0,0354	0,005	0,0004	0,0002
I квартал 2020	0,7486	0,1066	0,0816	0,0522	0,002	0,0003	0,0008
II квартал 2020	0,7428	0,125	0,2	0,054	0,002	0,0005	0,0007

Таблиця 4.2 – Коефіцієнт неготовності, обумовлений впливом загроз ІБ

Склад обладнання вузла зв'язку ККМ	$F_a^{(2)}$
Маршрутизатор	0,00061
Маршрутизатор спеціалізованим ЗЗІ	0,000071

4.2 Розрахунок коефіцієнта готовності вузла мережі

Розрахунок значення коефіцієнта готовності проводиться для 3 станів:

- без врахування впливу загроз безпеці і без ЗЗІ мережі;
- з врахування впливу загроз безпеці і без ЗЗІ мережі;
- з врахування впливу загроз безпеці і з ЗЗІ мережі.

Для 1 випадку коефіцієнт готовності вузла ($F_a^{вузла(1)}$) розраховується за (4.1):

$$F_a^{вузла(1)} = \frac{1}{t_1 - t_2} \int_t^{t_2} e^{-\lambda_{м-р} \times t} dt, \qquad (4.1)$$

$$Fa^{м-р} = \frac{1}{43824}\int_0^{43824} e^{-0,0000000001749\times t}dt = 0,999996.$$

Для 2 випадку коефіцієнт готовності вузла ($K_г^{вузла(1)}$) розраховується за (4.2):

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

$$F_a^{вузла(2)} = \frac{1}{43824}\int_0^{43824} e^{-0,0000000001749\times t}dt - 0,514\times 1\times 0,00118 = 0,999996 - 0,00061 = 0,999386.$$

Для 3 випадку коефіцієнт готовності вузла ($F_a^{вузла(1)}$) розраховується за (4.3):

$$F_a^{вузла(3)} = \frac{1}{t_2 - t_1}\int_t^{t_2} e^{-\lambda_{м-р}\times t}dt \times \int_{t_1}^{t_2} e^{-\lambda_{ФПСУ}\times t}\,dt - П_B \times П_{P|B}^{м-р} \times Кнг^{П.В.}, \quad (4.3)$$

$$F_s^{вузла(3)} = \frac{1}{43824}\int_0^{43824} e^{-0,0000000001749\times t}dt \times 0,514\times \frac{1}{43824}\int_0^{43824} e^{-0,000000000282\times t}dt - 0,514\times$$

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

Занесемо відповідні значення до таб.4.3

Таблиця 4.3 – Коефіцієнти готовності та неготовності вузлів

Тип моделювання	Склад обладнання вузла зв'язку ККМ	$F_{una}^{(1)}$ випадок 1	$F_{una}^{(3)}$ випадок 3	$F_{una}^{(2)}$ випадок 2
1	2	3	4	5
Без впливу загроз ІБ $F_a^{вузла(1)}$	Маршрутизатор	0,999995	0,000005	0

Кінець таблиці 4.3 – Коефіцієнти готовності та неготовності вузлів

1	2	3	4	5
З урахуванням впливу загроз ІБ $F_a^{вузла(2)}$	Маршрутизатор	0,999486	0,000005	0,00061
З урахуванням впливу загроз ІБ ($F_a^{вузла(3)}$)	Маршрутизатор, спеціалізований ЗЗІ	0,999825	0,000015	0,000071

4.3 Розрахунок показників надійності сегментів ККМ

Розглянемо ділянку мережі складної топології (рис. 4.3). Розіб’ємо її на умовні сегменти.

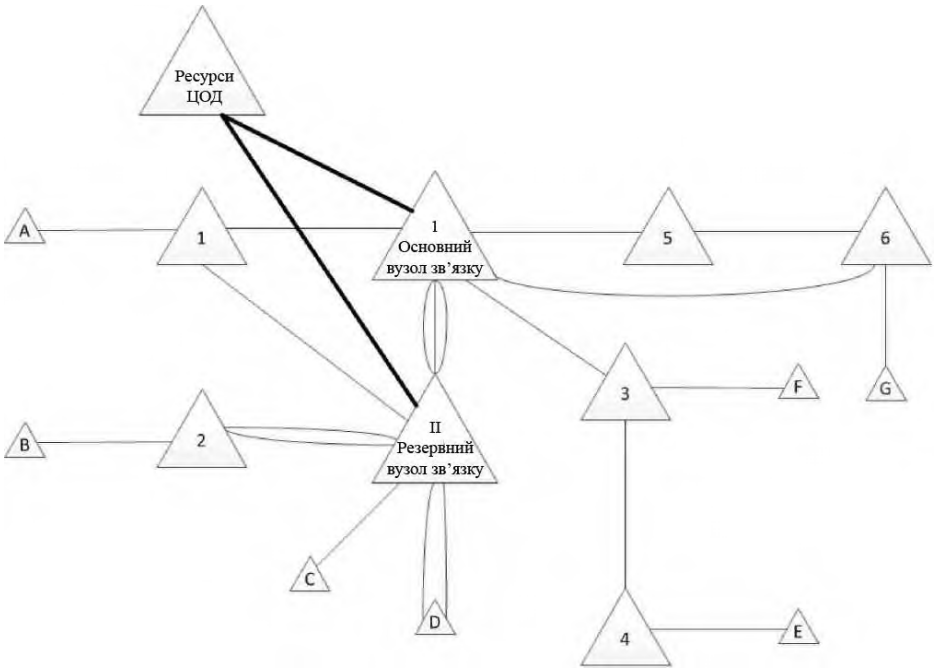


Рисунок 4.3 – Фрагмент експериментальної мережі

Наведена схема показує можливі способи підключення філій до дата-центру (ДЦ). Вузли I і II – виступають основним і резервним вузлом зв'язку, Вони

підключені до ДЦ високошвидкісними каналами підвищеної надійності. Інші вузи можуть виступати кінцевими вузлами, або через них можливе підключення додаткових вузлів. Вузли A - G є кінцевими вузлами. Ці пристрої організовують доступ до централізованих ресурсів. Для прикладу наведемо розрахунки коефіцієнта готовності сегменту E.

В наведеній схемі зображено різні можливості резервування каналів зв'язку:

- розподілений (A-ДЦ);
- кумулятивний (B, C,D-ДЦ);
- резервування за допомогою додаткового ребра (G-ДЦ);
- без резервування (E, F-ДЦ).

Для організації зв'язку між основним і резервним вузлами використовуються 3 канали, що працюють незалежно. В табл. 4.4 наведено необхідні данні для розрахунку:

Таблиця 4.4 - Значення величин для розрахунку коефіцієнтів готовності вузлів мережі

Величина	Значення
Fa канали зв'язку між кінцевими і проміжними елементами	$Кг_{л}=0,997$
Fa канали зв'язку між основним / резервним елементами та ДЦ	$Кг_{ЦОД}=0,9998$
Fa канали зв'язку між основним і резервним елементами	$Кг_{I-II}=0,9999999$
Fa вузла з без врахування впливу загроз	$Кг_{г}^{ВУЗЛА(1)}=0,999997$
Fa вузла з урахуванням впливу загроз	$Кг_{г}^{ВУЗЛА(2)}=0,999385$
Fa вузла з урахуванням впливу загроз ІБ і з спеціалізованим ЗЗІ	$Кг_{г}^{ВУЗЛА(3)}=0999926$

Зробимо розрахунок *Fa* сегментів ККМ. Для чисельного розрахунку топологія формалізується. Відповідно до нормативних вимог, мінімально допустимий коефіцієнт готовності повинен складати $K_{2\min}$=0,996.

Для прикладу розглянемо топологію сегмента Е-ДЦ.

Вона наведена на рис. 4.4. даний сегмент ККМ не має резервування ліній зв'язку.

$$Fa_{E-ДЦ} = Fa_E \times Fa_{E-4} \times Fa_4 \times Fa_{4-3} \times Fa_3 \times Fa_{3-1} \times Fa_1 \times \\ \times (1-(1-Fa_{1-ДЦ}) \times (1-Fa_{I-II} \times Fa_{II} \times Fa_{II-ДЦ})), \quad (4.4)$$

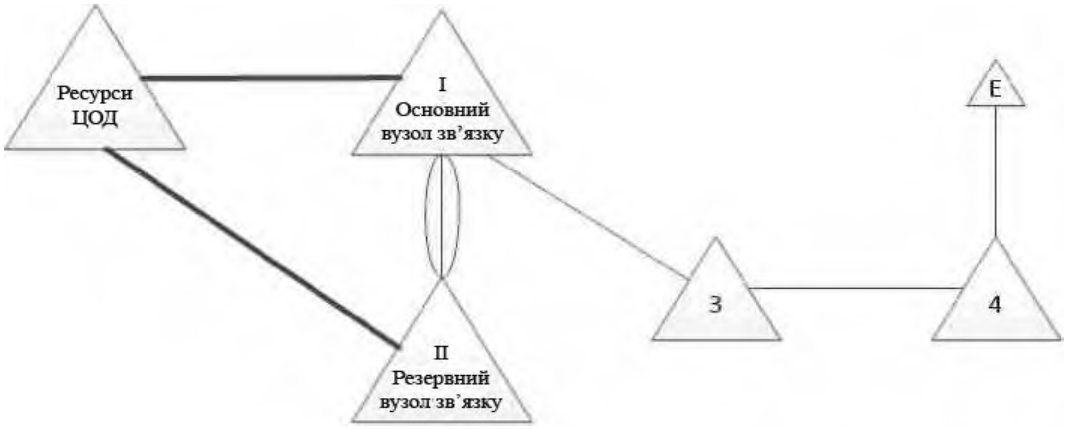


Рисунок 4.4 – Топологія сегмента Е-ДЦ

Розрахункову формула для даного сегмента:

$$Fa_{E-ДЦ} = Fa^4_У \times Fa^3_У \times (1-(1-Fa_{ДЦ}) \times (1-Fa_{I-II} \times Fa_У \times Fa_{ДЦ})). \quad (4.5)$$

Підставивши відомі значення складових величин в (4.27), отримаємо значення $Fa_{E-ДЦ}$ для всіх досліджуваних випадків. Отримані значення об'єднані в таблицю 4.5.

Аналогічно розраховуються значення для інших сегментів

Таблиця 4.5 –Коефіцієнт готовності сегменту Е

Склад устаткування на вузлі зв'язку та вплив загроз на захищеність	$Fa_{E-ДЦ}$
Маршрутизатор, загрози безпеці не враховуються	$F_a^{E-ДЦ(1)}$=0,99101
Маршрутизатор, загрози безпеці враховуються	$F_a^{E-ДЦ(2)}$=0,9886
Маршрутизатор і спеціалізоване ЗЗІ», загрози ІБ враховується	$F_a^{E-ДЦ(3)}$=0,99073

Так як мінімальний допустимий поріг коефіцієнту готовності - 0,996, то використовуване устаткування і топологія даного мережного сегмента не задовольняють нормативні вимоги, В наступному підрозділі буде проведено оптимізацію мережної топології або та її устаткування.

4.4 Підвищення ефективності функціонування мережі

Для наочності коефіцієнти готовності сегментів мережі для трьох можливих станів кожного сегменту зображено на рис 4.5.

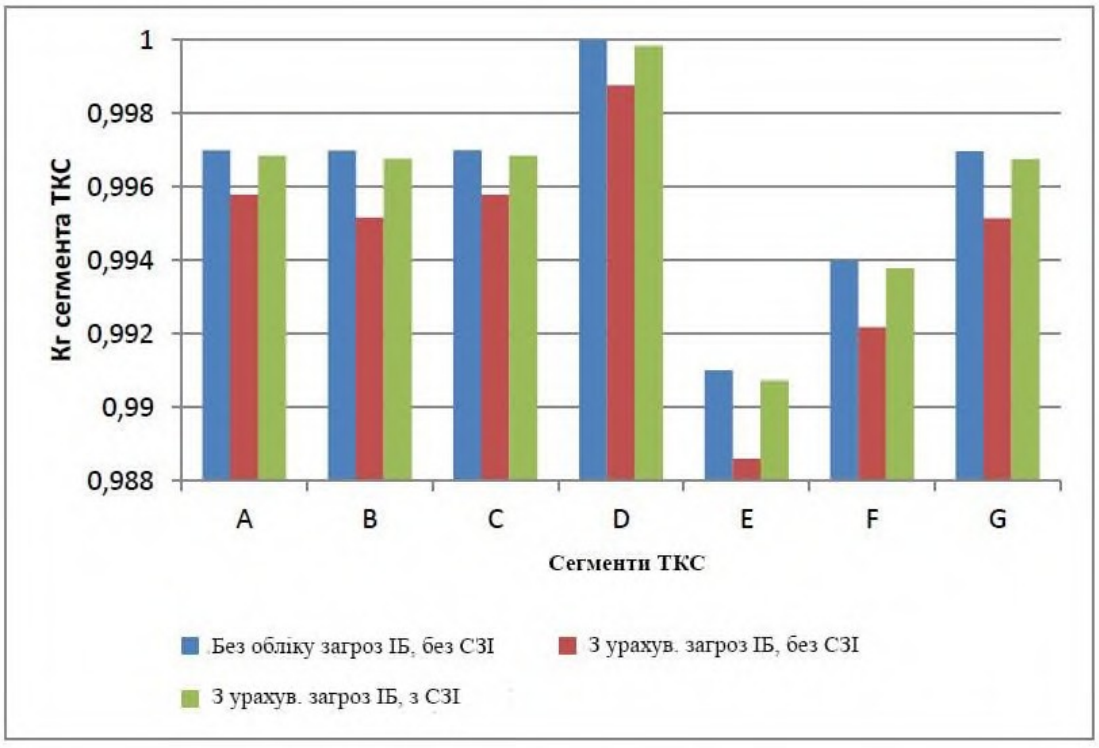


Рисунок 4.5 – Гістограма впливу коефіцієнтів готовності різних сегментів

Отримані результати відповідають теоретичним розрахункам в 2 розділі магістерської роботи, що підтверджує достовірність запропонованої математичної моделі.

У розділі 2 розглядалися еталонні топології сегментів ККМ, а в розділі 4 досліджувалися топології, що мають більш складну будову, комбінації зарезервованих і не зарезервованих ділянок.

На рис. 4.5 чітко видно, що при використанні спеціалізованого захисту від загроз ІБ (високих значеннях коефіцієнта готовності вузла) тип резервування не грає вагому роль. Однак при зниженні коефіцієнта готовності без використання ЗЗІ від DoS атак, розподілене резервування каналів зв'язку впливає на надійність роботи мережі.

Але, зрозуміло, що резервування каналів зв’язку накладає додаткові фінансові витрати. Коефіцієнта готовності в топологіях мереж з резервуванням приведено на рис. 4.6

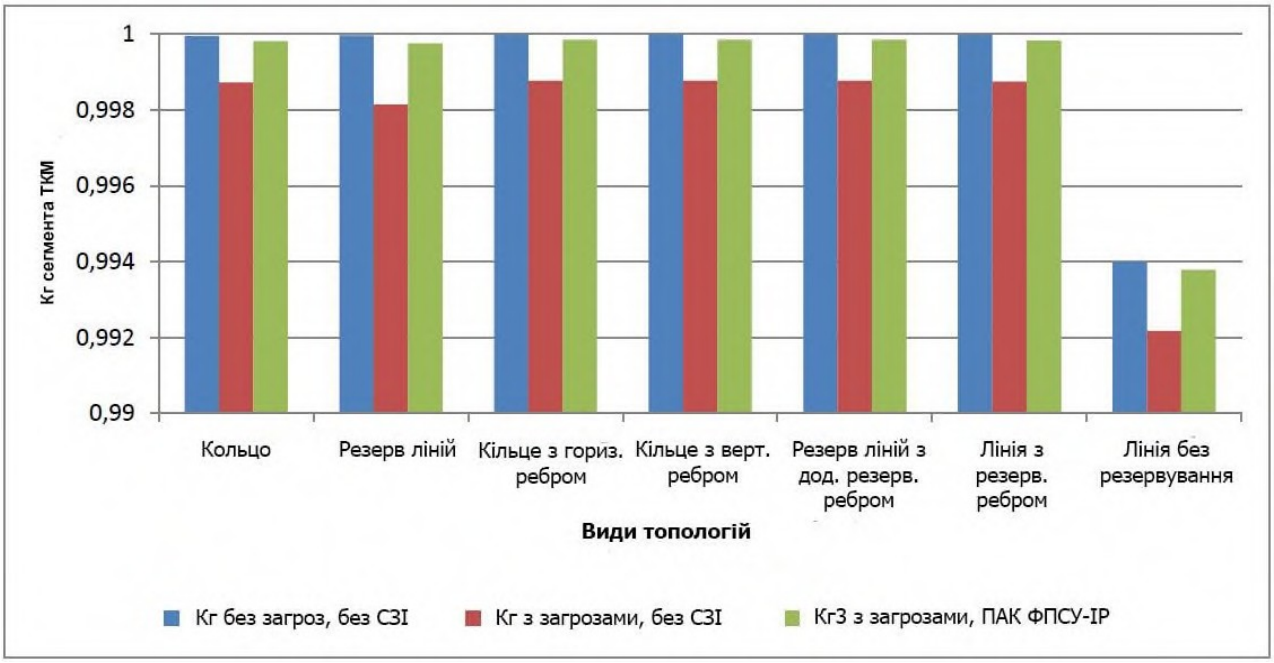


Рисунок 4.6 - Гістограма впливу коефіцієнтів готовності вузлів на топології мереж з резервування

З графіка (рис. 4. 6) випливає, що в розглянутих граничних умовах діапазону зміни коефіцієнтів готовності вузла зв'язку та каналу, з метою оптимізації

найбільш доцільно використовувати кільцеву топологію. Найбільш перспективною є кільцева топологія з вертикальним резервним ребром, яка може являти собою об'єднання на одному фізичному вузлі двох незалежних комплектів устаткування і каналів зв'язку

Проведемо оптимізацію досліджуваного в 4.3 сегменту Е (рис 4.4).

Оптимізована топологія сегмента Е'-ДЦ представлена на рис. 4.7. У представлених рішенні добавлено вузли 3' і 4'. Вони відображають наявність на вузлах 3 і 4 додаткових комплектів устаткування зв'язку з незалежним підключенням до корпоративної мережі..

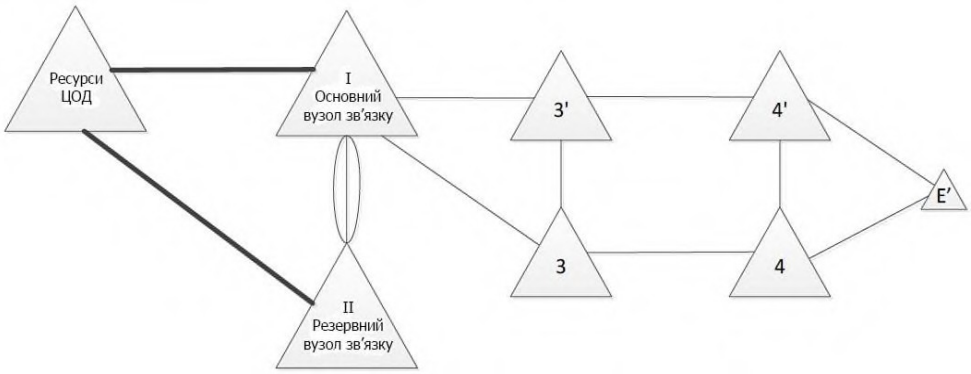


Рисунок 4.7 - Оптимізована топологія сегмента мережі Е'-ДЦ

Розраховані значення коефіцієнтів готовності занесено до таб. 4.6

Таблиця 4.6 – Коефіцієнти готовності оптимізованих топологій

Сегмент	Топологія і характеристики сегмента ККМ	*Fa* сегмента		
		Стан1	Стан 2	Стан 3
Е’	Резервування кільцевою топологією з вертикальним ребром	$Кг_г^{E'-ЦОД(1)} = 0{,}99999$	$Кг_г^{E'-ЦОД(2)} = 0{,}99877$	$Кг_г^{E'-ЦОД(3)} = 0{,}99985$

4.5 Висновки

В розділі проведено дослідження корпоративної мережі, на якій опробуванні математична модель та запропонований в роботі метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі

Отримані результати відповідають теоретичним розрахункам в 2 розділі магістерської роботи, що підтверджує достовірність запропонованої математичної моделі.

Проведено оцінку ефективності функціонування ККМ ПАТ «ПриватБанк». Для оцінку ефективності обрані ряд сегменти з різними топологіями та числом вузлів.

В результаті дослідження встановлено, що вплив загроз безпеки на коефіцієнт готовності вузла перевершує вплив технічних неполадок. Тому доведено актуальність дослідження і наведено рекомендації по першочерговості прийняття заходів для забезпечення інформаційної безпеки з метою підвищення ефективності функціонування мережі.

Розроблено рекомендації щодо оптимізації топологій ККМ з найменшими коефіцієнтом готовності. Отримані результати допускають забезпечення безпеки мережі топологічними методами без використання додаткових ЗЗІ.

ВИСНОВКИ

В роботі вирішено наукове завдання – вдосконалено метод дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації, особливістю якого є можливість кількісної оцінки ступеня впливу загроз на ефективність функціонування корпоративної мережі.

Основні результати магістерської роботи є такими:

1. Проаналізовано актуальні методи дослідження мережі, що дозволяють проводити оцінку захисту від атак, спрямованих на порушення доступності інформації.

2. Доведено можливість використання математичного та методологічного апарату теорії надійності як методу мережевих досліджень та коефіцієнта готовності як показника для оцінки ефективності вузлів зв'язку.

3. Розроблена математична модель, яка дозволяє врахувати вплив розподілених атак на систему, що описується графом трьох станів та відповідною системою рівнянь

4. Удосконалено метод дослідження корпоративної мережі, що дозволяє оцінити ефективність функціонування вузла зв'язку в умовах впливу розподілених атак, пов’язаних з доступністю інформації. На підставі отриманих розрахунків і цільового значення коефіцієнту готовності вузлів мережі, можливо прийняти рішення про необхідність проведення заходів щодо підвищення ефективності функціонування мережі.

5. Запропоновано підхід до організації внутрішньої топології вузлів зв'язку мережі, що приводить її до форми кільця з вертикальним резервним фронтом, що дозволяє значно збільшити коефіцієнт готовності елементів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

6. Агеев, Д.В. Методика описания структуры современных телекоммуникационных систем с использованием многослойных графов / Д.В. Агеев // Восточно-Европейский журнал передовых технологий. – 2010. – Т. 6 – №4 (48). – С. 56–59.

7. Ботуз С.П. Интеллектуальные интерактивные системы и технологии управления удаленным доступом./ С.П. Ботуз – М.: Соломон-Прессс, 2014. –360 с

8. Буторов, В.В. Оценка надежности клиент-серверных приложений корпоративной системы управления предприятием / В.В. Буторов, С.В. Тынченко, Р.Ю. Царев // Фундаментальные исследования. – 2015. – №5-3. – С. 488–492.

9. Гольдштейн, Б.С. Сети связи пост-NGN /Б.С. Гольдштейн, А.Е. Кучеря-вый. –СПб.:БХВ-Петербург, 2014. –160с.: ил.

10. Голуб, Б.В. Методика оценки живучести распределенных информационных систем / Б.В. Голуб, Е.М. Кузнецов, Р.В. Максимов // Вестник Самарского государственного университета. – 2014. – №7 (118) – С. 221–232.

11. Егунов, М.М. Анализ структурной надежности транспортной сети / М.М. Егунов, В.П. Шувалов // Вестник Сиб ГУТИ. – 2012. – №1. – С. 54–60.

12. Евглевская, Н.В. Модель информационного воздействия на объекты телекоммуникационной сети / Н.В. Евглевская, А.А. Привалов // Известия Петербургского университета путей сообщения. – 2015. – №1 (42). – С. 72–77.

13. Ермаков А. Основы конфигурирования корпоративных сетей Cisco. А. Ермаков – М.: ФГБОУ "Учебно-методический центр по образованию на железнодорожном транспорте", 2013. — 457 с.

14. Закиров, В.И. Моделирование умышленного воздействия инсайдеров на информационную систему / В.И. Закиров, Д.Ю. Пономарев // Современные проблемы науки и образования. – 2015. – №1. – Режим доступа: http://science-education.ru/ru/article/view?id=18267.

15. Золотухин, В.В., Шестаков, Н.А. Проблемы анализа и обеспечения

надежности современных инфокоммуникационных систем и сетей / В.В. Золотухин, Н.А. Шестаков // Перспективы развития информационных технологий. – 2011. – №4. – С. 225–234.

16. Каяшев, А.И. Анализ показателей надежности двухуровневых магистральных сетей / А.И. Каяшев, П.А. Рахман, М.И. Шарипов // Вестник Уфимского государственного авиационного технического университета. – 2014. – Т. 18. – №2 (63). – С. 197–207.

17. Кулаков, Ю.А. Анализ структуры телекоммуникационной сети путем представления ее топологии предфрактальным графом / Ю.А. Кулаков, В.В. Воротников, И.В. Гуменюк // Вісник НТУУ «КПІ» Інформатика, управління та обчислювальна техніка. – 2013. – №58. – С. 68–73.

18. Кутузов, О. И. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик [Текст] : монография / О. И. Кутузов, Т. М. Татарникова - СПб. : ГУАП, 2015. – 381 с.

19. Макаренко, С.И. Адаптация параметров сигнализации в протоколе маршрутизации с установлением соединений при воздействии на сеть дестабилизирующих факторов / С.И. Макаренко, Р.Л. Михайлов // Системы управления, связи и безопасности. – 2015. – №1. – С. 98–126.

20. Молочков В.П. Компьютерные сети / Молочков В.П. – М.: ИНТУИТ, 2013. — 982 с.

21. Орлов, А.И. Организационно-экономическое моделирование : учебник для вузов В 3 ч. Ч. 2. Экспертные оценки / А.И. Орлов. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2011. – 486 с.

22. Орлов, А.И. Экспертные оценки / А.И. Орлов // Журнал «Заводская лаборатория». – 1996. – Т.62. №1. – С. 54–60.

23. Петренко, С. Информационная безопасность: экономические аспекты / С. Петренко, С. Симонов, Р. Кислов // Jet Info, Информационный Бюллетень. – 2003. – № 10 (125). – С. 3–24.

24. Поповский, В.В. Методы анализа динамических структур телекоммуникационных систем / В.В. Поповский, В.С. Волотка // Восточно-Европейский

журнал передовых технологий. – 2013. – Т. 5 – №2 (65). – С. 18–22.

25. Поповский, В.В. Математическое моделирование надежности инфокоммуникационных сетей / В.В. Поповский, В.С. Волотка // Телекомунікаційні та інформаційні технології. – 2014. – №3. – С. 5–9.

26. Привалов А. А. Модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя / А.А. Привалов, Н.В. Евглевская, К.Н. Зубков // Известия Петербургского университета путей сообщения. 2014. №2 (39).

27. Рахман, П.А. Коэффициент готовности трехуровневых локальных сетей передачи данных / П.А. Рахман // Международный журнал прикладных и фундаментальных исследований. – 2015. – №9. – С. 463–466.

28. Рахман, П.А. Марковская цепь гибели и размножения в моделях надежности технических систем / П.А. Рахман, // Вестник Уфимского государственного авиационного технического университета. – 2015. – Т. 19. – №1 (67). – С. 140–154.

29. Рикун В. В. Метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки / В.В. Рикун, І.В. Муляр // Збірник наукових праць за матеріалами XII всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2020». Хмельницький – 2020. – С. 193-198.

30. Рикун В. В. Дослідження характеристик надійності та інформаційної безпеки вузлів комп’ютерної мережі / І.В. Толок, Ю.П. Кльоц, А.О Рамський., В.В. Рикун // Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє" Том 2 [Текст] / за заг. редакцією Ігоря Толока. – К. : ВІКНУ, 2020. – С. 63

31. Сердюк В. А. Организация и технологии защиты информации / В. А. Сердюк. – М.: Издательский дом Государственного университета – Высшей школы экономики, 2017. – 571 с.

32. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. - К.:

CAMMIT-Книга, 2010. - 708 с.: іл.

33. Ярощук Д.О. Удосконалення методу обрахунку впливу загроз інформаційної безпеки на ефективність функціонування закритої телекомунікаційної мережі / Д.О. Ярощук, О.А. Мясищев // Вісник Хмельницького Національного Університету «серія: Технічні науки». – 2017 –Т. 6. – С. 64–70.

34. Avizienis, A. Basic concepts and taxonomy of dependable and secure computing / A. Avizienis, J-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1. – №1. – P. 11–33.

A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674-678, 2014, URL: http://iicsit.com/docs/Volume 5/vol5issue01/iicsit20140501145.pdf/.

A. M. Plaskovsky, A. G. Novopashenny, Y. E. Podgurskiy, and S. Zaborowski, Metodyi i sredstva zaschity i kompyuternoy informatsii. Mezhsetevoe ekranirovanie. Razgranichenie dostupa na prikladnom urovne [Methods and means of protection of computer information. Firewall. Access control at the application level]. St. Petersburg, Russia: Publishing House of STU, 2012.

35. 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.

36. Bondavalli, A. Modeling and analysis of a scheduled maintenance system: a DSPN approach / A. Bondavalli, R. Filippini // Computer Journal. – 2004. – №47. – P. 634–650.

37. 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. – 2017. – №7. – P. 522–533.

38. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Елекктроник ресурс]. Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product data sheet0900aecd802da1b5.html.

39. 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

40. Dobryshin M M Calculation of correlations between the values of the parameters of the technical condition of means of communication Certificate of registration of computer programs 2018615232

41. Gupta, V. Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks / V. Gupta, S. Dhamaraja // Reliability Engineering and System Safety. – 2011. – № 12. – P. 1627–1635

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

43. Limited liability company 'trust'. Method and system for analysis malware, protocols for interaction with the control centres and identifying computer attacks/RF Patent No. 2634211 24.10.2017 Newsletter. №. 30.

44. P. V. Kucherniuk, Kompiuterni merezhi: navchalnii posibnyk z distsipliny «Kompiuterni merezhi ta zasoby telekomunikatsii» dlia studentiv spetsialnosti 7.05090201, 8.05090201 «Radioelektronni aparaty ta zasoby» [Computer Networks [Electronic publications]: a textbook on discipline "Computer networks and telecommunications"]. Kyiv, Ukraine: NTUU "KPI," 2014, URL: http://ela.kpi.ua/handle/123456789/12042.

45. S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-2802.

46. 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.

ДОДАТОК А

(Обов’язковий)

Статистика непрацездатності обладнання вузлів зв’язку

Таблиця А.1 Інформація про непрацездатність маршрутизаторів

Інцидент	Тв, часи	Причина інциденту
1	12	Відмова блоку живлення
2	12	Відмова системної плати
3	2	Зависання ПЗ
4	6	Відмова флеш пам’яті
5	8	Відмова системної плати
6	9	Відмова блоку живлення
7	5	Відмова мережевого інтерфейсу
8	4	Відмова блоку живлення

Таблиця А.2 Інформація про непрацездатність ПАК «ФПМР-IP»

Інцидент	Тв, години	Причина інциденту
1	2	3
1	3,33	Відмова материнської плати
2	1,67	Відмова блоку живлення
3	2,33	Відмова блоку живлення
4	2,67	Відмова материнської плати
5	2,17	Відмова блоку живлення
6	2,83	Відмова материнської плати
7	0,167	Зависання ПЗ
8	2	Відмова блоку живлення
10	3	Відмова материнської плати
11	2,83	Відмова блоку живлення

Продовження таблиці А.2

Інцидент	Тв, години	Причина інциденту
1	2	3
12	1,5	Відмова блоку живлення
13	4	Відмова материнської плати
14	0,0833	Зависання ПЗ
15	0,0833	Зависання ПЗ
16	0,25	Зависання ПЗ
17	0,0833	Зависання ПЗ
18	2	Відмова материнської плати
19	0,0833	Зависання ПЗ
20	0,167	Відмова блоку живлення
21	3	Зависання ПЗ
22	3	Відмова блоку живлення
23	0,0833	Зависання ПЗ
24	0,0833	Зависання ПЗ
25	0,25	Зависання ПЗ
26	0,0833	Зависання ПЗ
27	0,0833	Зависання ПЗ
28	0,0833	Зависання ПЗ
29	0,167	Зависання ПЗ
30	0,0833	Зависання ПЗ
31	0,167	Зависання ПЗ
32	0,417	Пошкодження файлів ОС
33	0,667	Пошкодження файлів ОС
34	0,417	Пошкодження файлів ОС
35	0,417	Пошкодження файлів ОС

Продовження таблиці А.2

Інцидент	Тв, години	Причина інциденту
1	2	3
36	0,333	Пошкодження файлів ОС
37	0,417	Пошкодження файлів ОС
38	0,333	Пошкодження файлів ОС
39	0,417	Пошкодження файлів ОС
40	0,0833	Зависання ПЗ
41	0,333	Пошкодження файлів ОС
42	0,0833	Зависання ПЗ
43	0,417	Пошкодження файлів ОС
44	0,333	Пошкодження файлів ОС
45	0,333	Пошкодження файлів ОС
46	0,333	Пошкодження файлів ОС
47	0,333	Пошкодження файлів ОС
48	0,167	Зависання ПЗ
49	0,0833	Зависання ПЗ
50	0,333	Пошкодження файлів ОС
51	0,417	Пошкодження файлів ОС
52	0,333	Пошкодження файлів ОС
53	0,25	Зависання ПЗ
54	0,333	Пошкодження файлів ОС
55	0,833	Пошкодження файлів ОС
56	0,333	Пошкодження файлів ОС
57	0,833	Пошкодження файлів ОС
58	0,167	Зависання ПЗ
59	8	Комплексна відмова

Продовження таблиці А.2

Інцидент	Тв, години	Причина інциденту
1	2	3
60	0,0833	Зависання ПЗ
61	0,167	Зависання ПЗ
62	5	Комплексна відмова
63	0,0833	Зависання ПЗ
64	0,25	Зависання ПЗ
65	0,0833	Зависання ПЗ
66	10,7	Комплексна відмова
67	0,25	Зависання ПЗ

ДОДАТОК Б

(Обов'язковий)

Копії наукових праць

УДК 004.891

Муляр І. В, Рикун В. В.

Хмельницький національний університет

МЕТОД ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ВУЗЛА ЗВ'ЯЗКУ КОРПОРАТИВНОЇ МЕРЕЖІ З ВРАХУВАННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У роботі розглядаються перспективні напрямки розвитку корпоративних мереж, які можуть задовольнити зростаючі потреби користувачів, це перехід від використання власних або орендованих каналів зв'язку до відкритих, побудованих за допомогою Інтернету чи інших мереж зв'язку. Однак використання відкритих мереж Інтернету супроводжується тим, що вони піддаються конкретним загрозам інформаційній безпеці, що впливає на ефективність телекомунікаційних мереж.

Аналіз показав, що існуючі методи оцінки ефективності мереж не враховують вплив загроз інформаційної безпеки. В ході подальших досліджень пропонується їх вдосконалення, що дозволяє оцінити ефективність функціонування вузлів зв'язку як елементів телекомунікаційної мережі з урахуванням впливу загроз інформаційної безпеки та технічних збоїв обладнання.

Загроза інформаційній безпеці - це сукупність умов та факторів, що створюють потенційну або фактичну загрозу інформації. Запропонований метод дозволяє оцінити ефективність роботи корпоративної мережі з формуванням результату оцінки у вигляді кількісного показника, тим самим покращуючи якість оцінки.

The article considers promising areas of development of corporate networks that can meet the growing needs of users, is the transition from the use of own or leased communication channels to open, built using the Internet or other communication networks. However, the use of open Internet networks is accompanied by the fact that they are exposed to specific threats to information security, which affects the efficiency of telecommunications networks.

The analysis showed that the existing methods of assessing the effectiveness of networks do not take into account the impact of information security threats. In the course of further research their improvement is offered that allows to estimate efficiency of functioning of communication nodes as elements of a telecommunication network taking into account influence of threats of information security and technical failures of the equipment.

An information security threat is a set of conditions and factors that create a potential or actual threat to information. The proposed method allows to evaluate the effectiveness of the corporate network with the formation of the evaluation result in the form of a quantitative indicator, thereby improving the quality of evaluation.

Вступ

Використання ресурсів у всіх сферах глобальної комунікаційної мережі сприяло тому, що зловмисники вже десятки років активно здійснюють різні

правопорушення у сфері високих технологій [1] і в даний час активно розробляють різні способи та стратегії впливу інформаційних технологій.

Розуміння сутності та функції кіберзлочинців та мережевої безпеки; якісний описовий механізм є найбільш ідеальним засобом збору та аналізу даних завдяки гнучкості, адаптивності та безпосередності теми. Це призводить до властивих упереджень, але ще однією характеристикою таких досліджень є виявлення та моніторинг цих упереджень, включаючи, таким чином, їх вплив на збір та аналіз даних, а не намагання їх усунути. Нарешті, аналіз даних у інтерпретаційному якісному дослідженні є індуктивним процесом. Дані є досить описовими та суттєво сприяють цьому дослідженню.

В магістерській роботі під корпоративними комп'ютерними мережами (ККМ) розуміються в першу чергу ККМ установ банківської системи України, так як характеристики ККМ, статистичні дані про вторгнення, досвід впровадження безпосередньо відноситься до підприємств банківської сфери. У той же час, результати дослідження показали, що їх доцільно використовувати і на підприємствах в інших сферах економіки.

Так як системи зв'язку досить важливі для правильного функціонування організації, вони стають пріоритетом для злочинців. Впливаючи на мережу, організовуються атаки, спрямовані на різні характеристики інформації. Загроза інформаційної безпеки - це сукупність умов і факторів, які створюють потенційну або фактичну загрозу інформації. При атаках зловмисників існує небезпека втрати, перекручення, блокування, копіювання, поширення інформації, а також інших несанкціонованих дій з нею.

Незалежно від конкретних типів загроз необхідно забезпечити наступні основні властивості: цілісність, конфіденційність і доступність [2]. Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Завдання цілісності і конфіденційності успішно вирішується за рахунок використання криптографічного захисту інформації. У цьому магістерському дослідженні запропоновано метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з урахуванням інформаційної безпеки. Це дає можливість вжити заходи щодо їх нейтралізації та оцінити ефективність їх використання.

Головним завданням цього дослідження є об'єднання в єдину математичну модель характеристик надійності та інформаційної безпеки. Для моделювання характеристик надійності та інформаційної безпеки можна використовувати марківські процеси і експоненціальний розподіл можливих подій [3]. Як показник, що безпосередньо характеризує властивості системи, доцільно використовувати коефіцієнт готовності (Fa). Класичним підходом до моделювання ККМ є приведення її до деревовидного графу. Одним з підходів є нормування Fa для ККМ та ліній зв'язку для мереж передачі даних, але існуючі правила не застосовуються до корпоративних мереж передачі даних, побудованих поверх Інтернету, оскільки

мережа, сформована таким чином, частково абстрагується від певного постачальника послуг [4].

Постановка задачі

Отже необхідно дослідити можливість застосування методичного та математичного апарату теорії надійності як методу дослідження ККМ для оцінки впливу загроз ІБ на забезпечення ефективного функціонування ККМ. Проаналізувати можливість підвищення ефективності функціонування вузлів зв'язку ККМ шляхом вдосконалення їх мережевих топологій.

Основна частина

Оцінка ефективності функціонування базується на порівнянні коефіцієнту готовності ККМ, розрахованих для різних варіантів, кожен з яких відображає можливий стан вузла зв'язку і обладнання на ньому:

1. Коефіцієнт готовності ККМ розраховується без врахування впливу на захищеність мережі.
2. Коефіцієнт готовності ККМ розраховується з урахуванням впливу, але без використання засобів захисту інформації.
3. Коефіцієнт готовності ККМ розраховується з урахуванням впливу загроз захищеності.

Взявши до уваги, що потоки подій, які впливають на стан досліджуваного вузла зв'язку ККМ, мають експоненціальний характер, для визначення імовірностей безвідмовної роботи елементів мережі використаємо математичний апарат марківських випадкових процесів [5].

Для дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації, пропонується застосувати метод, особливістю якого є можливість кількісної оцінки ступеня впливу загроз на ефективність функціонування корпоративної мережі. Процес проведення оцінки захищеності ККМ зображена на рис.1.

1. Визначається мінімально допустимий коефіцієнт готовності сегмента ККМ (*Fa_min*) відповідно до нормативних вимог комплексної системи захисту інформації.
2. Визначається склад устаткування вузлів мережі, та розраховується коефіцієнт неготовності.
3. Будується модель загроз ІБ
4. Обраховується вплив загроз ІБ на коефіцієнт готовності вузла ККМ, проводиться розрахунок коефіцієнт неготовності
5. Розраховується коефіцієнт готовності усього досліджуваного сегмента ККМ.
6. Порівнюються результати отриманого коефіцієнта готовності з мінімально допустимим. Якщо значення коефіцієнту готовності менше допустимого, необхідно повернутися до етапу 2 і зробити вибір обладнання, що задовольняє критерії захисту.

7. Порівнюються результати, коли в складі обладнання вузла зв'язку використовується тільки маршрутизатор. У разі, коли значення *Fa_2* перевищує значення *Fa_min*, можна дійти висновку, що виявлені загрози захищеності інформації не надають істотного впливу на надійність функціонування мережі.
8. Порівнюються результати, коли в складі обладнання вузла зв'язку встановлений маршрутизатор і засобів захисту інформації. Проводиться порівняння розрахованого значення *Fa_3*з*Fa_min*. В випадку, коли значення *Fa_3* перевищує значення *Fa_min*, робиться висновок, щодо обраного рішення.

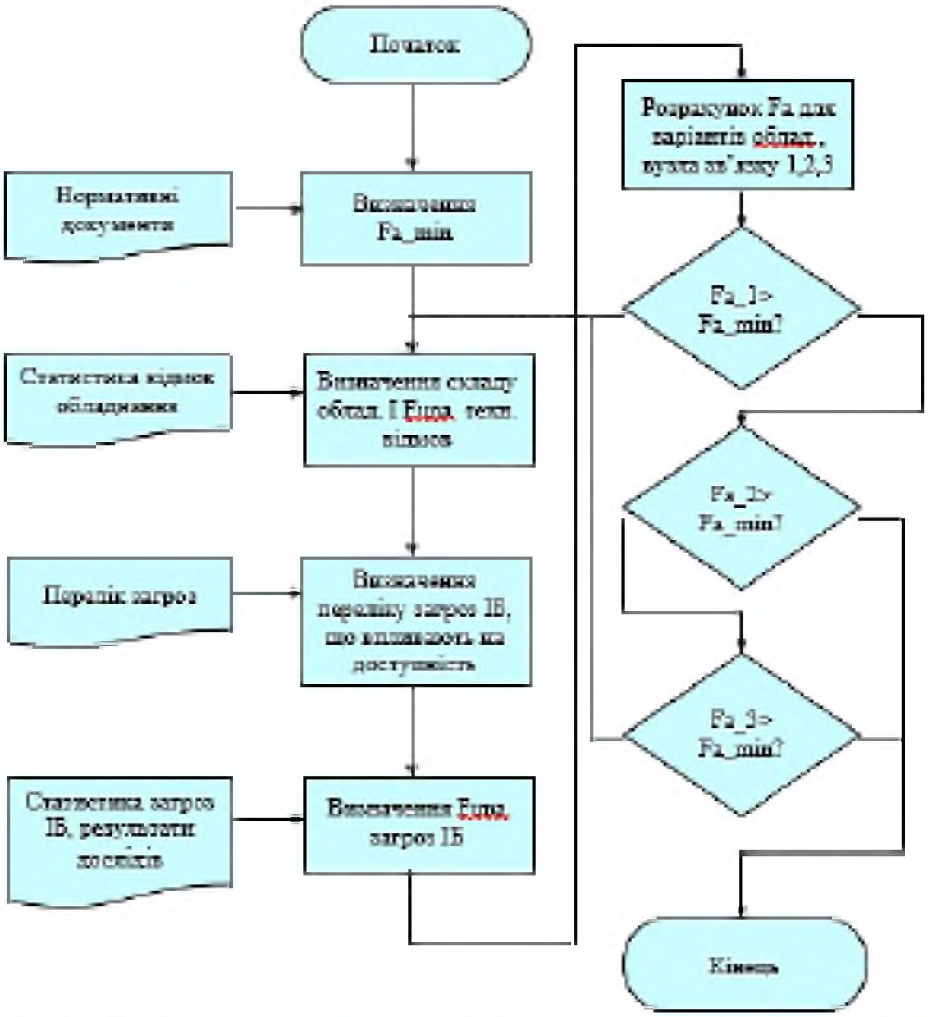


Рисунок 1 – Блок-схема процесу оцінки захищеності ККМ від загроз ІБ

Висновки

В рамках цієї роботи проведено оцінку можливості застосування засобів захисту інформації для захисту від загроз ІБ, спрямованих на порушення доступу до інформації.

В умовах DoS атаки пропускна здатність вузла мережі значно знижується, що обґрунтовується самою природою атаки, проте застосування засобів захисту інформації на вузлі зв'язку, дозволяє організувати безперебійне функціонування мережі зі зниженими, але допустимими характеристиками

Розроблений метод визначення імовірності знаходження в стані непрацездатності, обґрунтовані впливом загроз ІБ, які промодельовано реальним експериментом. Відповідно до цього методу, імовірність знаходження вузла у стані неготовності (коефіцієнт неготовності) є сумою імовірності загрози безпеці, імовірності реалізації загрози, а також середнього часу знаходження вузла в режимі неготовності.

Перелік посилань

1. Романов А.І. Основи теорії телекомунікаційних мереж: навчальний посібник для вузів / О.І. Романов. - К., 2012. - 152 с.
2. Шувалов В.П. Забезпечення показників надійності телекомунікаційних систем і мереж / В.П. Шувалов, М.М. Егузов, Е.А. Мініна Є.М. : Гаряча Лінія - Телеком, 2015. - 168 с.
3. Каяпев, А.І. Аналіз показників надійності локальних комп'ютерних мереж / А.І. Каяпев, П.А. Ратмин, М.І. Шарипов - 2013. - Т. 17. - №5 (58). - С. 140-149.
4. Казарін, О.В., Підходи до кількісної оцінки захищеності ресурсів автоматизованих систем / О.В. Казарін, С.Є. Кондаков, І.І. Троїцький // Питання кібербезпеки. - 2015. - №2 (10) - С. 31-35.
5. Ярошук, Д.О. Удосконалення методу обрахунку впливу загроз інформаційної безпеки на ефективність функціонування закритої телекомунікаційної мережі [Текст] / Д. О. Ярошук, О. А. Максимів // Вісник Хмельницького національного університету. Технічні науки. – 2017. – № 6. – С. 64-69.

к.пед., доц. Толок І.В. (ВІКНУ)
к.т.н., доц. Кльоц Ю.П. (ХмНУ)
к.ф.-м.н., доц. Рамський А.О. (ХмНУ)
Рикун В.В (ХмНУ)

Дослідження характеристик надійності та інформаційної безпеки вузлів комп'ютерної мережі

Так як системи зв'язку досить важливі для правильного функціонування організації, вони стають пріоритетом для злочинців. Впливаючи на мережу, організовуються атаки, спрямовані на різні характеристики інформації. Загроза інформаційної безпеки - це сукупність умов і факторів, які створюють потенційну або фактичну загрозу інформації. При атаках зловмисників існує небезпека втрати, перекручення, блокування, копіювання, поширення інформації, а також інших несанкціонованих дій з нею.

Незалежно від конкретних типів загроз необхідно забезпечити наступні основні властивості: цілісність, конфіденційність і доступність. Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Конфіденційність – це захист від несанкціонованого доступу до інформації.

Завдання цілісності і конфіденційності успішно вирішується за рахунок використання криптографічного захисту інформації. У роботі запропоновано метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки. Це дає можливість вжити заходи щодо їх нейтралізації та оцінити ефективність їх використання.

Головним завданням цього дослідження є об'єднання в єдину математичну модель характеристик надійності та інформаційної безпеки. Для моделювання характеристик надійності та інформаційної безпеки можна використовувати марківські процеси і експоненціальний розподіл можливих подій. Як показник, що безпосередньо характеризує властивості системи, доцільно використовувати коефіцієнт готовності. Класичним підходом до моделювання мережі є приведення її до деревовидного графу. Одним з підходів є нормування коефіцієнту готовності ліній зв'язку та мереж передачі даних, але існуючі правила не застосовуються до корпоративних мереж передачі даних, побудованих поверх Інтернету, оскільки мережа, сформована таким чином, частково абстрагується від певного постачальника послуг.

З врахуванням вищесказаного, розробка методу оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки є актуальним науково-технічним завданням.

ДОДАТОК В

(Обов’язковий)

Презентація

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Рикун Валентин

МЕТОД ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ВУЗЛА ЗВ'ЯЗКУ КОРПОРАТИВНОЇ МЕРЕЖІ З ВРАХУВАННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Науковий керівник
к.т.н., доц., Муляр Ігор Володимирович

Метою магістерської роботи є вдосконалення методу врахування загроз ІБ на вузли мережі та їх впливу на функціонування вузла зв'язку корпоративної мережі.

Об'єкт дослідження є процес функціонування корпоративних мереж в умовах загроз інформаційної безпеки.

Предмет дослідження: є властивості вузла зв'язку, що впливають на ефективність функціонування мережі

Задачі досліджень у роботі сформульовані наступним чином:

1 Проаналізувати фактори, що впливають на ефективне функціонування ККМ, Визначити критерії та фактори, що впливають на ефективність функціонування мережі з врахуванням загроз ІБ.

2. Дослідити можливість використання математичного апарату теорії надійності як методу дослідження ККМ для оцінки впливу загроз ІБ. Перевірити можливість підвищення ефективності функціонування мережі за рахунок топологічних засобів (зміна топології мережі).

3. Розробити модель надійності вузла ККМ з урахуванням впливу загроз ІБ та відмов обладнання.

4. Провести експериментальне дослідження впливу загроз доступності інформації на коефіцієнт готовності.

5. Удосконалити метод обліку впливу загроз ІБС на надійність та ефективність вузлів зв'язку.

6. Розробити спосіб підвищення ефективності вузлів зв'язку ККМ під впливом хакерських атак та забезпечити ІБ в корпоративних мережах топологічними засобами.

7. Провести оцінку ефективності комунікаційних вузлів існуючих ККМ, підтвердити їх придатність для різних фізичних топологій.

Наукова новизна роботи полягає в наступному:

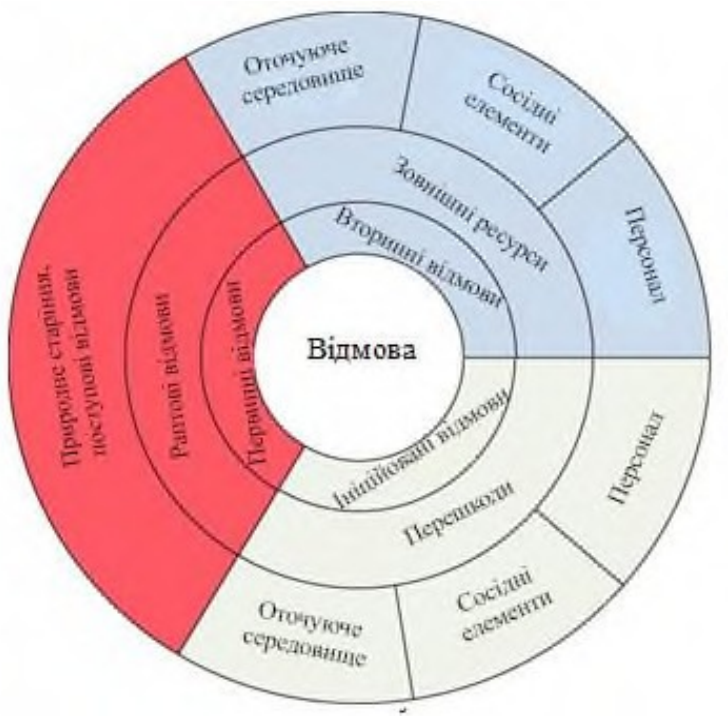
1. Вдосконалено модель надійності вузла зв'язку мережі, що відрізняється від відомих врахуванням впливу загроз інформаційної безпеки, спрямованих на порушення доступності інформації.

2. Вдосконалено метод дослідження стану працездатності вузлів зв'язку мережі в умовах впливу загроз доступності інформації, особливістю якого є можливість кількісної оцінки ступеня впливу загроз на ефективність функціонування корпоративної мережі.

Практична цінність Практична реалізація розроблених у магістерській роботі моделей, алгоритмів та методівдозволило прогнозувати стан ККМ в умовах впливу непрацездатності обладнання та загроз ІБ, та оцінювати ефективність функціонування ККМ у вигляді кількісного показника, тим самим підвищуючи якість оцінки.

Публікації. По темі магістерської роботи опубліковано 1 стаття, 1 - теза доповідей на всеукраїнських конференціях.

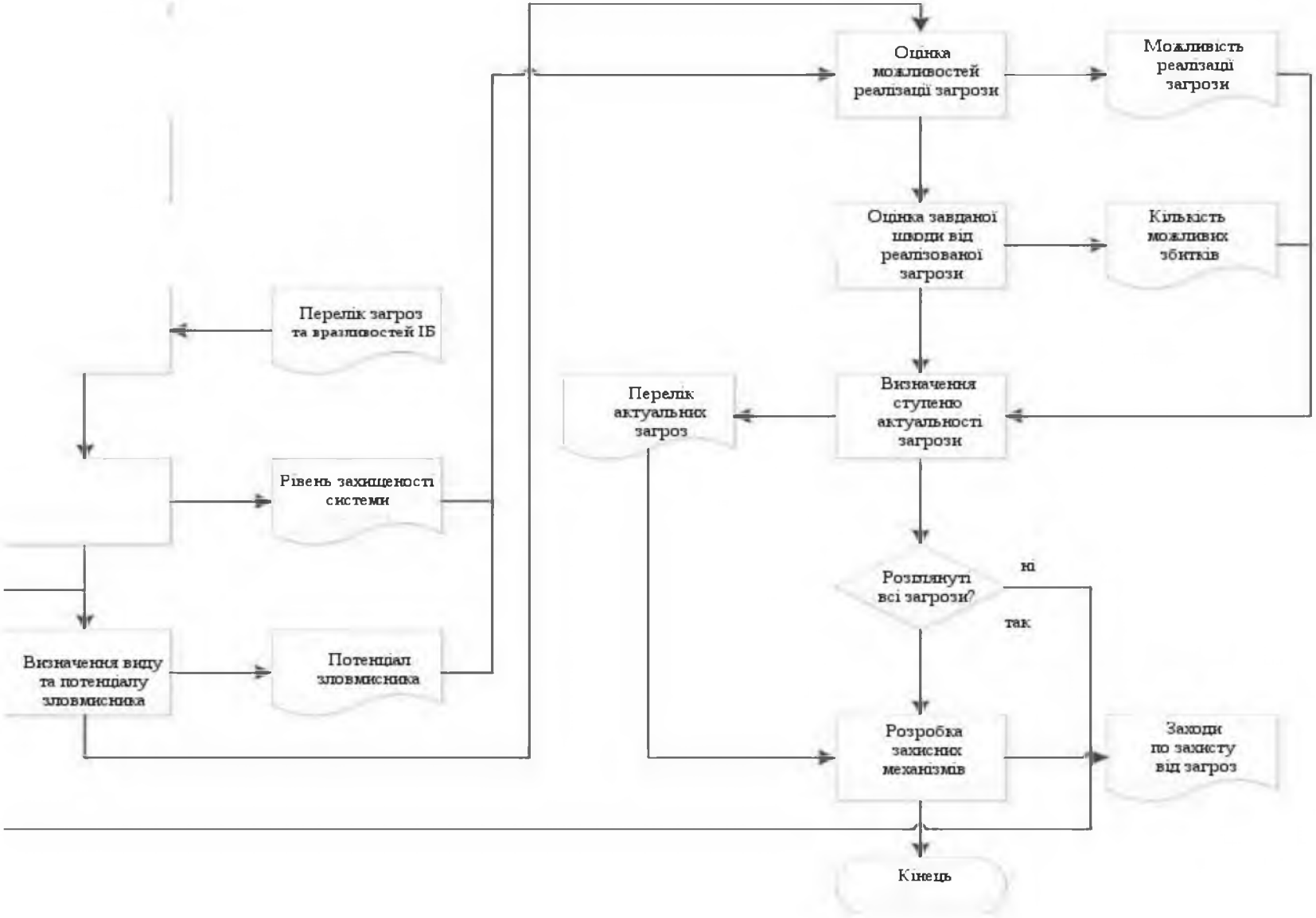
Діаграма причин відмов елементів ККМ



У червоному секторі згруповані первинні відмови елемента, причиною яких є довільна відмова. Причини первинних відмов можуть бути обумовлені як недосконалістю технологічних процесів при виробництві елемента (заводським браком), так і природним старінням елементів по закінченню рекомендованого періоду експлуатації. У синьому секторі згруповані вторинні відмови елементів. Причини вторинних відмов є не довільні, а якісь зовнішні чинники. У зеленому секторі згруповані відмови, викликані людським фактором і неправильною експлуатацією обладнання. Переважно до них відносяться неправильні команди персоналу. Незважаючи на те, що в кінцевому підсумку наслідком будь-якої з перерахованих вище причин є порушення працездатності елемента ККМ, відмови з різними причинами їх виникнення враховуються в показниках надійності по-різному.

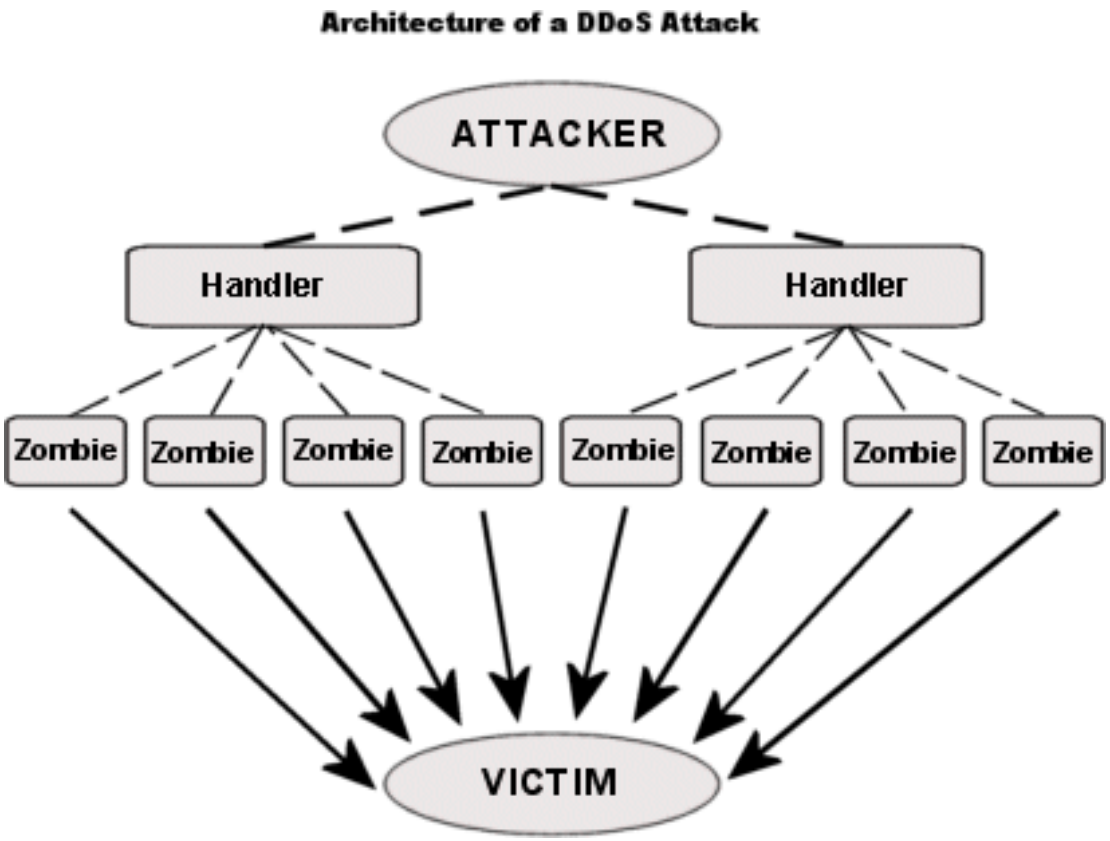
Для оцінки працездатності виробу використовується група показників коефіцієнта готовності. Фізичним змістом коефіцієнта готовності є ймовірність знаходження виробу в працездатному стані, за умови, що для цього надані всі необхідні зовнішні ресурси.

Алгоритм процесу оцінки захищеності мережі по відомій методиці



ЗАГРОЗИ ІБ, СПРЯМОВАНІ НА ОБМЕЖЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЇ

Механізм здійснення атак типу «відмова в обслуговуванні»

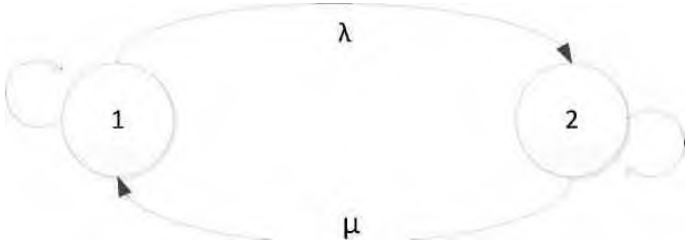


1 Загроза спрямована на порушення доступності інформації.

2. Об'єктом загрози є вузли зв'язку, їх компоненти та телекомунікаційне обладнання, яке розташоване на вузлах зв'язку досліджуваного ККМ.

3. Загроза ІБ реалізується в рамках інфраструктури, що використовується в ККМ.

ГРАФ СТАНУ ОБЛАДНАННЯ ЕЛЕМЕНТА МЕРЕЖІ



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

інтенсивність потоку відмов буде розраховуватись

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

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

Δt – інтервал часу.

Nср – середнє число пристроїв, що знаходяться в працездатному стані на інтервалі часу Δt.

МАТЕМАТИЧНИЙ АПАРАТ ПРОГНОЗУВАННЯ ЧИСЛА ПРИСТРОЇВ, ЩО ЗНАХОДЯТЬСЯ В ПРАЦЕЗДАТНОМУ СТАНІ

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

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

$t_{\text{в}}$ - середній час знаходження пристрою в непрацездатному стані,

N_0 - число пристроїв, що знаходяться в працездатному стані

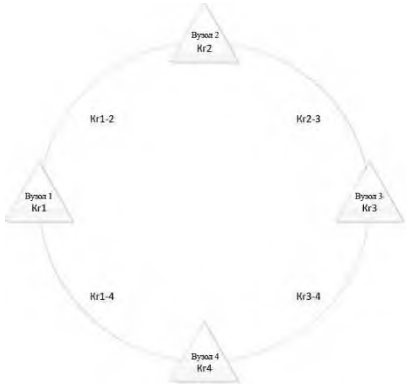
Δt - інтервал часу.

$t_{\text{в}} = \frac{1}{\text{i}}\int_{\text{i}}^{1} f(i)$, - середній час відновлення

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

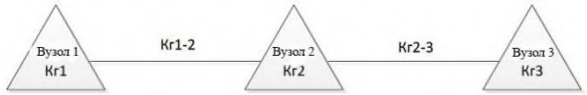
f (i) - функція розподілу часу відновлення.

ДОСЛІДЖУВАНІ ТОПОЛОГІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖІ



Кільцева топологія

Топологія двох сполучених кілець



Лінійна топологія без резервування

Для підвищення надійності мережі між вузлами зв'язку додаються надлишкові зв'язку (резервування ліній зв'язку), що дозволяє забезпечити функціонування мережі в разі відмов.

Всі розглянуті топології зводяться до формалізованих, що складається з однакових вузлів і однакових ребер. Fa всіх розглянутих вузлів ($Fa_{\text{в}}$) і Fa всіх розглянутих ребер ($Fa_{\text{р}}$) приймаються стабілізованими і рівними.

Оскільки Fa являє собою випадкову величину і його розрахунки спираються на математичну теорію ймовірностей.

$$Fa_{1-3}^{\text{КІЛЬЦЕ}} = Fa_1 \times (1 - (1 - Fa_{1-2} \times Fa_2 \times Fa_{2-3}) \times (1 - Fa_{1-4} \times Fa_4 \times Fa_{4-3})) \times Fa_3 = Fa_{\text{в}}^2 \times (1 - (1 - Fa_{\text{р}}^2 \times -Fa_{\text{в}})^2),$$

спростивши отримаємо

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

МАРКІВСЬКА МОДЕЛЬ НАДІЙНОСТІ ВУЗЛА ЗВ'ЯЗКУ МЕРЕЖІ

Перший науковий результат

Представлення математичної моделі вузла зв'язку мережі

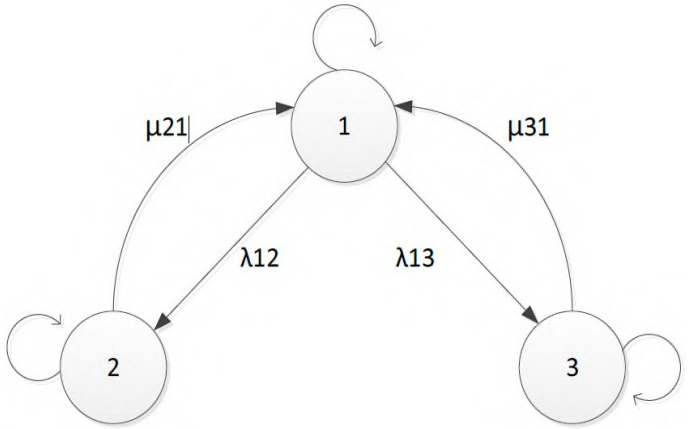
В обробці трафіку задіяно багато обладнання, яке являє собою сукупність пристроїв, кожен з яких має власні технічні характеристики та показники, що характеризують його надійність *(Fa*). Також відомо, що трафік проходить послідовно всі пристрої вузла зв'язку, задіяні в інформаційному обміні. Таким чином, для розрахунку *Fa* вузла зв'язку розраховується:

$Fa_y = Fa_1 \times Fa_2 \times ... \times Fa_n$,

де Fa_1 ... $Fa_n - Fa$ пристроїв вузла мережі.

В рамках досліджувальної проблематики цими станами є :

1. Вузол мережі в стані готовності.
2. Вузол в стані неготовності через реалізацію загрози захищеності, спрямованої на обмеження доступності інформації.
3. Вузол мережі в стані неготовності через відмови обладнання



Граф станів вузла зв'язку мережі

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

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

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

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

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

λ_{12},λ_{13}– інтенсивність потоків відмов вузла зв'язку мережі;

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

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

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

Представлена математична модель елемента корпоративної мережі, яка враховує вплив не тільки відмов технічного обладнання, а й загрозу доступності інформації. Загроза інформаційній безпеці означає сукупність умов та факторів, що створюють потенційну або фактичну загрозу. У цій роботі вважається, що атаки є активним обладнанням вузла мережі.

ОПТИМІЗАЦІЇ МЕРЕЖЕВИХ ТОПОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖІ

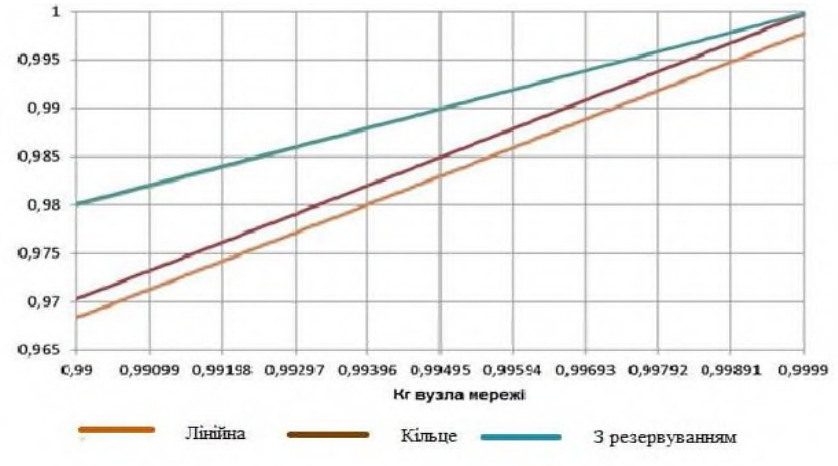
Залежність коефіцієнту готовності формалізованих топологій від коефіцієнту готовності вузла

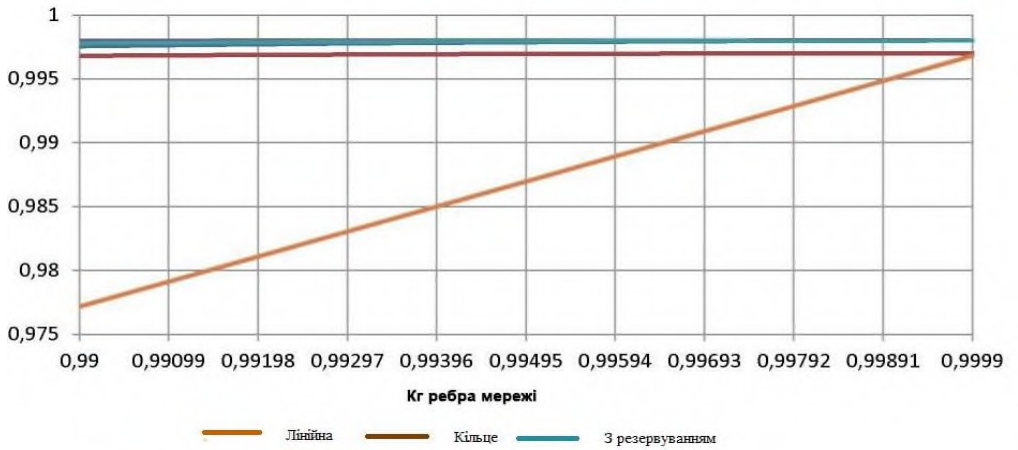
$Fa_в$	Кільце	З резервуванням	лінійна
0,99	0,979959	0,98009	0,968359
0,99099	0,981943	0,982052	0,971267
0,99198	0,983926	0,984016	0,974181
0,99297	0,985909	0,985982	0,977101
0,99396	0,987893	0,987951	0,980026
0,99595	0,989876	0,989921	0,982958
0,99594	0,99186	0,991892	0,985895
0,99693	0,993844	0,993866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

Залежність коефіцієнту готовності формалізованих топологій від коефіцієнту готовності ребра

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

Графіки залежності коефіцієнта готовності мережі в цілому від елемента

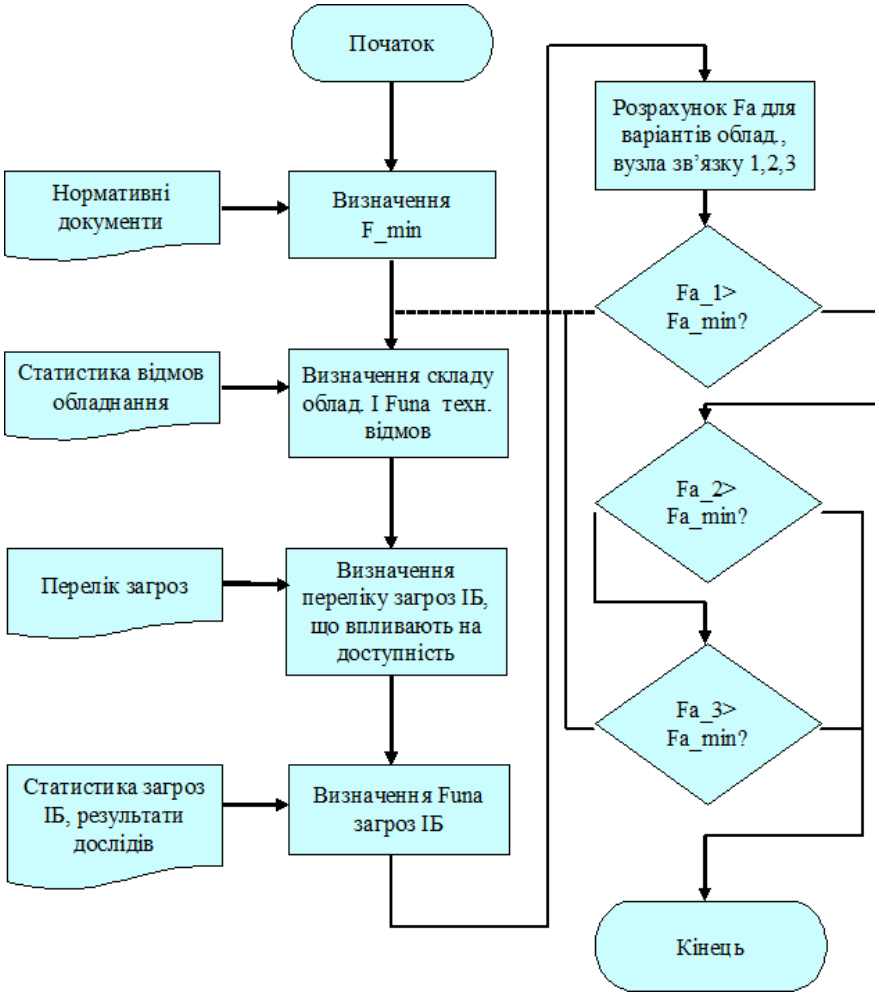




З графіка випливає що коефіцієнт готовності розглянутих топологій, що мають у своєму складі, резервування ліній зв'язку майже не реагують на зміну коефіцієнт готовності ребра. Це підтверджує доцільність врахування впливу загрози на ефективність функціонування мережі саме у значеннях коефіцієнту готовності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

ВДОСКОНАЛЕННЯ МЕТОДУ ДОСЛІДЖЕННЯ СТАНУ ПРАЦЕЗДАТНОСТІ ВУЗЛІВ ЗВ'ЯЗКУ

Другий науковий результат



Блок-схема алгоритму оцінки ефективності функціонування мережі

Оцінка захищеності відбувається поетапно:

1. На першому кроці визначається мінімально допустимий коефіцієнт готовності сегмента мережі, відповідно до нормативних вимог комплексної системи захисту інформації.
2. Визначається склад устаткування вузлів мережі, та проводиться розрахунок коефіцієнт неготовності.
3. Будується модель загроз інформаційної безпеки
4. Проводиться розрахунок коефіцієнт неготовності, з врахуванням впливу загроз доступності інформації.
5. Розраховується коефіцієнт готовності усього досліджуваного сегмента мережі.
6. Проводиться порівняння коефіцієнта готовності з мінімально допустимим. Якщо значення коефіцієнту готовності менше допустимого, необхідно повернутися до етапу 2 і замінити мережне устаткування, щоб задовольняло критерії захисту.
7. Аналізуються результати, при використанні тільки маршрутизатору. При умові, коли значення *Fa_2* перевищує значення *Fa_min*, робиться висновок, що маршрутизатор справляється з загрозами захищеності інформації
8. Порівнюються результати, коли в складі обладнання вузла зв'язку встановлений маршрутизатор і додатковий засіб захисту інформації. При умові, коли значення *Fa_3 перевищує значення Fa_min,* можна зробити висновок, що обране рішення ефективно справляється з поставленою задачею.

У випадку, коли вузол зв'язку піддається більш ніж одній загрозі, тоді $F_{una}^{п.в.}$ буде розраховуватися:

$$Funf_{В(i)} = Р_B \times Р_{P|B} \times Кнг^{п.в}$$

$Р_B$ – ймовірність виникнення загрози ІБ,

$Р_{P|}$ – ймовірність реалізації загрози ІБ,

$Funa_{В(i)}$ – коефіцієнт неготовності, обґрунтований реалізацією загрози;

$$Funa_В = Fa_{В(1)} \times Fa_{В(2)} \times ... \times Fa_{В(n)},$$

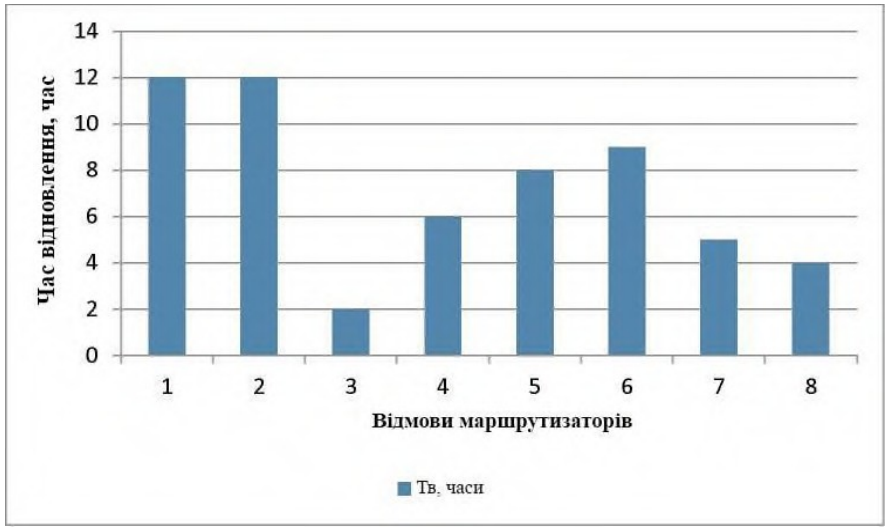
де $Funa_{В1}$ ... $Кг_{Вn}$ – Кг, що відображають вплив загроз ІБ відповідно до прийнятої моделі загроз.

РІВНЯННЯ АПРОКСИМУЮЧОЇ ФУНКЦІЇ ЧАСУ ВІДНОВЛЕННЯ РОБОТИ МАРШРУТИЗАТОРІВ

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

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

$$\overline{t_B} = \frac{1}{8}\int_{2}^{8}(-0.0152\times x_4 + 0.0808\times -8.307 + x + 20.143)dx = \frac{51.712}{8} = 6{,}464 \text{ годин.}$$

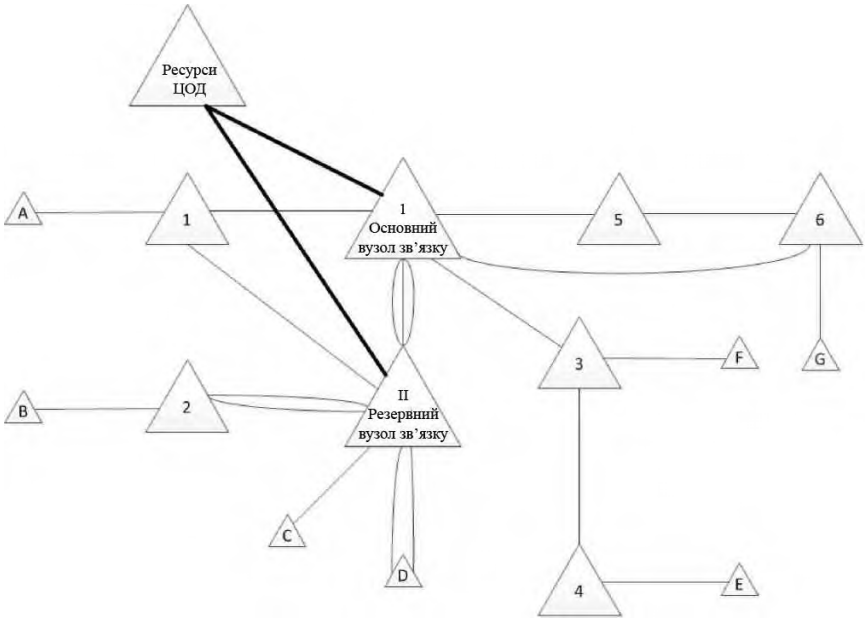


Розподіл часу відновлення працездатності маршрутизаторів

Середня тривалість атак типу «відмова в обслуговуванні»

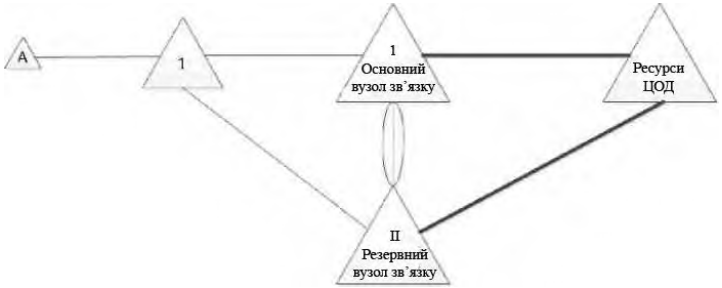
Період	Частка атак φ_i для відповідного інтервалу часу атаки						
	0-4 ч	5-9 ч	10-19	20-49 ч	50-99 ч	100-149 ч	150-200 ч
	t_{B1}= 2 ч	t_{B2}= 7 ч	t_{B3}= 14.5	t_{B4}= 34.5 ч	t_{B5}= 74.5 ч	t_{B6}= 124.5 ч	t_{B7}=175 ч
III квартал 2019	0,7813	0,1161	0,0572	0,0353	0,0099	0,0002	0
IV квартал 2019	0,7234	0,1382	0,1084	0,0254	0,004	0,0003	0,0003
I квартал 2020	0,7586	0,1065	0,0766	0,0512	0,001	0,0002	0,0009
II квар-тал 2020	0,7328	0,121	0,1	0,044	0,001	0,0006	0,0006

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ЗАСТОСОВАНІ НА ЧАСТИНІ МЕРЕЖІ



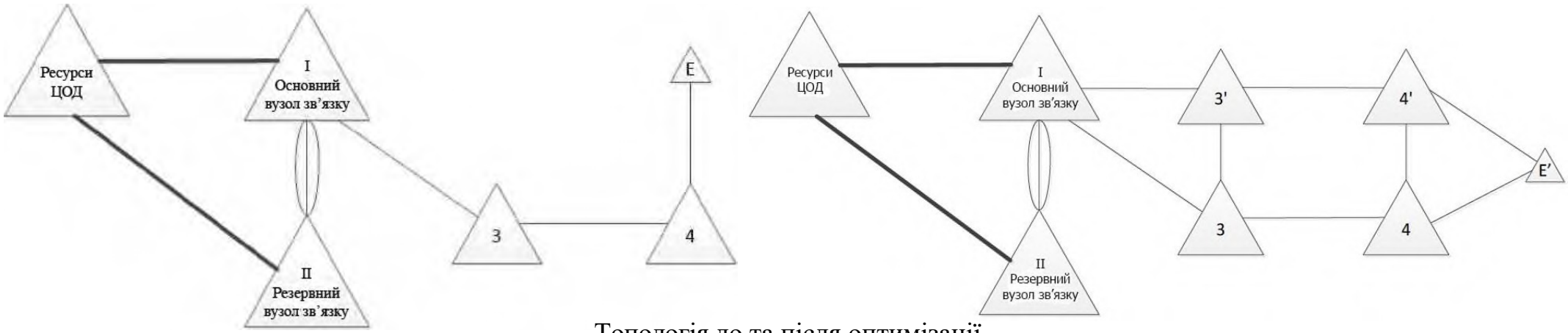
В представленій схемі використовуються наступні способи резервування ліній зв'язку:

- розподілений, при якому основний і резервний канал зв'язку термінуються відповідно в основному і резервному комутаційному центрах (А-ЦОД)
- кумулятивний, при якому і основний, і резервний канал зв'язку термінуються на одному з переважно або резервному вузлах зв'язку (B, C,D-ЦОД) з повним (D-ЦОД) або неповним (B, C-ЦОД) резервуванням ліній зв'язку сегмента;
- резервування за допомогою додаткового резервного ребра (G-ЦОД);
- без резервування (E,F-ЦОД).

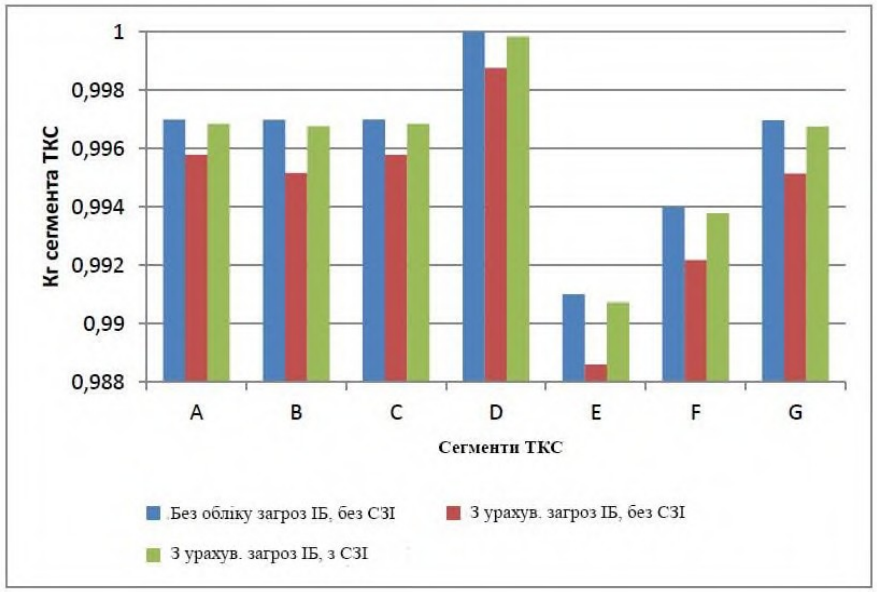


Даний сегмент, а саме, топологія А-ЦОД (розподілене резервування) має безпосереднє підключення як до основного, так і до резервного вузла зв'язку мережі.

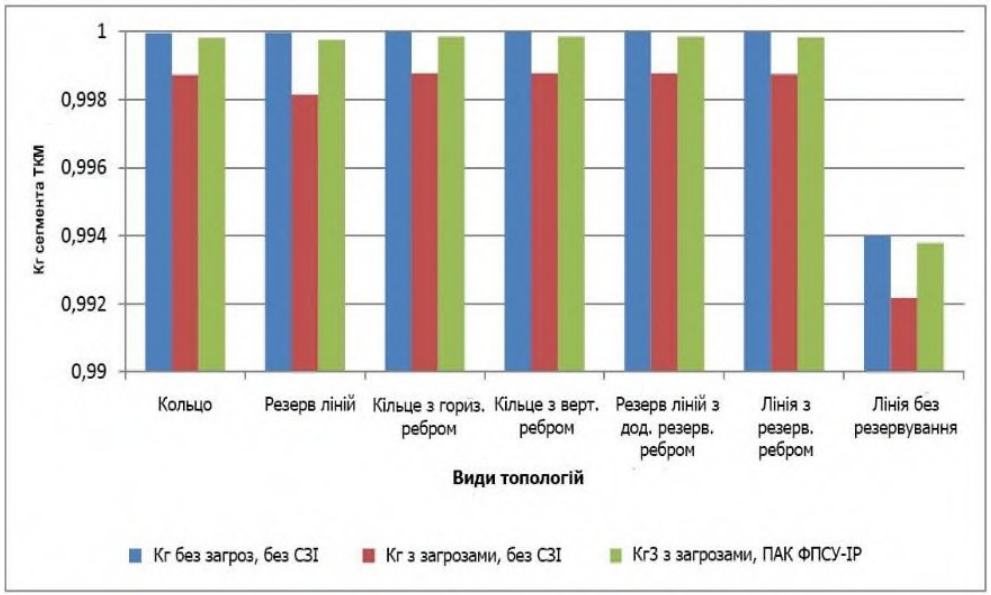
ПОРІВНЯЛЬНА ОЦІНКА КОЕФІЦІЄНТА ГОТОВНОСТІ ОПТИМІЗОВАНИХ ТОПОЛОГІЙ



Топологія до та після оптимізації



Графік залежності Кг сегментів різних топологій в залежності від впливу атак та складу обладнання



Коефіцієнти готовності сегментів мережі з резервуванням, що складаються з трьох вузлів

Оскільки вузли зв'язку є елементами мережі, вдосконалення їх топологій безпосередньо впливає на характеристики надійності та ефективності мережі. В результаті аналізу сегментів, побудованих згідно вдосконалення вузла зв'язку, встановлено, що значення Fa досліджуваних сегментів зростає і стає достатнім для функціонування з необхідним рівнем якості послуг зв'язку.

Для сегментів мережі з різною топологією різниця між отриманими значеннями Fa становить менше 1%, і це відображає той факт, що запропоновані захисні заходи ефективні.

ВИСНОВКИ

В результаті проведеного дослідження вдосконалено метод оцінки ефективності функціонування вузлів зв'язку мережі і метод обліку впливу атак доступності інформації на ефективність функціонування корпоративної мережі. Розроблено математичну модель надійності вузла зв'язку, яка враховує вплив загроз інформаційної безпеки. При цьому досягнуті наступні результати:

Основні результати магістерської роботи є такими:

1. Проаналізовано актуальні методи дослідження мережі, що дозволяють проводити оцінку захисту від атак, спрямованих на порушення доступності інформації.
2. Доведено можливість використання математичного та методологічного апарату теорії надійності як методу мережевих досліджень та коефіцієнта готовності як показника для оцінки ефективності вузлів зв'язку.
3. Розроблена математична модель, яка дозволяє врахувати вплив розподілених атак на систему, що описується графом трьох станів та відповідною системою рівнянь
4. Удосконалено метод дослідження корпоративної мережі, що дозволяє оцінити ефективність функціонування вузла зв'язку в умовах впливу розподілених атак, пов’язаних з доступністю інформації. На підставі отриманих розрахунків і цільового значення коефіцієнту готовності вузлів мережі, можливо прийняти рішення про необхідність проведення заходів щодо підвищення ефективності функціонування мережі.
5. Запропоновано підхід до організації внутрішньої топології вузлів зв'язку мережі, що приводить її до форми кільця з вертикальним резервним фронтом, що дозволяє значно збільшити коефіцієнт готовності елементів.

UNICHECK

Имя пользователя:
Kafedra TMIT KhNU

ID проверки:
1005391408

Дата проверки:
07.12.2020 17:03:14 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
07.12.2020 17:11:46 EET

ID пользователя:
100005657

Название файла: Рикун_ПМм-19-1

Количество страниц: 79 **Количество слов:** 14745 **Количество символов:** 113264 **Размер файла:** 1.72 MB **ID файла:** 1005683463

---

390 слов помечены как "исключенные" и не учитываются в подсчете слов

2.64%
Совпадения

Наибольшее совпадение: 0.64% с **Интернет-источником** (https://sibsutis.ru/upload/iblock/772/dis_Ringenblium.pdf)

2.55% Источники из Интернета	28	Страница 81
0.08% Источники из Библиотеки	1	Страница 81

0.1% Цитат

Цитаты	3	Страница 82
Ссылки	1	Страница 82

0% Исключений

Нет исключенных источников

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы	93

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 2.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 6%**

ID: 80948 Название: Метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки Добавлено в БД: 2020-11-23 Авторы: Рикун Валентин Володимирович Руководители: Муляр Ігор Володимирович Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	94419	717	4670 (5%)	54 (8%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

Завідувачу кафедри ТМІТ
д-р.техн.наук Підченку С.К.

Гецун Валентин Володимирович
ПІБ здобувача вищої освіти

ФПКТС, 2 курсу, групи ПМм-19-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

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

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

04.12.20
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ ТЕЛЕКОМУНІКАЦІЙ, МЕДІЙНИХ ТА ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Метод оцінки ефективності комунікаційного вузла корпоративної мережі з урахуванням інформаційної безпеки

Автор: Рикун Валентин Володимирович

Спеціальність: 113 – прикладна математика

Освітня програма: освітньо-професійна

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

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) запозичення розміщені в розділах, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) більшість джерел запозичення дублюють одне одного;
4) плагіату в роботі виявлено 2.6%, найбільше було з джерелом https://sibsutis.ru/upload/iblock/772/dis_Ringenblium.pdf - 0.6%.

9. 12. 2020
Дата

Підпис /Муляр І.К

Підпис /Підченко О.Л

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

Магістр Рикун Валентин Володимирович

Тема Метод оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки

Спеціальність 113 – Прикладна математика

Обсяг дипломної роботи:

Кількість листів креслень 12; кількість сторінок записки 81

1.Короткий зміст ДР та прийнятих рішень В рамках магістерської роботи проведено оцінку функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки. Створено математичну модель стану ефективності вузла за допомогою системи рівнянь Колмогорова-Чепмена. Розроблено метод визначення імовірності знаходження вузла мережі в стані непрацездатності. Удосконалено метод дослідження корпоративної мережі та оцінки ефективності функціонування вузла звязку.

2. Висновок про відповідність ДР поставленому завданню Дипломна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині дипломної роботи

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 дослідження підходів до врахування впливу загроз. Наступні розділи присвячені розробці матиматичної моделі та удосконалення метода дослідження корпоративних мереж. Розглянуто питання застосування розробленого методу.

4. Позитивні сторони роботи Дипломна робота містить ряд інноваційних рішень, зокрема, розроблено метод експериментального дослідження впливу DDoSатак на працездатність мережі, які допомогли значно підвищити коефіцієнт роботи мережі.

5. Негативні сторони роботи Впровадження розробленої моделі та методу ускладнюється масштабними та складними топологіями мережі та матеріальними затратами.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми дипломної роботи з дотриманням стандартів. В загальному графічне оформлення виконане на достатньому рівні. Пояснювальна записка відповідає нормам для її оформлення.

7. Відгук про роботу в цілому цілому В загальному дипломна робота 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 дипломної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження

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

РЕЦЕНЗЕНТ (прізвище, ім'я, по-батькові, посада, місце роботи)
к.т. н. доц. кафедри кібербезпеки та комп'ютерних систем і мереж Кльоц Ю. П.

"8" 12 2020 р.
(підпис)